Lenovo

Lenovo XClarity Administrator Fehlerbestimmungshandbuch

Version 4.3

Anmerkung

Lesen Sie vor der Verwendung dieser Informationen und des entsprechenden Produktes die allgemeinen und rechtlichen Hinweise in der Onlinedokumentation von XClarity Administrator.

Vierte Ausgabe (April 2025)

© Copyright Lenovo 2015, 2025.
HINWEIS ZU EINGESCHRÄNKTEN RECHTEN: Werden Daten oder Software gemäß einem GSA-Vertrag (General Services Administration) ausgeliefert, unterliegt die Verwendung, Vervielfältigung oder Offenlegung den in Vertrag Nr. GS-35F-05925 festgelegten Einschränkungen.

Inhaltsverzeichnis

Inhaltsverzeichnis i

Zusammenfassung der Änderungen . . v

Kapitel 1. Hilfe und technische Unterstützung anfordern 1

Kapitel 2. Alerts, Ereignisse und Jobs anzeigen 3

Einheiten in den Wartungsmodus versetzen 3
Mit Alerts arbeiten 4
Aktive Alerts anzeigen 4
Alerts ausschließen 8
Einen Alert beheben 9
Alerts bestätigen 10
Ereignisse handhaben 11
Ereignisse im Ereignisprotokoll überwachen . . 11
Ereignisse im Prüfprotokoll überwachen . . . 13
Ein Ereignis beheben 15
Ereignisse ausschließen 16
Ereignisse weiterleiten 17
Mit Jobs arbeiten 54
Jobs überwachen 54
Jobs planen 57
Auflösung und Kommentare zu einem Job hinzufügen 60

Kapitel 3. Mit Service und Unterstützung arbeiten 61

Bulletins von Lenovo erhalten 61
Informationen zur Garantie anzeigen. 62
Automatische Problembenachrichtigung einrichten 63
Automatische Problembenachrichtigung an den Lenovo Support einrichten (Call-Home-Funktion) 64
Automatische Problembenachrichtigung an die Lenovo Upload-Funktionalität 70
Automatische Problembenachrichtigung an einen bevorzugten Service Provider einrichten 74
Kennwort zur Service-Wiederherstellung ändern 77
Servicedateien prüfen 77
Support-Kontakte für bestimmte Einheiten definieren 78
Servicedaten für eine Einheit sammeln und herunterladen 79
Lenovo XClarity Administrator Servicedaten sammeln und herunterladen 81
Servicedateien für ein nicht reagierendes Lenovo XClarity Administrator sammeln und herunterladen 83
Übermitteln einer Serviceanforderung zu Hardwareproblemen an das Lenovo-Support Center 84
Probleme mit XClarity Administrator melden. . . . 86
Servicedatei an ein offenes Service-Ticket anhängen 88
Service-Tickets und Status anzeigen 89
Servicedateien an den Lenovo Support senden . . 90
Protokolleinstellungen für Verwaltungsserver konfigurieren 91
Call-Home-Funktion auf allen verwalteten Einheiten erneut aktivieren 92
Regelmäßig Daten an Lenovo senden 92
Beispiel von Nutzungdaten 94
Beispiel-Hardwaredaten 98

Kapitel 4. Plattenspeicher verwalten. 113

Kapitel 5. Ermittlungs- und Verwaltungsprobleme 117

Einheit kann nicht erkannt werden 117
Einheit kann nicht verwaltet werden 118
Speichereinheit kann aufgrund eines ungültigen SSL-/TSL-Zertifikats nicht verwaltet werden. . . . 121
Switch kann aufgrund eines ungültigen SSL-/TSL-Zertifikats nicht verwaltet werden 121
Nach dem Ersetzen der rückseitigen LED-Karte oder Mittelplatinenbaugruppe kann die Konnektivität für ein verwaltetes Flex System-Gehäuse nicht wiederhergestellt werden 122
Konnektivität des verwalteten Servers kann nach dem Austausch der Systemplatine nicht wiederhergestellt werden 122
Kapselung ist nicht deaktiviert, nachdem die Verwaltung eines Servers aufgehoben wurde . . . 123
Der Rechenknoten wird nach der Verwaltung nicht in der Benutzerschnittstelle angezeigt 123
Stromversorgungsstatusstatus ist nicht korrekt . . 123

Kapitel 6. Probleme bei Installation, Entfernung, Aktualisierung und Datenmigration 125

Keine Videoausgabe, wenn XClarity Administrator in Red Hat KVM installiert wird 125
Adapteränderungen werden nicht erkannt. 125

© Copyright Lenovo 2015, 2025

Konfigurationsassistent kann bei der Erstkonfiguration nicht mit einem Webbrowser erreicht werden 125
Implementierung von Lenovo XClarity Administrator schlägt unerwartet fehl. 126
Lenovo XClarity Administrator-Aktualisierung fehlgeschlagen 126

Kapitel 7. Verbindungsprobleme . . .127

Zugriff auf Lenovo XClarity Administrator nicht möglich 127
Herstellen einer Verbindung zu Lenovo XClarity Administrator über den Safari-Browser nicht möglich 127
Anmelden nicht möglich 127
Anmelden bei Lenovo XClarity Administrator nicht möglich 127
Kennwort für eine lokale Wiederherstellung oder einen Supervisor-Benutzer vergessen . . 128
Direkte Anmeldung beim verwalteten CMM nicht möglich 131
Direkte Anmeldung beim Management-Controller nicht möglich 131
Anmelden bei Flex Power System-Servern nicht möglich 132
Plötzlicher Verbindungsausfall bei einer Einheit . . 132

Kapitel 8. Lenovo XClarity Administrator-Konfigurationsprobleme 135

Externe LDAP-Konfigurationsprobleme 135
Benutzer hat keine ausreichende Berechtigung zum Konfigurieren des Servers.. 135
Aktivierungsprobleme bei Features on Demand . . 135
VMware warnt davor, dass der VMXNET 3-Treiber nicht unterstützt wird. 135

Kapitel 9. Leistungsprobleme 137

Leistungsprobleme mit Lenovo XClarity Administrator 137
Schlechte oder langsame Netzwerkleistung 137

Kapitel 10. Sicherheitsprobleme . . .139

SSL-Zertifikat ist nicht vertrauenswürdig 139
Serverzertifizierungsüberprüfung fehlgeschlagen 139
Sicherheitsrisiken bei Samba und Apache 140

Kapitel 11. Fehlerbehebung bei Problemen mit Sicherung und Wiederherstellung 143

Sicherungsvorgang scheint beim Neustart des Verwaltungsservers nicht mehr zu reagieren. . . . 143
XClarity Administrator Fenster ist nach einer Aktualisierung während der Sicherung leer 143

Kapitel 12. Ereignisüberwachungs- und weiterleitungsprobleme 145

Ereignisse werden nicht weitergeleitet. 145

Kapitel 13. Probleme bei der Einheitenverwaltung 147

Daten auf blockierten Laufwerken können nicht sicher gelöscht werden 147
SATA-SDD-Datenträger können nicht sicher gelöscht werden, wenn sie mit Marvell RAID verbunden sind 147
Bestandsdaten sind nach dem Hinzufügen oder Austauschen von Karten nicht auf dem neuesten Stand 147

Kapitel 14. Serverkonfigurationsprobleme 149

Beim Erstellen eines Musters von einem vorhandenen Server ist ein Fehler aufgetreten. . . . 149
Beim Implementieren eines Musters in einer Einheit ist ein Aktivierungsfehler aufgetreten. . . . 149
Auf einem Switch ist eine ungültige Konfiguration implementiert. 150

Kapitel 15. Probleme bei Firmwareaktualisierung und Repository 151

Es konnte keine Verbindung mit dem Lenovo Repository hergestellt werden. 151
Nach erfolgreicher Firmwareaktualisierung wird auf der Seite „Übernehmen/Aktivieren“ nicht die aktualisierte Firmwareversion angezeigt 151
Firmware kann auf einer Einheit nicht aktualisiert werden 151
Blockierungen des CMM-Firmwareaktualisierung 151
Firmware ist auf dem neuesten Stand, besteht aber die Konformitätsprüfung nicht. 152
Firmwareaktualisierungen der Flex System-Switches schlagen unerwartet fehl. 152
Firmwareaktualisierung des Flex-Switches mit folgender Fehlernachricht fehlgeschlagen: „Firmwaredownload fehlgeschlagen.“ 153
Firmwareaktualisierung des Flex-Switches mit folgender Fehlernachricht fehlgeschlagen: „DCSS_RC_CDT_FAIL“ 153
Firmwareaktualisierung des Flex-Switches mit folgender Fehlernachricht fehlgeschlagen: „Zeitlimitüberschreitung“ 153
Firmwareaktualisierung des Flex-Switch mit folgender Fehlermeldung fehlgeschlagen: „Es kann nicht die gleiche Firmwareversion heruntergeladen werden. Laden Sie eine andere Firmware herunter.“ 154
Firmwareaktualisierung des Flex-Switch mit folgender Fehlernachricht fehlgeschlagen: Host konnte nicht kontaktiert werden 154

Firmwareaktualisierung des Flex-Switch mit folgender Fehlernachricht fehlgeschlagen: „Datei ist nicht vorhanden“. 154
Firmwareaktualisierung des Flex-Switches mit folgender Fehlernachricht fehlgeschlagen: „Flashen mit Fehler beendet“. 154
Firmwareaktualisierung des EN6131 40 Gb Ethernet Switch oder IB6131 Infiniband Switch unerwartet fehlgeschlagen 155
Firmwareaktualisierung des Lenovo EN4091 Pass-through-Moduls schlägt fehl. 155
Firmwareaktualisierung des Flex System-Switches mit folgender Fehlernachricht fehlgeschlagen: „Authentifizierung des Hostschlüssels fehlgeschlagen“ 155
Bei der Durchführung einer Aktualisierung wird das System nicht in den Wartungsmodus versetzt. . . . 156
Beim Neustart eines Servers aus dem Betriebssystem wird der Wartungsmodus nicht aktiviert. 156
Server, auf dem Red Hat Enterprise Linux (RHEL) ausgeführt wird, wird nicht neu gestartet 156

Kapitel 16. Probleme mit der Aktualisierung von BS-Einheitentreibern und Repository 157

Verbindung mit der Lenovo Support-Website zum Herunterladen von Einheitentreiberaktualisierungen nicht möglich. . . 157
Aktualisierung von Einheitentreiber auf einem Server nicht möglich 157

Kapitel 17. Probleme bei der Betriebssystembereitstellung 159

Probleme bei der Statusmeldung während der BS-Implementierung 159
Betriebssystem kann nicht implementiert werden. 159
Datei kann nicht in das BS-Images-Repository importiert werden 160
Betriebssystem-Installationsprogramm kann das Plattenlaufwerk nicht finden, auf dem Sie installieren möchten. 161
Betriebssystem-Installationsprogramm kann auf einem ThinkServer-Server nicht starten 162
Probleme bei der Implementierung von VMware ESXi 162
VMware-Bereitstellung verursacht Blockierung des Systems oder Neustart . . . 162
VMware-Implementierung schlägt mit Laufwerksfehlern fehl 163
Betriebssystem startet nicht neu, um die ESXi-Implementierung auf einem ThinkServer-Server abzuschließen 163
Probleme bei der Implementierung von Red Hat und SUSE Linux 164
Redhat 6.x kann nicht auf Rack-basierten Servern mit statischer IP implementiert werden 164
BS-Implementierung schlägt wegen fehlender Treiber fehl 164
Probleme bei der Implementierung von Microsoft Windows 164
BS-Implementierung schlägt wegen vorhandener Systempartitionen auf angeschlossenem Plattenlaufwerk fehl 165

Kapitel 18. Fernsteuerungsprobleme 167

Fernsteuerungssitzung startet nicht. 167
Fernsteuerungssitzung nach der Anmeldung blockiert. 167
Es wird keine Verbindung zu einem Server hergestellt. 168
Kann nicht mit einem Flex System-Switch nach dem Start einer Fernsteuerungssitzung kommunizieren 168
Im Einzelbenutzermodus kann keine Verbindung zu einem Server hergestellt werden. 168
Fernsteuerung kann eine Verbindung mit einem Server herstellen, doch es ist kein Video verfügbar 169
Ein Server wird nicht in der Liste zum Hinzufügen einer neuen Sitzung angezeigt 169
Serverstatus in Fernsteuerungssitzung stimmt nicht mit Status in Lenovo XClarity Administrator überein 169
Laufwerk oder Image kann nicht an einen Server angehängt werden. 170
Das optionale Speichermedium wird in der Liste der fernen Medieneinheiten, die zum Anhängen verfügbar sind, nicht angezeigt 170
Stromversorgungsoption kann nicht ausgeführt werden. 170
Videoübertragung bei Verbindung mit Flex System x280 X6-, x480 X6- und x880 X6-Server nicht verfügbar 171

Kapitel 19. Benutzerschnittstellenprobleme . . .173

Menüelemente, Symbolleistensymbole und Schaltflächen sind deaktiviert (ausgegraut) 173
Der Webbrowser reagiert nicht, wenn mehrere Registerkarten geöffnet sind 173
JSON-Antwort fehlgeschlagen, Parsing-Fehler und andere unerwartete Fehler. 173
Die Benutzeroberfläche ist nicht in der bevorzugten Sprache 173
Ladezeiten langsam oder scheinbar inaktiv, lange Wartezeit für Aktualisierung, falsches Rendering 174
Unerwarteter Datenverlust. 174

© Copyright Lenovo 2015, 2025

Änderungen der Einheitenposition werden nicht in der Rack-Ansicht angezeigt. 174

Zusammenfassung der Änderungen

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

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

In dieser Version gibt es keine Erweiterungen zur Problembestimmung und -lösung.

Diese Version unterstützt die folgenden Erweiterungen bei der Problembestimmung und -lösung.

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

Funktion	Beschreibung
Service und Support	Die Unterstützung für die tcpdump-API wurde hinzugefügt, um den Lenovo Support bei Kundeninteraktionen zu unterstützen.

© Copyright Lenovo 2015, 2025

Kapitel 1. Hilfe und technische Unterstützung anfordern

Wenn Sie Hilfe, Service oder technische Unterstützung für Lenovo XClarity Administratorbenötigen, finden Sie bei Lenovo eine Vielzahl von hilfreichen Quellen.

Vorbereitende Schritte

Allgemeine Informationen zu Kontaktnummern und Ressourcen sowie Hinweise dazu, wo Sie bestmögliche Unterstützung erhalten, wann und wo immer Sie diese benötigen, finden Sie unter der Website Lenovo Support-Plan – Software.

Vorgehensweise

- Sie können Fragen stellen und Antworten finden, indem Sie auf das Benutzeraktions-Menü (

) auf der XClarity Administrator Titelleiste und dann auf **Forum besuchen** klicken oder direkt zur Community-Forumswebsite für Lenovo XClarity navigieren.
- Senden Sie Ideen zu XClarity Administrator, indem Sie auf das Benutzeraktionen-Menü (

) auf der XClarity Administrator Titelleiste und dann auf **Ideen einreichen** klicken oder direkt zur Website für Lenovo XClarity Ideation navigieren.
- Prüfen Sie das Ereignisprotokoll und befolgen Sie die vorgeschlagenen Aktionen, um die Probleme der Ereigniscodes zu beheben (siehe Ereignisse handhaben).
- Finden Sie Lösungen zu Fehlern mit klaren Symptomen und befolgen Sie die vorgeschlagenen Aktionen, um mögliche Probleme zu beheben. Die neuesten Anleitungen für die Fehlerbehebung finden Sie unter Fehlerbehebung in der Onlinedokumentation von XClarity Administrator.
- Lesen Sie Website für den Lenovo Support für Rechenzentren, um mehr über aktuelle Tipps und Verfahren zu erfahren, die Sie zur Lösung von Problemen anwenden können, die möglicherweise bei XClarity Administrator auftreten. Diese *Tech-Tipps* stellen Vorgehensweisen zur Umgehung von Fehlern im Betrieb von XClarity Administrator zur Verfügung.

  So finden Sie die für Ihren Server verfügbaren Tech-Tipps:

  1. Navigieren Sie zu Website für den Lenovo Support für Rechenzentren.
  2. Geben Sie „XClarity Administrator“ im Feld **Suchen** ein.
  3. Klicken Sie im Abschnitt **Topartikel** auf **Alle anzeigen**, um alle Tipps anzuzeigen oder geben Sie Schlüsselwörter im Feld **Suchen** ein, um einen bestimmten Tipp zu finden.

     Tipp: Sie können die Liste nach **Relevanz**, **Beliebtheit** oder **Neueste** Tipps sortieren.
- Falls es sich um ein Problem mit der Hardware oder dem Baseboard Management Controller bei einer verwalteten Einheit handelt, finden Sie weitere Informationen über Probleme sowie vorgeschlagene Aktionen in der Dokumentation zu der Einheit.
  - Informationen zu ThinkAgile-Einheiten finden Sie unter ThinkAgile-Onlinedokumentation.
  - Informationen zu ThinkSystem-Produkten, einschließlich Servern und Netzwerkeinheiten, finden Sie unter ThinkSystem-Onlinedokumentation.
  - Weitere Informationen über Converged-, System x- und RackSwitch-Produkte, einschließlich der Server und Top-of-Rack-Switches, finden Sie unter System x-Onlinedokumentation.
  - Weitere Informationen über NeXtScale-Produkte finden Sie unter NeXtScale-Onlinedokumentation.
  - Weitere Informationen über Flex System-Produkte, einschließlich der Gehäuse, Switches, Speichereinheiten und Rechenknoten, finden Sie unter Lenovo Flex System-Onlinedokumentation.

© Copyright Lenovo 2015, 2025

- Wenn das Problem am XClarity Administrator Verwaltungsserver liegt, können Sie manuell ein Service-Ticket senden (siehe Probleme mit XClarity Administrator melden).
- Wenn das Problem weiterhin auftritt und Sie ein berechtigter Kunde mit einem Telefonunterstützungsvertrag, Wartungsverträgen und/oder Garantieanspruch sind, übermitteln Sie online eine Serviceanforderung.

  Anmerkung: Lenovo XClarity Pro umfasst die Berechtigung für Service und Support sowie die Lizenz für den vollständigen Funktionsumfang für XClarity Administrator. Informationen zum Kauf von Lenovo XClarity Pro erhalten Sie von Ihrem Lenovo-Ansprechpartner oder autorisierten Business Partner.

  Mit der Übermittlung einer Serviceanforderung wird der Lösungsfindungsprozess für Ihr Problem initiiert, da der Lenovo-Support schnell und effizient die relevanten Informationen erhält. Die Lenovo-Kundendiensttechniker können mit der Fehlerbehebung beginnen, sobald Sie eine Anforderung ausgefüllt und abgesendet haben.

  Anmerkung: Nach der Konfiguration und Aktivierung eines Call-Home-Funktion öffnet XClarity Administrator beim Auftreten eines wartungsfähigen Ereignisses automatisch ein Service-Ticket und überträgt Servicedateien an das Lenovo-Support Center, damit das Problem behoben werden kann. Weitere Informationen über die Aktivierung der Call-Home-Funktion finden Sie unter Automatische Problembenachrichtigung an den Lenovo Support einrichten (Call-Home-Funktion).

  Falls die Call-Home-Funktion nicht aktiviert ist, können Sie eine Serviceanforderung manuell übermitteln und Servicedateien senden (siehe Übermitteln einer Serviceanforderung zu Hardwareproblemen an das Lenovo-Support Center).

  Anmerkung: IBM ist der von Lenovo bevorzugte Service Provider für XClarity Administrator. Serviceanforderungen für einige Einheiten werden an IBM für Support weitergeleitet.
- Über die Lenovo Support-Hotline erhalten Sie gegen Gebühr technische Unterstützung bei der Verwendung, bei der Konfiguration und bei Softwareproblemen mit Ihren Produkten von Lenovo.

  Die örtlichen und gebührenfreien Telefonnummern für die Unterstützung finden Sie unter Website mit Telefonliste für Support. Sie können die Nummer wählen, die Sie für Ihre Region finden, oder auf der Webseite auf **Kontakt** klicken, um Unterstützung zu erhalten.

  Für Probleme mit Schweregrad 1 steht die Unterstützung rund um die Uhr zur Verfügung. Für alle anderen Schweregrade finden Sie die Öffnungszeiten und Sprachen auf der Website für Ihre Region.

  Wenden Sie sich an Website zu Lenovo Services – China, um Produktunterstützung in China zu erhalten: Für Produktunterstützung können Sie auch die Nummer 400-106-8888 anrufen. Telefonische Unterstützung ist von Montag bis Freitag von 9 bis 18 Uhr verfügbar.

Kapitel 2. Alerts, Ereignisse und Jobs anzeigen

Lenovo XClarity Administrator bietet verschiedene Methoden, um den Status verwalteter Einheiten zu überwachen.

- Die Alert-Liste enthält eine Echtzeitansicht der Probleme, die mit XClarity Administrator oder verwalteten Einheiten identifiziert wurden.
- Das Prüfprotokoll und Ereignisprotokoll bieten eine historische Ansicht der Benutzer- und Ereignisaktionen, die von XClarity Administrator identifiziert wurden.
- Das Jobprotokoll enthält eine Liste der länger laufenden Tasks, die auf einer oder mehreren verwalteten Einheiten ausgeführt werden.

Einheiten in den Wartungsmodus versetzen

Wenn sich ein Gerät im Wartungsmodus befindet, schließt Lenovo XClarity Administrator alle Ereignisse und Alerts für dieses Gerät aus allen Seiten aus, auf denen Ereignisse und Alerts angezeigt werden. Ausgeschlossene Alerts werden weiterhin protokolliert, sind aber ausgeblendet.

Zu dieser Aufgabe

Es werden nur die Ereignisse und Alerts ausgeschlossen, die für eine Einheit generiert wurden, während sich diese im Wartungsmodus befand. Es werden die Ereignisse und Alerts angezeigt, wie generiert wurden, bevor die Einheit in den Wartungsmodus versetzt wurde.

Wird ein Gerät in den Wartungsmodus und anschließend wieder in den Servicemodus versetzt, kann dies dazu führen, dass der Bestand für dieses Gerät nicht mehr auf dem neuesten Stand ist. Falls Abweichungen auftreten, können Sie den Bestand auf der Einheitenseite aktualisieren, indem Sie die Einheit auswählen und auf **Alle Aktionen → Bestand → Bestand aktualisieren** klicken.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um Einheiten in den Wartungsmodus zu versetzen.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite Service und Support wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Endpunktaktionen**, um die Seite Endpunktaktionen anzuzeigen.

Schritt 3. Wählen Sie ein oder mehrere Einheiten aus, die in den Wartungsmodus versetzt werden sollen.

Schritt 4. Klicken Sie auf **Aktionen → Wartung**, um das Dialogfeld Wartungsmodus mode anzuzeigen.

Schritt 5. Wählen Sie das Datum und die Uhrzeit aus, zu dem/zu der das Gerät vom Wartungsmodus wieder in den Servicemodus versetzt werden soll.

Wählen Sie **Unbegrenzt** aus, wenn das Gerät nicht wieder in den Servicemodus versetzt werden soll.

Schritt 6. Klicken Sie auf **Bestätigen**. Die Spalte „Wartung“ in der Tabelle wird für dieses Gerät in „Ja“ geändert.

Nach dieser Aufgabe

Wenn Sie die Wartung für das Gerät abgeschlossen haben, können Sie es wieder in den Servicemodus versetzen, indem Sie das Gerät auswählen, auf **Aktionen → Wartung** und dann auf das Dialogfeld **Wartung**

© Copyright Lenovo 2015, 2025

ausschalten klicken. Wenn Sie das Gerät nicht manuell wieder im Servicemodus versetzen, wird es nach Ablauf des angegebenen Enddatums. bzw. der angegebenen Endzeit automatisch in den Servicemodus versetzt.

Mit Alerts arbeiten

Alerts sind Hardware- oder Verwaltungsbedingungen, die eine Überprüfung und Benutzeraktion erfordern. Lenovo XClarity Administrator ruft die verwalteten Einheiten asynchron ab und zeigt Alerts, die von diesen Einheiten empfangen wurden.

Zu dieser Aufgabe

Weitere Informationen: XClarity Administrator: Überwachung

In der Regel wird ein entsprechendes Ereignis im Ereignisprotokoll gespeichert, wenn ein Alert empfangen wird. Es ist möglich, einen Alert ohne ein entsprechendes Ereignis im Ereignisprotokoll zu haben (selbst wenn das Protokoll abgeschlossen ist). Ereignisse, die auftreten, bevor Sie ein Gehäuse verwalten, werden nicht im Ereignisprotokoll angezeigt. Allerdings werden die Alerts für das Gehäuse im Alertprotokoll angezeigt, da Lenovo XClarity Administrator das CMM abruft, nachdem das Gehäuse verwaltet wurde.

Aktive Alerts anzeigen

Sie können eine Liste aller aktiven Hardware- und Verwaltungsalerts anzeigen.

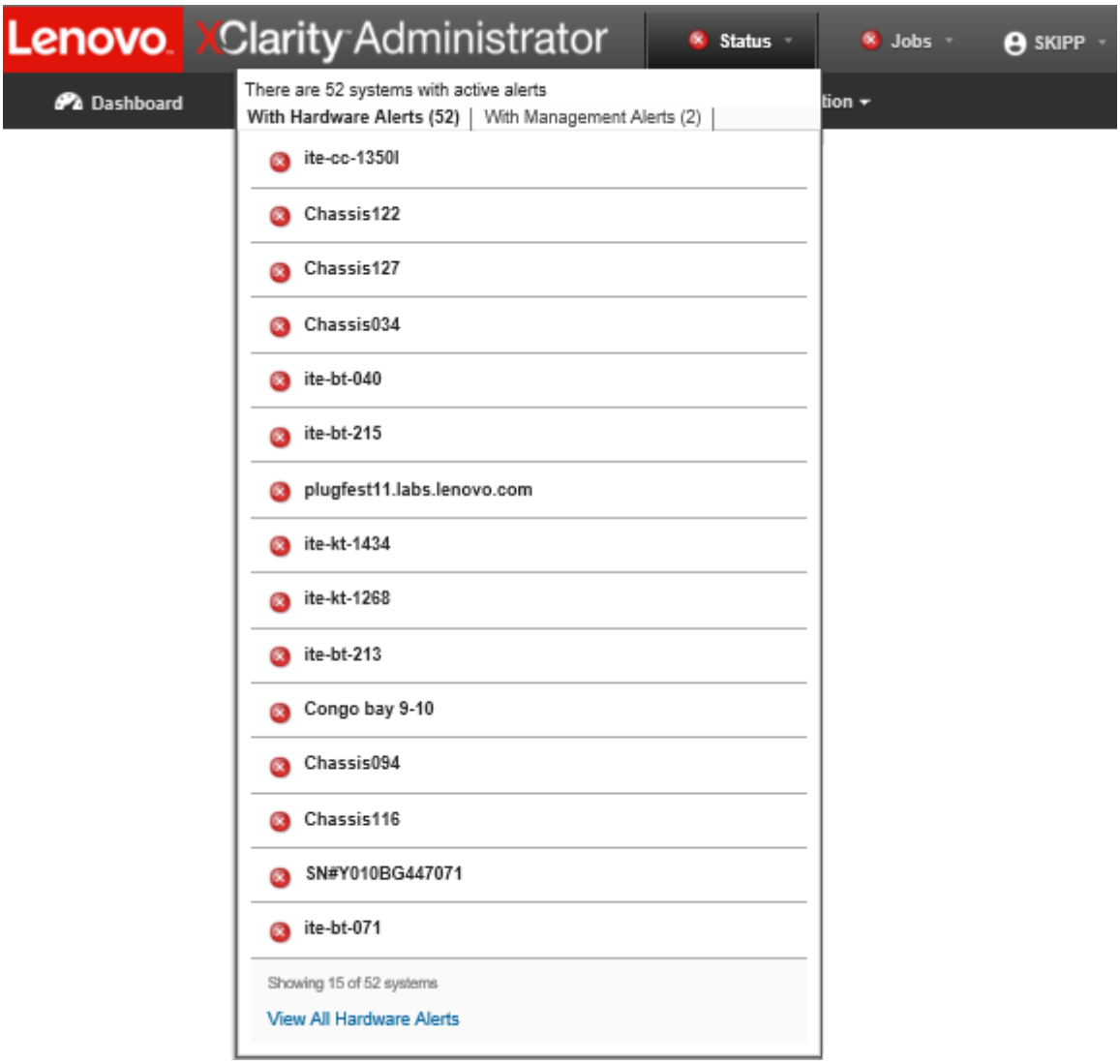
Zu dieser Aufgabe

Anmerkung: Alerts für Lenovo Storage-Einheiten stehen nur auf Englisch verfügbar, selbst wenn die Ländereinstellung für Lenovo XClarity Administrator auf eine andere Sprache festgelegt ist. Verwenden Sie ein externes Übersetzungssystem, um die Nachrichten bei Bedarf manuell zu übersetzen.

Vorgehensweise

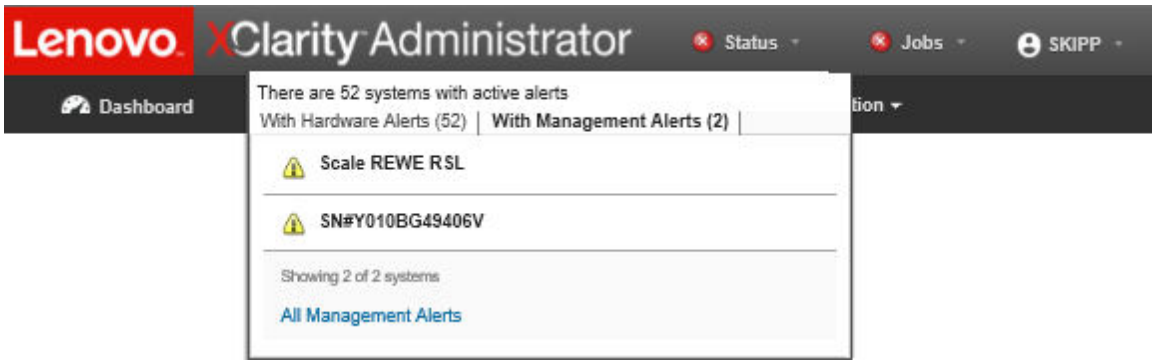
Führen Sie eines der folgenden Verfahren durch, um die aktiven Alerts anzuzeigen.

- So zeigen Sie Alerts nur für verwaltete Einheiten an (als *Hardware-Alerts* bekannt):
  1. Klicken Sie in der XClarity Administrator-Titelleiste auf das Pulldown-Menü **Status**, um eine Zusammenfassung der Hardware- und Verwaltungsalerts anzuzeigen.
  2. Klicken Sie auf die Registerkarte **Mit Hardware-Alerts**, um eine Zusammenfassung der Alerts für jede verwaltete Einheit anzuzeigen.



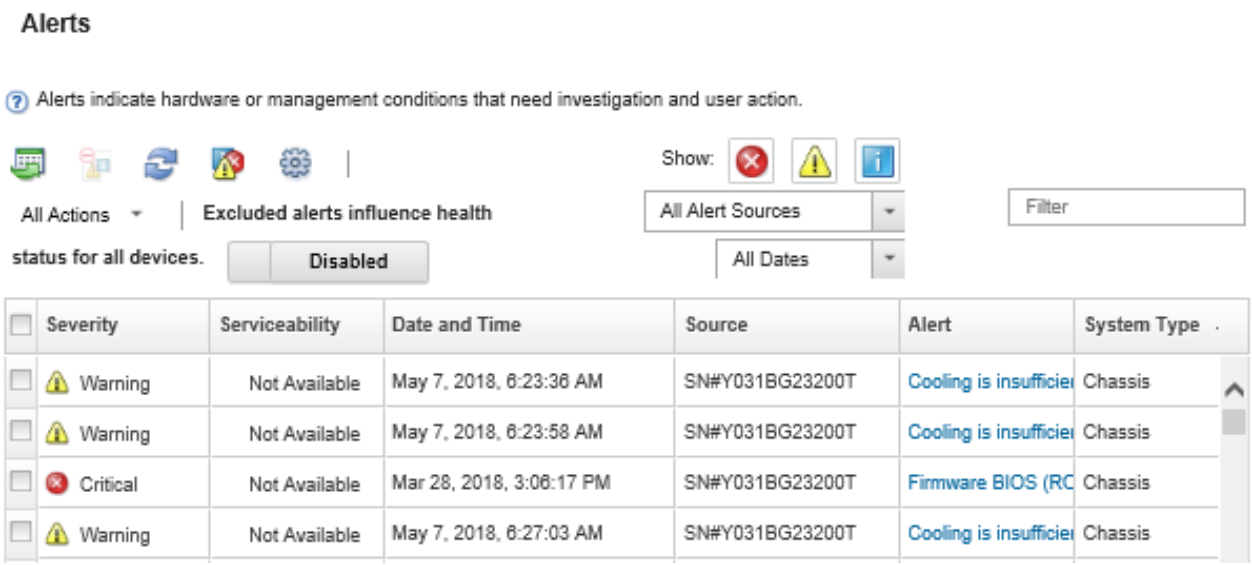
3. Bewegen Sie den Cursor über eine Einheit, die unter dieser Registerkarte aufgelistet ist, um eine Liste der Alerts für diese Einheit anzuzeigen.
4. Klicken Sie auf den Link **Alle Hardware-Alerts**, um die Seite „Alerts“ mit einer gefilterten Liste aller Hardware-Alerts anzuzeigen.

- So zeigen Sie nur Alerts von XClarity Administrator an (als *Verwaltungsalerts* bekannt):
  1. Klicken Sie in der XClarity Administrator-Titelleiste auf das Pulldown-Menü **Status**, um eine Zusammenfassung der Hardware- und Verwaltungsalerts anzuzeigen.
  2. Klicken Sie auf die Registerkarte **Mit Verwaltungsalerts**, um eine Zusammenfassung aller CMM- und XClarity Administrator-Alerts anzuzeigen.



3. Bewegen Sie den Cursor über eine Einheit, die unter dieser Registerkarte aufgelistet ist, um eine Liste der Alerts für diese Einheit anzuzeigen.
4. Klicken Sie auf den Link **Alle Verwaltungssalerts**, um die Seite „Alerts“ mit einer gefilterten Liste aller CMM- und XClarity Administrator-Alerts anzuzeigen.

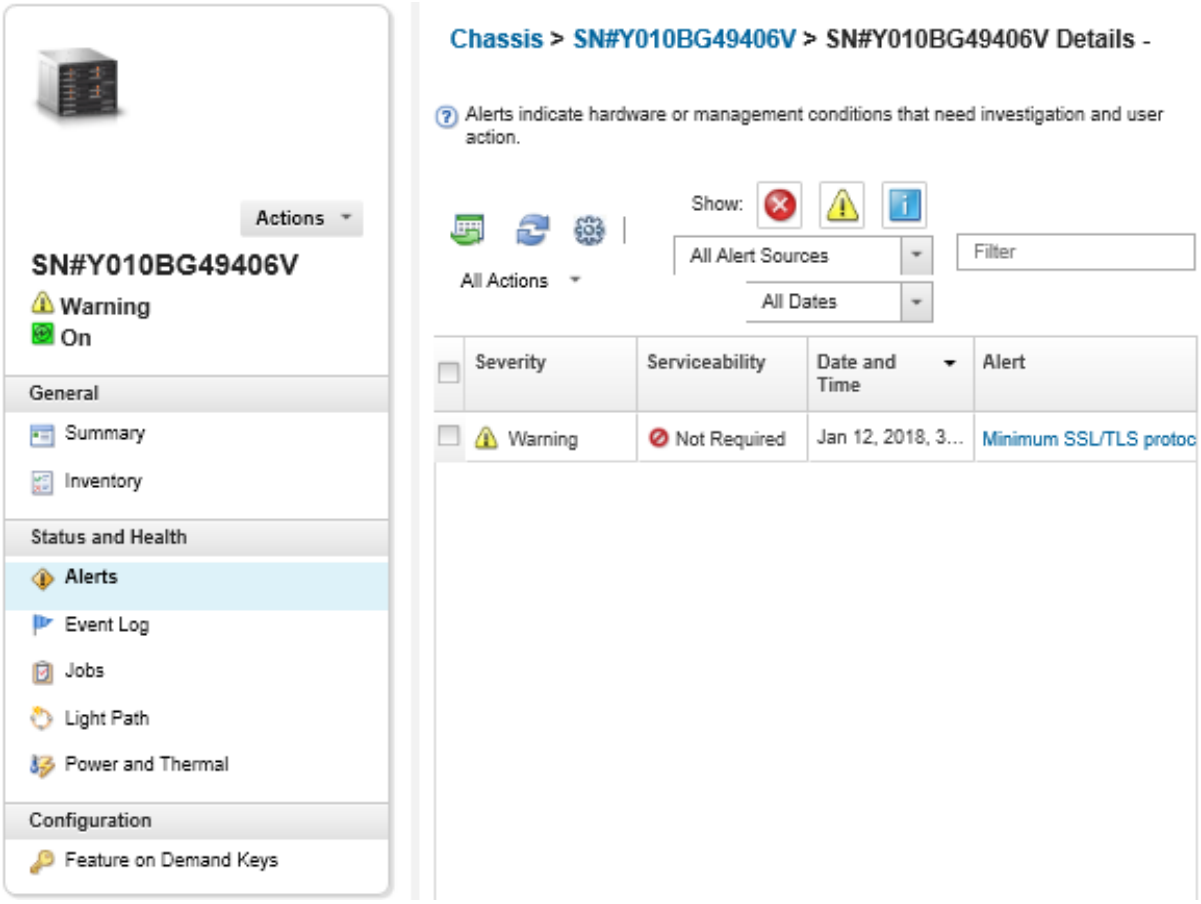
- Um alle Alerts in XClarity Administrator anzuzeigen, klicken Sie auf **Überwachung → Alerts** in der XClarity Administrator-Menüleiste. Die Seite „Alerts“ wird mit einer Liste aller aktiven Alerts angezeigt.



- So zeigen Sie Alerts für eine bestimmte Einheit an:
  1. Klicken Sie in der Menüleiste XClarity Administrator auf **Hardware** und anschließend auf einen Einheitentyp. Es wird eine Seite mit einer Tabellenansicht aller verwalteten Einheiten dieses Typs angezeigt. Klicken Sie beispielsweise auf **Hardware → Server**, um die Seite Server anzuzeigen.
  2. Klicken Sie auf eine bestimmte Einheit, um die Zusammenfassungsseite für die Einheit anzuzeigen.
  3. Klicken Sie unter „Status und Zustand“ auf **Alerts**, um eine Liste aller Alerts anzuzeigen, die dieser Einheit zugeordnet sind.

     Anmerkungen: Die Spalte „Wartbarkeit“ kann „Nicht verfügbar“ anzeigen, wenn:

     – Der Alert auf der Einheit aufgetreten ist, bevor XClarity Administrator mit der Verwaltung begonnen hat
     – Das Ereignisprotokoll wurde abgeschlossen und das Ereignis, das diesem Alert zugeordnet ist, befindet sich nicht mehr im Ereignisprotokoll.



Ergebnisse

Über diese Seite „Alerts“ können Sie die folgenden Aktionen ausführen:

- Die Liste der Alerts durch Klicken auf das Symbol **Aktualisieren** ( ) aktualisieren

  Tipp: Das Alertprotokoll wird alle 30 Sekunden automatisch aktualisiert, wenn neue Alerts erkannt werden.
- Auf den Link in der Spalte **Alert** klicken, um Informationen zu einem bestimmten Alert (einschließlich einer Erläuterung und Benutzeraktion) und zu der Einheit anzuzeigen, die die Quelle des Alerts ist (wie der Universally Unique Identifier). Ein Dialogfenster mit Informationen zu den Alerteigenschaften und Details wird angezeigt.

  Anmerkung: Wenn die Erläuterungen und Wiederherstellungsaktionen für einen Alert nicht auf der Registerkarte **Details** angezeigt werden, gehen Sie zu Lenovo Flex System-Onlinedokumentation und suchen Sie nach der Alert-ID (zum Beispiel `FQXHMSE0004G`). Die Website enthält immer die aktuellen Informationen.
- Standardmäßig beeinflussen ausgeschlossene Alerts nicht den Allgemeinzustand von verwalteten Einheiten. Sie können ausgeschlossene Alerts zulassen, um den Integritätsstatus der verwalteten Einheiten über die Seite „Alerts“ zu beeinflussen, indem Sie auf den Schalter klicken, um **Ausgeschlossene Alerts beeinflussen Integritätsstatus für alle Einheiten** zu aktivieren.
- Sie können Schwellenwerteinstellungen für das Auslösen von Alerts und Ereignissen festlegen, wenn ein bestimmter Wert wie die Lebensdauer einer SSD in einem ThinkSystem- oder ThinkServer-Server eine Warnung oder einen kritischen Wert überschreitet (siehe Schwellenwerteinstellungen für die Generierung von Alerts und Ereignissen festlegen in der Onlinedokumentation von XClarity Administrator).

- Das Alertprotokoll durch Klicken auf das Symbol **Als CSV exportieren** ( ) exportieren.

  Anmerkung: Die Zeitmarken in den exportierten Protokollen verwenden die Ortszeit, die vom Webbrowser angegeben wurde.
- Schließen Sie bestimmte Alerts aus allen Seiten aus, auf denen Alerts angezeigt werden (siehe Alerts ausschließen).
- Liste der Alerts eingrenzen, die auf der aktuellen Seite angezeigt werden:
  - Alerts mit einem bestimmten Schweregrad durch Klicken auf die folgenden Symbole anzeigen oder einblenden:
    - Symbol für **Kritische Alerts** ( )
    - Symbol für **Warnalerts** ( )
    - Symbol für **Informationsalerts** ( )
  - Ausschließlich Alerts aus bestimmten Quellen anzeigen. Sie können eine der folgenden Optionen aus der Dropdown-Liste auswählen:
    - Alle Alert-Quellen
    - Hardware-Ereignisse
    - Management-Ereignisse
    - Service Center-Ereignisse
    - Für Kunden wartungsfähige Ereignisse
    - Nicht wartungsfähige Ereignisse
  - Nur Alerts mit einem bestimmten Datum und einer bestimmten Uhrzeit anzeigen. Sie können eine der folgenden Optionen aus der Dropdown-Liste auswählen:
    - Alle Daten
    - Vergangene zwei Stunden
    - Vergangene 24 Stunden
    - Letzte Woche
    - Letzter Monat
  - Nur Alerts anzeigen, die einen bestimmten Text enthalten (durch Eingabe des Textes in das Feld **Filter**)
  - Alerts durch Klicken auf eine Spaltenüberschrift spaltenweise sortieren

Alerts ausschließen

Wenn bestimmte Alerts für Sie nicht relevant sind, können Sie diese Alerts auf allen Seiten ausschließen, auf denen Alerts angezeigt werden. Ausgeschlossene Alerts werden weiterhin im Protokoll festgehalten, aber auf den Seiten mit Alerts ausgeblendet, einschließlich Protokollansichten und Gerätestatus.

Zu dieser Aufgabe

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

Sie können Einheiten in den Wartungsmodus versetzen, sodass alle Ereignisse und Alerts für diese Einheiten ausgeschlossen sind (siehe Einheiten in den Wartungsmodus versetzen).

Einschränkung: Nur Benutzer mit Administratorberechtigung können Alerts ausschließen und wiederherstellen.

Wichtig: Wenn Sie Statusalerts ausschließen, ändert sich der Gerätestatus in der Gerätezusammenfassung und auf den Detailseiten nicht.

VorgehensweiseGehen Sie wie folgt vor, um Alerts aus den Alertprotokollen auszuschließen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Alerts**. Die Seite Alerts wird angezeigt.

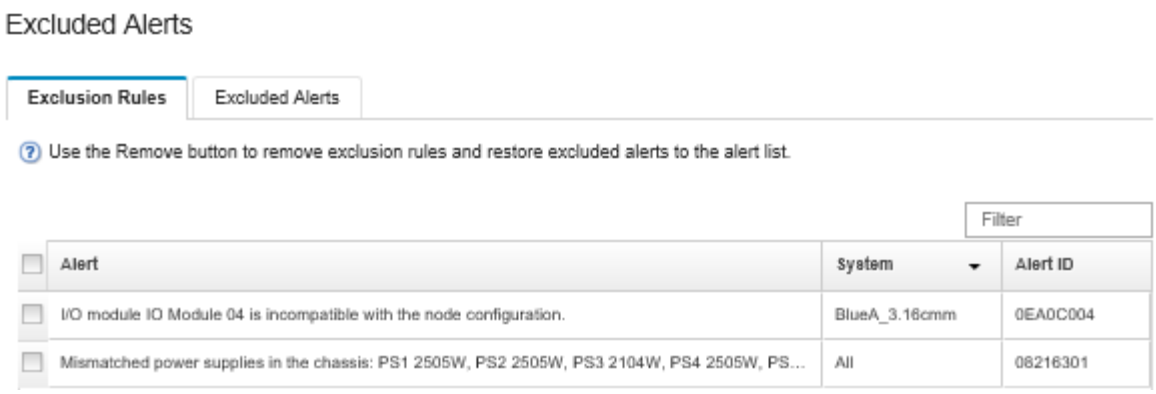
Schritt 2. Wählen Sie die auszuschließenden Alerts aus und klicken Sie auf das Symbol **Alerts ausschließen** (). Das Dialogfenster „Ereignisse ausschließen“ wird angezeigt.

Schritt 3. Wählen Sie eine der folgenden Optionen:
- **Ausgewählte Alerts von allen Systemen ausschließen**. Schließt die ausgewählten Alerts von allen verwalteten Einheiten aus.
- **Nur Alerts aus Systemen im Bereich der ausgewählten Instanzen ausschließen**. Schließt die ausgewählten Alerts von den verwalteten Einheiten aus, auf die sich die ausgewählten Alerts beziehen.

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

Nach dieser Aufgabe

Wenn Sie Alerts ausschließen, erstellt Lenovo XClarity Administrator Ausschlussregeln basierend auf den von Ihnen bereitgestellten Angaben. Sie können eine Liste der Ausschlussregeln und ausgeschlossenen Alerts über die Seite „Alerts“ anzeigen. Klicken Sie dazu auf das Symbol **Ausgeschlossene/Bestätigte Alerts anzeigen** (). Klicken Sie im Dialogfenster Ausgeschlossene/Bestätigte Alerts auf die Registerkarte **Ausschlussregeln**, um die Liste der Ausschlussregeln anzuzeigen, oder klicken Sie auf die Registerkarte **Ausgeschlossene Alerts**, um die Liste der ausgeschlossenen Alerts anzuzeigen.



Standardmäßig beeinflussen ausgeschlossene Alerts nicht den Allgemeinzustand von verwalteten Einheiten. Sie können ausgeschlossene Alerts zulassen, um den Integritätsstatus der verwalteten Einheiten über die Seite „Alerts“ zu beeinflussen, indem Sie auf den Schalter klicken, um **Ausgeschlossene/Bestätigte Alerts anzeigen** zu aktivieren.

Sie können Alerts wiederherstellen, die vom Alertprotokoll ausgeschlossen wurden, indem Sie die entsprechende Ausschlussregel entfernen. Um eine Ausschlussregel zu entfernen, klicken Sie auf das **Ausgeschlossene Alerts anzeigen**-Symbol (). Das Dialogfenster „Ausgeschlossene Alerts“ wird angezeigt. Wählen Sie die wiederherzustellenden Ausschlussregeln oder ausgeschlossenen Alerts aus und klicken Sie auf **Entfernen**.

Einen Alert beheben

Lenovo XClarity Administrator enthält Informationen über die geeigneten Maßnahmen zum Beheben von Alerts.

VorgehensweiseGehen Sie wie folgt vor, um ein Alert zu beheben.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Überwachung → Alerts**, um die Seite Alerts anzuzeigen.

Schritt 2. Suchen Sie den Alert im Alertprotokoll.

Schritt 3. Klicken Sie auf den Link in der Spalte **Alert**, um Informationen zum Alert (einschließlich einer Erläuterung und Wiederherstellungsaktionen) und Eigenschaften für die Einheit anzuzeigen, die die Quelle des Alerts ist (wie der Universally Unique Identifier).

Schritt 4. Führen Sie die auf der Registerkarte **Details** aufgelisteten Wiederherstellungsaktionen aus, um den Alert zu beheben. Das folgende Beispiel zeigt Wiederherstellungsaktionen für ein Ereignis.

Ändern Sie die Sicherheitsrichtlinieneinstellung auf dem referenzierten verwalteten Gehäuse, sodass sie mit der aktuellen Sicherheitsrichtlinie auf dem Verwaltungsserver übereinstimmen.

Um die Sicherheitsrichtlinie auf dem Gehäuse zu ändern, öffnen Sie eine Sitzung der Befehlszeilenschnittstelle auf dem Chassis Management Module (CMM) und führen Sie einen der folgenden Befehle aus:

- Ändern der Sicherheitsrichtlinie in `Secure`:
  `security -p secure -T mm[p]`
- Ändern der Sicherheitsrichtlinie in `Legacy`:
  `security -p legacy -T mm[p]`

Anmerkung: Wenn die Erläuterungen und Wiederherstellungsaktionen für einen Alert nicht auf der Registerkarte **Details** angezeigt werden, gehen Sie zu Lenovo Flex System-Onlinedokumentation und suchen Sie nach der Alert-ID (zum Beispiel `FQXHMSE0004G`). Die Website enthält immer die aktuellen Informationen.

Wenn Sie die empfohlenen Aktionen ausführen und das Problem weiterhin auftritt, wenden Sie sich an den Lenovo-Support.

Alerts bestätigen

Wenn ein aktiver Alert bestätigt wird, wird er auf den Seiten aufgelistet, auf denen Alerts angezeigt werden, hat aber keinen Einfluss auf den Wertigkeitsstatus der entsprechenden Einheit.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Alert zu bestätigen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Alerts**. Die Seite Alerts wird angezeigt.

Schritt 2. Wählen Sie die zu bestätigenden Alerts aus.

Schritt 3. Klicken Sie auf das Symbol **Alerts bestätigen** ( ).

Nach dieser Aufgabe

- Sie können eine Liste der bestätigten Alerts über die Seite „Alerts“ anzeigen. Klicken Sie auf das Symbol **Ausgeschlossene/Bestätigte Alerts anzeigen** ( ), um das Dialogfenster „Ausgeschlossene/Bestätigte Alerts“ anzuzeigen, und klicken Sie dann auf die Registerkarte **Bestätigte Alerts**.
- Sie können die Bestätigung eines aktiven Alerts entfernen. Klicken Sie dazu auf das Symbol **Ausgeschlossene/Bestätigte Alerts anzeigen** ( ), um das Dialogfenster „Ausgeschlossene/Bestätigte Alerts“ anzuzeigen, und klicken Sie dann auf die Registerkarte **Bestätigte Alerts**. Wählen Sie die Alerts aus und klicken Sie auf das Symbol **Bestätigung entfernen** ( ).

Ereignisse handhaben

Über Lenovo XClarity Administrator haben Sie Zugriff auf ein Ereignisprotokoll und ein Prüfprotokoll.

Zu dieser Aufgabe

Weitere Informationen: XClarity Administrator: Überwachung

Das *Ereignisprotokoll* enthält eine Liste aller archivierten Hardware- und Verwaltungsereignisse.

Das *Prüfprotokoll* stellt eine historische Aufzeichnung aller Benutzeraktionen dar, z. B. Anmelden an Lenovo XClarity Administrator, Erstellen eines neuen Benutzers und Ändern eines Benutzerkennworts. Sie können das Prüfprotokoll verwenden, um die Authentifizierung und Kontrollen in IT-Systemen zu verfolgen und zu dokumentieren.

Ereignisse im Ereignisprotokoll überwachen

Das *Ereignisprotokoll* enthält eine Liste aller archivierten Hardware- und Verwaltungsereignisse.

Zu dieser Aufgabe

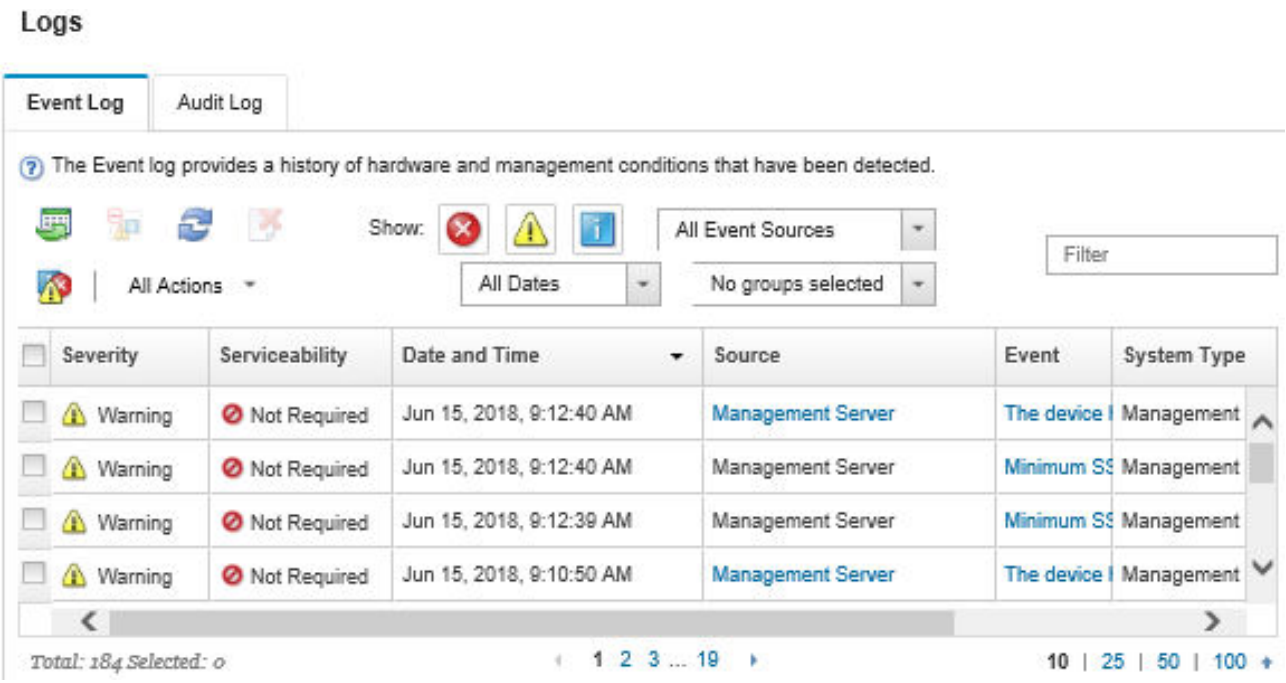
Das Ereignisprotokoll enthält Informations- und Nicht-Informationsereignisse. Die Anzahl an Einträgen für jedes dieser Ereignisse ist variabel, bis die maximale Anzahl von 50.000 Ereignissen im Ereignisprotokoll erreicht wird. Zu diesem Zeitpunkt gibt es maximal 25.000 Informations- und 25.000 Nicht-Informationsereignisse. Beispiel: Zu Beginn gab es 0 Ereignisse im Ereignisprotokoll. Die empfangenen Ereignisse teilen sich wie folgt auf: 20.000 Informationsereignisse und 30.000 Nicht-Informationsereignisse. Wenn das nächste Ereignis empfangen wird, wird jedes Mal das älteste Informationsereignis gelöscht. Dies gilt auch, wenn ein Nicht-Informationsereignis vorhanden ist, das älter ist. Dies führt dazu, dass das Protokoll nach einer gewissen Zeit ausgeglichen ist, d. h., es enthält 25.000 Einträge jedes Ereignistyps.

Lenovo XClarity Administrator sendet ein Ereignis, wenn das Ereignisprotokoll 80 Prozent der maximalen Größe erreicht und ein weiteres Ereignis, wenn die Summe der Ereignis- und Prüfprotokolle 100 Prozent der maximalen Größe erreicht.

Tipp: Sie können das Ereignisprotokoll exportieren, um sicherzustellen, dass Ihnen eine vollständige Aufzeichnung aller Hardware- und Verwaltungsereignisse vorliegt. Klicken Sie zum Exportieren des Ereignisprotokolls auf das Symbol für **Als CSV exportieren** ( ).

Vorgehensweise

Um das Ereignisprotokoll anzuzeigen, klicken Sie auf **Überwachung → Ereignisprotokolle** in der Menüleiste von Lenovo XClarity Administrator und dann die Registerkarte **Ereignisprotokoll**. Die Seite „Ereignisprotokoll“ wird angezeigt.



Die Spalte **Wartbarkeit** gibt an, ob die Einheit gewartet werden muss. Diese Spalte kann einen der folgenden Werte aufweisen:

- **Nicht erforderlich**. Das Ereignis ist informativ und erfordert keine Aktion.
- **Benutzer**. Führen Sie die entsprechende Wiederherstellungsaktion durch, um das Problem zu beheben.

  Um Informationen über ein bestimmtes Ereignis anzuzeigen, klicken Sie auf den Link in der Spalte **Ereignis**. Es wird ein Dialogfenster angezeigt mit Informationen zu den Eigenschaften der Einheit, die das Ereignis gesendet hat, Details zum Ereignis und Wiederherstellungsaktionen.
- **Unterstützung**. Wenn Call-Home-Funktion in Lenovo XClarity Administrator aktiviert ist, wird das Ereignis in der Regel zum Lenovo-Support Center gesendet. Ausnahme: Es existiert bereits ein offenes Service-Ticket mit dieser Ereignis-ID für die Einheit.

  Wenn Call-Home-Funktion nicht aktiviert ist, wird empfohlen, dass Sie manuell ein Service-Ticket öffnen, um das Problem zu beheben (siehe Service-Ticket öffnen in der Onlinedokumentation von Lenovo XClarity Administrator).

Ergebnisse

Über die Seite „Ereignisprotokoll“ können Sie die folgenden Aktionen ausführen:

- Zeigen Sie die Quelle des Ereignisses an, indem Sie in der Spalte **Quelle** auf den Link klicken.
- Liste der Ereignisse durch Klicken auf das Symbol **Aktualisieren** ( ) aktualisieren.

  Tipp: Das Ereignisprotokoll wird alle 30 Sekunden automatisch aktualisiert, wenn neue Ereignisse erkannt werden.
- Wählen Sie zum Löschen aller Ereignisse im Ereignisprotokoll **Alle Aktionen → Ereignisprotokoll löschen** aus.
- Details über ein bestimmtes Ereignis durch Klicken auf den Link in der Spalte **Ereignis** und dann Klicken auf die Registerkarte **Details** anzeigen
- Ereignisprotokoll durch Klicken auf das Symbol **Als CSV exportieren** ( ) exportieren.

Anmerkung: Die Zeitmarken in den exportierten Protokollen verwenden die Ortszeit, die vom Webbrowser angegeben wurde.

- Schließen Sie bestimmte Ereignisse von allen Seiten aus, auf denen Ereignisse angezeigt werden (siehe Ereignisse ausschließen).
- Liste der Hardware- und Verwaltungsereignisse eingrenzen, die auf der aktuellen Seite angezeigt werden:
  - Ereignisse mit einem bestimmten Schweregrad durch Klicken auf die folgenden Symbole in der Dropdown-Liste anzeigen oder einblenden:
    - Symbol für **Kritische Ereignisse** ( )
    - Symbol für **Warnereignisse** ( )
    - Symbol für **Informationsereignisse** ( )
  - Ausschließlich Ereignisse aus bestimmten Quellen anzeigen. Sie können eine der folgenden Optionen aus der Dropdown-Liste auswählen:
    - Alle Alert-Quellen
    - Hardware-Ereignisse
    - Management-Ereignisse
    - Wartungsfähige Ereignisse
    - Für Kunden wartungsfähige Ereignisse
    - Nicht wartungsfähige Ereignisse
  - Nur Ereignisse mit einem bestimmten Datum und einer bestimmten Uhrzeit anzeigen. Sie können eine der folgenden Optionen auswählen:
    - Alle Daten
    - Vergangene 2 Stunden
    - Vergangene 24 Stunden
    - Letzte Woche
    - Letzter Monat
    - Custom

    Wenn Sie **Angepasst** auswählen, können Sie Hardware- und Verwaltungsereignisse filtern, die zwischen einem benutzerdefinierten Startdatum und dem aktuellen Datum ausgelöst wurden.
  - Nur Ereignisse anzeigen, die einen bestimmten Text enthalten (durch Eingabe des Textes in das Feld **Filter**)
  - Ereignisse durch Klicken auf eine Spaltenüberschrift spaltenweise sortieren.

Ereignisse im Prüfprotokoll überwachen

Das *Prüfprotokoll* stellt eine historische Aufzeichnung aller Benutzeraktionen dar, z. B. Anmelden an Lenovo XClarity Administrator, Erstellen eines neuen Benutzers und Ändern eines Benutzerkennworts. Sie können das Prüfprotokoll verwenden, um die Authentifizierung und Kontrollen in IT-Systemen zu verfolgen und zu dokumentieren.

Zu dieser Aufgabe

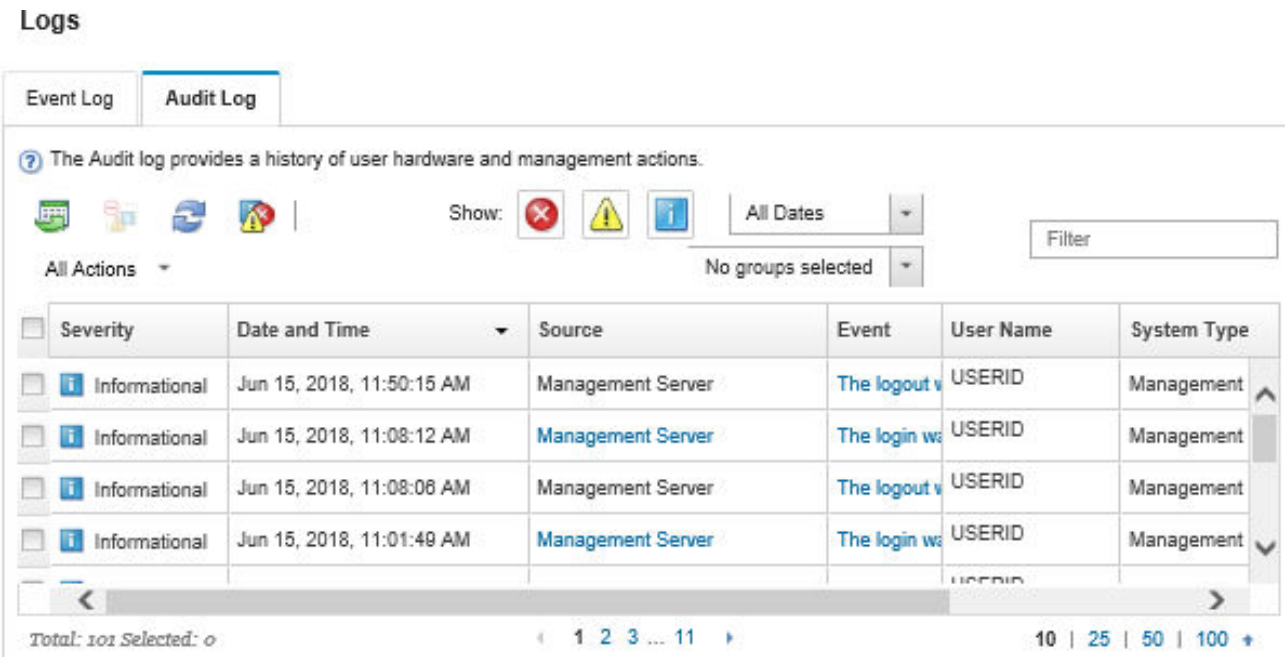
Das Prüfprotokoll kann maximal 50.000 Ereignisse enthalten. Wenn die maximale Größe erreicht ist, wird das älteste Ereignis im Protokoll gelöscht und das neue Ereignis zum Protokoll hinzugefügt.

XClarity Administrator sendet ein Ereignis, wenn das Prüfprotokoll 80 Prozent der maximalen Größe erreicht und ein weiteres Ereignis, wenn die Summe der Ereignis- und Prüfprotokolle 100 Prozent der maximalen Größe erreicht.

Tipp: Sie können das Prüfprotokoll exportieren, um sicherzustellen, dass Ihnen eine vollständige Aufzeichnung aller Prüfereignisse vorliegt. Um das Prüfprotokoll zu exportieren, klicken Sie auf das Symbol für **Als CSV exportieren** ( ).

Vorgehensweise

Um das Prüfprotokoll anzuzeigen, klicken Sie auf **Überwachung → Ereignisprotokolle** in der Menüleiste von XClarity Administrator und dann auf die Registerkarte **Prüfprotokoll**. Die Seite Prüfprotokoll wird angezeigt.



Um Informationen über ein bestimmtes Prüfereignis anzuzeigen, klicken Sie auf den Link in der Spalte **Ereignis**. Es wird ein Dialogfenster angezeigt mit Informationen zu den Eigenschaften der Einheit, die das Ereignis gesendet hat, Details zum Ereignis und Wiederherstellungsaktionen.

Ergebnisse

Über diese Seite können Sie die folgenden Aktionen ausführen:

- Zeigen Sie die Quelle des Prüfereignisses an, indem Sie in der Spalte **Quelle** auf den Link klicken.
- Liste der Prüfereignisse durch Klicken auf das Symbol **Aktualisieren** ( ) aktualisieren.

  Tipp: Das Ereignisprotokoll wird alle 30 Sekunden automatisch aktualisiert, wenn neue Ereignisse erkannt werden.
- Details über ein bestimmtes Prüfereignis durch Klicken auf den Link in der Spalte **Ereignis** und dann Klicken auf die Registerkarte **Details** anzeigen
- Prüfprotokoll durch Klicken auf das Symbol **Als CSV exportieren** ( ) exportieren.

  Anmerkung: Die Zeitmarken in den exportierten Protokollen verwenden die Ortszeit, die vom Webbrowser angegeben wurde.
- Schließen Sie bestimmte Prüfereignisse von allen Seiten aus, auf denen Ereignisse angezeigt werden (siehe Ereignisse ausschließen).

- Liste der Prüfereignisse eingrenzen, die auf der aktuellen Seite angezeigt werden:
  - Ereignisse mit einem bestimmten Schweregrad durch Klicken auf die folgenden Symbole anzeigen oder einblenden:
    - Symbol für **Kritische Ereignisse** ( )
    - Symbol für **Warnereignisse** ( )
    - Symbol für **Informationsereignisse** ( )
  - Nur Ereignisse mit einem bestimmten Datum und einer bestimmten Uhrzeit anzeigen. Sie können eine der folgenden Optionen aus der Dropdown-Liste auswählen:
    - Alle Daten
    - Vergangene 2 Stunden
    - Vergangene 24 Stunden
    - Letzte Woche
    - Letzter Monat
    - Custom

    Wenn Sie **Angepasst** auswählen, können Sie Hardware- und Verwaltungsereignisse filtern, die zwischen einem benutzerdefinierten Startdatum und dem aktuellen Datum ausgelöst wurden.
  - Nur Ereignisse anzeigen, die einen bestimmten Text enthalten (durch Eingabe des Textes in das Feld **Filter**)
  - Ereignisse durch Klicken auf eine Spaltenüberschrift spaltenweise sortieren.

Ein Ereignis beheben

Lenovo XClarity Administrator enthält Informationen über die geeigneten Maßnahmen zum Beheben von Ereignissen.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Ereignis zu beheben.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Ereignisprotokolle**, um die Seite Protokolle anzuzeigen.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisprotokoll**.

Schritt 3. Suchen Sie das Ereignis im Ereignisprotokoll.

Schritt 4. Klicken Sie auf den Link in der Spalte **Ereignis**, um Informationen zu diesem Ereignis (einschließlich Erläuterungen und Wiederherstellungsaktionen) und zu der Einheit anzuzeigen, die das Ereignis ausgelöst hat.

Schritt 5. Klicken Sie auf die Registerkarte **Details**.

Schritt 6. Führen Sie die auf der Registerkarte **Details** angegebenen Wiederherstellungsaktionen aus, um das Ereignis zu beheben.

Anmerkung: Wenn die Erläuterungen und Wiederherstellungsaktionen für ein Ereignis nicht angezeigt werden, rufen Sie die Lenovo Flex System-Onlinedokumentation auf und suchen Sie nach dem Ereignisnamen. Die Website enthält immer die aktuellen Informationen.

Wenn Sie die empfohlenen Aktionen ausführen und das Problem weiterhin auftritt, wenden Sie sich an den Lenovo-Support.

Ereignisse ausschließen

Wenn bestimmte Ereignisse für Sie nicht relevant sind, können Sie diese Ereignisse auf allen Seiten ausschließen, auf denen Ereignisse angezeigt werden. Ausgeschlossene Ereignisse werden weiterhin im Protokoll festgehalten, aber auf den Seiten mit Ereignissen ausgeblendet.

Zu dieser Aufgabe

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

Sie können Einheiten in den Wartungsmodus versetzen, sodass alle Ereignisse und Alerts für diese Einheiten ausgeschlossen sind (siehe Einheiten in den Wartungsmodus versetzen).

Einschränkung: Nur Benutzer mit Administratorberechtigung können Ereignisse ausschließen und wiederherstellen.

Vorgehensweise

Gehen Sie wie folgt vor, um Ereignisse aus den Ereignisprotokollen auszuschließen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Ereignisprotokolle** und wählen Sie dann die Registerkarte **Ereignisprotokoll** aus. Die Seite „Ereignisprotokolle“ wird angezeigt.

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

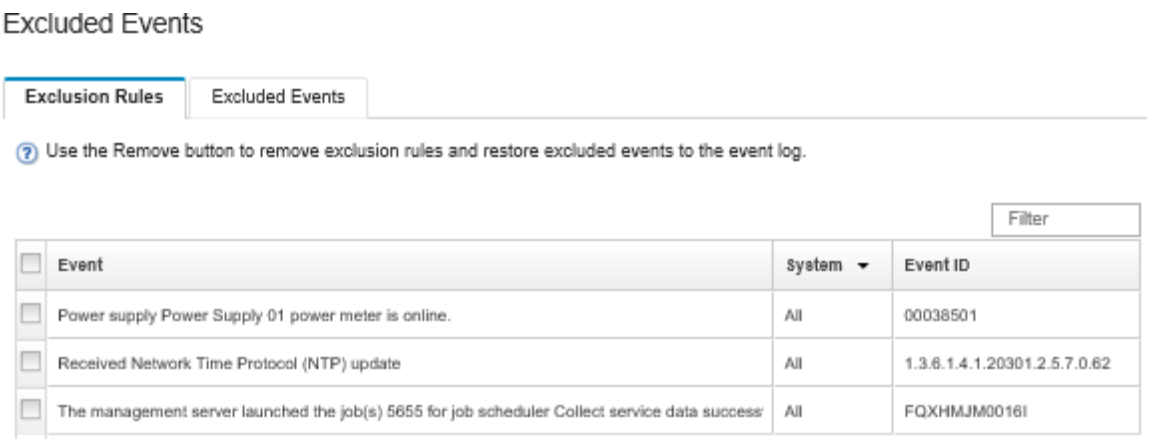
Schritt 3. Wählen Sie eine der folgenden Optionen:
- **Ausgewählte Ereignisse von allen Systemen ausschließen**. Schließt die ausgewählten Ereignisse von allen verwalteten Einheiten aus.
- **Nur Ereignisse aus Systemen im Bereich der ausgewählten Instanzen ausschließen**. Schließt die ausgewählten Ereignisse von den verwalteten Einheiten aus, auf die sich die ausgewählten Ereignisse beziehen.

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

Nach dieser Aufgabe

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

- Zeigen Sie eine Liste der Ausschlussregeln und ausgeschlossenen Ereignisse über die Seite für Protokolle an. Klicken Sie dazu auf das **Ausgeschlossene Ereignisse anzeigen**-Symbol ( ). Klicken Sie im Dialogfenster Ausgeschlossene Ereignisse auf die Registerkarte **Ausschlussregeln**, um die Ausschlussregeln anzuzeigen, oder klicken Sie auf die Registerkarte **Ausgeschlossene Ereignisse**, um ausgeschlossene Ereignisse anzuzeigen.



- Stellen Sie Ereignisse wieder her, die vom Ereignisprotokoll ausgeschlossen wurden, indem Sie die entsprechende Ausschlussregel entfernen. Um eine Ausschlussregel zu entfernen, klicken Sie auf das **Ausgeschlossene Ereignisse anzeigen**-Symbol ( ). Das Dialogfenster Ausgeschlossene Ereignisse wird angezeigt. Wählen Sie die wiederherzustellenden Ausschlussregeln aus und klicken Sie auf **Ausschlüsse entfernen**.
- Vermeiden Sie, das wartungsfähige Ereignisse, die sich in der Liste ausgeschlossener Ereignisse befinden, automatisch Problemberichte senden, in dem Sie auf **Verwaltung → Service und Support** in der Lenovo XClarity Administrator Menüleiste klicken. Klicken Sie anschließend auf die Registerkarte **Service-Weiterleiter** und wählen Sie dann **Nein** neben der Frage **Sollen bei ausgeschlossenen Ereignissen Problemberichte geöffnet werden?** aus.

Ereignisse weiterleiten

Sie können Lenovo XClarity Administrator so konfigurieren, dass Ereignisse an mobile Einheiten und verbundene Anwendungen in Ihrer Umgebung weitergeleitet werden. Dies hilft beim Erfassen und Überwachen von Hardwarestatus- und Laufzeitproblemen für Ihre Hardwareumgebung.

Weitere Informationen: XClarity Administrator: Überwachung

Ereignisse an syslog, Remote-SNMP-Manager, E-Mail und andere Ereignisservices weiterleiten

Sie können Lenovo XClarity Administrator so konfigurieren, dass Ereignisse an verbundene Anwendungen in Ihrer Umgebung weitergeleitet werden. Dies hilft beim Erfassen und Überwachen von Hardwarestatus- und Laufzeitproblemen für Ihre Hardwareumgebung. Basierend auf der Einheit, Ereignisklasse, Ereigniswertigkeit und Komponente können Sie festlegen, in welchem Umfang Ereignisse weitergeleitet werden.

Zu dieser Aufgabe

Lenovo XClarity Administrator kann Ereignisse für eine oder mehrere Einheiten weiterleiten. Bei Prüfereignissen können Sie auswählen, ob alle oder keine der Prüfereignisse weitergeleitet werden. Es ist nicht möglich, bestimmte Prüfereignisse weiterzuleiten. Bei Hardware- und Verwaltungsereignissen können Sie auswählen, dass Ereignisse für eine oder mehrere Wertigkeiten (kritische, Warn- und Informationsereignisse) und für eine oder mehrere Komponenten (z. B. Plattenlaufwerke, Prozessoren und Adapter) weitergeleitet werden.

Lenovo XClarity Administrator verwendet Ereignisweiterleitungen zum Weiterleiten von Ereignissen. Eine *Ereignisweiterleitung* enthält Informationen zum zu verwendenden Protokoll, zum Empfänger, zu den zu überwachenden Einheiten und zu den weiterzuleitenden Ereignissen. Nachdem Sie eine Ereignisweiterleitung erstellt und aktiviert, startet Lenovo XClarity Administrator die Überwachung der eingehenden Ereignisse

basierend auf den Filterkriterien. Wenn eine Übereinstimmung gefunden wird, wird das Ereignis basierend auf dem zugeordneten Protokoll weitergeleitet.

Die folgenden Protokolle werden unterstützt:

- **Azure Log Analytics**. Lenovo XClarity Administrator leitet die überwachten Ereignisse über das Netzwerk an Microsoft Azure Log Analytics weiter.
- **E-Mail**. Lenovo XClarity Administrator leitet die überwachten Ereignisse per SMTP an eine oder mehrere E-Mail-Adressen weiter. Die E-Mail enthält Informationen zum Ereignis, den Hostnamen der Quelleinheit sowie Links zur Lenovo XClarity Administrator-Webschnittstelle und zur Lenovo XClarity Mobile-App.
- **FTP**. Leitet die überwachten Ereignisse über das Netzwerk an einen FTP-Server weiter.
- **REST**. Lenovo XClarity Administrator leitet die überwachten Ereignisse über das Netzwerk an einen REST-Webservice weiter.
- **SNMP**. Lenovo XClarity Administrator leitet die überwachten Ereignisse über das Netzwerk an einen Remote-SNMP-Manager weiter. SNMPv1- und SNMPv3-Traps werden unterstützt.

  Informationen über die MIB-Datei (Management Information Base), in der die von Lenovo XClarity Administrator generierten SNMP-Traps beschrieben werden, finden Sie unter Datei „lenovoMgrAlert.mib“ in der Onlinedokumentation von Lenovo XClarity Administrator.
- **Syslog**. Lenovo XClarity Administrator leitet die überwachten Ereignisse über das Netzwerk an einen zentralen Protokollserver weiter, wobei systemeigene Tools für die syslog-Überwachung verwendet werden können.

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Anmerkung: Ereignisse werden nicht übermittelt, wenn beispielsweise keine funktionsfähige Verbindung zwischen Lenovo XClarity Administrator und der Ereignisweiterleitung vorhanden ist oder wenn der Port blockiert ist.

Ereignisweiterleitung an Azure Log Analytics einrichten

Sie können Lenovo XClarity Administrator für die Weiterleitung bestimmter Ereignisse an Azure Log Analytics konfigurieren.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für Azure Log Analytics zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **Azure Log Analytics** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Namen und optional eine Beschreibung für die Ereignisweiterleitung ein.
- Geben Sie den Primärschlüssel für die Azure Log Analytics-Schnittstelle ein.
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
- **Optional**: Wenn eine Authentifizierung erforderlich ist, wählen Sie einen der folgenden Authentifizierungstypen aus:
  - **Allgemein**. Authentifiziert den angegebenen Server mithilfe der angegebenen Benutzer-ID und des Kennworts.
  - **Keine Angabe**. Es wird keine Authentifizierung verwendet.

Schritt 5. Klicken Sie auf **Ausgabeformat**, um das Ausgabeformat der Ereignisdaten zu wählen, die weitergeleitet werden sollen. Die Informationen sind je nach Typ der Ereignisweiterleitung unterschiedlich.

Das folgende Beispiel-Ausgabeformat ist das Standardformat für Azure Log Analytics-Empfänger. Alle Begriffe in doppelten eckigen Klammern sind die Variablen, die durch tatsächliche Werte ersetzt werden, wenn ein Ereignis weitergeleitet wird. Die verfügbaren Variablen für Azure Log Analytics-Empfänger werden im Dialogfeld Ausgabeformat aufgeführt.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
\"LXCA\":\"[[LXCA_IP]]\"}
```

Sie können auf **Auf Standardwerte zurücksetzen** klicken, um das Ausgabeformat wieder in die Standardfelder zu ändern.

Schritt 6. Wählen Sie **Ausgeschlossene Ereignisse zulassen** aus, um zu verhindern , dass ausgeschlossene Ereignisse weitergeleitet werden, oder entfernen Sie **Ausgeschlossene Ereignisse zulassen**, um ausgeschlossene Ereignisse weiterzuleiten. Siehe Ereignisse ausschließen für weitere Informationen.

Schritt 7. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 8. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 9. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 10. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 11. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Nach Ereigniskategorie abgleichen**
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.
  1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
  2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
  5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.

- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 12. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.
- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Sendet Benachrichtigungen zu neuen Alerts.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 13. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 14. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 15. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 16. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

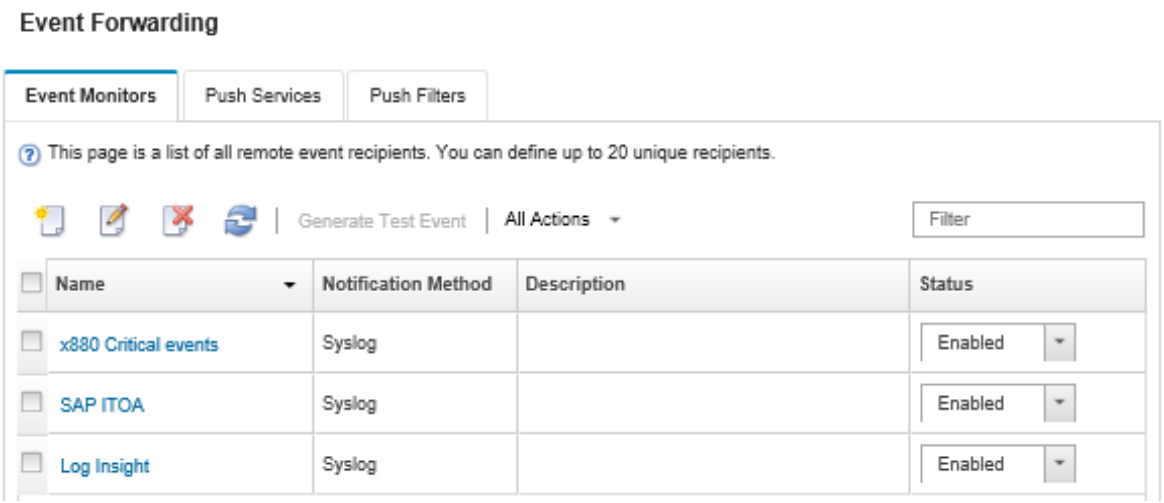
Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 17. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 18. Wählen Sie die neue Ereignisweiterleitung aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den entsprechenden Azure Log Analytics-Server weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).

Ereignisweiterleitung an einen E-Mail-Service über SMTP einrichten

Sie können Lenovo XClarity Administrator so konfigurieren, dass bestimmte Ereignisse über SMTP an einen E-Mail-Service weitergeleitet werden.

Vorbereitende Schritte

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

Lesen Sie sich vor der Einrichtung einer Ereignisweiterleitung an einen Gmail-Webservice die Informationen im Abschnitt Ereignisweiterleitung an syslog, Remote- SNMP-Manager oder E-Mail einrichten der Onlinedokumentation von Lenovo XClarity Administrator durch.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für E-Mail über SMTP zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **E-Mail** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Namen, den Zielhost und optional eine Beschreibung der Ereignisweiterleitung ein.
- Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist `25`.
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
- Geben Sie die E-Mail-Adresse für die einzelnen Empfänger ein. Trennen Sie mehrere E-Mail-Adressen, indem Sie ein Komma verwenden.

  Wählen Sie zum Senden der E-Mail an den Support-Kontakt, der für die Einheit zugewiesen ist, **Support-Kontakt-E-Mail verwenden** (siehe Support-Kontakte für eine Einheit definieren in der Onlinedokumentation von XClarity Administrator).
- **Optional:** Geben Sie die E-Mail-Adresse des Absenders der E-Mail ein (zum Beispiel `john@company.com`).

  Wenn Sie keine E-Mail-Adresse angeben, wird standardmäßig `LXCA.`<*source_identifier*>`@`<*smtp_host*> als Absenderadresse verwendet.

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

  Anmerkungen:

  – Wenn Sie festgelegt haben, dass Ihr SMTP-Server für das Weiterleiten von E-Mails einen Hostnamen benötigt und Sie keinen Hostnamen für XClarity Administrator definiert haben, lehnt der SMTP-Server unter Umständen weitergeleitete Ereignisse ab. Wenn XClarity Administrator nicht über einen Hostnamen verfügt, wird das Ereignis zusammen mit der IP-Adresse weitergeleitet. Wenn die IP-Adresse nicht abgerufen werden kann, wird stattdessen „localhost“ gesendet. Dies könnte dazu führen, dass der SMTP-Server das Ereignis ablehnt.

  – Wenn Sie die Absenderdomäne angeben, wird die Quelle in der Absenderadresse nicht identifiziert. Stattdessen werden Informationen über die Quelle des Ereignisses in den Text der E-Mail geschrieben, darunter Systemname, IP-Adresse, Typ/Modell und Seriennummer.

  - Wenn der SMTP-Server nur E-Mails akzeptiert, die von einem registrierten Benutzer gesendet wurden, wird die Standardabsenderadresse (`LXCA.<source_identifier>@<smtp_host>`) abgelehnt. In diesem Fall müssen Sie im Feld **Absender** mindestens einen Domänennamen angeben.

- **Optional:** Um eine sichere Verbindung zum SMTP-Server herzustellen, wählen Sie die folgenden Verbindungstypen aus:
  - **SSL**. Verwendet bei der Kommunikation das SSL-Protokoll.
  - **STARTTLS**. Verwendet TLS, um eine sichere Kommunikation über einen unsicheren Kanal aufzubauen.

  Wenn einer dieser Verbindungstypen ausgewählt ist, versucht LXCA, das Zertifikat des SMTP-Servers herunterzuladen und in seinen Truststore zu importieren. Sie werden aufgefordert, das Hinzufügen dieses Zertifikat zum Truststore zu akzeptieren.

- **Optional:** Wenn eine Authentifizierung erforderlich ist, wählen Sie einen der folgenden Authentifizierungstypen aus:
  - **Regulär**. Authentifiziert den angegebenen SMTP-Server mithilfe der angegebenen Benutzer-ID und des Kennworts.
  - **NTLM**. Verwendet das Protokoll „NT LAN Manager (NTLM)“, um sich mithilfe der angegebenen Benutzer-ID, des Kennworts und des Domänennamens am angegebenen SMTP-Server zu authentifizieren.
  - **OAUTH2**. Verwendet das Protokoll „Simple Authentication and Security Layer (SASL)“, um sich mithilfe des angegebenen Benutzernamens und Sicherheitstokens am angegebenen SMTP-Server zu authentifizieren. Gewöhnlich entspricht der Benutzername Ihrer E-Mail-Adresse.

    Achtung: Das Sicherheitstoken läuft nach einer kurzen Zeit ab. Sie sind selber dafür verantwortlich, das Sicherheitstoken zu aktualisieren.
  - **Keine Angabe**. Es wird keine Authentifizierung verwendet.

Schritt 5. Klicken Sie auf **Ausgabeformat**, um das Ausgabeformat der Ereignisdaten, die im E-Mail-Text weitergeleitet werden sollen, und das Format des E-Mail-Betreffs auszuwählen. Die Informationen sind je nach Typ der Ereignisweiterleitung unterschiedlich.

Das folgende Beispiel-Ausgabeformat ist das Standardformat für E-Mail-Empfänger. Alle Begriffe in doppelten eckigen Klammern sind die Variablen, die durch tatsächliche Werte ersetzt werden, wenn ein Ereignis weitergeleitet wird. Die verfügbaren Variablen für die E-Mail-Empfänger werden im Dialogfeld Ausgabeformat aufgeführt.

E-Mail-Betreff

```
[[DeviceName]]-[[EventMessage]]
```

E-Mail-Text

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
```

```
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n
```

Sie können auf **Auf Standardwerte zurücksetzen** klicken, um das Ausgabeformat wieder in die Standardfelder zu ändern.

Schritt 6. Wählen Sie **Ausgeschlossene Ereignisse zulassen** aus, um zu verhindern , dass ausgeschlossene Ereignisse weitergeleitet werden, oder entfernen Sie **Ausgeschlossene Ereignisse zulassen**, um ausgeschlossene Ereignisse weiterzuleiten. Siehe Ereignisse ausschließen für weitere Informationen.

Schritt 7. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 8. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 9. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 10. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 11. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Nach Ereigniskategorie abgleichen**
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).

- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.
  1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
  2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
  5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.
- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 12. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.
- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Sendet Benachrichtigungen zu neuen Alerts.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 13. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 14. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 15. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 16. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

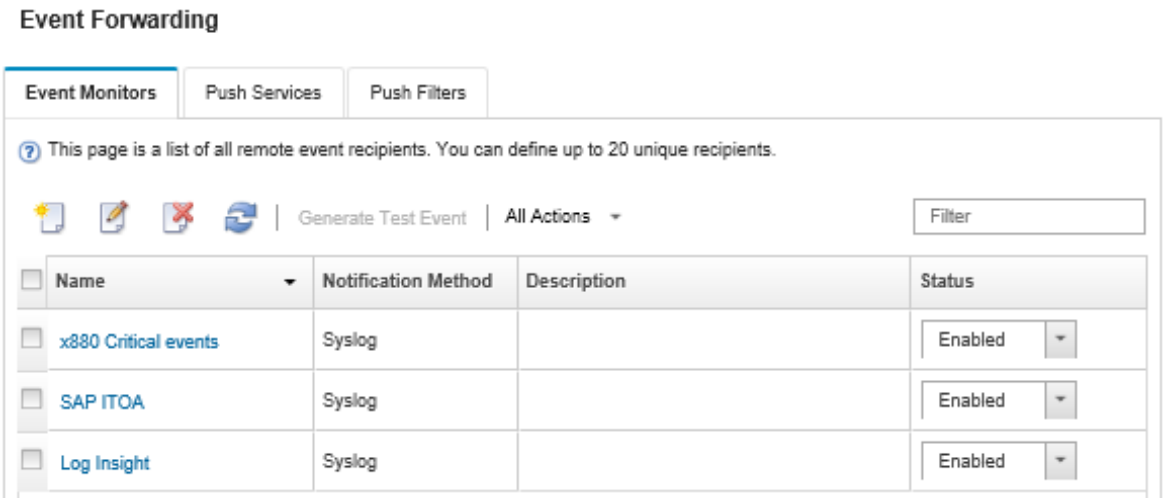
1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.

- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 17. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 18. Wählen Sie die neue Ereignisweiterleitung aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den entsprechenden E-Mail-Service weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).

Ereignisweiterleitung an einen SMTP-Service für Gmail einrichten

Sie können Lenovo XClarity Administrator so einrichten, dass überwachte Ereignis an einen webbasierten E-Mail-Service wie Gmail weitergeleitet werden.

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

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

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

Standardauthentifizierung über SSL auf Port 465

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

Parameter	Wert
Host	smtp.gmail.com
Port	465
SSL	Auswählen
STARTTLS	Löschen
Authentifizierung	Standard
Benutzer	Gültige E-Mail-Adresse für Gmail
Kennwort	Authentifizierungskennwort für Gmail
Absenderadresse	(optional)

Standardauthentifizierung über TLS auf Port 587

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

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

OAUTH2-Authentifizierung über TLS auf Port 587

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

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

1. Erstellen Sie ein Projekt in der Google-Entwicklerkonsole und rufen Sie die Client-ID und den geheimen Clientschlüssel ab. Weitere Informationen finden Sie auf der Website zur Google-Anmeldung bei Websites-Website.

a. Öffnen Sie in einem Webbrowser die Website zu Google-APIs.

b. Klicken Sie im Menü dieser Webseite auf **Projekt auswählen → Projekt erstellen**. Das Dialogfenster Neues Projekt wird angezeigt.

c. Geben Sie einen Namen ein und wählen Sie **Ja** aus, um der Lizenzvereinbarung zuzustimmen. Klicken Sie dann auf **Erstellen**.

d. Verwenden Sie das Suchfeld auf der Registerkarte **Übersicht**, um nach „gmail“ zu suchen.

e. Klicken Sie in den Suchergebnissen auf **GMAIL-API**.

f. Klicken Sie auf **Aktivieren**.

g. Klicken Sie auf die Registerkarte **Anmeldeinformationen**.

h. Klicken Sie auf **OAuth-Zustimmung**.

i. Geben Sie im Feld **Benutzern angezeigter Produktname** einen Namen ein und klicken Sie auf **Speichern**.

j. Klicken Sie auf **Anmeldeinformationen erstellen → OAuth-Client-ID**.

k. Wählen Sie **Sonstige** aus und geben einen Namen ein.

l. Klicken Sie auf **Erstellen**. Im Dialogfenster OAuth-Client werden Ihre Client-ID und der geheime Clientschlüssel angezeigt.

m. Notieren Sie die Client-ID und den geheimen Clientschlüssel für die spätere Verwendung.

n. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

2. Verwenden Sie das Python-Script oauth2.py, um ein Sicherheitstoken zu generieren und zu autorisieren. Geben Sie zu diesem Zweck die bei der Projekterstellung generierte Client-ID und den geheimen Clientschlüssel ein.

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

   a. Öffnen Sie in einem Webbrowser die Website zu „gmail-oauth2-tools“.

   b. Klicken Sie auf **Raw** und speichern Sie den Inhalt unter dem Dateinamen `oauth2.py` auf Ihrem lokalen System.

   c. Führen Sie den folgenden Befehl auf einem Terminal (Linux) oder über eine Befehlszeile (Windows) aus:

   ```
   py oauth2.py --user=<your_email> --client_id=<client_id>
      --client_secret=<client_secret> --generate_oauth2_token
   ```

   Beispiel:

   ```
   py oauth2.py --user=jon@gmail.com
      --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
      --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
   ```

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

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

   https://accounts.google.com/o/oauth2/auth?client_id=884243132302
   -458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
   urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;scope=https%3A%2F%2Fmail.
   google.com%2F

   Enter verification code:
   ```

   d. Öffnen Sie in einem Webbrowser die URL, die im vorherigen Schritt zurückgegeben wurde.

   e. Klicken Sie auf **Zulassen**, um diesem Service zuzustimmen. Es wird ein Überprüfungscode zurückgegeben.

f. Geben Sie den Überprüfungscode im `oauth2.py`-Befehl ein.

   Der Befehl gibt das Sicherheitstoken zurück und aktualisiert es. Beispiel:

   ```
   Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
   Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
   Access Token Expiration Seconds: 3600
   ```

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

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

Parameter	Wert
Host	smtp.gmail.com
Port	587
SSL	Löschen
STARTTLS	Auswählen
Authentifizierung	OAUTH2
Benutzer	Gültige E-Mail-Adresse für Gmail
Token	Sicherheitstoken
Absenderadresse	(optional)

Ereignisweiterleitung an einen FTP-Server einrichten

Sie können Lenovo XClarity Administrator für die Weiterleitung bestimmter Ereignisse an einen FTP-Server konfigurieren.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für einen FTP-Server zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **FTP** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Namen, den Zielhost und optional eine Beschreibung der Ereignisweiterleitungen ein.
- Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist 21.
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
- **Optional:** Geben Sie die Zeichenfolge an, die aus dem Dateiinhalt entfernt werden soll.
- Geben Sie das Dateinamenformat ein, das für die Datei verwendet werden soll, die das weitergeleitete Ereignis enthält. Das Standardformat ist `event_[[EventSequenceID]].txt`.

  Anmerkung: Jede Datei enthält Informationen zu einem einzelnen Ereignis.
- Geben Sie den Pfad auf dem Remote-FTP-Server ein, auf den die Datei hochgeladen werden soll.
- Wählen Sie den Zeichensatz, entweder **UTF-8** oder **Big5**. UTF-8 ist der Standardwert.
- Wählen Sie den Authentifizierungstyp aus. Es kann einen der folgenden Werte aufweisen.
  - **Anonym**. Es wird keine Authentifizierung verwendet. (Standardwert)
  - **Allgemein**. Authentifiziert den FTP-Server mithilfe der angegebenen Benutzer-ID und des Kennworts.

Schritt 5. Klicken Sie auf **Ausgabeformat**, um das Ausgabeformat der Ereignisdaten zu wählen, die weitergeleitet werden sollen. Die Informationen sind je nach Typ der Ereignisweiterleitung unterschiedlich.

Das folgende Beispiel-Ausgabeformat ist das Standardformat für FTP-Empfänger. Alle Begriffe in doppelten eckigen Klammern sind die Variablen, die durch tatsächliche Werte ersetzt werden, wenn ein Ereignis weitergeleitet wird. Die verfügbaren Variablen für FTP-Empfänger werden im Dialogfeld Ausgabeformat aufgeführt.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
```

```
Event Class     : [[EventClass]]\n
Sequence ID     : [[EventSequenceID]]\n
Event Source ID : [[EventSourceUUID]]\n
Component ID    : [[EventComponentUUID]]\n
Serial Num      : [[EventSerialNumber]]\n
MTM             : [[EventMachineTypeModel]]\n
EventService    : [[EventService]]\n
Console link    : [[ConsoleLink]]\n
iOS link        : [[iOSLink]]\n
Android link    : [[AndroidLink]]\n
System Name     : [[DeviceFullPathName]]\n"
```

Sie können auf **Auf Standardwerte zurücksetzen** klicken, um das Ausgabeformat wieder in die Standardfelder zu ändern.

Schritt 6. Wählen Sie **Ausgeschlossene Ereignisse zulassen** aus, um zu verhindern , dass ausgeschlossene Ereignisse weitergeleitet werden, oder entfernen Sie **Ausgeschlossene Ereignisse zulassen**, um ausgeschlossene Ereignisse weiterzuleiten. Siehe Ereignisse ausschließen für weitere Informationen.

Schritt 7. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 8. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 9. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 10. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 11. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Nach Ereigniskategorie abgleichen**
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.
  1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.

2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.

- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 12. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.
- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Sendet Benachrichtigungen zu neuen Alerts.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 13. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 14. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 15. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 16. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

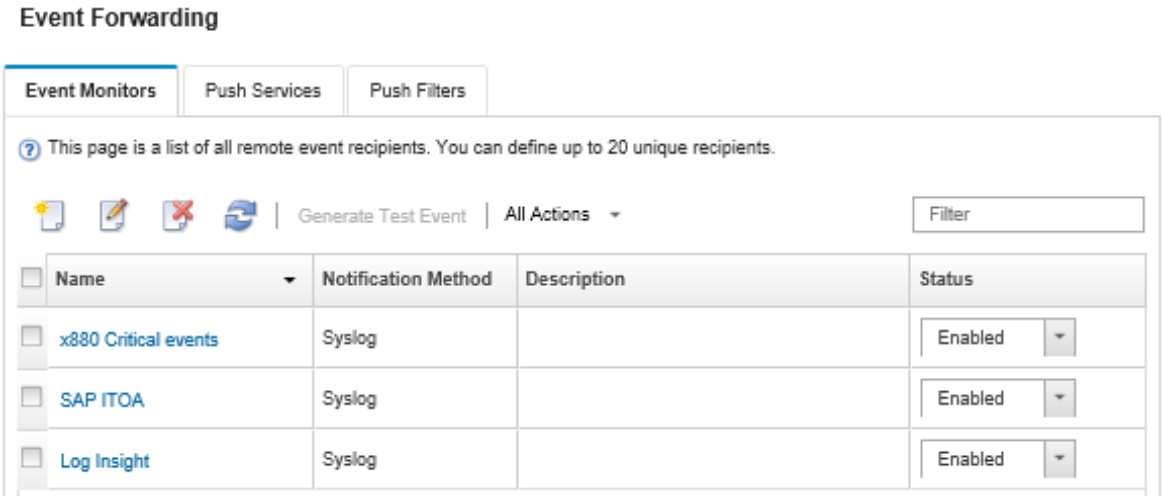
1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.

- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 17. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 18. Wählen Sie die neue Ereignisweiterleitung aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den entsprechenden FTP-Server weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).

Ereignisweiterleitung an einen REST-Web-Service einrichten

Sie können Lenovo XClarity Administrator für die Weiterleitung bestimmter Ereignisse an einen REST-Web-Service konfigurieren.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für einen REST-Web-Service zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **REST** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

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

Schritt 5. Klicken Sie auf **Ausgabeformat**, um das Ausgabeformat der Ereignisdaten zu wählen, die weitergeleitet werden sollen. Die Informationen sind je nach Typ der Ereignisweiterleitung unterschiedlich.

Das folgende Beispiel-Ausgabeformat ist das Standardformat für REST-Web-Service-Empfänger. Alle Begriffe in doppelten eckigen Klammern sind die Variablen, die durch tatsächliche Werte ersetzt werden, wenn ein Ereignis weitergeleitet wird. Die verfügbaren Variablen für REST-Web-Service-Empfänger werden im Dialogfeld Ausgabeformat aufgeführt.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
```

```
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

Sie können auf **Auf Standardwerte zurücksetzen** klicken, um das Ausgabeformat wieder in die Standardfelder zu ändern.

Schritt 6. Wählen Sie **Ausgeschlossene Ereignisse zulassen** aus, um zu verhindern , dass ausgeschlossene Ereignisse weitergeleitet werden, oder entfernen Sie **Ausgeschlossene Ereignisse zulassen**, um ausgeschlossene Ereignisse weiterzuleiten. Siehe Ereignisse ausschließen für weitere Informationen.

Schritt 7. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 8. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 9. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 10. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 11. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Nach Ereigniskategorie abgleichen**
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.
  1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
  2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.

5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.

- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 12. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.
- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Sendet Benachrichtigungen zu neuen Alerts.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 13. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 14. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 15. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 16. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

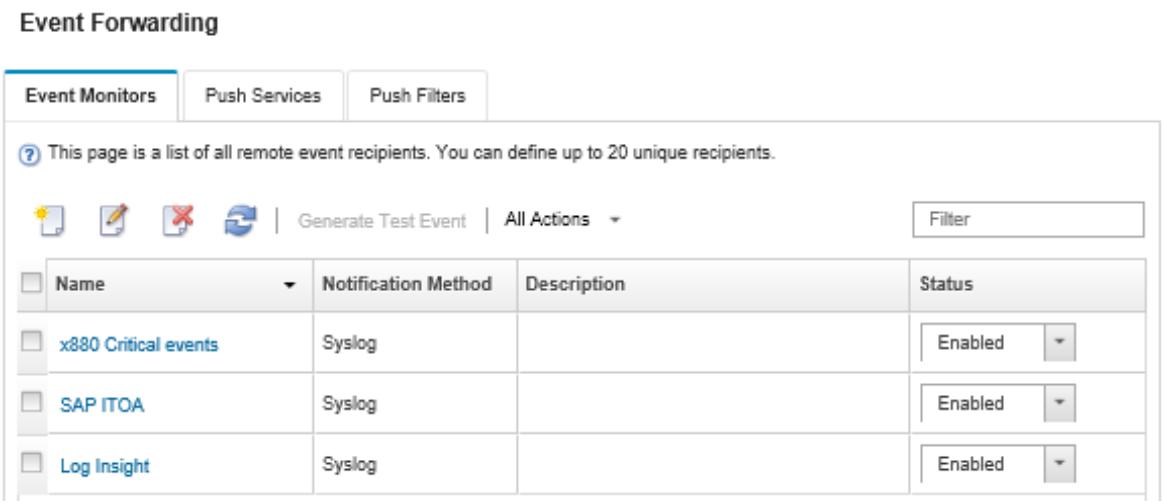
Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 17. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 18. Wählen Sie die neue Ereignisweiterleitung aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den entsprechenden REST-Web-Service weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).

Ereignisweiterleitung an einen Remote-SNMPv1- oder SNMPv3-Manager einrichten

Sie können Lenovo XClarity Administrator so konfigurieren, dass bestimmte Ereignisse an einen Remote-SNMPv1 oder SNMPv3-Manager weitergeleitet werden.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Informationen zur XClarity Administrator-MIB finden Sie unter Datei „lenovoMgrAlert.mib“.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für einen Remote-SNMPv1 oder SNMPv3-Manager zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **SNMPv1** oder **SNMPv3** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Namen und den Zielhost für die Ereignisweiterleitung ein.
- Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist `162`.
- **Optional**: Geben Sie zusätzliche Informationen wie die Beschreibung, den Namen des Ansprechpartners und die Position ein.
- Wählen Sie die SNMP-Version. Es kann einen der folgenden Werte aufweisen.
  - **SNMPv1**. Wenn Sie diese Version auswählen, müssen Sie das Community-Kennwort angeben, das zusammen mit der SNMP-Anforderung an die Einheit gesendet wird.
  - **SNMPv3**. Dies ist die Standardversion, die für eine größere Sicherheit empfohlen wird. Geben Sie bei Auswahl von SNMPv3 optional die Werte für Benutzer-ID, Authentifizierungstyp und -kennwort und Datenschutztyp und -kennwort an.

    Wenn der SNMPv3-Trap-Empfänger die Engine-ID für die Instanz von XClarity Administrator benötigt, können Sie diese wie folgt herausfinden:

    1. Stellen Sie sicher, dass die Verbindungsparameter (Benutzername, AuthProtokoll, AuthKennwort, DSProtokoll, DSKennwort) mit den in XClarity Administrator definierten Werten übereinstimmen.
    2. Führen Sie mithilfe Ihrer bevorzugten Software (wie snmpwalk) eine SNMP-GET-Anforderung auf dem XClarity Administrator-Server durch. Nutzen Sie hierzu eine der folgenden Objektkennungen:
       - EngineID: 1.3.6.1.6.3.10.2.1.1.0
       - EngineBoots: 1.3.6.1.6.3.10.2.1.2.0

       Verwenden Sie für den `snmpget`-Befehl das folgende Format. Beachten Sie, dass der Authentifizierungstyp für den -a Weiterleiter SHA oder leer (keine Authentifizierung) sein kann.
       ```
       snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDE
       ```

       Wenn die XClarity Administrator-IP-Adresse beispielsweise 192.0.1.0 lautet, der Authentifizierungstyp SHA und der Datenschutztyp AES ist, zeigt der folgende Befehl die EngineID an.
       ```
       snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_
       ```

       Die folgende Beispielantwort wird zurückgegeben. In diesem Beispiel ist die engineID 0x80001370017F00000134C27E12.
       ```
       iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
       ```
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.

- **Optional**: Wenn eine Trap-Authentifizierung erforderlich ist, geben Sie die Benutzer-ID und das Authentifizierungskennwort ein. Als Remote-SNMP-Manager muss die gleiche Benutzer-ID und das gleiche Kennwort eingegeben werden, zu dem auch die Traps weitergeleitet werden sollen.
- Wählen Sie das Authentifizierungsprotokoll aus, das vom Remote-SNMP-Manager verwendet wird, um den Trap-Sender zu verifizieren. Dies kann einer der folgenden Werte sein:
  - **SHA**. Verwendet das SHA-Protokoll, um sich mithilfe der angegebenen Benutzer-ID, des Kennworts und des Domänennamens am angegebenen SNMP-Server zu authentifizieren.
  - **Keine Angabe**. Es wird keine Authentifizierung verwendet.
- Wenn eine Trap-Verschlüsselung erforderlich ist, geben Sie den Datenschutztyp (Verschlüsselungsprotokoll) und das Kennwort ein. Es kann einen der folgenden Werte aufweisen. Als Remote-SNMP-Manager muss das gleiche Protokoll und das gleiche Kennwort eingegeben werden, zu dem die Traps weitergeleitet werden sollen.
  - **AES**
  - **DES**
  - **Keine Angabe**

Schritt 5. Wählen Sie **Ausgeschlossene Ereignisse zulassen** aus, um zu verhindern , dass ausgeschlossene Ereignisse weitergeleitet werden, oder entfernen Sie **Ausgeschlossene Ereignisse zulassen**, um ausgeschlossene Ereignisse weiterzuleiten. Siehe Ereignisse ausschließen für weitere Informationen.

Schritt 6. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 7. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 8. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 9. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 10. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Nach Ereigniskategorie abgleichen**
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.

1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.

- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 11. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.
- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Sendet Benachrichtigungen zu neuen Alerts.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 12. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 13. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 14. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 15. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

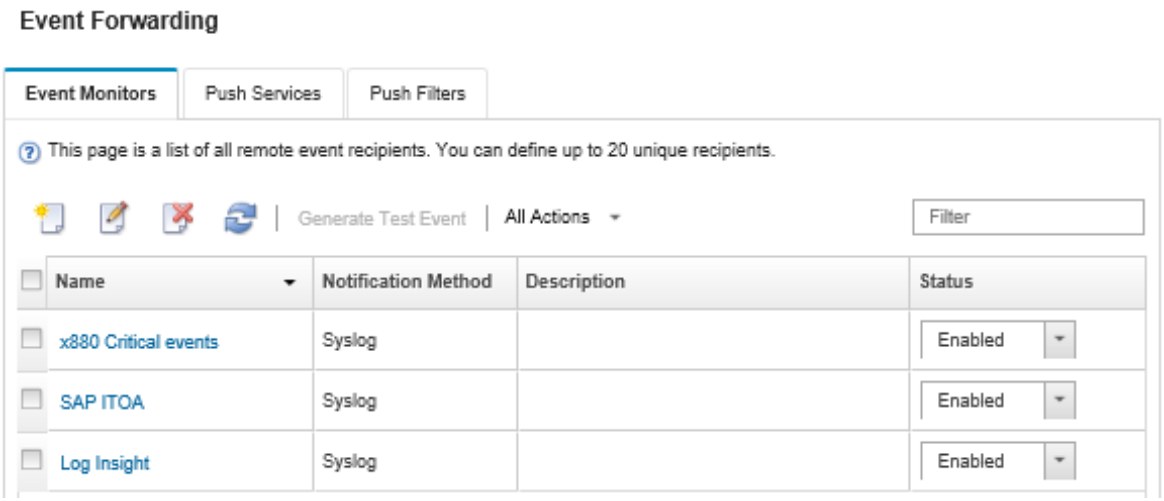
1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.

- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 16. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 17. Wählen Sie die neue Ereignisweiterleitung aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den entsprechenden Remote-SNMP-Manager weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).
- Laden Sie die MIB-Datei herunter, die Informationen zu SNMP-Traps enthält, indem Sie auf das Symbol **Erstellen** ( ) und dann auf **MIB-Datei herunterladen** auf der Registerkarte „Allgemein“ des Dialogfelds „Neue Ereignisweiterleitung“ klicken.

Datei „lenovoMgrAlert.mib“

Diese MIB-Datei (Management Information Base) beschreibt die SNMP-Traps, die von Lenovo XClarity Administrator generiert werden, einschließlich der Alerts, die von XClarity Administrator und verwalteten Einheiten ausgelöst wurden. Diese MIB-Datei kann in jedem SNMP-Trap-Manager kompiliert werden, sodass von XClarity Administrator gesendete SNMP-Traps sinnvoll wiedergegeben werden können.

Sie können die MIB-Datei von der Webschnittstelle herunterladen. Klicken Sie dazu in der Menüleiste auf **Überwachung → Ereignisweiterleitung** und dann auf das Symbol **Erstellen** ( ). Wählen Sie **SNMP** als Typ der Ereignisweiterleitung aus und klicken Sie dann unten im Dialogfenster auf **MIB-Datei herunterladen**.

Die folgenden Objekte sind in allen ausgehenden SNMP-Traps enthalten. Einige SNMP-Traps enthalten möglicherweise zusätzliche Objekte. Alle Objekte sind in der MIB-Datei beschrieben. Beachten Sie, dass die Wiederherstellungsinformationen nicht im Trap enthalten sind.

Anmerkung: Diese Liste kann in den verschiedenen Versionen von XClarity Administrator unterschiedlich sein.

- **mgrTrapAppId**. Dies ist der „Lenovo Event Manager“.
- **mgrTrapCommonEvtID**. Allgemeine Ereignis-ID
- **mgrTrapDateTime**. Das lokalisierte Datum und die Uhrzeit, die darstellen, wann das Ereignis aufgetreten ist
- **mgrTrapEventClass**. Ereignisquelle Hierbei kann es sich um Prüfung, Kühlung, Power, Datenträger, Hauptspeicher, Prozessoren, System, Test, Adapter, Erweiterung, IO-Modul oder Blade handeln.
- **mgrTrapEvtID**. Die eindeutige Kennung für das Ereignis
- **mgrTrapFailFRUs**. Eine durch Komma getrennte Liste der fehlerhaften FRU-UUIDs, falls zutreffend
- **mgrTrapFailSNs**. Eine durch Kommas getrennte Liste mit den Seriennummern der ausgefallenen FRUs, falls zutreffend
- **mgrTrapFullyQualifiedDomainName**. Der vollständig qualifizierte Domänenname: der Hostname und der Domänenname
- **mgrTrapID**. Trap-ID
- **mgrTrapMsgText**. Nachrichtentext (nur Englisch)
- **mgrTrapMsgID**. Nachrichten-ID
- **mgrTrapMtm**. Modelltyp der Einheit, die das Ereignis ausgelöst hat
- **mgrTrapService**. Wartbarkeitanzeige. Hierbei gibt es die Optionen 000 (Unbekannt), 100 (Keine), 200 (Service Center) oder 300 (Kunde)
- **mgrTrapSeverity**. Schweregradanzeige. Hierbei gibt es die Optionen Information, Warnung, Untergeordnet, Übergeordnet oder Kritisch
- **mgrTrapSN**. Seriennummer der Einheit, die das Ereignis ausgelöst hat
- **mgrTrapSrcIP**. IP-Adresse der Einheit, von der das ausgelöste Ereignis empfangen wurde
- **mgrTrapSrcLoc**. Position der Einheit, die das Ereignis ausgelöst hat, nur in Englisch (zum Beispiel Slot#xx)
- **mgrTrapSrcName**. Hostname oder Anzeigename der Einheit, die das Ereignis ausgelöst hat
- **mgrTrapSysContact**. Benutzerkonfigurierte Kontakt-ID
- **mgrTrapSysLocation**. Benutzerkonfigurierte Informationen zum Standort der Einheit
- **mgrTrapSystemName**. Einheitenname, Komponentenname und Steckplatzposition
- **mgrTrapTxtId**. Hostname oder IP-Adresse des Lenovo Event Manager-Servers, der den Trap ausgelöst hat
- **mgrTrapUserid**. Benutzer-ID, die dem Ereignis zugeordnet ist (wenn es sich um ein internes Ereignis handelt und die Ereignisklasse „Prüfung“ ist)
- **mgrTrapUuid**. UUID der Einheit, die das Ereignis ausgelöst hat

Ereignisweiterleitung an ein Syslog einrichten

Sie können Lenovo XClarity Administrator für die Weiterleitung bestimmter Ereignisse an ein Syslog konfigurieren.

Zu dieser Aufgabe

Sie können bis zu 20 Ereignisweiterleitungen erstellen und aktivieren, um Ereignisse an bestimmte Empfänger zu senden.

Wenn XClarity Administrator nach der Konfiguration von Ereignisweiterleitungen neu gestartet wird, müssen Sie warten, bis der Verwaltungsserver die internen Daten neu generiert hat, bevor die Ereignisse ordnungsgemäß weitergeleitet werden.

Anmerkung: Bei XClarity Administrator v1.2.0 und höher finden Sie in den Dialogfeldern „Neue Ereignisempfänger“ und „Ereignisempfänger ändern“ auf der Registerkarte **Ereignisse** den Eintrag **Switches**. Nach einem Upgrade von einer früheren Version auf Version 1.2.0 oder höher müssen Sie alle Ereignisweiterleitungen aktualisieren, um RackSwitch-Ereignisse nach Bedarf ein- oder ausschließen zu können. Dies gilt auch dann, wenn Sie das Kontrollkästchen **Alle Systeme** aktiviert haben, um alle Einheiten auszuwählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ereignisweiterleitung für ein Syslog zu erstellen.

Schritt 1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite Ereignisweiterleitung wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Ereignisweiterleitung**.

Schritt 3. Klicken Sie auf das Symbol für **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds Neue Ereignisweiterleitung wird angezeigt.

Schritt 4. Wählen Sie **Syslog** als Typ der Ereignisweiterleitung aus und geben Sie die protokollspezifischen Informationen ein:

- Geben Sie den Namen, den Zielhost und optional eine Beschreibung der Ereignisweiterleitung ein.
- Geben Sie den Port ein, der für die Ereignisweiterleitung verwendet werden soll. Der Standardwert ist `514`.
- Wählen Sie das Protokoll aus, das für die Ereignisweiterleitung verwendet werden soll. Es kann einen der folgenden Werte aufweisen.
  - **UDP**
  - **TCP**
- Geben Sie den Timeout-Zeitraum (in Sekunden) für die Anforderung ein. Der Standardwert ist 30 Sekunden.
- Optional können Sie das Format des Zeitstempels im Syslog auswählen. Es kann einen der folgenden Werte aufweisen.
  - **Ortszeit**. Das Standardformat, zum Beispiel `Fri Mar 31 05:57:18 EDT 2017`.
  - **GMT-Uhrzeit**. Internationaler Standard (ISO8601) für Datum und Uhrzeit, zum Beispiel `2017-03-31T05:58:20-04:00`.

Schritt 5. Klicken Sie auf **Ausgabeformat**, um das Ausgabeformat der Ereignisdaten zu wählen, die weitergeleitet werden sollen. Die Informationen sind je nach Typ der Ereignisweiterleitung unterschiedlich.

Das folgende Beispiel-Ausgabeformat ist das Standardformat für Sylog-Empfänger. Alle Begriffe in doppelten eckigen Klammern sind die Variablen, die durch tatsächliche Werte ersetzt werden, wenn ein Ereignis weitergeleitet wird. Die verfügbaren Variablen für Sylog-Empfänger werden im Dialogfeld Ausgabeformat aufgeführt.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

Sie können auf **Auf Standardwerte zurücksetzen** klicken, um das Ausgabeformat wieder in die Standardfelder zu ändern.

Schritt 6. Wählen Sie **Ausgeschlossene Ereignisse zulassen** aus, um zu verhindern , dass ausgeschlossene Ereignisse weitergeleitet werden, oder entfernen Sie **Ausgeschlossene Ereignisse zulassen**, um ausgeschlossene Ereignisse weiterzuleiten. Siehe Ereignisse ausschließen für weitere Informationen.

Schritt 7. Wählen Sie **Diese Weiterleitung aktivieren** aus, um die Ereignisweiterleitung für diese Ereignisweiterleitung zu aktivieren.

Schritt 8. Klicken Sie auf **Weiter**, um die Registerkarte **Einheiten** anzuzeigen.

Schritt 9. Wählen Sie die Einheiten und Gruppen aus, die für diese Ereignisweiterleitung überwacht werden sollen.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

Schritt 10. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.

Schritt 11. Wählen Sie die Filter, die für diese Ereignisweiterleitung verwendet werden sollen.

- **Nach Ereigniskategorie abgleichen**
  1. Um alle Prüfungsereignisse unabhängig vom Status-Level weiterzuleiten, wählen Sie **Alle Prüfungsereignisse einschließen** aus.
  2. Um alle Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus weiterzuleiten, wählen Sie **Statusänderungsereignisse einschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus weiterzuleiten, wählen Sie **Statusaktualisierungsereignisse einschließen**.
  5. Wählen Sie die Ereignisklassen und die Wartbarkeit aus, die Sie weiterleiten möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie von der Weiterleitung ausschließen möchten. Trennen Sie IDs durch ein Komma (z. B. `FQXHMEM0214I,FQXHMEM0214I`).
- **Übereinstimmung nach Ereignis-Code**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie mehrere IDs durch ein Komma.
- **Nach Ereigniskategorie ausschließen**.
  1. Um alle Überwachungsereignisse unabhängig vom Status-Level auszuschließen, wählen Sie **Alle Überwachungsereignisse ausschließen** aus.
  2. Um alle Garantie-Ereignisse auszuschließen, wählen Sie **Garantie-Ereignisse ausschließen** aus.
  3. Um alle Ereignisse der Änderung des Integritätsstatus auszuschließen, wählen Sie **Statusänderungsereignisse ausschließen**.
  4. Um alle Ereignisse der Aktualisierung des Integritätsstatus auszuschließen, wählen Sie **Statusaktualisierungsereignisse ausschließen**.
  5. Wählen Sie die Stufe der Ereignisklassen und der Wartbarkeit aus, die Sie ausschließen möchten.
  6. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie weiterleiten möchten. Trennen Sie IDs durch ein Komma.

- **Nach Ereignis-Code ausschließen**. Geben Sie die IDs für ein oder mehrere Ereignisse ein, die Sie ausschließen möchten. Trennen Sie mehrere IDs durch ein Komma.

Schritt 12. Wählen Sie aus, ob bestimmte Ereignistypen enthalten sein sollen.
- **Alle Prüfereignisse einschließen**. Sendet Benachrichtigungen zu Prüfereignissen basierend auf den ausgewählten Ereignisklassen und -schweregraden.
- **Garantie-Ereignisse einschließen**. Sendet Benachrichtigungen zu Garantien.
- **Statusänderungsereignisse einschließen**. Sendet Benachrichtigungen zu Statusänderungen.
- **Statusaktualisierungsereignisse einschließen**. Sendet Benachrichtigungen zu neuen Alerts.
- **Bulletin-Ereignisse einschließen**. Sendet Benachrichtigungen zu neuen Bulletins.

Schritt 13. Wählen Sie die Ereignistypen und -schweregrade aus, über die Sie benachrichtigt werden möchten.

Schritt 14. Wählen Sie aus, ob Ereignisse nach Wartbarkeit gefiltert werden.

Schritt 15. Klicken Sie auf **Weiter**, um die Registerkarte **Planer** anzuzeigen.

Schritt 16. **Optional:** Definieren Sie die Zeiten und Tage, an denen die angegebenen Ereignisse an diese Ereignisweiterleitung weitergeleitet werden sollen. Es werden nur Ereignisse weitergeleitet, die während des angegebenen Zeitfensters stattfinden.

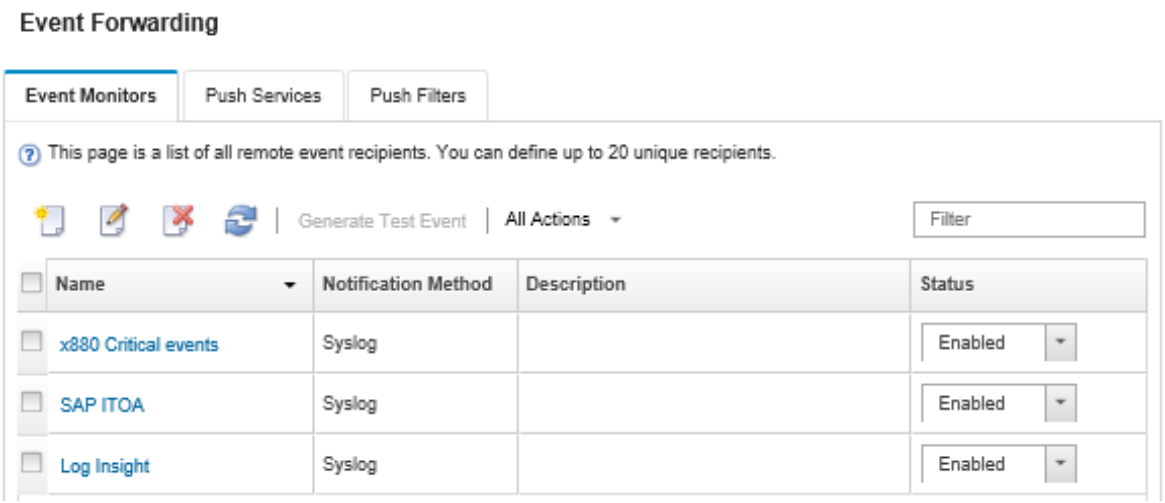
Wenn Sie keinen Zeitplan für die Ereignisweiterleitung erstellen, werden die Ereignisse rund um die Uhr weitergeleitet.

1. Verwenden Sie das Symbol für **Nach links blättern** (◀) und das Symbol für **Nach rechts blättern** (▶) und die Tasten **Tag**, **Woche** und **Monat**, um den Tag und die Uhrzeit für den Start des Plans auszuwählen.
2. Doppelklicken Sie auf das Zeitfenster, um das Dialogfeld „Neuer Zeitraum“ zu öffnen.
3. Geben Sie die erforderlichen Informationen einschließlich des Datums, der Start- und Endzeiten und der Angabe, ob sich der Plan wiederholen soll, ein.
4. Klicken Sie auf **Erstellen**, um den geplanten Zeitpunkt zu speichern und das Dialogfenster zu schließen. Der neue Plan wird zum Kalender hinzugefügt.

Tipp:
- Sie können das Zeitfenster ändern, indem Sie den Eintrag im Kalender in ein anderes Zeitfenster ziehen.
- Sie können der Dauer ändern, indem Sie oben oder unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können die Endzeit ändern, indem Sie unten auf den Planeintrag klicken und ihn auf die neue Zeit im Kalender ziehen.
- Sie können einen Plan ändern, indem Sie einen Doppelklick auf den Planeintrag im Kalender ausführen und dann auf **Eintrag bearbeiten** klicken.
- Sie können eine Zusammenfassung aller Planeinträge durch Auswahl von **Planer-Zusammenfassung anzeigen** anzeigen. Die Zusammenfassung enthält das Zeitfenster für jeden Eintrag und Informationen dazu, welche Einträge reproduzierbar sind.
- Sie können einen Planeintrag aus dem Kalender oder der Planer-Zusammenfassung löschen, indem Sie den Eintrag auswählen und auf **Eintrag löschen** klicken.

Schritt 17. Klicken Sie auf **Erstellen**.

Die Ereignisweiterleitung wird in der Tabelle „Ereignisweiterleitung“ aufgeführt.



Schritt 18. Wählen Sie die neue Ereignisweiterleitung, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an das entsprechende Syslog weitergeleitet werden.

Nach dieser Aufgabe

Auf der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für eine ausgewählte Ereignisweiterleitung ausführen.

- Aktualisieren Sie die Liste der Ereignisweiterleitungen, indem Sie auf Symbol für **Aktualisieren** ( ) klicken.
- Zeigen Sie Details zu einer bestimmten Ereignisweiterleitung an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien der Ereignisweiterleitung, indem Sie in der Spalte **Name** auf den Namen der Ereignisweiterleitung klicken.
- Löschen Sie die Ereignisweiterleitung, indem Sie auf das Symbol für **Löschen** ( ) klicken.
- Ereignisweiterleitung aussetzen (siehe Ereignisweiterleitung aussetzen).

Ereignisweiterleitung aussetzen

Sie können die Ereignisweiterleitung aussetzen, indem Sie die Ereignisweiterleitung deaktivieren. Das Aussetzen der Ereignisweiterleitung unterbricht die Überwachung der eingehenden Ereignisse. Ereignisse, die empfangen werden, während die Überwachung ausgesetzt ist, werden nicht weitergeleitet.

Zu dieser Aufgabe

Der Status „Deaktiviert“ ist nicht permanent. Wenn der Verwaltungsknoten erneut gestartet wird, werden alle Ereignisweiterleitungen aktiviert.

Vorgehensweise

Gehen Sie wie folgt vor, um die Weiterleitung von Ereignissen zu deaktivieren.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite „Ereignisweiterleitung“ wird angezeigt.

Schritt 2. Wählen Sie für jede Ereignisweiterleitung, die ausgesetzt werden soll, in der Spalte **Status** die Option **Deaktivieren** aus.

Ereignisse an mobile Einheiten weiterleiten

Sie können Lenovo XClarity Administrator so konfigurieren, dass Ereignisbenachrichtigungen per Push an mobile Einheiten übertragen werden.

Vorbereitende Schritte

Die folgenden Voraussetzungen müssen erfüllt sein, damit Ereignisse an mobile Einheiten weitergeleitet werden:

- Stellen Sie sicher, dass ein gültiger DNS-Server konfiguriert ist, damit Lenovo XClarity Administrator eine Verbindung zu den Push-Servern von Apple bzw. Google herstellen kann. Klicken Sie zum Konfigurieren auf **Verwaltung → Netzwerkzugriff → Netzwerkzugriff bearbeiten** und wählen Sie dann die Registerkarte **Interneteinstellungen** aus (siehe Netzwerkzugriff konfigurieren in der Onlinedokumentation von Lenovo XClarity Administrator).
- Stellen Sie sicher, dass alle für die Ereignisverwaltung erforderlichen Ports im Netzwerk und in den Firewalls geöffnet sind. Informationen zu den Portanforderungen finden Sie unter Portverfügbarkeit in der Onlinedokumentation von Lenovo XClarity Administrator.

Zu dieser Aufgabe

Wenn die Lenovo XClarity Mobile-App auf einer mobilen Einheit installiert ist, können Sie festlegen, dass jede angeschlossene Lenovo XClarity Administrator-Instanz Ereignisbenachrichtigungen per Push an diese mobile Einheit überträgt. Wenn Push-Benachrichtigungen für eine bestimmte Instanz aktiviert sind, wird in Lenovo XClarity Administrator ein Abonnement für diese mobile Einheit erstellt.

Sie können die Ereignisse definieren, die per Push an die mobile Einheit übertragen werden, indem Sie für jede Lenovo XClarity Administrator-Instanz vordefinierte oder angepasste Ereignisfilter zuordnen. Die vordefinierten globalen Ereignisfilter sind standardmäßig aktiviert. Lenovo XClarity Administrator beginnt die Überwachung für eingehende Ereignisse anhand der Filterkriterien. Wenn eine Übereinstimmung gefunden wird, wird das Ereignis an die mobile Einheit weitergeleitet.

Weitere Informationen zu Lenovo XClarity Mobile und den unterstützten mobilen Einheiten finden Sie unter Verwenden der Lenovo XClarity-Mobile-App in der Onlinedokumentation von Lenovo XClarity Administrator.

Vorgehensweise

Um Push-Benachrichtigungen für diese mobile Einheit einzurichten, führen Sie in der Lenovo XClarity Mobile-App auf der mobilen Einheit die folgenden Schritte aus.

Schritt 1. Aktivieren Sie Push-Benachrichtigungen:

- Sie können Push-Benachrichtigungen aktivieren, wenn Sie eine Verbindung zu einer Lenovo XClarity Administrator-Instanz herstellen. Push-Benachrichtigungen sind standardmäßig aktiviert.
- Sie können Push-Benachrichtigungen für vorhandene Verbindungen aktivieren, indem Sie einen oder mehrere Ereignisfilter aktivieren.

Schritt 2. Weisen Sie globale Ereignisfilter zu, um anzugeben, welche Ereignisse an die mobile Einheit weitergeleitet werden sollen:

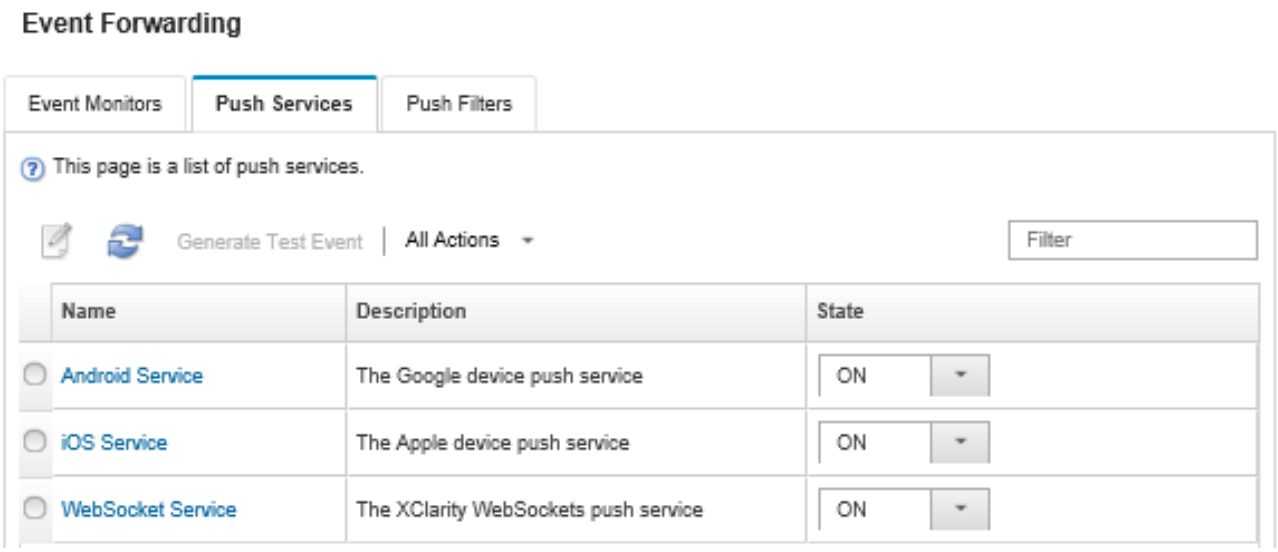
Anmerkung: Das Hinzufügen und Entfernen globaler Filter aus dem Abonnement ist nur über die Lenovo XClarity Mobile-App möglich. Sie können globale Filter nur über die Webschnittstelle von Lenovo XClarity Administrator erstellen. Informationen zum Erstellen von angepassten globalen Ereignisfiltern finden Sie unter Ereignisfilter für mobile Einheiten und WebSockets erstellen.

1. Tippen Sie auf **Einstellungen → Push-Benachrichtigungen**. Es wird eine Liste der Lenovo XClarity Administrator-Verbindungen angezeigt.

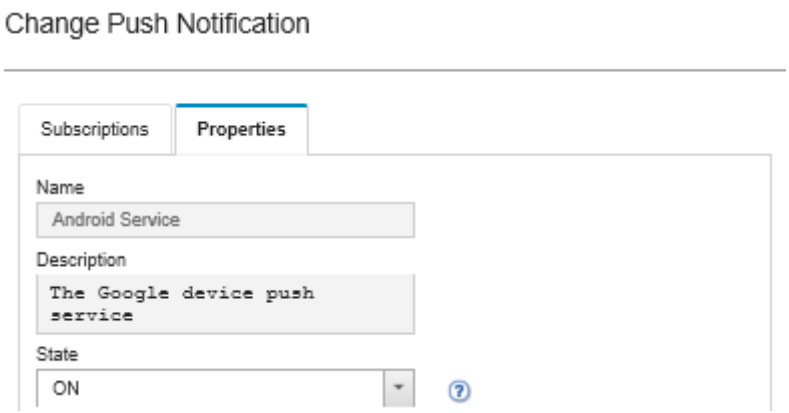
2. Tippen Sie auf die Instanz von Lenovo XClarity Administrator, um eine Liste der Push-Filter anzuzeigen.
3. Aktivieren Sie die Ereignisfilter für die Ereignisse, die für die Lenovo XClarity Administrator-Instanz an die mobile Einheit per Push übertragen werden sollen.
4. Tippen Sie auf **Test-Push-Benachrichtigung durch Berühren generieren**, um zu überprüfen, ob die Ereignisbenachrichtigungen ordnungsgemäß per Push übertragen werden.

Ergebnisse

Sie können Abonnements über die Seite „Ereignisweiterleitung“ der Lenovo XClarity Administrator-Webschnittstelle verwalten. Klicken Sie auf **Überwachung → Ereignisweiterleitung**, um die Seite „Ereignisweiterleitung“ anzuzeigen.



- Sie können die Eigenschaften für den Benachrichtigungs-Service der Einheit auf der Seite „Ereignisweiterleitung“ auf der Registerkarte **Push-Service** ändern. Klicken Sie dazu auf den Link für den Push-Benachrichtigungs-Service (Google oder Apple) in der Spalte **Name**, um das Dialogfenster „Push-Benachrichtigung ändern“ anzuzeigen. Klicken Sie dann auf die Registerkarte **Eigenschaften**.

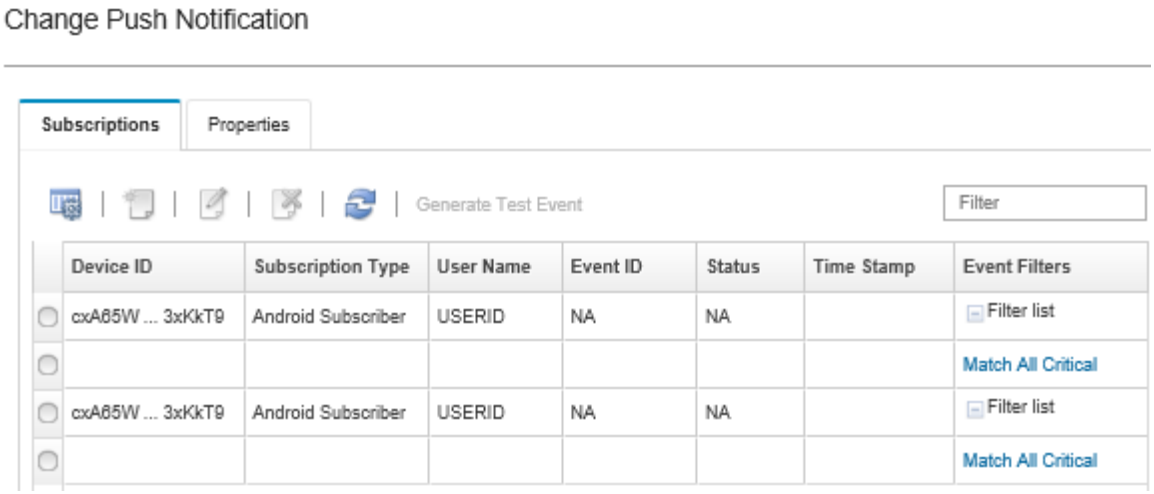


- Sie können Abonnements aktivieren und deaktivieren:
  - Zum Aktivieren und Deaktivieren aller Abonnements für einen bestimmten Einheitenbenachrichtigungs-Service legen Sie auf der Seite „Ereignisweiterleitung“ auf der Registerkarte **Push-Service** in der Tabelle für den Benachrichtigungs-Service dieser Einheit den Status **EIN** oder **AUS** fest.

  - Zum Aktivieren und Deaktivieren aller Abonnements für eine bestimmte Einheit tippen Sie in der Lenovo XClarity Mobile-App auf **Einstellungen → Push-Benachrichtigung** und aktivieren bzw. deaktivieren Sie dann die Option „Aktiviert“ für Push-Benachrichtigungen.
  - Zum Aktivieren und Deaktivieren eines bestimmten Abonnements tippen Sie in der Lenovo XClarity Mobile-App auf **Einstellungen → Push-Benachrichtigung** und dann auf eine Lenovo XClarity Administrator-Verbindung. Aktivieren Sie mindestens einen Ereignisfilter oder deaktivieren Sie alle Ereignisfilter.
- Sie können auf der Seite „Ereignisweiterleitung“ über die Registerkarte **Push-Service** ein Testereignis für alle Abonnements für einen bestimmten mobilen Service generieren, indem Sie den mobilen Service auswählen und auf **Testereignis generieren** klicken.
- Sie können eine Liste der aktuellen Abonnements anzeigen. Klicken Sie auf der Seite „Ereignisweiterleitung“ auf der Registerkarte **Push-Service** auf den Link für den Benachrichtigungs-Service der Einheit (Android oder iOS) in der Spalte **Name**, um das Dialogfenster Push-Benachrichtigung ändern anzuzeigen. Klicken Sie dann auf die Registerkarte **Abonnements**. Die einzelnen Abonnements werden über die Einheiten-ID identifiziert.

  Tipps:

  - Die Einheiten-ID besteht aus den ersten und letzten 6 Ziffern der Pushregistrierungskennung. Die Pushregistrierungskennung finden Sie in der Lenovo XClarity Mobile-App, indem Sie auf **Einstellungen → Info → Pushregistrierungskennung** tippen.
  - Wenn Sie als Benutzer mit einer der folgenden Rollen angemeldet sind, werden alle Abonnements angezeigt. Andernfalls werden nur Abonnements für den angemeldeten Benutzer angezeigt.
    - **lxc-admin**
    - **lxc-supervisor**
    - **lxc-security-admin**
    - **lxc-sysmgr**
- Sie können die Liste der Ereignisfilter anzeigen, die dem Abonnement zugeordnet sind. Erweitern Sie dazu im Dialogfenster „Push-Benachrichtigung ändern“ auf der Registerkarte **Abonnements** die **Filterliste** in der Spalte **Ereignisfilter** für das Abonnement.



- Sie können im Dialogfenster „Push-Benachrichtigung ändern“ auf der Registerkarte **Abonnements** Ereignisfilter für ein bestimmtes Abonnement erstellen, indem Sie das Abonnement auswählen und auf das Symbol für **Erstellen** ( ) klicken.

  Anmerkung: Diese Ereignisfilter gelten nur ein bestimmtes Abonnement und können nicht von anderen Abonnements verwendet werden.

Sie können auch einen Ereignisfilter bearbeiten oder entfernen, indem Sie den Ereignisfilter auswählen und auf das Symbol für **Bearbeiten** ( ) bzw. das Symbol für **Entfernen** ( ) klicken.

- Im Dialogfenster „Push-Benachrichtigung ändern“ können Sie auf der Registerkarte **Abonnements** den Status des zuletzt versuchten Push-Vorgangs für ein bestimmtes Abonnement ermitteln. Die Spalte **Zeitstempel** gibt Datum und Uhrzeit des letzten Push-Vorgangs an. Der **Status** gibt an, ob die Push-Benachrichtigung erfolgreich an den Push-Service übermittelt wurde. Es ist kein Status im Hinblick darauf verfügbar, ob die Push-Benachrichtigung erfolgreich vom Service an die Einheit übermittelt wurde. Wenn die Übermittlung an den Push-Service nicht erfolgreich war, werden in der Statusspalte weitere Informationen zum Fehler angezeigt.
- Sie können im Dialogfenster „Push-Benachrichtigung ändern“ auf der Registerkarte **Abonnements** ein Testereignis für ein bestimmtes Abonnement generieren, indem Sie das Abonnement auswählen und auf **Testereignis generieren** klicken.
- Sie können im Dialogfenster „Push-Benachrichtigung ändern“ auf der Registerkarte **Abonnements** ein Abonnement entfernen, indem Sie das Abonnement auswählen und auf das Symbol für **Entfernen** ( ) klicken.

Ereignisweiterleitung an WebSocket-Services

Sie können Lenovo XClarity Administrator so konfigurieren, dass Ereignisbenachrichtigungen an WebSocket-Services gepusht werden.

Zu dieser Aufgabe

Die WebSocket-Abonnements werden nicht dauerhaft in Lenovo XClarity Administrator gespeichert. Wenn Lenovo XClarity Administrator neu gestartet wird, müssen die WebSocket-Abonnements erneuert werden.

Vorgehensweise

Um Ereignisbenachrichtigungen an einen WebSocket-Service zu pushen, führen Sie die folgenden Schritte durch.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite „Ereignisweiterleitung“ wird angezeigt.

Schritt 2. Klicken Sie auf die Registerkarte **Push-Services**.

Schritt 3. Klicken Sie in der Spalte **Name** auf den Link für den **WebSocket-Service**. Das Dialogfenster „Push-Benachrichtigung ändern“ wird angezeigt.

Schritt 4. Klicken Sie auf die Registerkarte **Abonnements**.

Schritt 5. Klicken Sie auf das Symbol **Erstellen** ( ).

Schritt 6. Geben Sie die IP-Adresse des Zielhosts ein.

Schritt 7. Klicken Sie auf **Erstellen**.

Schritt 8. Wählen Sie das neue Abonnement aus, klicken Sie auf **Testereignis generieren** und überprüfen Sie anschließend, ob die Ereignisse ordnungsgemäß an den WebSocket-Service weitergeleitet werden.

Ergebnisse

Über die Registerkarte **Abonnements** auf dem Dialogfeld „Push-Benachrichtigung ändern“ können Sie die folgenden Aktionen für ein ausgewähltes WebSocket-Abonnement ausführen:

- Aktualisieren Sie die Liste der WebSocket-Services, indem Sie auf Symbol **Aktualisieren** ( ) klicken.
- Abonnements durch Auswahl der Abonnements und Klicken auf das Symbol **Löschen** ( ) löschen

- Status des letzten versuchten Pushs eines bestimmten Abonnements durch Anzeigen des Inhalts der Spalte **Status** ermitteln. Wenn der Versuch fehlgeschlagen ist, enthält diese Spalte eine Nachricht, die den Fehler beschreibt.

Über die Registerkarte **Eigenschaften** auf dem Dialogfeld Push-Benachrichtigung ändern können Sie die folgenden Aktionen ausführen:

- Eigenschaften des WebSocket-Services ändern, einschließlich der Verbindungsleerlaufzeit, der maximalen Puffergröße, der maximalen Anzahl an Abonnenten und des Registrierungstimeout-Zeitraums
- den WebSocket-Service durch Klicken auf **Standardwerte wiederherstellen** auf die Standardeinstellungen zurücksetzen
- das Pushen der Ereignisbenachrichtigungen für alle Abonnements des WebSocket-Services durch Setzen des **Status** auf „Aus“ aussetzen

Über die Registerkarte **Push-Service** auf der Seite „Ereignisweiterleitung“ können Sie für alle WebSocket-Abonnements ein Testereignis generieren, indem Sie den WebSocket-Service auswählen und auf **Testereignis generieren** klicken.

Ereignisfilter für mobile Einheiten und WebSockets erstellen

Sie können globale Ereignisfilter erstellen, die in einem oder mehreren Abonnements für mobile Einheiten und WebSockets verwendet werden können. Sie können auch Ereignisfilter erstellen, die nur für ein Abonnement gelten.

Vorbereitende Schritte

Zum Erstellen von Ereignisfiltern sind Supervisorberechtigungen erforderlich.

Sie können maximal 20 globale Ereignisfilter erstellen.

Zu dieser Aufgabe

Die folgenden globalen Ereignisfilter sind vordefiniert:

- **Alle kritischen Ereignisse abgleichen**. Dieser Filter findet Übereinstimmungen mit allen kritischen Ereignissen, die von einer verwalteten Einheit oder XClarity Administrator generiert werden.
- **Alle Warnungen abgleichen**. Dieser Filter findet Übereinstimmungen mit allen Warnereignissen, die von einer verwalteten Einheit oder XClarity Administrator generiert werden.

Vorgehensweise

Gehen Sie wie folgt vor, um einen globalen Ereignisfilter zu erstellen.

- Erstellen Sie einen globalen Ereignisfilter, der von jedem beliebigen Abonnement verwendet werden kann.
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite „Ereignisweiterleitung“ wird angezeigt.
  2. Klicken Sie auf die Registerkarte **Push-Filter**.
  3. Klicken Sie auf das Symbol **Erstellen** ( ). Die Registerkarte **Allgemein** des Dialogfelds „Neuer Ereignisfilter“ wird angezeigt.
  4. Geben Sie den Namen und eine Optionsbeschreibung für diesen Ereignisfilter an.
  5. Klicken Sie auf **Weiter**, um die Registerkarte **Systeme** anzuzeigen.
  6. Wählen Sie die Einheiten aus, die Sie überwachen möchten.

Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.

7. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.
8. Wählen Sie die Komponenten und Schweregrade aus, für die Sie Ereignisse weiterleiten möchten.

   Tipp:
   - Um alle Hardwareereignisse weiterzuleiten, wählen Sie **Alle Ereignisse abgleichen** aus.
   - Um Prüfereignisse weiterzuleiten, wählen Sie **Alle Prüfereignisse einschließen** aus.
   - Um Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
9. Klicken Sie auf **Erstellen**.

- Erstellen Sie einen Ereignisfilter für ein bestimmtes Abonnement:
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachung → Ereignisweiterleitung**. Die Seite „Neue Ereignisweiterleitung“ wird angezeigt.
  2. Klicken Sie auf die Registerkarte **Push-Filter**.
  3. Wählen Sie in der Tabellenspalte „Name“ den Link für den Typ der mobilen Einheit (Android oder iOS) aus. Das Dialogfenster „Push-Benachrichtigung ändern“ wird angezeigt.
  4. Klicken Sie auf die Registerkarte **Abonnements**, um eine Liste der aktiven Abonnements anzuzeigen.
  5. Wählen Sie das Abonnement aus und klicken Sie auf das Symbol **Erstellen** ( ). Das Dialogfenster „Neuer Ereignisfilter“ wird mit der Registerkarte **Allgemein** angezeigt.
  6. Geben Sie den Namen und eine Optionsbeschreibung für diesen Ereignisfilter an.
  7. Klicken Sie auf **Weiter**, um die Registerkarte **Systeme** anzuzeigen.
  8. Wählen Sie die Einheiten aus, die Sie überwachen möchten.

     Tipp: Um die Ereignisse aller (aktuellen und zukünftigen) verwalteten Einheiten weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Systeme abstimmen**.Wenn Sie das Kontrollkästchen **Alle Systeme abstimmen** nicht auswählen, müssen Sie sicherstellen, dass für die ausgewählten Einheiten keine DUMMY-UUID in der UUID-Spalte stehen. Einheiten, die nach einem Neustart noch nicht wiederhergestellt wurden oder nicht vollständig vom Verwaltungsserver erkannt wurden, wird eine DUMMY-UUID zugewiesen. Wenn Sie eine Einheit mit einer Dummy-UUID auswählen, funktioniert die Ereignisweiterleitung für diese Einheit bis zu dem Zeitpunkt, an dem die Einheit vollständig erkannt oder wiederhergestellt ist und die DUMMY-UUID zu einer echten UUID geworden ist.
  9. Klicken Sie auf **Weiter**, um die Registerkarte **Ereignisse** anzuzeigen.
  10. Wählen Sie die Komponenten und Schweregrade aus, für die Sie Ereignisse weiterleiten möchten.

      Tipp:
      - Um alle Hardwareereignisse weiterzuleiten, wählen Sie **Alle Ereignisse abgleichen** aus.
      - Um Prüfereignisse weiterzuleiten, wählen Sie **Alle Prüfereignisse einschließen** aus.
      - Um Garantie-Ereignisse weiterzuleiten, wählen Sie **Garantie-Ereignisse einschließen** aus.
  11. Klicken Sie auf **Erstellen**.

Nach dieser Aufgabe

Über die Registerkarte „Push-Filter“ der Seite „Ereignisweiterleitung“ können Sie die folgenden Aktionen für einen ausgewählten Ereignisfilter ausführen:

- Aktualisieren Sie die Liste der Ereignisfilter durch Klicken auf das Symbol für **Aktualisieren** ( ).
- Zeigen Sie Details zu einem bestimmten Ereignisfilter an, indem Sie auf den Link in der Spalte **Name** klicken.
- Ändern Sie die Eigenschaften und Filterkriterien von Ereignisfiltern, indem Sie auf das Symbol für **Bearbeiten** ( ) klicken.

Löschen Sie den Ereignisfilter, indem Sie auf das Symbol für **Löschen** ( ) klicken.

Mit Jobs arbeiten

Jobs sind länger laufende Tasks, die auf einer oder mehreren Einheiten ausgeführt werden. Sie können bestimmte Jobs planen, damit sie nur einmal (sofort oder zu einem späteren Zeitpunkt), wiederkehrend oder nur bei Auftreten eines bestimmten Ereignisses ausgeführt werden.

Jobs werden im Hintergrund ausgeführt. Sie können den Status jedes Jobs im Jobprotokoll anzeigen.

Jobs überwachen

Sie können ein Protokoll aller Jobs anzeigen, die von Lenovo XClarity Administrator gestartet wurden. Das Jobprotokoll umfasst Jobs, die aktiv oder abgeschlossen sind oder Fehler enthalten.

Zu dieser Aufgabe

Jobs sind länger laufende Tasks, die auf einer oder mehreren Einheiten ausgeführt werden. Wenn Sie beispielsweise ein Betriebssystem auf mehreren Servern implementieren, wird jede Serverimplementierung als separater Job aufgelistet.

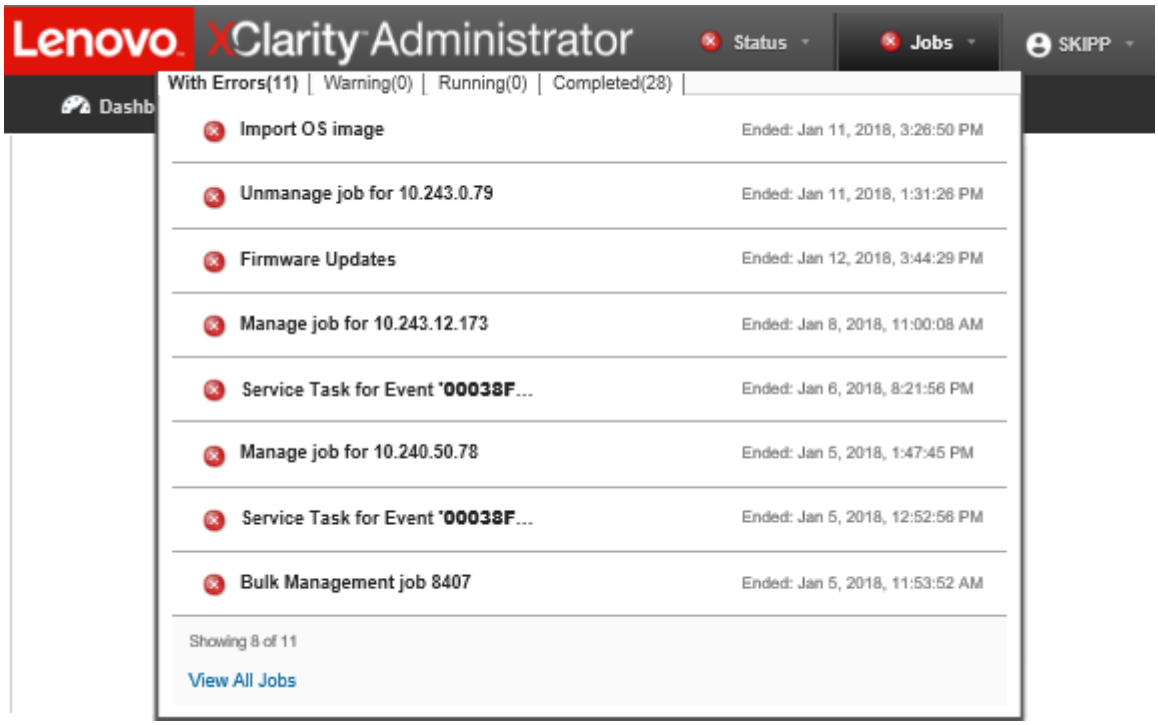
Jobs werden im Hintergrund ausgeführt. Sie können den Status jedes Jobs im Jobprotokoll anzeigen.

Das Jobprotokoll enthält Informationen zu jedem Job. Das Protokoll kann maximal 1.000 Jobs oder 1 GB enthalten. Wenn die maximale Größe erreicht ist, werden die ältesten Jobs, die erfolgreich abgeschlossen wurden, gelöscht. Wenn es keine Jobs gibt, die erfolgreich im Protokoll abgeschlossen wurden, werden die ältesten Jobs, die mit Warnungen abgeschlossen wurden, gelöscht. Wenn es keine Jobs gibt, die erfolgreich oder mit Warnungen im Protokoll abgeschlossen wurden, werden die ältesten Jobs, die mit Fehlern abgeschlossen wurden, gelöscht.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um das Jobprotokoll anzuzeigen.

- Klicken Sie auf der Titelleiste von XClarity Administrator auf **Jobs**, um eine Übersicht der Jobs anzuzeigen, die ausgeführt werden, abgeschlossen sind oder Fehler aufweisen.



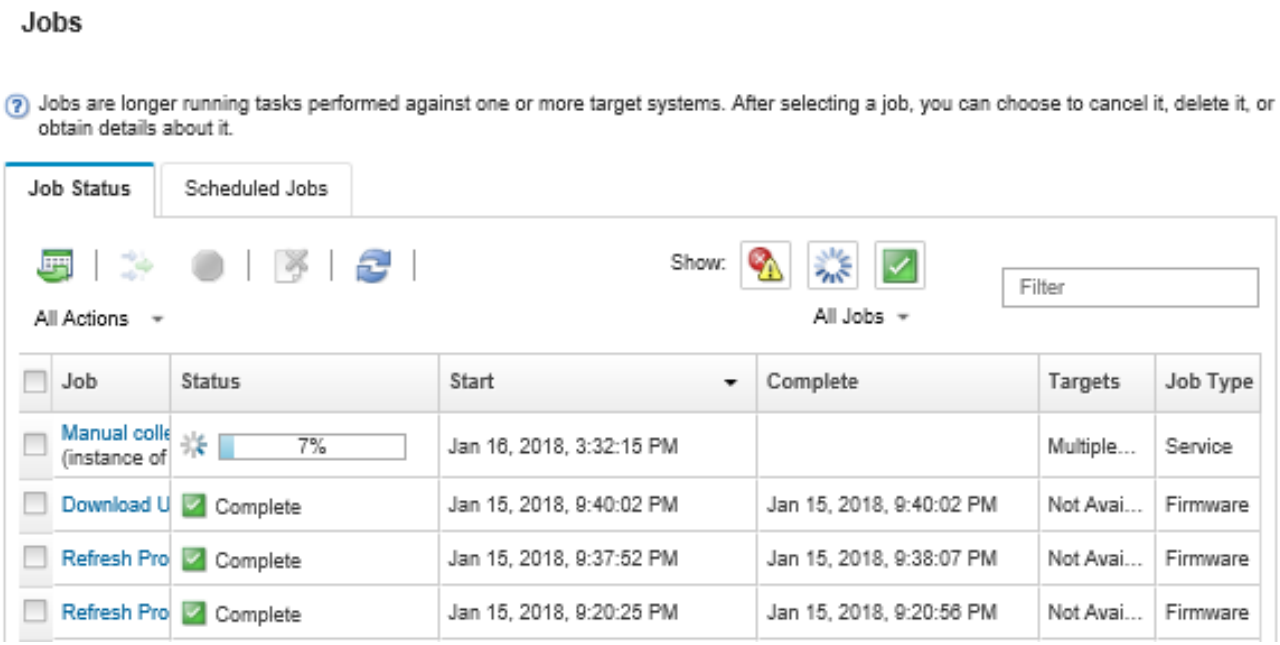
In dieser Pulldown-Liste können Sie auf die folgenden Registerkarten klicken:
- **Fehler**. Zeigt eine Liste aller Jobs an, denen Fehler zugeordnet sind.
- **Warnungen**. Zeigt eine Liste aller Jobs an, denen Warnungen zugeordnet sind.
- **Laufend**. Zeigt eine Liste aller Jobs an, die derzeit ausgeführt werden.
- **Abgeschlossen**. Zeigt eine Liste aller Jobs an, die abgeschlossen sind.

Bewegen Sie den Mauszeiger in der Pulldown-Liste über einen Jobeintrag, um weitere Informationen zum Job zu erhalten, darunter Status, Fortschritt und Benutzer, der den Job erstellt hat.

- Klicken Sie in der Titelleiste von XClarity Administrator auf **Jobs** und klicken Sie anschließend auf den Link **Alle Jobs anzeigen**, um die Seite Jobstatus anzuzeigen.
- Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachen → Jobs** und klicken Sie anschließend auf die Registerkarte **Jobstatus**, um die Seite Jobstatus anzuzeigen.

Nach dieser Aufgabe

Die Seite Jobs wird mit einer Liste aller aktiven Jobs für XClarity Administrator angezeigt.



Über diese Seite können Sie die folgenden Aktionen ausführen:

- Erstellen Sie Jobpläne, indem Sie auf die Registerkarte **Geplante Jobs** klicken (siehe Jobs planen).
- Sie können weitere Informationen zu einem bestimmten Job anzeigen, indem Sie auf die Jobbeschreibung in der Spalte **Jobs** klicken. Ein Dialogfenster wird mit einer Liste von Subtasks (Subjobs) und deren Zielen, einer Zusammenfassung der Subtasks, einschließlich aller erforderlichen Aktionen und Protokolldetails mit Schweregrad und Zeitstempel für jede Nachricht angezeigt. Sie können auswählen, ob Sie die Protokolle für untergeordnete Tasks ausblenden oder anzeigen möchten.
- Bei geplanten Jobs können Sie Informationen zum Zeitplan des Jobs anzeigen, indem Sie auf „diesen“ Link unter der Jobbeschreibung in der Spalte **Jobs** klicken.
- Ändern Sie die Anzahl der Jobs, die pro Seite angezeigt werden. Der Standardwert ist zehn Jobs. Sie können 25, 50 oder alle Jobs anzeigen.
- Grenzen Sie die Liste der angezeigten Jobs ein:
  - Listen Sie nur Jobs von einer bestimmten Quelle auf, indem Sie auf **Jobtypen** klicken und eine der folgenden Optionen auswählen.
    - **Alle Jobtypen**
    - **Service**
    - **Management**
    - **Configuration**
    - **Firmware**
    - **Health**
    - **Power**
    - **Fernzugriff**
    - **System-ID**
    - **BS-Images**
    - **BS-Bereitstellung**
    - **BS-Profil-Export**
    - **Custom**
    - **Inventory**
    - **Unknown**
  - Listen Sie nur geplante Jobs auf, die einem bestimmten Zeitplantyp zugeordnet sind, indem Sie auf **Zeitplantypen** klicken und eine der folgenden Optionen auswählen.

  - **Alle Zeitplantypen**
  - **Einmalig**
  - **Wiederkehrend**
  - **Ausgelöst**
- Klicken Sie auf das Symbol **Jobs mit Fehler-/Warnmeldung ausblenden** ( ) um Jobs mit Fehler- oder Warnmeldung anzuzeigen oder auszublenden.
- Klicken Sie auf das Symbol **Laufende Jobs ausblenden** ( ), um Jobs, die gerade ausgeführt werden, anzuzeigen oder auszublenden.
- Klicken Sie auf das Symbol **Abgeschlossene Jobs ausblenden** ( ), um abgeschlossene Jobs anzuzeigen oder auszublenden.
- Zeigen Sie nur Jobs an, die einen bestimmten Text enthalten (durch Eingabe des Textes in das Feld **Filter**)
- Wenn auf der Seite ein Filter angewendet wird, entfernen Sie den Filter, indem Sie auf das Symbol **Alle Jobs anzeigen** klicken ( ).
- Sortieren Sie die Jobs durch Klicken auf eine Spaltenüberschrift spaltenweise.

- Exportieren Sie die Jobliste als CSV-Datei, indem Sie auf das Symbol **Als CSV exportieren** ( ) klicken.

  Anmerkung: Die Zeitmarken in den exportierten Protokollen verwenden die Ortszeit, die vom Webbrowser angegeben wurde.
- Brechen Sie laufende Jobs oder Subtasks ab, indem Sie einen oder mehrere laufende Jobs auswählen und auf das Symbol **Stoppen** ( ) klicken.

  Anmerkung: Es kann einige Minuten dauern, den Job abzubrechen.
- Löschen Sie abgeschlossenen Jobs oder Subtasks aus dem Jobprotokoll, indem Sie einen oder mehrere abgeschlossene Jobs oder Subtasks auswählen und auf das Symbol **Löschen** ( ) klicken.
- Exportieren Sie Informationen zu bestimmten Jobs, indem Sie die Jobs auswählen und auf das Symbol **Als CSV exportieren** klicken ( ).
- Aktualisieren Sie das Jobprotokoll durch Klicken auf das Symbol **Aktualisieren** ( ).

Jobs planen

Sie können Zeitpläne in Lenovo XClarity Administrator erstellen, um bestimmte Tasks zu bestimmten Zeiten auszuführen.

Zu dieser Aufgabe

Sie können die folgenden Jobtypen planen:
- Einfache Tasks, z. B. Ausschalten und Neustarten
- Servicedaten für bestimmte Einheiten sammeln
- Firmwareaktualisierungs- und BS-Einheitentreiber-Kataloge auf der Lenovo Website aktualisieren
- Aktualisierungskatalog von XClarity Administrator auf der Lenovo Website aktualisieren
- Firmware von der Lenovo Website herunterladen
- Firmware und BS-Einheitentreiber auf verwalteten Einheiten aktualisieren
- Daten und Einstellungen von XClarity Administrator sichern
- Switch-Konfigurationsdaten sichern und wiederherstellen

Sie können die folgenden Zeitplantypen für Jobs auswählen:

- nur einmal (sofort oder zu einem späteren Zeitpunkt)
- wiederkehrend
- wenn ein bestimmtes Ereignis auftritt

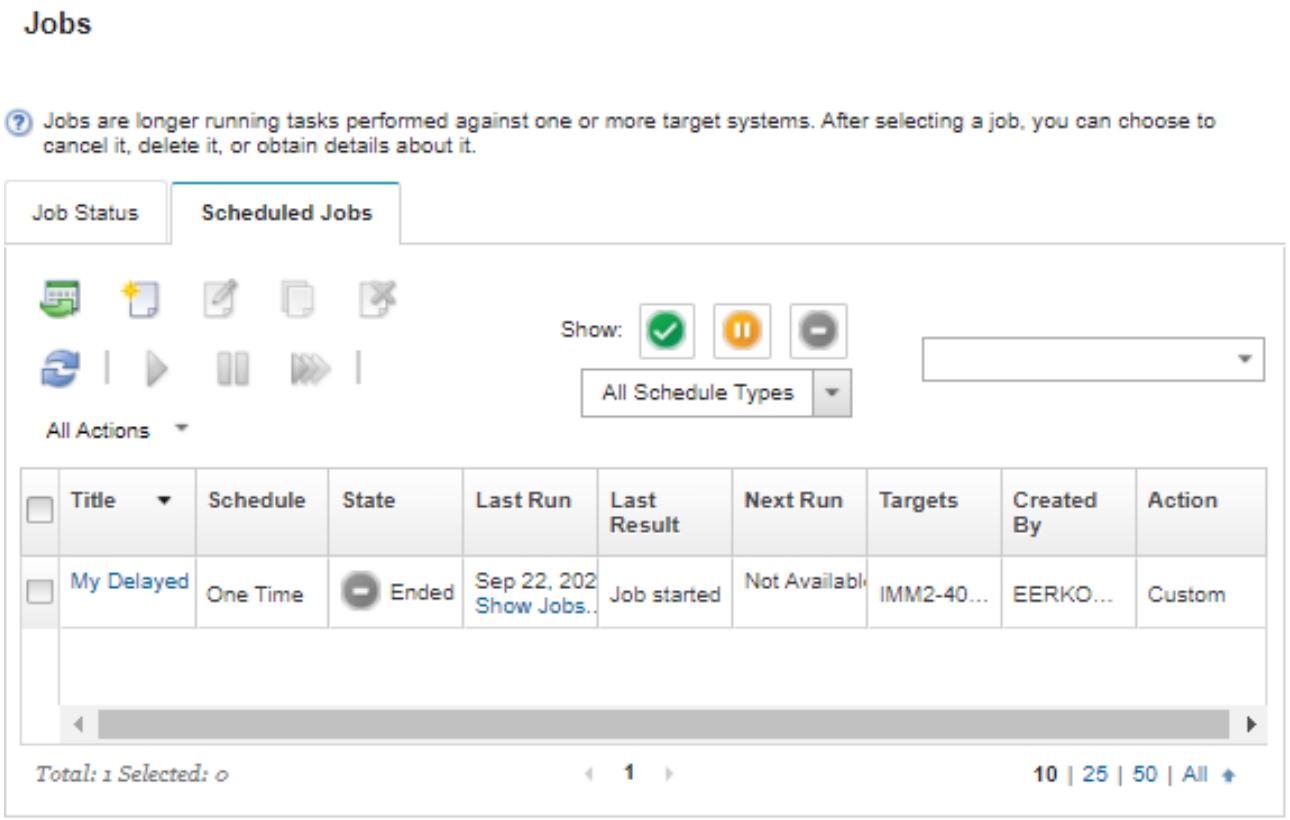
Vorgehensweise

Gehen Sie wie folgt vor, um einen Job zu erstellen und zu planen.

- Erstellen Sie den Jobplan bei komplexen Tasks, z. B. Aktualisieren von Firmware und Sammeln von Servicedaten, auf der aktuellen Taskseite oder im aktuellen Dialogfenster.
  1. Klicken Sie auf **Zeitplan**, um einen Zeitplan zum Ausführen dieses Tasks zu erstellen. Das Dialogfenster „Neuen Job planen“ wird angezeigt.
  2. Geben Sie einen Namen für den Job ein.
  3. Geben Sie an, wann der Job ausgeführt werden soll. Die verfügbaren Optionen sind vom Jobtyp abhängig. Manche Jobs können nicht wiederkehren oder durch ein Ereignis ausgelöst werden.
     - **Einmalig**. Diese Jobs werden nur einmal ausgeführt. Geben Sie Datum und Uhrzeit an, um festzulegen, wann dieser Job ausgeführt werden soll.
     - **Wiederkehrend**. Diese Jobs werden mehrmals ausgeführt. Geben Sie an, wann und wie häufig dieser Job ausgeführt werden soll.
     - **Durch Ereignis ausgelöst**. Diese Jobs werden ausgeführt, wenn ein bestimmtes Ereignis auftritt.
       a. Geben Sie Datum und Uhrzeit an, um festzulegen, wann dieser Job ausgeführt werden soll, und klicken Sie auf **Weiter**.
       b. Wählen Sie das Ereignis aus, das den Job auslösen soll.
  4. Klicken Sie auf **Job erstellen**.
- Erstellen Sie den Jobplan bei einfachen Tasks, z. B. Einschalten und Neustarten, auf der Seite „Jobs“.
  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Überwachen → Jobs** und klicken Sie anschließend auf die Registerkarte **Geplanter Job**, um die Seite „Geplante Jobs“ anzuzeigen.
  2. Klicken Sie auf das Symbol **Erstellen** ( ), um das Dialogfenster „Neue Jobs planen“ anzuzeigen.
  3. Geben Sie einen Namen für den Job ein.
  4. Geben Sie an, wann der Job ausgeführt werden soll.
     - **Einmalig**. Diese Jobs werden nur einmal ausgeführt.
       a. Geben Sie Datum und Uhrzeit an, um festzulegen, wann dieser Job ausgeführt werden soll, und klicken Sie auf **Weiter**.
       b. Wählen Sie verwaltete Einheiten aus, auf denen der Job ausgeführt werden soll.
     - **Wiederkehrend**. Diese Jobs werden mehrmals ausgeführt.
       a. Geben Sie an, wann und wie häufig dieser Job ausgeführt werden soll.
       b. Wählen Sie verwaltete Einheiten aus, auf denen der Job ausgeführt werden soll**.**
     - **Durch Ereignis ausgelöst**. Diese Jobs werden ausgeführt, wenn ein bestimmtes Ereignis auftritt.
       a. Geben Sie Datum und Uhrzeit an, um festzulegen, wann dieser Job ausgeführt werden soll, und klicken Sie auf **Weiter**.
       b. Wählen Sie verwaltete Einheiten aus, auf denen der Job ausgeführt werden soll, und klicken Sie auf **Weiter**.
       c. Wählen Sie das Ereignis aus, das den Job auslösen soll.
  5. Klicken Sie auf **Erstellen**.

Nach dieser Aufgabe

Die Registerkarte Geplante Jobs wird mit einer Liste aller Jobpläne in XClarity Administrator angezeigt.



Über diese Seite können Sie die folgenden Aktionen ausführen:

- Sie können Informationen zu allen aktiven und abgeschlossenen Jobs für einen bestimmten Jobplan anzeigen, indem Sie auf den Link in der Spalte **Job** klicken.
  - Sie können die Liste der angezeigten Jobpläne auf einen bestimmten Zeitplantyp beschränken, indem Sie auf **Zeitplantypen** klicken und eine der folgenden Optionen auswählen:
    - **Alle Zeitplantypen**
    - **Einmalig**
    - **Wiederkehrend**
    - **Ausgelöst**
  - Sie können Jobpläne mit einem bestimmten Status ausblenden oder anzeigen, indem Sie auf eines der folgenden Symbole klicken:
    - Alle geplanten Jobs, die aktiv sind, indem Sie auf das Symbol **Aktiv** klicken ( ).
    - Alle geplanten Jobs, die nicht aktiv sind, indem Sie auf das Symbol **Pausiert** klicken ( ).
    - Alle geplanten Jobs, die bereits ausgeführt wurden und die gemäß Planung nicht erneut ausgeführt werden sollen, indem Sie auf das Symbol **Beendet** klicken ( ).
  - Zeigen Sie nur geplante Jobs an, die einen bestimmten Text enthalten, indem Sie Text in das Feld **Filter** eingeben.
  - Sortieren Sie die geplanten Jobs spaltenweise durch Klicken auf eine Spaltenüberschrift.
- Wann der Job zuletzt ausgeführt wurde, wird in der Spalte **Letzte Ausführung** angezeigt. Zeigen Sie den Status des zuletzt ausgeführten Jobs an, indem Sie auf den Link „Jobstatus“ in dieser Spalte klicken.
- Wann der Job zum nächsten Mal ausgeführt wird, wird in der Spalte **Nächste Ausführung** angezeigt. Zeigen Sie eine Liste aller zukünftigen Daten und Uhrzeiten an, indem Sie auf den Link „Mehr“ in dieser Spalte klicken.

- Führen Sie den diesem Zeitplan zugeordneten Job sofort aus, indem Sie auf das Symbol **Ausführen** klicken ( ).
- Deaktivieren oder aktivieren Sie einen Jobplan, indem Sie auf das Symbol **Pausieren** ( ) oder das Symbol **Aktivieren** ( ) klicken.
- Kopieren und bearbeiten Sie einen Jobplan, indem Sie auf das Symbol **Kopieren** klicken ( ).
- Bearbeiten Sie einen Jobplan, indem Sie auf das Symbol **Bearbeiten** klicken ( ).
- Löschen Sie einen oder mehrere ausgewählte Jobpläne, indem Sie auf das Symbol **Löschen** klicken ( ).
- Exportieren Sie Informationen zu bestimmten Jobplänen, indem Sie die Pläne auswählen und auf das Symbol **Als CSV exportieren** klicken ( ).
- Aktualisieren Sie die Liste der Jobpläne, indem Sie auf **Alle Aktionen → Aktualisieren** klicken.

Auflösung und Kommentare zu einem Job hinzufügen

Sie können eine Auflösung und Kommentare zu abgeschlossenen Jobs hinzufügen, unabhängig vom Erfolgs- oder Fehlerstatus. Dies kann für einen übergeordneten Job und Subtasks im Job durchgeführt werden.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um eine Auflösung und Kommentare zu einem Job hinzuzufügen.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Überwachen → Jobs** und klicken Sie anschließend auf die Registerkarte **Jobstatus**, um die Seite „Jobstatus“ anzuzeigen.

Schritt 2. Klicken Sie auf den Link des Jobs in der Spalte **Job**, um die Jobdetails anzuzeigen.

Schritt 3. Klicken Sie auf das Symbol **Hinweise** ( ), um das Dialogfeld „Hinweise“ anzuzeigen.

In diesem Dialogfenster finden Sie einen Verlauf aller Hinweise und Lösungen, die zum Job hinzugefügt wurden. Sie können den Verlauf löschen, indem Sie auf **Alle Datensätze löschen** klicken.

Schritt 4. Wählen Sie eine der folgenden Lösungen aus.
- **Keine Änderungen**
- **Untersuchen**
- **Behoben**
- **Abgebrochen**

Schritt 5. Fügen Sie eine Anmerkung im Feld **Hinweis** hinzu.

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

Die Lösung wird auf der Seite „Jobstatus“ in der **Status**-Spalte für diesen Job angezeigt.

Kapitel 3. Mit Service und Unterstützung arbeiten

Die Lenovo XClarity Administrator-Webschnittstelle bietet Ihnen eine Reihe von Tools, um Supportkontakte für jede verwaltete Einheit zu definieren, Servicedaten zu sammeln und an den Lenovo-Support zu senden, automatische Benachrichtigungen des Service Providers im Falle von bestimmten wartungsfähigen Ereignissen auf bestimmten Einheiten einzurichten sowie den Status von Service-Tickets und Informationen zur Garantie anzuzeigen. Sie können sich an den Lenovo-Support wenden, um bei Problemen Hilfe und technische Unterstützung zu erhalten.

Weitere Informationen: XClarity Administrator: Service und Support

Bulletins von Lenovo erhalten

Lenovo aktualisiert die Unterstützungswebsite regelmäßig mit Informationen, darunter Sicherheitswarnungen und Auswirkungen auf Onlineservices. Sie können festlegen, dass Lenovo diese Informationen in Form von Bulletins über die Lenovo XClarity Administrator-Webschnittstelle an Sie sendet.

Vorbereitende Schritte

XClarity Administrator benötigt Internetzugriff, um Informationen von Lenovo zu erhalten.

Stellen Sie sicher, dass eine Verbindung zu den Internetadressen hergestellt werden kann, die zum Abrufen der Bulletins benötigt sind.

Zu dieser Aufgabe

Das Abrufen von Bulletins ist standardmäßig aktiviert.

Wenn diese Option aktiviert ist, sendet Lenovo die folgenden Typen von Bulletins.
- Neue Versionen von XClarity Administrator oder Firmware sind verfügbar
- Sicherheitswarnungen wurden gefunden, z. B. Schwachstellen, die die Firmware oder den Verwaltungsserver beeinträchtigen
- Geplante Ausfälle, die sich auf Lenovo XClarity-Onlineservices auswirken

Bulletins können auf verschiedene Arten angezeigt werden.

- Neue Bulletins werden in der XClarity Administrator-Webschnittstelle als Popup-Nachrichten angezeigt.
- Sie erhalten eine Liste der Bulletins der letzten 30 Tage auf der Seite Anmelden und indem Sie auf das Benutzeraktionen-Menü (ADMIN_USER) und dann auf **Lenovo Bulletins-Service** klicken.
- Sie können eine E-Mail-Weiterleitung einrichten, über die die Option **Bulletin-Ereignisse einschließen** aktiviert wird, um Bulletins per E-Mail an Sie zu senden (siehe Ereignisweiterleitung an einen E-Mail-Service über SMTP einrichten in der Onlinedokumentation von XClarity Administrator).

Vorgehensweise

Gehen Sie wie folgt vor, um den Erhalt von Bulletins zu aktivieren.

Schritt 1. Klicken Sie in der Menüleiste von Lenovo XClarity Administrator auf **Verwaltung → Service und Support** und klicken Sie dann im linken Navigationsbereich auf **Lenovo Bulletins-Service**, um die Übersicht Lenovo Service-Bulletin anzuzeigen.

Schritt 2. Wählen Sie **Ich bin damit einverstanden, Bulletins von Lenovo zu erhalten** aus.

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

© Copyright Lenovo 2015, 2025

Informationen zur Garantie anzeigen

Sie können den Garantiestatus (einschließlich erweiterte Garantien) der verwalteten Einheiten bestimmen.

Vorbereitende Schritte

Lenovo XClarity Administrator muss Zugriff auf die folgenden URLs haben, um Informationen zur Garantie für die verwalteten Einheiten zu sammeln. Stellen Sie sicher, dass der Zugriff auf die URLs nicht von Firewalls blockiert wird. Weitere Informationen finden Sie unter Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.

- Lenovo Warranty Datenbank (weltweit) – https://ibase.lenovo.com/POIRequest.aspx
- Lenovo Warranty Datenbank (nur China) – http://service.lenovo.com.cn:83/webservice/NewProductQueryService.asmx
- Lenovo Warranty Webservice – http://supportapi.lenovo.com/warranty/ oder https://supportapi.lenovo.com/warranty/

Sie können diese Garantie-URLs in XClarity Administrator aktivieren oder inaktivieren, indem Sie auf **Alle Aktionen → Garantieverknüpfungen konfigurieren** klicken.

Anmerkung: Für RackSwitch-Einheiten wird in der Spalte **Seriennummer** die berechtigte Seriennummer angezeigt.

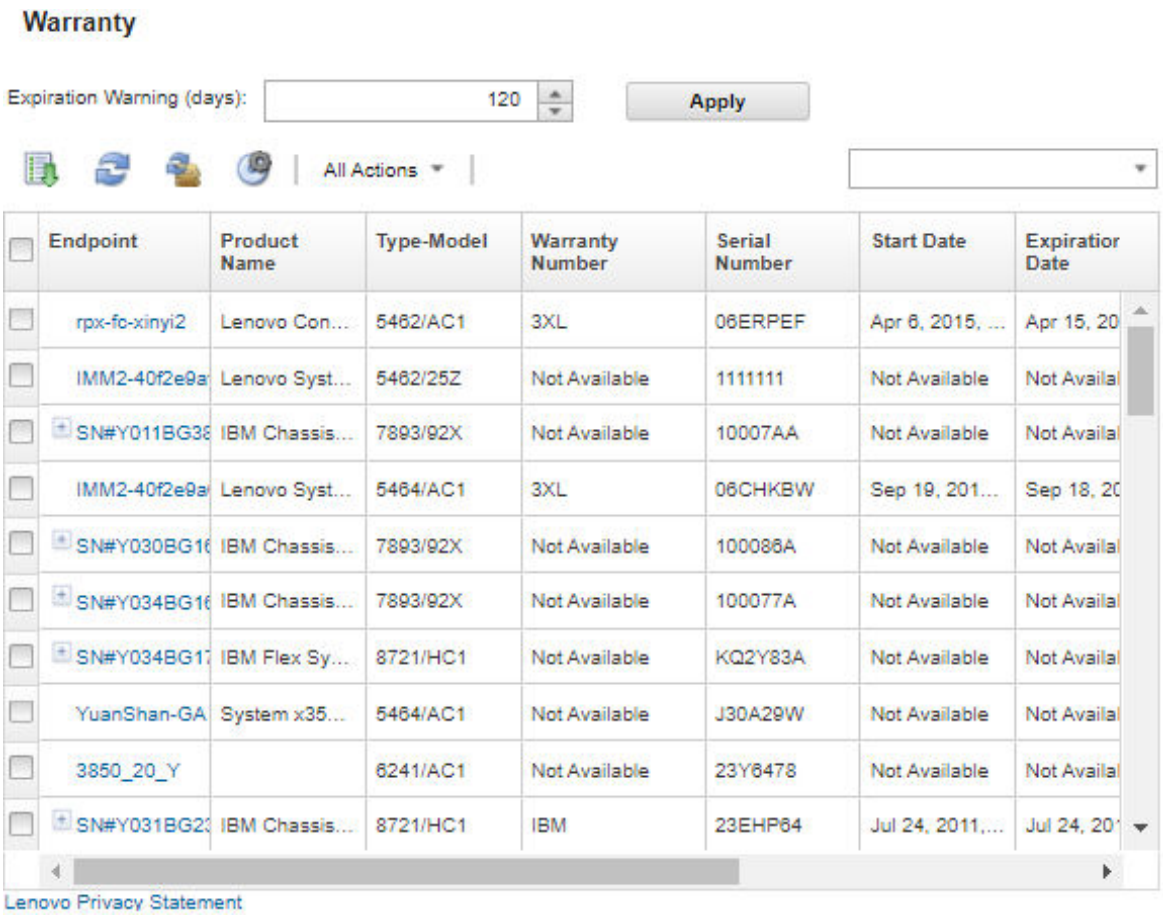
Vorgehensweise

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

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Garantie**, um die Seite Garantie zu öffnen.

Diese Seite enthält eine Tabelle, in der Informationen zur Garantie (wie Anfangsdatum, Enddatum und Status) für jede verwaltete Einheit aufgelistet sind.



Nach dieser Aufgabe

Über die Seite Garantie können Sie die folgenden Aktionen ausführen:

- Legen Sie im Feld **Warnung vor Ablauf** fest, wann eine Warnmeldung über den Garantieablauf für eine verwaltete Einheit ausgegeben werden soll. Der Standardwert beträgt 30 Tage vor Ablauf der Garantie.
- Prüfen Sie die Informationen zur Garantie (falls verfügbar) für eine bestimmte Einheit auf der Lenovo Support-Website, indem Sie auf den Link in der Spalte **Status** klicken.
- Exportieren Sie den Garantiestatus für alle verwalteten Einheiten in eine CSV-Datei, indem Sie auf das Symbol zum Herunterladen im CSV-Format **CSV herunterladen** klicken ( ).
- Aktualisieren Sie die Informationen zur Garantie für alle verwalteten Einheiten, indem Sie auf das Symbol **Serverliste aktualisieren** ( ) klicken.

Automatische Problembenachrichtigung einrichten

Sie können einen Service-Weiterleiter erstellen, der Servicedaten automatisch an Ihren bevorzugten Service Provider sendet, wenn auf bestimmten verwalteten Einheiten ein wartungsfähiges Ereignis auftritt. Sie können Servicedaten für die Einheit an Lenovo-Support (Call-Home-Funktion), an Ihren Lenovo Kundendiensttechniker mithilfe der Lenovo Upload-Funktionalität oder an einen anderen Service Provider senden.

Sie können insgesamt bis zu 50 Service-Weiterleiter für die Call-Home-Funktion, die Lenovo Upload-Funktionalität oder SFTP erstellen und aktivieren.

Automatische Problembenachrichtigung an den Lenovo Support einrichten (Call-Home-Funktion)

Sie können mithilfe der Call-Home-Funktion-Funktion einen Service-Weiterleiter erstellen, der automatisch Servicedaten für jede beliebige verwaltete Einheit an den Lenovo-Support sendet. Dies dient der Problembehebung in Fällen, bei denen bestimmte wartungsfähige Ereignisse (z. B. ein nicht wiederherstellbarer Speicher) von bestimmten verwalteten Einheiten übermittelt werden. Dieser Service-Weiterleiter heißt „Standard-Call-Home-Funktion."

Lenovo setzt sich für Ihre Sicherheit ein. Wenn Call-Home-Funktion aktiviert ist, sendet die Funktion Servicedaten an die Lenovo Upload-Funktionalität, wenn ein Gerät einen Hardwarefehler meldet oder wenn Sie sich dazu entscheiden, einen manuellen Call-Home-Funktion zu starten. Servicedaten, die Sie normalerweise manuell auf die Lenovo Support-Website hochladen, werden mit TLS 1.2 oder höher automatisch über HTTPS an die Lenovo Upload-Funktionalität gesendet. Ihre Geschäftsdaten werden niemals übertragen. Der Zugriff auf Servicedaten der Lenovo Upload-Funktionalität ist auf autorisiertes Servicepersonal beschränkt.

Vorbereitende Schritte

Achtung: Sie müssen die Lenovo Datenschutzerklärung akzeptieren, bevor Sie Daten an den Lenovo Support übertragen können.

Stellen Sie sicher, dass alle von Lenovo XClarity Administrator benötigten Ports (darunter auch die Ports, die für die Call-Home-Funktion erforderlich sind) zur Verfügung stehen, bevor Sie die Call-Home-Funktion aktivieren. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.

Stellen Sie sicher, dass eine Verbindung zu den Internetadressen von Call-Home-Funktion hergestellt werden kann. Weitere Informationen zu Firewalls finden Sie unter Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.

Wenn XClarity Administrator über einen HTTP-Proxy-Server auf das Internet zugreift, muss der Proxy-Server die Standardauthentifizierung verwenden und ein Non-Termination-Proxy sein. Weitere Informationen über die Proxy-Einrichtung finden Sie unter Netzwerkzugriff konfigurieren in der Onlinedokumentation von XClarity Administrator.

Wenn Sie die Call-Home-Funktion konfiguriert haben, wird der **standardmäßige Lenovo Call-Home**-Service-Weiterleiter zur Seite „Service-Weiterleiter" hinzugefügt. Sie können diesen Weiterleiter bearbeiten, um zusätzliche Einstellungen zu konfigurieren, einschließlich der Geräte, die mit diesem Weiterleiter verknüpft werden sollen. Standardmäßig werden alle Geräte abgeglichen.

Achtung: Wenn **Alle Geräte abgleichen** deaktiviert ist, werden nicht explizit ausgewählte Einheiten – einzeln oder über Ressourcengruppen – in einem beliebigen aktivierten Call-Home-Weiterleiter bei wartungsfähigen Ereignisse *keinen* Call Home an den Lenovo Support starten.

Derzeit gibt es keine Option, mit der bestimmte Einheiten von der Call-Home-Funktion ausgeschlossen werden. In der unwahrscheinlichen Situation, dass Sie für eine Untergruppe von Einheiten festlegen möchten, dass kein Call Home bei wartungsfähigen Ereignissen gestartet wird, können Sie eine Kombination aus statischen und dynamischen Ressourcengruppen erstellen, die die vorgesehenen Einheiten vermeiden, und diese Ressourcengruppen dann zum Call-Home-Weiterleiter hinzufügen.

Achtung: Wenn **Alle Geräte abgleichen** für keinen Call-Home-Weiterleiter aktiviert ist, wird die Call-Home-Funktion für keine der Einheiten gestartet. Daher wird empfohlen, dass mindestens ein Standard-Call-Home-Weiterleiter mit **Alle Geräte abgleichen** als Weiterleiter für den letzten Ausweg aktiviert ist.

Wichtig:

- Wenn Sie einen Call-Home-Funktion Service-Weiterleiter in Lenovo XClarity Administrator aktivieren, wird Call-Home-Funktion auf allen verwalteten Einheiten deaktiviert, damit keine doppelten Problemdatensätze generiert werden. Sollen die Einheiten nicht mehr mit XClarity Administrator verwaltet werden oder wenn Sie Call-Home-Funktion in XClarity Administrator deaktivieren möchten, können Sie Call-Home-Funktion auf allen verwalteten Einheiten über XClarity Administrator wieder aktivieren – anstatt Call-Home-Funktion später auf jeder einzelnen Einheit erneut zu aktivieren. Weitere Informationen dazu, wie Sie Call-Home-Funktion auf allen verwalteten Einheiten erneut aktivieren, wenn die Serviceweiterleitung für Call-Home-Funktion deaktiviert ist, finden Sie unter Call-Home-Funktion auf allen verwalteten Einheiten erneut aktivieren
- Obwohl XClarity Administrator Call-Home-Funktion für ThinkAgile und ThinkSystem Einheiten unterstützt, unterstützt der Baseboard Management Controller für manche ThinkAgile und ThinkSystem Einheiten kein Call-Home-Funktion. Daher können Sie die Call-Home-Funktion auf diesen Einheiten weder aktivieren noch deaktivieren. Die Call-Home-Funktion kann nur für diese Einheiten auf der Ebene XClarity Administrator aktiviert werden.

Zu dieser Aufgabe

Mit einem *Service-Weiterleiter* wird festgelegt, an welchen Empfänger die Servicedatendateien nach einem aufgetretenen wartungsfähigen Ereignis gesendet werden sollen. Sie können bis zu 50 Service-Weiterleiter definieren.

- **Ist kein Call-Home-Funktion Service-Weiterleiter konfiguriert**, können Sie ein Service-Ticket manuell öffnen und Servicedateien an das Lenovo-Support Center übertragen. Folgen Sie dazu den Anweisungen unter Website für neue Serviceanforderung. Weitere Informationen über das Sammeln und den Download von Servicedateien finden Sie unter Lenovo XClarity Administrator Servicedaten sammeln und herunterladen und Servicedaten für eine Einheit sammeln und herunterladen
- **Sofern ein Call-Home-Funktion Service-Weiterleiter konfiguriert, aber nicht aktiviert ist**, können Sie ein Service-Ticket *manuell* mithilfe der Call-Home-Funktion-Funktion öffnen, um Servicedateien zu sammeln und an das Lenovo-Support Center zu senden. Weitere Informationen finden Sie unter Übermitteln einer Serviceanforderung zu Hardwareproblemen an das Lenovo-Support Center.
- **Wenn ein Call-Home-Funktion-Service-Weiterleiter konfiguriert und aktiviert ist**, öffnet XClarity Administrator beim Auftreten eines wartungsfähigen Ereignisses *automatisch* ein Service-Ticket, erfasst Servicedaten und speichert diese als Archivdatei und überträgt die Service-Archivdatei an die Lenovo Upload-Funktionalität, damit das Problem behoben werden kann. Die Archiv-Servicedatei enthält die Servicedaten für das Gerät und für XClarity Administrator.

  Anmerkungen: Für ThinkSystem V3 und V4 Server (mit XCC2 oder XCC3) speichert XClarity Administrator Servicedaten in zwei Dateien im Repository.

  – **Servicedateien**. (.zip) Diese Datei enthält Serviceinformationen und Bestandsdaten der Einheit in einem leicht lesbaren Format. Diese Datei wird automatisch an die Lenovo Upload-Funktionalität gesendet, wenn ein wartungsfähiges Ereignis auftritt.

  – **Debugdatei**. (.tzz) Die Datei enthält alle Serviceinformationen, Bestandsdaten und Debugprotokolle der Einheit zur Verwendung durch die Lenovo Upload-Funktionalität. Sie können diese Datei manuell an den Lenovo Support senden, wenn zusätzliche Informationen zur Problemlösung erforderlich sind.

  Bei anderen Einheiten speichert XClarity Administrator Servicedaten (einschließlich XClarity Administrator und Serviceinformationen, Bestandsdaten und Debugprotokolle der Einheit) in einer einzelnen Servicedatei im Repository. Diese Datei wird an das Lenovo-Support Center gesendet, wenn ein wartungsfähiges Ereignis auftritt.

  Die Call-Home-Funktion wird für wiederholte Ereignisse für alle Einheiten unterdrückt, wenn bereits ein Service-Ticket für dieses Ereignis auf dieser Einheit erstellt wurde. Die Call-Home-Funktion wird auch für ähnliche Ereignisse für die ThinkAgile und ThinkSystem Einheiten unterdrückt, wenn bereits ein Service-Ticket für ein Ereignis auf dieser Einheit erstellt wurde. ThinkAgile und ThinkSystem Ereignisse sind

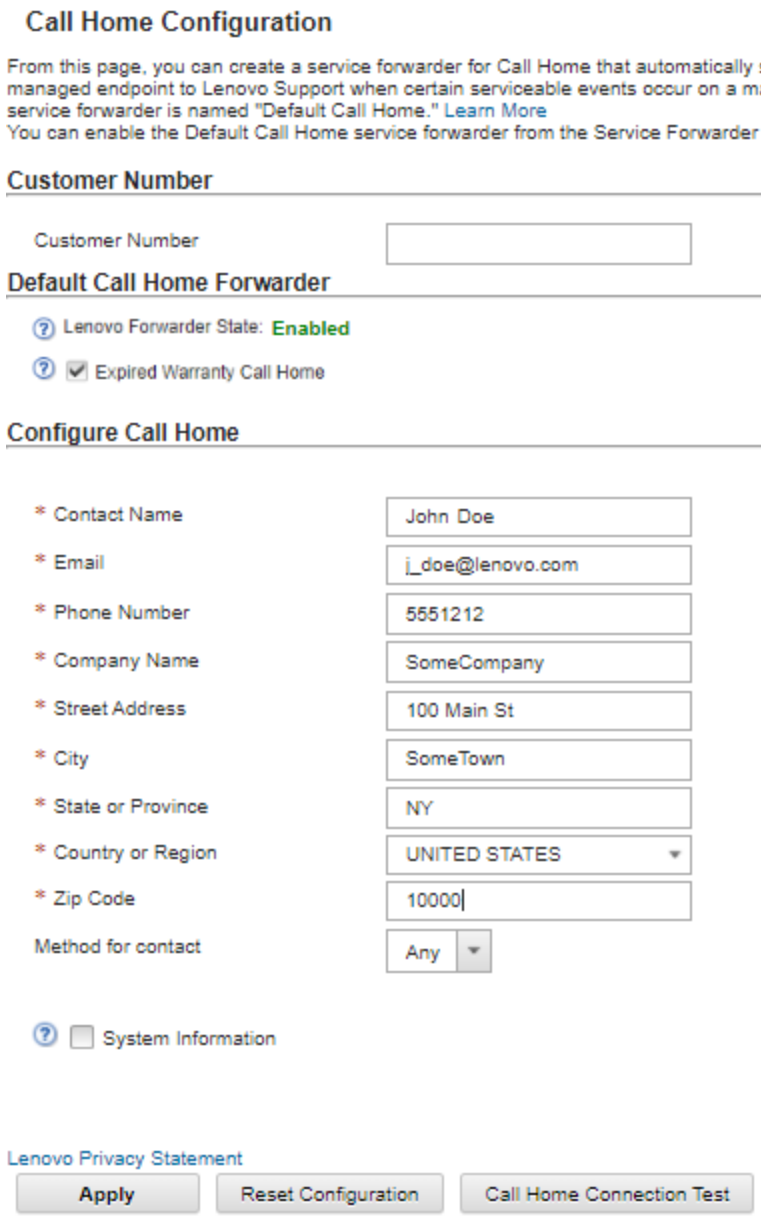
Zeichenfolgen mit 16 Zeichen im Format *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx* (z. B. `806F010D0401FFFF`). Ereignisse ähneln sich, wenn Sie über denselben Lesetyp, denselben Sensortyp und dieselbe Entitäts-ID verfügen. Wenn z. B. auf einer bestimmten ThinkAgile oder ThinkSystem Einheit ein Service-Ticket für Ereignis 806F010D0401FFFF erstellt wurde, werden alle Ereignisse, die auf dieser Einheit mit Ereignis-IDs wie *xx*`6F01`*xx*`04`*xxxxxx* auftreten (wobei es sich bei *x* um irgendein alphanumerisches Zeichen handeln kann) unterdrückt.

Weitere Informationen über die Anzeige von Service-Tickets, die von einem Call-Home-Funktion Service-Weiterleiter automatisch geöffnet wurden, finden Sie unter Service-Tickets und Status anzeigen.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Service-Weiterleiter für Call-Home-Funktion einzurichten.

- Richten Sie Call-Home-Funktion für alle verwalteten Einheiten (aktuelle und zukünftige) ein:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**.
  2. Klicken Sie im linken Navigationsbereich auf **Call-Home-Konfiguration**, um die Seite Call-Home-Konfiguration zu öffnen.



3. (Optional) Geben Sie die standardmäßige Lenovo Kundennummer an, die beim Melden von Problemen mit XClarity Administrator verwendet werden soll.

   Tipp: Ihre Kundennummer finden Sie in der E-Mail mit dem Berechtigungsnachweis, die Sie beim Kauf von Lenovo XClarity Pro erhalten haben.

4. (Optional) Entfernen Sie **Call-Home bei abgelaufener Garantie**, um das automatische Öffnen von Service-Tickets durch die Call-Home-Funktion für Einheiten mit abgelaufener Garantie zu blockieren.

   Anmerkung: Sie können Service-Tickets für Einheiten mit abgelaufener Garantie weiterhin manuell öffnen.

5. Geben Sie die Kontakt- und Standortinformationen ein.
6. Wählen Sie die bevorzugte Kontaktmethode für den Lenovo Support aus.
7. (Optional) Geben Sie die Systeminformationen an.
8. Klicken Sie auf **Übernehmen**.

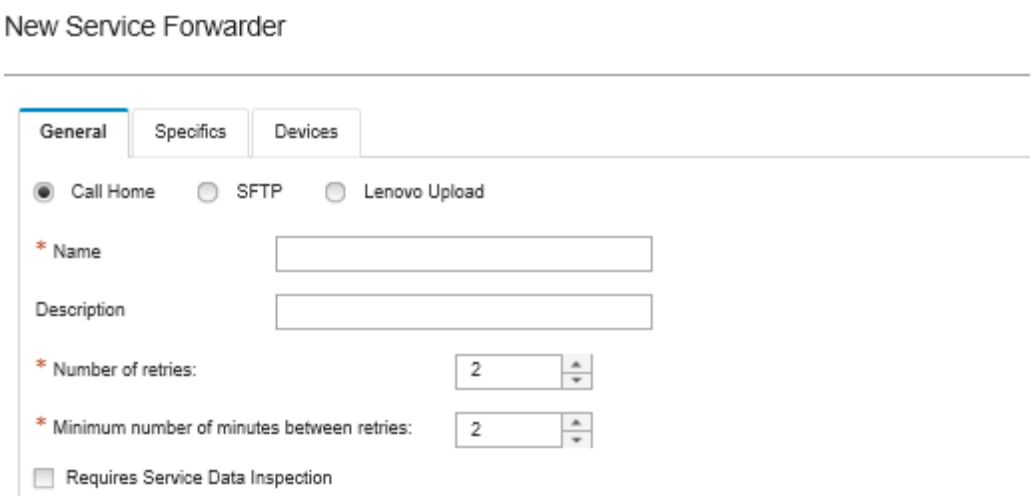
Für die Call-Home-Funktion-Funktion wird unter Verwendung der angegebenen Kontaktinformationen ein Service-Weiterleiter mit dem Namen „Standard-Call Home“ für alle verwalteten Einheiten erstellt.

9. Aktivieren und testen Sie den Service-Weiterleiter „Standard-Call Home“.
   a. Klicken Sie im linken Navigationsbereich auf **Service-Weiterleiter**, um die Seite Service-Weiterleiter zu öffnen.
   b. Wählen Sie **Aktivieren** in der Spalte **Status** des Service-Weiterleiters „Standard-Call Home“ aus.
   c. Markieren Sie den Service-Weiterleiter „Standard-Call Home“ und klicken Sie auf **Service-Weiterleiter testen**, um ein Testereignis für den Service-Weiterleiter zu generieren und die Kommunikation zwischen der XClarity Administrator und dem Lenovo Support-Center zu überprüfen.

      Sie können den Testfortschritt überwachen, indem Sie auf **Überwachung → Jobs** in der XClarity Administrator-Menüleiste klicken.

      Anmerkung: Der Service-Weiterleiter muss erst aktiviert werden, bevor er getestet werden kann.

- Richten Sie Call-Home-Funktion für bestimmte verwaltete Einheiten ein:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**.
  2. Klicken Sie im linken Navigationsbereich auf **Service-Weiterleiter**, um die Seite Service-Weiterleiter zu öffnen.
  3. Klicken Sie auf das Symbol **Service-Weiterleiter** erstellen ( ), um das Dialogfenster Neuer Service-Weiterleiter zu öffnen.
  4. Klicken Sie auf die Registerkarte **Allgemein**.



   a. Wählen Sie die **Call-Home-Funktion** als Service-Weiterleiter aus:
   b. Geben Sie den Namen des Service-Weiterleiters und eine Beschreibung ein.
   c. Geben Sie an, wie häufig die automatische Benachrichtigung wiederholt werden soll. Der Standardwert ist 2.
   d. Geben Sie an, wie viele Minuten zwischen den Wiederholungen verstreichen sollen. Der Standardwert ist 2.
   e. (Optional) Klicken Sie auf **Servicedatenüberprüfung erforderlich**, wenn die Servicedatendateien vor dem Versenden überprüft werden sollen. Optional können Sie die E-Mail-Adresse des Kontakts angeben, der bei einer erforderlichen Prüfung der Servicedateien benachrichtigt werden soll.
  5. Klicken Sie auf die Registerkarte **Bestimmt** und geben Sie die Kontakt- und Systeminformationen an.

Tipp: Um dieselben Kontakt- und Standortinformationen zu verwenden, die auf der Seite „Call-Home-Konfiguration“ konfiguriert sind, wählen Sie im Dropdown-Menü **Konfiguration** die Option **Allgemeine Konfiguration** aus.

6. Klicken Sie auf die Registerkarte **Einheiten** und wählen Sie die verwalteten Einheiten und Ressourcengruppen aus, für die dieser Service-Weiterleiter Servicedateien weiterleiten soll.

   Tipp: Um Servicedateien für alle verwalteten Einheiten (derzeitige und künftige) weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Geräte abgleichen**.

7. Klicken Sie auf **Erstellen**. Der Service-Weiterleiter wird zur Seite Service und Support hinzugefügt.
8. Wählen Sie auf der Seite Service-Weiterleiter in der Spalte **Status** die Option **Aktivieren** aus, um den Service-Weiterleiter zu aktivieren.
9. Markieren Sie den Service-Weiterleiter und klicken Sie auf **Service-Weiterleiter testen**, um für den Service-Weiterleiter ein Testereignis zu generieren und die Kommunikation zwischen XClarity Administrator und dem Lenovo Support-Center zu überprüfen.

   Sie können den Testfortschritt überwachen, indem Sie auf **Überwachung → Jobs** in der XClarity Administrator-Menüleiste klicken.

   Anmerkung: Der Service-Weiterleiter muss erst aktiviert werden, bevor er getestet werden kann.

Nach dieser Aufgabe

Auf der Seite Service und Support können Sie zudem folgende Aktionen ausführen:

- Wenn die Option **Servicedatenüberprüfung erforderlich** ausgewählt ist und bei einer der verwalteten Einheiten dieses Service-Weiterleiters ein wartungsfähiges Ereignis aufgetreten ist, müssen Sie die Servicedateien prüfen, bevor diese an den Service Provider weitergeleitet werden. Weitere Informationen finden Sie unter .
- Ermitteln Sie, ob die Call-Home-Funktion auf einer verwalteten Einheit aktiviert oder deaktiviert ist. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen** und überprüfen Sie den Status in der Spalte **Call-Home-Funktion-Status**.

  Tipp: Wenn „Status unbekannt“ in der Spalte **Call-Home-Funktion-Status** angezeigt wird, aktualisieren Sie den Webbrowser, damit der richtige Status angegeben wird.

- Definieren Sie die Support-Kontakt- und Standortinformationen einer bestimmten verwalteten Einheit. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf das Symbol **Kontaktprofil erstellen** ( ) oder **Kontaktprofil bearbeiten** ( ). Die Kontakt- und Standortinformationen für die verwaltete Einheit werden in das Service-Ticket eingebunden, den dieCall-Home-Funktion an das Lenovo-Support Center sendet. Sofern eindeutige Kontakt- und Standortinformationen für eine verwaltete Einheit angegeben sind, werden diese in das Service-Ticket aufgenommen. Andernfalls werden die allgemeinen Informationen herangezogen, die für die XClarity AdministratorCall-Home-Funktion-Konfiguration angegeben sind (auf der Seite **Call-Home-FunktionKonfiguration** oder **Service-Weiterleiter**) angegeben sind. Siehe Lenovo-Support Center für weitere Informationen. Weitere Informationen finden Sie unter Support-Kontakte für bestimmte Einheiten definieren.
- Zeigen Sie die Service-Tickets an, die an das Lenovo-Support Center übermittelt wurden. Klicken Sie dazu im linken Navigationsbereich auf **Status des Service-Tickets**. Auf dieser Seite werden die automatisch oder manuell von einem Call-Home-Funktion Service-Weiterleiter geöffneten Service-Tickets, der Status sowie die Servicedateien angezeigt, die an das Lenovo-Support Center übertragen wurden. Weitere Informationen finden Sie unter Service-Tickets und Status anzeigen.
- Sammeln Sie die Servicedaten für eine bestimmte Einheit. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf das Symbol **Servicedaten**

sammeln ( ). Weitere Informationen finden Sie unter Servicedaten für eine Einheit sammeln und herunterladen.

- Öffnen Sie manuell ein Service-Ticket im Lenovo-Support Center, sammeln Sie Servicedaten für eine bestimmte Einheit und senden Sie diese Dateien an das Lenovo-Support Center. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf **Alle Aktionen → Call-Home-Funktion manuell ausführen**.Falls das Lenovo-Support Center weitere Daten benötigt, werden Sie vom Lenovo-Support aufgefordert, die Servicedaten für diese oder eine andere Einheit erneut zu sammeln.

  Weitere Informationen finden Sie unter Übermitteln einer Serviceanforderung zu Hardwareproblemen an das Lenovo-Support Center.

- Aktivieren Sie die Call-Home-Funktion wieder auf allen verwalteten Einheiten. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen** und anschließend auf **Alle Aktionen → Call-Home-Funktion auf allen Einheiten aktivieren**.

  Wenn Sie einen Call-Home-Funktion Service-Weiterleiter in Lenovo XClarity Administrator aktivieren, wird Call-Home-Funktion auf allen verwalteten Einheiten deaktiviert, damit keine doppelten Problemdatensätze generiert werden. Sollen die Einheiten nicht mehr mit XClarity Administrator verwaltet werden oder wenn Sie Call-Home-Funktion in XClarity Administrator deaktivieren möchten, können Sie Call-Home-Funktion auf allen verwalteten Einheiten über XClarity Administrator wieder aktivieren – anstatt Call-Home-Funktion später auf jeder einzelnen Einheit erneut zu aktivieren.

Automatische Problembenachrichtigung an die Lenovo Upload-Funktionalität

Sie können mithilfe der Lenovo Upload-Funktionalität einen Service-Weiterleiter erstellen, der automatisch Servicedaten für jede beliebige verwaltete Einheit an den Lenovo Kundendiensttechniker sendet. Dies dient der Problembehebung in Fällen, bei denen bestimmte wartungsfähige Ereignisse (z. B. ein nicht wiederherstellbarer Speicher) von bestimmten verwalteten Einheiten übermittelt werden. Dieser Service-Weiterleiter heißt „Lenovo Upload-Standardfunktionalität.“

Lenovo setzt sich für Ihre Sicherheit ein. Ihre Geschäftsdaten werden niemals übertragen. Der Zugriff auf Servicedaten der Lenovo Upload-Funktionalität ist auf autorisiertes Servicepersonal beschränkt.

Vorbereitende Schritte

Achtung: Sie müssen die Lenovo Datenschutzerklärung akzeptieren, bevor Sie Daten an den Lenovo Support übertragen können.

Stellen Sie sicher, dass alle Ports, die für Lenovo XClarity Administrator erforderlich sind, verfügbar sind, bevor Sie einen Service-Weiterleiter einrichten. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.

Stellen Sie sicher, dass eine Verbindung zu den entsprechenden Internetadressen der Lenovo Upload-Funktionalität hergestellt werden kann. Weitere Informationen zu Firewalls finden Sie unter Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.

Wenn XClarity Administrator über einen HTTP-Proxy-Server auf das Internet zugreift, muss der Proxy-Server die Standardauthentifizierung verwenden und ein Non-Termination-Proxy sein. Weitere Informationen über die Proxy-Einrichtung finden Sie unter Netzwerkzugriff konfigurieren in der Onlinedokumentation von XClarity Administrator.

Anmerkung: Falls die Funktion bei mehreren Service-Weiterleitern für dieselbe Einheit konfiguriert ist, überträgt nur ein Service-Weiterleiter Servicedaten. Die verwendete E-Mail- und Upload-URL hängt davon ab, welcher Service-Weiterleiter zuerst ausgelöst wird.

Zu dieser Aufgabe

Mit einem *Service-Weiterleiter* wird festgelegt, an welchen Empfänger die Servicedatendateien nach einem aufgetretenen wartungsfähigen Ereignis gesendet werden sollen. Sie können bis zu 50 Service-Weiterleiter definieren.

- **Sofern ein Service-Weiterleiter der Lenovo Upload-Funktionalität konfiguriert, aber nicht aktiviert ist**, können Sie gesammelte Servicedateien jederzeit *manuell* an die Lenovo Upload-Funktionalität senden. Weitere Informationen finden Sie unter Übermitteln einer Serviceanforderung zu Hardwareproblemen an das Lenovo-Support Center.
- **Wenn ein Lenovo Upload-Funktionalität-Service-Weiterleiter konfiguriert und aktiviert ist**, erfasst XClarity Administrator beim Auftreten eines wartungsfähigen Ereignisses *automatisch* Servicedaten, öffnet ein Service-Ticket und überträgt die Servicedatei an die Lenovo Upload-Funktionalität, damit das Problem behoben werden kann.

  Für ThinkSystem V3 und V4 Server (mit XCC2 oder XCC3) speichert XClarity Administrator Servicedaten in zwei Dateien im Repository.

  – **Servicedateien**. (.zip) Diese Datei enthält Serviceinformationen und Bestandsdaten in einem leicht lesbaren Format. Diese Datei wird automatisch an die Lenovo Upload-Funktionalität gesendet, wenn ein wartungsfähiges Ereignis auftritt.

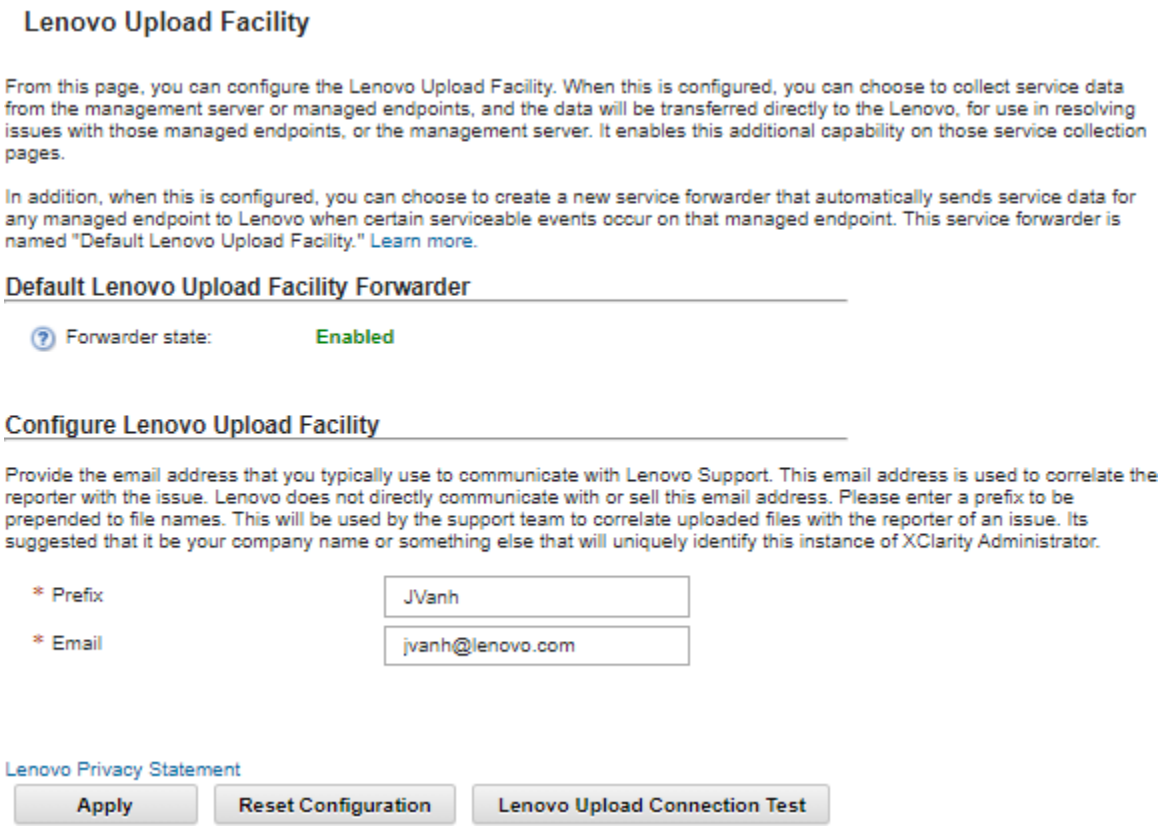
  – **Debugdatei**. (.tzz) Die Datei enthält alle Serviceinformationen, Bestand und Debugprotokolle zur Verwendung durch den Lenovo Support. Sie können diese Datei manuell an den Lenovo Support senden, wenn zusätzliche Informationen zur Problemlösung erforderlich sind.

  Bei anderen Einheiten speichert XClarity Administrator Servicedaten (einschließlich Serviceinformationen, Bestand und Debugprotokolle) in einer einzelnen Servicedatei im Repository. Diese Datei wird an die Lenovo Upload-Funktionalität gesendet, wenn ein wartungsfähiges Ereignis auftritt.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Service-Weiterleiter für die Lenovo Upload-Funktionalität einzurichten.

- Richten Sie einen Service-Weiterleiter zur Lenovo Upload-Funktionalität für alle verwalteten Einheiten ein:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**.
  2. Klicken Sie im linken Navigationsbereich auf **Lenovo Upload-Funktionalität**, um die Seite Lenovo Upload-Funktionalität anzuzeigen.



3. Geben Sie die E-Mail-Adresse und die URL ein, die Sie vom Lenovo Support erhalten haben.
4. Klicken Sie auf **Übernehmen**.

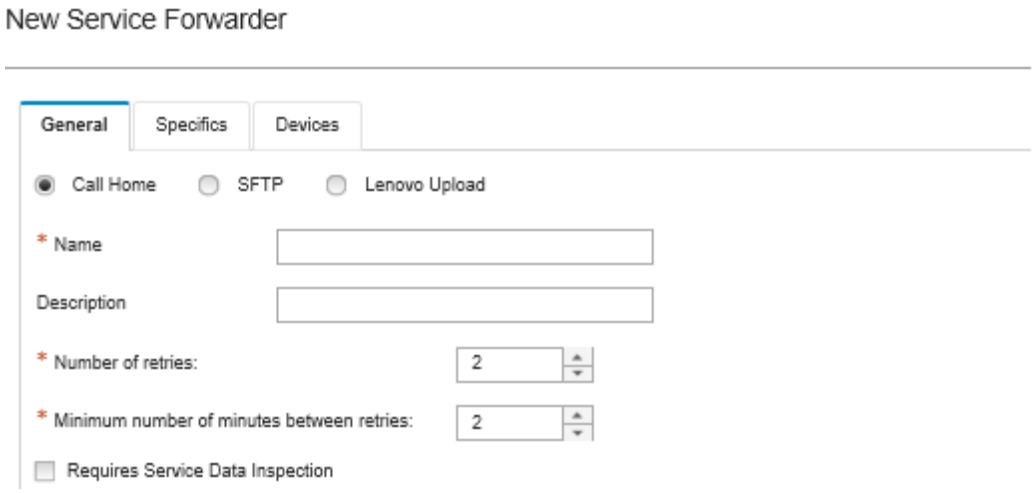
   Ein Service-Weiterleiter mit dem Namen „Standard-Lenovo Upload-Funktionalität“ wird unter Verwendung der angegebenen Kontaktinformationen für alle verwalteten Einheiten erstellt.
5. Aktivieren und testen Sie den Service-Weiterleiter „Standard-Lenovo Upload-Funktionalität“.
   a. Klicken Sie im linken Navigationsbereich auf **Service-Weiterleiter**, um die Seite Service-Weiterleiter zu öffnen.
   b. Wählen Sie **Aktivieren** in der Spalte **Status** des Service-Weiterleiters „Standard-Lenovo Upload-Funktionalität“ aus.
   c. Markieren Sie den Service-Weiterleiter „Standard-Lenovo Upload-Funktionalität“ und klicken Sie auf **Service-Weiterleiter testen**, um ein Testereignis für den Service-Weiterleiter zu generieren und die Kommunikation zwischen der Lenovo Upload-Funktionalität und dem XClarity Administrator zu überprüfen.

      Sie können den Testfortschritt überwachen, indem Sie auf **Überwachung → Jobs** in der XClarity Administrator-Menüleiste klicken.

      Anmerkung: Der Service-Weiterleiter muss erst aktiviert werden, bevor er getestet werden kann.

- Richten Sie einen Service-Weiterleiter zur Lenovo Upload-Funktionalität für spezifischen verwalteten Einheiten ein:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite „Service und Support“ wird angezeigt.
  2. Klicken Sie im linken Navigationsbereich auf **Service-Weiterleiter**, um die Seite Service-Weiterleiter zu öffnen.

3. Klicken Sie auf das Symbol **Service-Weiterleiter erstellen** icon ( ), um das Dialogfenster Neuer Service-Weiterleiter zu öffnen.
4. Klicken Sie auf die Registerkarte **Allgemein**.



   a. Wählen Sie **Lenovo Upload** für den Service-Weiterleiter aus.
   b. Geben Sie den Namen des Service-Weiterleiters und eine Beschreibung ein.
   c. Geben Sie an, wie häufig die automatische Benachrichtigung wiederholt werden soll. Der Standardwert ist 2.
   d. Geben Sie an, wie viele Minuten zwischen den Wiederholungen verstreichen sollen. Der Standardwert ist 2.
   e. (Optional) Klicken Sie auf **Servicedatenüberprüfung erforderlich**, wenn die Servicedateien vor dem Versenden überprüft werden sollen. Optional können Sie die E-Mail-Adresse des Kontakts angeben, der bei einer erforderlichen Prüfung der Servicedatendateien benachrichtigt werden soll.
5. Klicken Sie auf die Registerkarte **Bestimmt** und geben Sie die E-Mail-Adresse und Upload-URL an, die Sie vom Lenovo Support erhalten haben.
6. Klicken Sie auf die Registerkarte **Einheiten** und wählen Sie die verwalteten Einheiten und Ressourcengruppen aus, für die dieser Service-Weiterleiter Servicedaten weiterleiten soll.

   Tipp: Um Servicedaten für alle verwalteten Einheiten (derzeitige und künftige) weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Geräte abgleichen**.
7. Klicken Sie auf **Erstellen**. Der Service-Weiterleiter wird zur Seite Service und Support hinzugefügt.
8. Wählen Sie auf der Seite „Service und Support“ in der Spalte **Status** die Option **Aktivieren** aus, um den Service-Weiterleiter zu aktivieren.
9. Wählen Sie den Service-Weiterleiter und klicken Sie auf **Service-Weiterleiter testen**, um ein Testereignis für jeden Service-Weiterleiter zu generieren und zu überprüfen, dass eine Übertragung von XClarity Administrator an die Lenovo Upload-Funktionalität stattfinden kann.

   Anmerkung: Der Service-Weiterleiter muss erst aktiviert werden, bevor er getestet werden kann.

Nach dieser Aufgabe

Auf der Seite Service und Support können Sie zudem folgende Aktionen ausführen:

- Wenn die Option **Servicedatenüberprüfung erforderlich** ausgewählt ist und bei einer der verwalteten Einheiten dieses Service-Weiterleiters ein wartungsfähiges Ereignis aufgetreten ist, müssen Sie die

Servicedateien prüfen, bevor diese an den Service Provider weitergeleitet werden. Siehe Servicedateien prüfen für weitere Informationen.

- Bearbeiten Sie die Informationen für den Service-Weiterleiter. Klicken Sie dazu im linken Navigationsbereich auf **Service-Weiterleiter** und dann auf das Symbol **Service-Weiterleiter bearbeiten** ( ).
- Aktivieren oder deaktivieren Sie einen Service-Provider. Klicken Sie dazu auf **Service-Weiterleiter** und wählen Sie in der Spalte **Status** entweder **Aktivieren** oder **Deaktivieren** aus.
- Löschen Sie den Service-Provider. Klicken Sie dazu auf **Service-Weiterleiter** und auf das Symbol **Service-Weiterleiter löschen** ( ).
- Sammeln Sie die Servicedaten für eine bestimmte Einheit. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf das Symbol **Servicedaten sammeln** ( ). Siehe Servicedaten für eine Einheit sammeln und herunterladen für weitere Informationen.

Automatische Problembenachrichtigung an einen bevorzugten Service Provider einrichten

Sie können einen Service-Weiterleiter erstellen, der Servicedaten automatisch mit SFTP an Ihren bevorzugten Service Provider sendet. Dies dient der Problembehebung, wenn bestimmte wartungsfähige Ereignisse (z. B. nicht wiederherstellbarer Speicher) von bestimmten verwalteten Einheiten empfangen werden.

Vorbereitende Schritte

Achtung: Sie müssen die Lenovo Datenschutzerklärung akzeptieren, bevor Sie Daten an den Lenovo Support übertragen können.

Stellen Sie sicher, dass alle von XClarity Administrator benötigten Ports (darunter auch die Ports, die für die Call-Home-Funktion erforderlich sind) zur Verfügung stehen, bevor Sie die einen Service-Weiterleiter konfigurieren. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.

Stellen Sie sicher, dass eine Verbindung zu den Internetadressen des Service Providers hergestellt werden kann.

Wenn Sie Lenovo-Support verwenden möchten, stellen Sie sicher, dass eine Verbindung zu den Internetadressen von Call-Home-Funktion hergestellt werden kann. Weitere Informationen zu Firewalls finden Sie unter Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.

Wenn XClarity Administrator über einen HTTP-Proxy-Server auf das Internet zugreift, muss es sich um einen Non-Termination-Proxy handeln. Weitere Informationen über die Proxy-Einrichtung finden Sie unter Netzwerkzugriff konfigurieren in der Onlinedokumentation von XClarity Administrator.

Zu dieser Aufgabe

Mit einem *Service-Weiterleiter* wird festgelegt, an welchen Empfänger die Servicedatendateien nach einem aufgetretenen wartungsfähigen Ereignis gesendet werden sollen. Sie können bis zu 50 Service-Weiterleiter definieren.

Sie können für jeden Service-Weiterleiter automatisch Servicedaten an den Lenovo Support (*Call-Home-Funktion* genannt), an Ihren Lenovo Kundendiensttechniker mithilfe der Lenovo Upload-Funktionalität oder an einen anderen Service Provider senden. Informationen zum Einrichten eines Service-Weiterleiters für Call-Home-Funktion finden Sie unter Automatische Problembenachrichtigung einrichten. Informationen zur

Einrichten eines Service-Weiterleiters für die Lenovo Upload-Funktionalität finden Sie unter Automatische Problembenachrichtigung an die Lenovo Upload-Funktionalität.

Ist für SFTP ein Service-Weiterleiter konfiguriert und aktiviert, erfasst XClarity Administrator *automatisch* die Servicedatendateien und übermittelt sie an die angegebene SFTP-Site des bevorzugten Service Providers.

Für ThinkSystem V3 und V4 Server (mit XCC2 oder XCC3) speichert XClarity Administrator Servicedaten in zwei Dateien im Repository.

- **Servicedateien**. (.zip) Diese Datei enthält Serviceinformationen und Bestandsdaten in einem leicht lesbaren Format. Diese Datei wird automatisch an Ihren bevorzugten Service-Provider gesendet, wenn ein wartungsfähiges Ereignis auftritt.
- **Debugdatei**. (.tzz) Die Datei enthält alle Serviceinformationen, Bestand und Debugprotokolle zur Verwendung durch den Lenovo Support. Sie können diese Datei manuell an den Lenovo Support senden, wenn zusätzliche Informationen zur Problemlösung erforderlich sind.

Bei anderen Einheiten speichert XClarity Administrator Servicedaten (einschließlich Serviceinformationen, Bestand und Debugprotokolle) in einer einzelnen Servicedatei im Repository. Diese Datei wird an Ihren bevorzugten Service-Provider gesendet, wenn ein wartungsfähiges Ereignis auftritt.

Anmerkung: Falls die SFTP-Funktion bei mehreren Service-Weiterleitern für dieselbe Einheit konfiguriert ist, überträgt nur ein Service-Weiterleiter Servicedaten. Die verwendete Adresse und der verwendete Port hängen davon ab, welcher Service-Weiterleiter zuerst ausgelöst wird.

Vorgehensweise

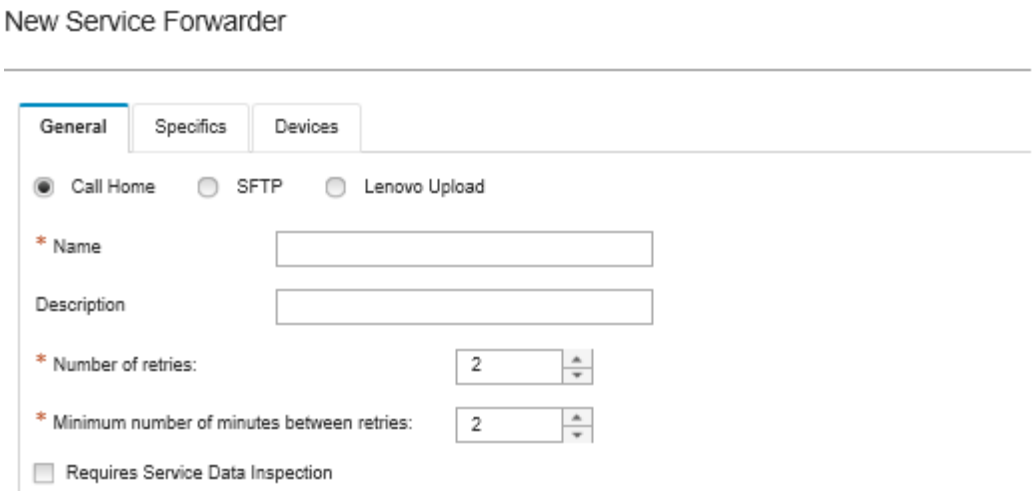
Gehen Sie wie folgt vor, um einen Service-Weiterleiter zu definieren und zu aktivieren.

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

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Service-Weiterleiter**, um die Seite Service-Weiterleiter zu öffnen.

Schritt 3. Klicken Sie auf das Symbol **Service-Weiterleiter erstellen** ( ), um das Dialogfenster Neuer Service-Weiterleiter zu öffnen.

Schritt 4. Klicken Sie auf die Registerkarte **Allgemein**.



1. Wählen Sie **SFTP** für den Service-Weiterleiter aus:
2. Geben Sie den Namen des Service-Weiterleiters und eine Beschreibung ein.

3. Geben Sie an, wie häufig die automatische Benachrichtigung wiederholt werden soll. Der Standardwert ist 2.
4. Geben Sie an, wie viele Minuten zwischen den Wiederholungen verstreichen sollen. Der Standardwert ist 2.
5. (Optional) Klicken Sie auf **Servicedatenüberprüfung erforderlich**, wenn die Servicedateien vor dem Versenden überprüft werden sollen. Optional können Sie die E-Mail-Adresse des Kontakts angeben, der bei einer erforderlichen Prüfung der Servicedatendateien benachrichtigt werden soll.

Schritt 5. Klicken Sie auf die Registerkarte **Bestimmt** und geben Sie die folgenden Informationen an:
- IP-Adresse und Portnummer des SFTP-Servers
- Benutzer-ID und Kennwort für die Authentifizierung am SFTP-Server

Schritt 6. Klicken Sie auf die Registerkarte **Einheit** und wählen Sie die verwalteten Einheiten und Ressourcengruppen aus, für die dieser Service-Weiterleiter Servicedaten weiterleiten soll.

Tipp: Um Servicedaten für alle verwalteten Einheiten (derzeitige und künftige) weiterzuleiten, aktivieren Sie das Kontrollkästchen **Alle Geräte abgleichen**.

Schritt 7. Klicken Sie auf **Erstellen**. Der Service-Weiterleiter wird zur Seite Service und Support hinzugefügt.

Schritt 8. Wählen Sie auf der Seite Service und Support in der Spalte **Status** die Option **Aktivieren** aus, um den Service-Weiterleiter zu aktivieren.

Schritt 9. Um zu verhindern, dass wartungsfähige Ereignisse, die in der Liste der ausgeschlossenen Ereignisse aufgeführt sind, automatisch Problemberichte öffnen, wählen Sie **Nein** neben der Frage **Sollen bei ausgeschlossenen Ereignissen Problemberichte geöffnet werden?** aus.

Schritt 10. Markieren Sie den Service-Weiterleiter und klicken Sie auf **Service-Weiterleiter testen**, um für den Service-Weiterleiter ein Testereignis zu generieren und die Kommunikation zwischen XClarity Administrator und den einzelnen Service Providern zu überprüfen.

Anmerkung: Der Service-Weiterleiter muss erst aktiviert werden, bevor er getestet werden kann.

Nach dieser Aufgabe

Auf der Seite Service und Support können Sie zudem folgende Aktionen ausführen:

- Wenn die Option **Servicedatenüberprüfung erforderlich** ausgewählt ist und bei einer der verwalteten Einheiten dieses Service-Weiterleiters ein wartungsfähiges Ereignis aufgetreten ist, müssen Sie die Servicedateien prüfen, bevor diese an den Service Provider weitergeleitet werden. Weitere Informationen finden Sie unter Servicedateien prüfen.
- Bearbeiten Sie die Informationen für den Service-Weiterleiter. Klicken Sie dazu im linken Navigationsbereich auf **Service-Weiterleiter** und dann auf das Symbol **Service-Weiterleiter bearbeiten** ( ).
- Aktivieren oder deaktivieren Sie einen Service-Provider. Klicken Sie dazu auf **Service-Weiterleiter** und wählen Sie in der Spalte **Status** entweder **Aktivieren** oder **Deaktivieren** aus.
- Löschen Sie den Service-Provider. Klicken Sie dazu auf **Service-Weiterleiter** und auf das Symbol **Service-Weiterleiter löschen** ( ).
- Definieren Sie die Support-Kontakt- und Standortinformationen einer bestimmten verwalteten Einheit. Klicken Sie dazu im linken Navigationsbereich auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf das Symbol **Kontaktprofil erstellen** ( ) oder **Kontaktprofil bearbeiten** ( ). Die Kontakt- und Standortinformationen für die verwaltete Einheit werden in den Problemdatensatz eingebunden, der im Lenovo-Support Center von der Call-Home-Funktion erstellt wird. Sofern eindeutige Kontakt- und Standortinformationen für eine verwaltete Einheit angegeben sind, werden diese in den Problemdatensatz einbezogen. Andernfalls werden die allgemeinen Informationen herangezogen, die in

XClarity Administrator in der Call-Home-Konfiguration angegeben sind (auf der Seite **Call-Home-Konfiguration** oder der Seite **Service-Weiterleiter**). Weitere Informationen finden Sie unter Support-Kontakte für bestimmte Einheiten definieren.

- Sammeln Sie die Servicedaten für eine bestimmte Einheit. Klicken Sie dazu auf **Endpunktaktionen**, wählen Sie die Einheit aus und klicken Sie dann auf das Symbol **Servicedaten sammeln** ( ). Weitere Informationen finden Sie unter Servicedaten für eine Einheit sammeln und herunterladen.

Weitere Informationen über diese Service und Support-Aufgaben finden Sie unter Mit Service und Unterstützung arbeiten.

Kennwort zur Service-Wiederherstellung ändern

Wenn Lenovo XClarity Administrator nicht mehr reagiert und nicht wiederhergestellt werden kann, können Sie Servicedaten und Protokolle für diese XClarity Administrator-Instanz sammeln und herunterladen. Das Kennwort zur Service-Wiederherstellung wird benötigt, um auf den Service zu zugreifen, mit dem Daten erfasst und heruntergeladen werden.

Vorbereitende Schritte

Sie müssen die Berechtigung **lxc-service-admin** oder **lxc-supervisor** haben, um das Kennwort ändern zu können.

Anmerkung: Notieren Sie sich das Kennwort für die spätere Verwendung. Sie können einen Verwaltungshub, der nicht reagiert, ohne dieses Kennwort wiederherstellen.

Weitere Informationen zur Verwendung des Kennworts zur Service-Wiederherstellung erhalten Sie unter Servicedateien für ein nicht reagierendes Lenovo XClarity Administrator sammeln und herunterladen.

Vorgehensweise

Gehen Sie wie folgt vor, um das Kennwort zur Service-Wiederherstellung zu ändern.

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

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Kennwort zur Service-Wiederherstellung**, um die Seite Kennwort zur Service-Wiederherstellung zu öffnen.

Schritt 3. Geben Sie das neue Kennwort ein.

Kennwörter müssen **16** bis **256** Zeichen lang sein, und mindestens einen oder mehrere Großbuchstaben und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.

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

Servicedateien prüfen

Sie können einen Service-Weiterleiter so konfigurieren, dass die Servicedateien geprüft und akzeptiert werden müssen, bevor sie gesendet werden.

Zu dieser Aufgabe

Mithilfe der Spalte **Erfordert Aufmerksamkeit** in der Tabelle des Service-Weiterleiters wird ermittelt, ob Servicedateien vor der Weiterleitung an den Service Provider geprüft werden müssen. Stehen eine oder mehrere Servicedateien zur Prüfung bereit, wird in der Spalte **Ja** angezeigt (andernfalls wird **Nein** angezeigt).

Vorgehensweise

Gehen Sie wie folgt vor, um bestimmte Servicedateien an den Service Provider weiterzuleiten.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite Service und Support wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Service-Weiterleiter**, um eine Tabelle mit Service-Weiterleitern zu öffnen.

Schritt 3. Klicken Sie auf den Link **Ja** in der Spalte **Erfordert Aufmerksamkeit**, um das Dialogfenster Erforderte Aufmerksamkeit mit einer Liste der zu prüfenden Servicedateien anzuzeigen.

Schritt 4. Wählen Sie mindestens eine Servicedatei aus und klicken Sie auf **Herunterladen**, um die Datei herunterzuladen und zu prüfen.

Schritt 5. Wählen Sie erneut mindestens eine Servicedatei aus und klicken Sie auf „Akzeptieren“, um mit der Datenübertragung an den angegebenen Service Provider zu beginnen.

Anmerkung: Wenn Sie stattdessen **Ablehnen** auswählen, werden die Servicedateien aus dem Dialogfenster Erfordert Aufmerksamkeit entfernt. Sie bleiben im Repository, bis sie gelöscht werden.

Support-Kontakte für bestimmte Einheiten definieren

Geben Sie Support-Kontaktinformationen an, die für eine oder mehrere bestimmte Einheiten eindeutig sind. Dies ist hilfreich, wenn Einheiten von mehreren Benutzern verwaltet werden.

Zu dieser Aufgabe

Wenn Support-Kontaktinformationen für eine Einheit definiert sind, werden diese spezifischen Angaben in die Problemdatensätze einbezogen, die von der Call-Home-Funktion automatisch für diese Einheit geöffnet werden. Falls keine spezifischen Informationen für die Einheit definiert sind, werden stattdessen allgemeine Kontaktinformationen für Lenovo XClarity Administrator herangezogen, die auf der Seite **Service-Weiterleiter** oder auf der Seite **Call-Home-Funktion-Konfiguration** angegeben wurden.

Vorgehensweise

Gehen Sie wie folgt vor, um Standort- und Support-Kontaktinformationen für eine bestimmte Einheit zu definieren.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite „Service und Support“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Endpunktaktionen**, um die Seite Endpunktaktionen anzuzeigen.

Schritt 3. Wählen Sie eine oder mehrere Einheiten aus und klicken Sie auf das Symbol **Kontaktprofil erstellen** ( ), um das Dialogfenster Kontaktprofil erstellen anzuzeigen.

Schritt 4. Geben Sie Daten in die erforderlichen Felder ein und klicken Sie auf **Speichern**.

Nach dieser Aufgabe

Wenn Sie die Kontaktinformationen für eine Einheit definiert haben, können Sie diese ändern oder löschen. Dazu markieren Sie die Einheit und klicken auf das Symbol **Kontaktprofil bearbeiten** ( ) oder **Kontaktprofil löschen** ( ).

Anmerkung: Wenn für die ausgewählte Einheit kein Kontaktprofil vorhanden ist, wird das Dialogfenster Kontaktprofil erstellen angezeigt, wenn Sie versuchen, das Profil bearbeiten.

Servicedaten für eine Einheit sammeln und herunterladen

Wenn bei einer verwalteten Einheit ein Problem auftritt, bei dessen Lösung die Hilfe eines Service Providers erforderlich ist, können Sie über die Lenovo XClarity Administrator-Webschnittstelle die Servicedaten (mit Protokollen, Serviceinformationen, Bestand und Debugprotokollen) für diese verwaltete Einheit manuell sammeln und herunterladen und so die Ermittlung der Problemursache unterstützen. Die Servicedaten werden als Servicedatei im TAR GZ-Format gespeichert. Sie können die Servicedateien herunterladen oder an Ihren bevorzugten Service Provider senden.

Zu dieser Aufgabe

Sie können bis zu 20 Erfassungsprozesse für Servicedaten gleichzeitig ausführen.

Für ThinkSystem V3 und V4 Server (mit XCC2 oder XCC3) speichert XClarity Administrator Servicedaten in zwei Dateien im Repository.

- **Servicedateien**. (.zip) Diese Datei enthält Serviceinformationen und Bestandsdaten in einem leicht lesbaren Format.
- **Debugdatei**. (.tzz) Die Datei enthält alle Serviceinformationen, Bestand und Debugprotokolle zur Verwendung durch den Lenovo Support.

Bei anderen Einheiten speichert XClarity Administrator Servicedaten (einschließlich Serviceinformationen, Bestand und Debugprotokolle) in einer einzelnen Servicedatei im Repository.

Wenn eine verwaltete Einheit ein wartungsfähiges Ereignis generiert, das Call-Home-Funktion auslöst (siehe Hardwareereignisse mit automatischer Benachrichtigung des Supports in der Onlinedokumentation von XClarity Administrator), erfasst XClarity Administrator automatisch Servicedaten für diese Einheit. Ist ein Service-Weiterleiter konfiguriert und aktiviert, sendet XClarity Administrator die Servicedatei auch an den angegebene Service Provider (z. B. an das Lenovo-Support Center über Call-Home-Funktion oder an eine SFTP-Site). Falls der Service Provider weitere Daten benötigt, werden Sie aufgefordert, Servicedaten für diese oder eine andere Einheit mithilfe des nachfolgend beschriebenen Verfahrens erneut zu sammeln.

Wenn das Servicedaten-Repository die maximale Kapazität erreicht hat, werden die ältesten Dateien gelöscht, um Speicherplatz für die neue Datei zu schaffen.

Anmerkungen:

- Bei Stacking-Switches können Sie Servicedaten für den *Master-Switch* und die *Standby-Switches* sammeln, auf die XClarity Administrator über die IP-Adressen zugreifen kann. Servicedaten für *Member-Switches* oder Switches im Schutzmodus können nicht erfasst werden.
- Ebenso können keine Servicedaten für Switches gesammelt werden, die zwar den Stacking-Modus unterstützen, sich aber im Standalone-Modus befinden.

Weitere Informationen über das Herunterladen von Servicedaten für XClarity Administrator finden Sie unter Lenovo XClarity Administrator Servicedaten sammeln und herunterladen.

Weitere Informationen über das manuelle Senden von Servicedaten an das Lenovo-Support Center finden Sie unter Übermitteln einer Serviceanforderung zu Hardwareproblemen an das Lenovo-Support Center.

Informationen zum Einrichten eines automatisierten Service-Weiterleiters für Automatische Problembenachrichtigung einrichten finden Sie unter .

Vorgehensweise

Gehen Sie wie folgt vor, um Servicedaten für eine angegebene verwaltete Einheit zu sammeln und herunterzuladen.

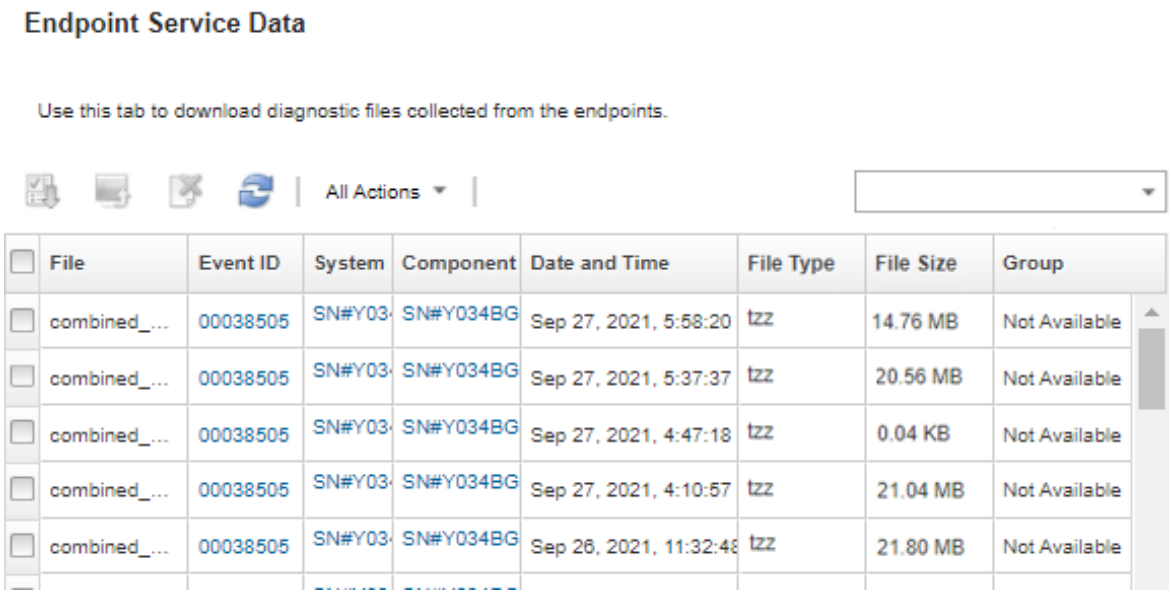
Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Endpunktaktionen**, um die Seite Endpunktaktionen anzuzeigen.

Schritt 3. Wählen Sie die Einheit aus, für die Servicedaten gesammelt werden sollen, und klicken Sie auf das Symbol **Servicedaten sammeln** ( ).

Schritt 4. Optional können Sie die Servicedatei auf dem lokalen System speichern.

Schritt 5. Klicken Sie im linken Navigationsbereich auf **Servicedaten für Einheit**, um die Seite Servicedaten für Einheit zu öffnen. Das Servicedaten-Archiv wird in der Tabelle aufgeführt.



Nach dieser Aufgabe

Auf der Seite Servicedaten für Einheit können Sie zudem folgende Aktionen ausführen.

- Senden Sie manuell Servicedateien direkt an einen Lenovo Kundendiensttechniker (siehe Servicedateien an den Lenovo Support senden).
- Senden Sie die Servicedateien manuell an das Lenovo Support-Center und öffnen Sie ein Service-Ticket (siehe Übermitteln einer Serviceanforderung zu Hardwareproblemen an das Lenovo-Support Center).
- Hängen Sie Servicedateien an ein vorhandenes Service-Ticket an und senden Sie es an das Lenovo Support-Center. Markieren Sie dazu die Dateien und klicken Sie auf **An Service-Ticket anfügen**. Wählen Sie anschließend das Service-Ticket aus und klicken Sie auf **Zuordnen**.
- Laden Sie Servicedateien herunter. Markieren Sie dazu mindestens eine Datei und klicken Sie auf das Symbol **Ausgewählte Servicedateien herunterladen** ( ). Wenn mehrere Dateien ausgewählt sind, werden diese vor dem Herunterladen in einer einzelnen TAR.GZ-Datei komprimiert.
- Entfernen Sie nicht mehr benötigte Servicedateien. Markieren Sie dazu mindestens eine Datei und klicken Sie auf das Symbol **Ausgewählte Servicedateien löschen** ( ).

Lenovo XClarity Administrator Servicedaten sammeln und herunterladen

Sie können Servicedaten manuell für Lenovo XClarity Administrator und bestimmte verwaltete Einheiten sammeln, die Informationen dann als Servicedatei im TAR.GZ-Format speichern und die Servicedaten anschließend herunterladen oder an Ihren bevorzugten Service Provider senden, um Unterstützung bei der Behebung von Problemen zu erhalten, sobald sie auftreten.

Zu dieser Aufgabe

Anmerkung: Stellen Sie sicher, dass *zurzeit kein* Job zum Herunterladen aller Servicedateien ausgeführt wird (siehe Jobs überwachen). Wenn ein Benutzer einen Job gestartet hat, der immer noch ausgeführt wird, muss dieser Benutzer auf die Beendigung des Jobs warten. Anschließend kann er erneut versuchen, alle Servicedateien herunterzuladen. Andernfalls schlägt der zweite Versuch fehl.

Konsultieren Sie den Lenovo-Support, um zu ermitteln, ob Sie alle oder bestimmte Servicedateien oder Protokolle herunterladen sollten.

Im Repository können bis zu 100 Servicedateien für XClarity Administrator gespeichert werden.

Wenn Sie Servicedaten und Protokolle von XClarity Administrator herunterladen, können Sie Servicedaten für bestimmte Einheiten in der heruntergeladenen Datei aufnehmen. Sie können Servicedateien verwenden, die bereits vorhanden sind oder aktuelle Servicedaten als Teil des Downloadprozesses sammeln.

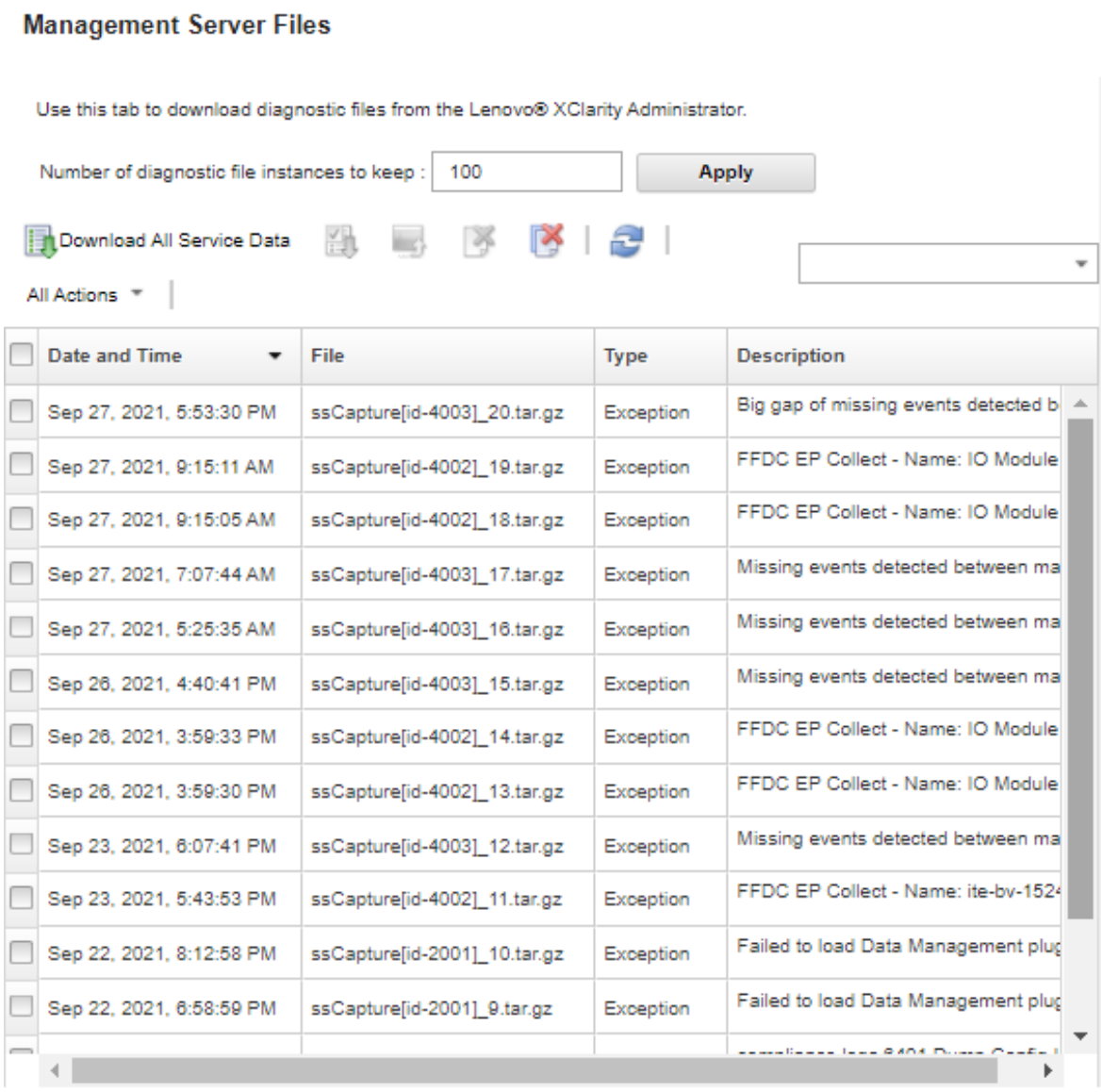
Achtung: Ändern Sie die Anzahl der zu behaltenden Servicedateien nur, wenn Sie vom Service Provider dazu aufgefordert werden.

Vorgehensweise

Gehen Sie wie folgt vor, um die XClarity Administrator Servicedaten oder Protokolle zu sammeln und herunterzuladen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Verwaltungsserverdateien**, um die Seite Verwaltungsserverdateien anzuzeigen.



Schritt 3. Wählen Sie aus, ob Sie alle Servicedaten oder alle Serviceprotokolle herunterladen möchten.

- Klicken Sie auf **Alle Servicedaten herunterladen**, um alle Servicedateien, Verwaltungsserverprotokolle und Servicedateien von bestimmten Einheiten herunterzuladen.
- Klicken Sie auf **Alle Aktionen → Alle Serviceprotokolle herunterladen**, um alle Verwaltungsserverprotokolle und Servicedateien von bestimmten Einheiten herunterzuladen.

In einer angezeigten Nachricht finden Sie eine Schätzung der herunterzuladenden Datenmenge. Je nach Dateianzahl und -größe kann es sehr lange dauern, alle Servicedateien herunterzuladen.

Schritt 4. Wählen Sie **Servicedaten einbeziehen, die bereits für verwaltete Einheiten gesammelt wurden** aus, wählen Sie die gewünschten Servicedatendateien aus, und klicken Sie anschließend auf **Übernehmen**.

Schritt 5. Wählen Sie **Verwaltete Einheiten auswählen, für die neue Servicedaten gesammelt werden sollen** aus, wählen Sie die Zieleinheiten aus, und klicken Sie anschließend auf **Übernehmen**.

Schritt 6. Senden Sie die Servicedateien an den Lenovo Support oder speichern Sie die Dateien auf dem lokalen System oder im Netzwerkspeicher. Die Servicedaten oder Protokolldateien werden vor dem Senden in eine einzelne .tar.gz-Datei komprimiert.

- Wenn Sie auf **Lenovo Upload** klicken, können Sie optional eine Fallnummer eingeben und dann auf **OK** klicken, um die Servicedaten zu sammeln und an die Lenovo Upload-Funktionalität zu übertragen.

  Anmerkung: Es wird empfohlen, dass Sie die Fallnummer bereithalten, damit der Lenovo Support die Datei leichter finden kann.
- Wenn Sie auf **Lokal speichern** klicken, verwenden Sie die Webbrowser-Funktionen, um die Datei auf dem lokalen System zu speichern.
- Wenn Sie auf **Auf Netzwerkspeicher speichern** klicken, geben Sie IP-Adresse, Anmeldeinformationen, Verzeichnis und Port ein und klicken Sie auf „Speichern“, um die Servicedateien an den fernen Server zu übertragen.

Nach dieser Aufgabe

Auf der Seite Verwaltungsserverdateien können Sie auch die folgenden Tasks ausführen:

- Laden Sie vorhandene Servicedateien herunter, indem Sie mindestens eine Datei markieren und auf **Alle Aktionen → Ausgewählte Servicedateien herunterladen** klicken.

  Sie können die Servicedateien an den Lenovo Support senden oder die Dateien auf dem lokalen System oder im Netzwerkspeicher speichern. Wenn mehrere Dateien ausgewählt sind, werden die Dateien vor dem Senden in eine einzelne TAR GZ-Datei komprimiert.
- Löschen Sie eine oder mehrere ausgewählte Servicedateien. Klicken Sie dazu auf das Symbol **Ausgewählte Servicedateien löschen** ( ).
- Löschen Sie alle Servicedateien. Klicken Sie dazu auf **Alle Servicedateien löschen** ( ).
- Löschen Sie alle Verwaltungsserverprotokolle, indem Sie auf **Alle Aktionen → Alle Serviceprotokolle löschen** klicken.

Servicedateien für ein nicht reagierendes Lenovo XClarity Administrator sammeln und herunterladen

Wenn Lenovo XClarity Administrator nicht mehr reagiert und nicht wiederhergestellt werden kann, können Sie Servicedaten und Protokolle für diese XClarity Administrator-Instanz sammeln und herunterladen. Servicedaten und Protokolle werden als Servicedatei im TAR.GZ-Format auf das lokale System heruntergeladen.

Vorbereitende Schritte

Die XClarity Administrator-Webschnittstelle funktioniert mit den folgenden Webbrowsern.
- Chrome™ 48.0 oder höher (55.0 oder höher für Ferne Konsole)
- Firefox® ESR 38.6.0 oder höher
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 oder höher (IOS7 oder höher und OS X)

Stellen Sie sicher, dass Sie sich bei der Webschnittstelle über ein System anmelden, das über eine Netzwerkverbindung mit dem System verfügt, auf dem XClarity Administrator installiert ist.

Vorgehensweise

Gehen Sie wie folgt vor, um die Servicedaten oder Protokolle für eine nicht reagierende XClarity Administrator-Instanz zu sammeln und herunterzuladen.

Schritt 1. Geben Sie in Ihrem Browser die IP-Adresse der virtuellen XClarity Administrator-Maschine mithilfe der folgenden URL ein.
`https://<IP_address>:58081`

Beispiele:

`https://192.0.2.0:58081`

Schritt 2. Geben Sie das Kennwort zur Service-Wiederherstellung im Feld **Kennwort** ein.

Dies ist das Kennwort, das Sie bei der Erstkonfiguration von XClarity Administrator angegeben oder in der Registerkarte **Kennwort zur Service-Wiederherstellung** auf der Seite „Service und Support“ geändert haben (siehe „Kennwort zur Service-Wiederherstellung ändern “ auf Seite 77).

Schritt 3. Wählen Sie die Dateitypen aus, die Sie sammeln möchten.
- **Alle Servicedaten**. Sammeln Sie alle Servicedateien und Verwaltungsserver-Protokolle.
- **Alle Serviceprotokolle**. Sammeln Sie alle Verwaltungsserver-Protokolle.

Schritt 4. Klicken Sie auf **Sammeln** und verwenden Sie anschließend die Webbrowser-Funktionen, um die Datei auf Ihrem lokalen System zu speichern. Die Servicedaten oder Protokolldateien werden vor dem Senden in eine einzelne .tar.gz-Datei komprimiert.

Übermitteln einer Serviceanforderung zu Hardwareproblemen an das Lenovo-Support Center

Wenn Call-Home-Funktion unter Verwendung eines Service-Weiterleiters aktiviert wird und auf einer verwalteten Einheit ein wartungsfähiges Ereignis auftritt, öffnet Lenovo XClarity Administrator automatisch ein Service-Ticket, erfasst Servicedaten und speichert diese als Archivdatei und überträgt die Service-Archivdatei an die Lenovo Upload-Funktionalität. Die Archiv-Servicedatei enthält die Servicedaten für das Gerät und für XClarity Administrator. Sie können die Servicedateien für eine verwaltete Einheit auch manuell sammeln, herunterladen und mit Lenovo-Support Center jederzeit an das XClarity Administrator senden. Mit dem Öffnen eines Service-Tickets wird der Lösungsfindungsprozess für Ihre Hardwareprobleme initiiert, da derLenovo-Support schnell und effizient die relevanten Informationen erhält. Die Lenovo-Kundendiensttechniker können mit der Fehlerbehebung beginnen, sobald Sie ein Service-Ticket ausgefüllt und geöffnet haben.

Lenovo setzt sich für Ihre Sicherheit ein. Servicedaten, die Sie normalerweise manuell auf die Lenovo Support-Website hochladen, werden mit TLS 1.2 oder höher automatisch über HTTPS an die Lenovo Upload-Funktionalität gesendet. Ihre Geschäftsdaten werden niemals übertragen. Der Zugriff auf Servicedaten der Lenovo Upload-Funktionalität ist auf autorisiertes Servicepersonal beschränkt.

Vorbereitende Schritte

Achtung: Sie müssen die Lenovo Datenschutzerklärung akzeptieren, bevor Sie Daten an den Lenovo Support übertragen können.

Stellen Sie sicher, dass die Call-Home-Kontaktinformationen konfiguriert sind.

1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite „Service und Support“ wird angezeigt.
2. Klicken Sie im linken Navigationsbereich auf **Call-Home-Funktion-Konfiguration**, um die Seite Call-Home-Konfiguration zu öffnen.
3. Geben Sie die Kontakt- und Standortinformationen ein.
4. Optional: Geben Sie die Systeminformationen an.
5. Klicken Sie auf **Übernehmen**.

Stellen Sie sicher, dass alle von XClarity Administrator benötigten Ports (darunter auch die Ports, die für die Call-Home-Funktion erforderlich sind) zur Verfügung stehen, bevor Sie die Call-Home-Funktion aktivieren. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.

Stellen Sie sicher, dass eine Verbindung zu den Internetadressen von Call-Home-Funktion hergestellt werden kann. Weitere Informationen zu Firewalls finden Sie unter Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.

Wenn XClarity Administrator über einen HTTP-Proxy-Server auf das Internet zugreift, muss der Proxy-Server die Standardauthentifizierung verwenden und ein Non-Termination-Proxy sein. Weitere Informationen über die Proxy-Einrichtung finden Sie unter Netzwerkzugriff konfigurieren in der Onlinedokumentation von XClarity Administrator.

Zu dieser Aufgabe

Auf der Seite Endpunktaktionen gibt die Spalte **Call-Home-Status** an, ob die Call-Home-Funktion auf dem Baseboard Management Controller aktiviert ist. Der Wert „Nicht anwendbar“ gibt an, dass die Call-Home-Funktion vom Management-Controller nicht unterstützt wird. XClarity Administrator kann eine Call-Home-Funktion unabhängig davon für eine Einheit ausführen, ob der Management-Controller die Call-Home-Funktion unterstützt. So stellen Sie fest, ob die Call-Home-Funktion für eine bestimmte Einheit unterstützt wird, siehe Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator.

Weitere Informationen über die Konfiguration und Aktivierung von Call-Home-Funktion für das automatische Senden von Servicedaten an das Lenovo-Support Center finden Sie unter Automatische Problembenachrichtigung an den Lenovo Support einrichten (Call-Home-Funktion).

Informationen zum manuellen Sammeln und Herunterladen von Servicedaten finden Sie unter Servicedaten für eine Einheit sammeln und herunterladen und Lenovo XClarity Administrator Servicedaten sammeln und herunterladen.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Service-Ticket manuell zu öffnen.

- Sofern die Call-Home-Funktion konfiguriert, aber nicht aktiviert ist, führen Sie die folgenden Schritte aus, um ein Service-Ticket zu öffnen, Servicedaten zu sammeln und herunterzuladen und die Daten an das Lenovo-Support Center zu senden:
  1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite „Service und Support“ wird angezeigt.
  2. Klicken Sie im linken Navigationsbereich auf **Endpunktaktionen**, um die Seite Endpunktaktionen anzuzeigen.
  3. Wählen Sie die Einheit aus und klicken Sie auf **Alle Aktionen → Call-Home-Funktion manuell ausführen**.

     Tipp: Sie können die Kommunikation mit dem Lenovo-Support Center testen und so prüfen, ob die Call-Home-Funktion korrekt eingerichtet ist (bei diesem Test werden keine Daten an den Lenovo-Support gesendet). Klicken Sie auf **Alle Aktionen → Call-Home-Funktion-Test durchführen**.
  4. Geben Sie eine Beschreibung des gemeldeten Problems einschließlich aller relevanter Ereignis-IDs ein.
  5. Klicken Sie auf **OK**.

- Falls Call-Home-Funktion nicht konfiguriert oder aktiviert ist, können Sie durch Anrufen der Lenovo Support-Hotline eine Serviceanforderung senden. Siehe Hilfe und technische Unterstützung anfordern für weitere Informationen.

Nach dieser Aufgabe

Sie können offene Service-Tickets auf der Seite **Status des Service-Tickets** überwachen (siehe Service-Tickets und Status anzeigen).

Probleme mit XClarity Administrator melden

Wenn Sie eine Serviceanforderung zur Meldung von Softwareproblemen (Verwaltungsserver) übermitteln, öffnet Lenovo XClarity Administrator ein Service-Ticket, sammelt Servicedaten vom Verwaltungsserver und sendet die Dateien über die Call-Home-Funktion an das Lenovo Support-Center. Durch Öffnen eines Service-Tickets wird der Lösungsfindungsprozess für Ihre Softwareprobleme gestartet, indem die relevanten Informationen des Lenovo Support schnell und effizient zur Verfügung gestellt werden. Die Lenovo Kundendiensttechniker können beginnen, an einer Lösung für Ihr Problem zu arbeiten, sobald Sie ein Service-Ticket ausgefüllt und geöffnet haben.

Lenovo setzt sich für Ihre Sicherheit ein. Service Daten, die Sie normalerweise manuell auf die Lenovo Support-Website hochladen, werden automatisch mit TLS 1.2 oder höher über HTTPS an Lenovo-Support Center gesendet. Ihre Geschäftsdaten werden nicht übertragen. Der Zugriff auf Servicedaten in Lenovo-Support Center ist auf autorisiertes Servicepersonal beschränkt.

Vorbereitende Schritte

Achtung: Sie müssen die Lenovo Datenschutzerklärung akzeptieren, bevor Sie Daten an den Lenovo Support übertragen können.

- Bevor Sie eine Problemanforderung zu XClarity Administrator übermitteln, sollten Sie Hilfe in den folgenden Ressourcen suchen:
  - Senden Sie Ideen zu XClarity Administrator, indem Sie auf das Benutzeraktionen-Menü (

) auf der XClarity Administrator Titelleiste und dann auf **Ideen einreichen** klicken oder direkt zur Website für Lenovo XClarity Ideation navigieren.
  - Sie können Fragen stellen und Antworten finden, indem Sie auf das Benutzeraktions-Menü (

) auf der XClarity Administrator Titelleiste und dann auf **Forum besuchen** klicken oder direkt zur Community-Forumswebsite für Lenovo XClarity navigieren.
  - Lesen Sie Website für den Lenovo Support für Rechenzentren, um mehr über aktuelle Tipps und Verfahren zu erfahren, die Sie zur Lösung von Problemen anwenden können, die möglicherweise bei XClarity Administrator auftreten. Diese *Tech-Tipps* stellen Vorgehensweisen zur Umgehung von Fehlern im Betrieb von XClarity Administrator zur Verfügung.

    So finden Sie die für Ihren Server verfügbaren Tech-Tipps:

    1. Navigieren Sie zu Website für den Lenovo Support für Rechenzentren.
    2. Geben Sie „XClarity Administrator“ im Feld **Suchen** ein.
    3. Klicken Sie im Abschnitt **Topartikel** auf **Alle anzeigen**, um alle Tipps anzuzeigen oder geben Sie Schlüsselwörter im Feld **Suchen** ein, um einen bestimmten Tipp zu finden.

       Tipp: Sie können die Liste nach **Relevanz**, **Beliebtheit** oder **Neueste** Tipps sortieren.
- Zum Übermitteln einer Serviceanforderung bei Problemen mit XClarity Administrator über den Lenovo Support ist Lenovo XClarity Pro erforderlich. Lenovo XClarity Pro umfasst die Berechtigung für Service und Unterstützung sowie die Lizenz für den vollständigen Funktionsumfang. Weitere Informationen zum

Kauf von Lenovo XClarity Pro erhalten Sie von Ihrem Lenovo-Ansprechpartner oder autorisierten Business Partner.

- Stellen Sie sicher, dass der **Lenovo Standard-Call-Home**-Weiterleiter konfiguriert und aktiviert ist (siehe Automatische Problembenachrichtigung an den Lenovo Support einrichten (Call-Home-Funktion)).
- Stellen Sie sicher, dass alle von XClarity Administrator benötigten Ports (darunter auch die Ports, die für die Call-Home-Funktion erforderlich sind) zur Verfügung stehen, bevor Sie die Call-Home-Funktion aktivieren. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.
- Stellen Sie sicher, dass eine Verbindung zu den Internetadressen hergestellt werden kann, die von der Call-Home-Funktion benötigt werden. Weitere Informationen zu Firewalls finden Sie unter Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.
- Wenn XClarity Administrator über einen HTTP-Proxy-Server auf das Internet zugreift, muss der Proxy-Server die Standardauthentifizierung verwenden und ein Non-Termination-Proxy sein. Weitere Informationen über die Proxy-Einrichtung finden Sie unter Netzwerkzugriff konfigurieren in der Onlinedokumentation von XClarity Administrator.

Zu dieser Aufgabe

Wenn bei Initiierung einer Call-Home-Funktion bereits eine andere Call-Home-Funktion ausgeführt wird, werden Daten für die erste Call-Home-Funktion erfasst und an den Lenovo Support gesendet, bevor die Daten für die zweite Call-Home-Funktion erfasst und übermittelt werden. Daher kann es möglicherweise beim Senden der Daten zur zweiten Call-Home-Funktion Verzögerungen geben.

Vorgehensweise

Gehen Sie wie folgt vor, um ein Problem mit XClarity Administrator zu melden.

- Wenn die Call-Home-Funktion konfiguriert ist, führen Sie die folgenden Schritte aus, um ein Service-Ticket zu öffnen, Servicedaten für den Verwaltungsserver zu sammeln und herunterzuladen und die Daten an das Lenovo Support-Center zu senden:
  1. Klicken Sie in der Titelleiste von XClarity Administrator auf **Problem melden**. Der Verwaltungsserver testet die Verbindung mit dem Lenovo Support.
  2. Klicken Sie auf **Fortfahren**, um das Dialogfenster Softwareprobleminformationen anzuzeigen.
  3. Geben Sie Ihre Lenovo Kundennummer an, die Sie beim Kauf von Lenovo XClarity Pro erhalten haben.
  4. Stellen Sie Informationen über das Problem bereit, einschließlich der relevanten Ereignis-IDs und Einheiten, die mit dem Fehler verbunden sind.

     Anmerkungen:

     – Die Serviceprotokolle und -daten für den Verwaltungsserver werden automatisch erfasst und gesendet.

     – Wenn Sie Einheiten ausgewählt haben, die mit dem Problem zusammenhängen, werden auch die Servicedaten für diese Einheiten automatisch erfasst und übermittelt.

     – Sie können weitere Dateien anhängen, um dem Lenovo Support die Fehlerbehebung zu erleichtern (z. B. Screenshots und Videoclips), indem Sie auf **Datei hochladen** klicken.
  5. Stellen Sie Schritte zum Reproduzieren des Problems zur Verfügung.
  6. Wählen Sie den funktionellen Bereich aus, in dem das Problem aufgetreten ist.
  7. Klicken Sie auf **Weiter**.
  8. Geben Sie Informationen über den primären Ansprechpartner im Zusammenhang mit dem Problem an. Um weitere Kontaktpersonen anzugeben, klicken Sie auf **Weiteren Kontakt hinzufügen**.

9. Klicken Sie auf **An Lenovo senden**, um ein Service-Ticket mit dem Lenovo Support zu erstellen.

- Falls die Call Home-Funktion nicht konfiguriert oder konfiguriert, aber nicht aktiviert ist, können Sie durch Anrufen der Lenovo Support-Hotline eine Serviceanforderung senden. Siehe Hilfe und technische Unterstützung anfordern für weitere Informationen.

Nach dieser Aufgabe

Sie können offene Service-Tickets auf der Seite **Status des Service-Tickets** überwachen (siehe Service-Tickets und Status anzeigen).

Sie können weitere Dateien an das geöffnete Service-Ticket anhängen, nachdem die Informationen zum Problem übermittelt wurden.

1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite „Service und Support“ wird angezeigt.
2. Klicken Sie im linken Navigationsbereich auf **Status des Service-Tickets**, um die Seite Status des Service-Tickets anzuzeigen.
3. Wählen Sie das Service-Ticket aus.
4. Klicken Sie auf **Servicedatei anhängen** und wählen Sie dann das Servicedatenarchiv oder eine andere Datei aus, die Sie an das Service-Ticket anhängen und an den Lenovo Support senden möchten.

Servicedatei an ein offenes Service-Ticket anhängen

Sie können Servicedatendateien für eine bestimmte Einheit an ein offenes Service-Ticket im Lenovo-Support Center anhängen.

Vorbereitende Schritte

Achtung: Sie müssen die Lenovo Datenschutzerklärung akzeptieren, bevor Sie Daten an den Lenovo Support übertragen können.

Zu dieser Aufgabe

Sie können weitere Dateien zu einem offenen Service-Ticket hinzufügen, z. B. aktuelle Servicedatenarchive, Screenshots und Videoclips.

Vorgehensweise

Gehen Sie wie folgt vor, um eine Servicedatei zu einem offenen Service-Ticket hinzuzufügen.

- Über die Seite **Servicedaten für Einheit**:
  1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite „Service und Support“ wird angezeigt.
  2. Klicken Sie im linken Navigationsbereich auf **Endpunkt-Servicedaten**, um die Seite Servicedaten für Endpunkt zu öffnen.
  3. Wählen Sie eine Service-Datei aus, die Sie an das Serviceticket anhängen möchten.
  4. Klicken Sie auf **Aktionen → An Service-Ticket anhängen** und wählen Sie dann das Service-Ticket aus, an das Sie die Servicedatei anhängen möchten.
  5. Klicken Sie auf **Zuordnen**, um die Datei an das Service-Ticket anzuhängen und an den Lenovo Support zu senden.
- Über die Registerkarte **Status des Service-Tickets**:

1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite „Service und Support“ wird angezeigt.
2. Klicken Sie im linken Navigationsbereich auf **Status des Service-Tickets**, um die Seite Status des Service-Tickets anzuzeigen.
3. Wählen Sie das Service-Ticket aus.
4. Klicken Sie auf **Servicedatei anhängen** und wählen Sie dann die Servicedatei aus, die Sie an das Service-Ticket anhängen möchten, und senden Sie dieses an den Lenovo Support.

Service-Tickets und Status anzeigen

Sie können Informationen zu Service-Tickets anzeigen, die manuell oder automatisch durch die Call-Home-Funktion an das Lenovo-Support Center übermittelt wurden, einschließlich des aktuellen Status und der zugeordneten Servicedateien, die an das Lenovo-Support Center gesendet wurden, und Service-Tickets, die von anderen Supportservices als der Call-Home-Funktion erstellt wurden.

Vorgehensweise

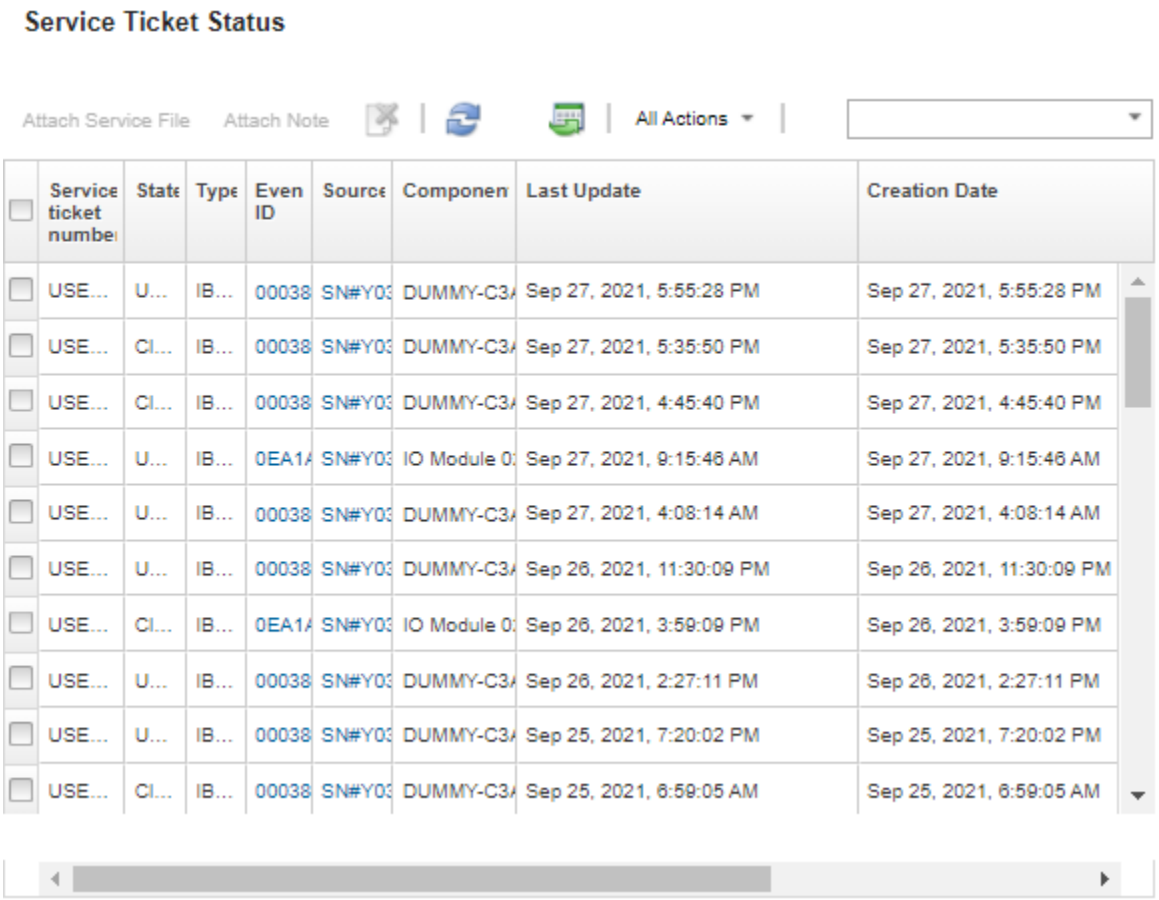
Um Service-Tickets in XClarity Administrator anzuzeigen, klicken Sie auf **Verwaltung → Service und Support**. Wählen Sie dann die Registerkarte **Service-Ticket-Status** im linken Navigationsfenster aus, um die Seite Service-Ticket-Status anzuzeigen.

Die Spalte **Service-Ticketnummer** zeigt die ID des Service-Tickets an, das für ein Ereignis geöffnet wurde. Wenn mehrere Service-Tickets für dasselbe Ereignis (z. B. eines beim Lenovo Support und ein weiteres in einem ServiceNow-Integrator) geöffnet wurden, existiert für jedes Service-Ticket eine separate Zeile in der Tabelle. Das entsprechende Service-Ticket finden Sie in der Spalte **Querverweis-ID**. Wenn z. B. die **Service-Ticketnummer** die Service-Ticket-ID des Lenovo Support angibt, zeigt die **Querverweis-ID** die ServiceNow-Service-Ticket-ID und umgekehrt.

Die Spalte **Typ** gibt den Typ des Service-Tickets an, der in der Spalte **Service-Ticketnummer** aufgeführt ist. Der Service-Ticket-Typ kann einer der folgenden Werte sein:
- **IBM Call-Home-Funktion**
- **IBM Call-Home-Test**
- **Lenovo Call-Home**
- **Lenovo Call-Home-Test**
- **Lenovo Call-Home per Software**
- **Lenovo Call-Home-Test per Software**
- **Cherwill**
- **ServiceNow**

Ein Service-Ticket kann einen der folgenden Status aufweisen:
- **Aktiv**
- **Abgebrochen**
- **Behoben**
- **Unbekannt**

Die Spalte **Querverweis-ID** enthält die ID des Service-Tickets von externen Supportservices (z. B. ServiceNow), die sich auf das Lenovo Service-Ticket beziehen.



Nach dieser Aufgabe

Auf der Seite Status des Service-Tickets können Sie die folgenden Schritte für ein ausgewähltes Service-Ticket ausführen.

- Hängen Sie eine Servicedatei für eine bestimmte Einheit an ein offenes Service-Ticket im Lenovo-Support Center an, indem Sie auf **Servicedatei anhängen** klicken (siehe Servicedatei an ein offenes Service-Ticket anhängen).
- Fügen Sie im Lenovo-Support Center eine Notiz an ein geöffnete Service Ticket, indem Sie auf **Notiz anfügen** klicken.
- Löschen Sie ein Service-Ticket, indem Sie auf das Symbol **Service-Tickets löschen** ( ) klicken. Sie können nur Service-Tickets löschen, die *nicht* den Status „Aktiv“ haben.
- Rufen Sie die neuesten Informationen zu allen geöffneten Service-Tickets vom Lenovo-Support Center ab, indem Sie auf das Symbol **Service-Ticket-Status aktualisieren** ( ) klicken.
- Exportieren Sie den Status für alle Service-Tickets in eine CSV-Datei, indem Sie auf das Symbol **Alle als CSV exportieren** ( ) klicken.

Servicedateien an den Lenovo Support senden

Wenn Sie zur Lösung eines Problems mit dem Lenovo Support zusammenarbeiten, können Sie Servicedateien manuell mit der Lenovo Upload-Funktionalität direkt an den Lenovo Support-Mitarbeiter übertragen.

Vorbereitende Schritte

Achtung: Sie müssen die Lenovo Datenschutzerklärung akzeptieren, bevor Sie Daten an den Lenovo Support übertragen können.

Vorgehensweise

Gehen Sie wie folgt vor, um Servicedateien direkt an den Lenovo Support zu übertragen.

Schritt 1. Konfigurieren Sie die Lenovo Upload-Funktionalität.

a. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite Service und Support wird angezeigt.

b. Klicken Sie im linken Navigationsbereich auf **Lenovo Upload-Funktionalität**.

c. Geben Sie eine E-Mail-Adresse ein.

d. Klicken Sie auf **Übernehmen**.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Verwaltungsserverdateien** oder **Endpunkt-Servicedaten**, je nach den Protokollen, die Sie senden möchten.

Schritt 3. Wählen Sie eine oder mehrere Servicedateien zum Senden an den Lenovo Support aus und klicken Sie auf das Symbol **Ausgewählter Lenovo Upload** ( ). Ein Dialogfenster mit Informationen zum Lenovo Upload wird angezeigt.

Schritt 4. Geben Sie optional eine Fallnummer ein.

Schritt 5. Klicken Sie auf **OK**, um die Servicedateien zu übertragen.

Protokolleinstellungen für Verwaltungsserver konfigurieren

Die Protokolleinstellungen werden vom Lenovo-Support nur zur Anpassung der Protokollgranularität verwendet.

Zu dieser Aufgabe

Achtung: Ändern Sie die Einstellungen auf dieser Seite nur, wenn Sie vom Lenovo-Support dazu aufgefordert werden.

Vorgehensweise

Gehen Sie wie folgt vor, um die Protokollierungseinstellungen zu konfigurieren.

Schritt 1. Klicken Sie in der Lenovo XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite Service und Support wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Serverprotokollierungseinstellungen**, um die Seite Serverprotokollierungseinstellungen anzuzeigen.

Schritt 3. Passen Sie die einzelnen Einstellungen laut Anweisung vom Lenovo-Support an und klicken Sie auf **Übernehmen**.

Nach dieser Aufgabe

Sie können auf der Seite Serverprotokollierungseinstellungen zudem die folgenden Schritte ausführen.

- Laden Sie Protokoll-Konfigurationseinstellungen des Verwaltungsservers auf das lokale System herunter, indem Sie auf **LogBack herunterladen** klicken. Die Einstellungen werden als Datei mit dem Namen „logback.xml“ in das Standard-Downloadverzeichnis heruntergeladen.
- Stellen Sie die Standardeinstellungen wieder her, indem Sie auf **Standardwerte wiederherstellen** klicken.

- Importieren Sie eine Konfigurationsdatei, indem Sie auf **Konfigurationsdatei hochladen** klicken und die Datei für den Import in XClarity Administrator auswählen. Die Datei muss den Namen „logback.xml“ haben.

  Wichtig: Sie sollten nur Konfigurationsdateien importieren, die Sie vom Lenovo Kundendiensttechniker erhalten haben, und auch nur auf Anweisung des Kundendiensttechnikers.

Call-Home-Funktion auf allen verwalteten Einheiten erneut aktivieren

Wenn Sie einen Call-Home-Funktion Service-Weiterleiter in Lenovo XClarity Administrator aktivieren, wird Call-Home-Funktion auf allen verwalteten Einheiten deaktiviert, damit keine doppelten Problemdatensätze generiert werden. Sollen die Einheiten nicht mehr mit XClarity Administrator verwaltet werden oder wenn Sie Call-Home-Funktion in XClarity Administrator deaktivieren möchten, können Sie Call-Home-Funktion auf allen verwalteten Einheiten über XClarity Administrator wieder aktivieren – anstatt Call-Home-Funktion später auf jeder einzelnen Einheit erneut zu aktivieren.

Zu dieser Aufgabe

Achtung: Die erneute Aktivierung von Call-Home-Funktion auf allen Einheiten führt möglicherweise nicht dazu, dass Call-Home-Funktion auf diesen Einheiten betriebsbereit ist. Unter Umständen muss jede Einheit einzeln konfiguriert werden, wenn die Konfiguration nicht vorher durchgeführt wurde.

Obwohl XClarity Administrator Call-Home-Funktion für ThinkAgile und ThinkSystem Einheiten unterstützt, unterstützt der Baseboard Management Controller für manche ThinkAgile und ThinkSystem Einheiten kein Call-Home-Funktion. Daher können Sie die Call-Home-Funktion auf diesen Einheiten weder aktivieren noch deaktivieren. Die Call-Home-Funktion kann nur für diese Einheiten auf der Ebene XClarity Administrator aktiviert werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Call-Home-Funktion auf allen verwalteten Einheiten erneut zu aktivieren.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite „Service und Support“ wird angezeigt.

Schritt 2. Klicken Sie im linken Navigationsbereich auf **Service-Weiterleiter**, um die Seite Service-Weiterleiter zu öffnen.

Schritt 3. Ändern Sie den Status für alle Service-Weiterleiter für Call Home, einschließlich „Standard-Call Home“, in **Deaktiviert**.

Schritt 4. Klicken Sie im linken Navigationsbereich auf **Endpunktaktionen**, um die Seite Endpunktaktionen anzuzeigen.

Schritt 5. Klicken Sie auf **Alle Aktionen → Call-Home-Funktion-Funktion auf allen Einheiten aktivieren**, um Call-Home-Funktion auf sämtlichen verwalteten Einheiten zu aktivieren.

Regelmäßig Daten an Lenovo senden

Sie können optional zulassen, dass XClarity Administrator Informationen zur Verwendung des Produkts und zu Änderungen in Ihrer Umgebung sammelt und diese Daten regelmäßig an Lenovo sendet. Lenovo verwendet diese Daten, um Ihre Erfahrungen mit den Lenovo Produkten und dem Lenovo Support zu verbessern.

Vorbereitende Schritte

Achtung: Sie müssen die Lenovo Datenschutzerklärung akzeptieren, bevor Sie Daten an den Lenovo Support übertragen können.

Zu dieser Aufgabe

Sie können die folgenden Datentypen sammeln und an Lenovo senden.

- **Nutzungsdaten**

  Durch die Analyse der Nutzungsdaten mehrerer Benutzer kann Lenovo weitere Informationen zur Verwendung von XClarity Administrator erfassen. Auf diese Weise erfährt Lenovo, welche Funktionen am häufigsten verwendet werden, und kann mögliche Fehler, die bei den XClarity Administrator-Instanzen auftreten, erkennen. Diese Daten können dann verwendet werden, um zukünftige Investitionsentscheidungen über Produktverbesserungen zu treffen, sodass diese Ihren Anforderungen besser entsprechen, es können Probleme in zukünftigen Versionen behoben und die Produktqualität verbessert werden.

  Wenn Sie zustimmen, Nutzungsdaten an Lenovo zu senden, werden die folgenden Daten gesammelt und wöchentlich gesendet. Diese Daten sind *anonym*. Es werden keine privaten Daten (einschließlich Seriennummern, UUIDs, Hostnamen, IP-Adressen und Benutzernamen) gesammelt oder an Lenovo gesendet.
  - Protokoll der ausgeführten Aktionen
  - Liste der ausgelösten Ereignisse und des Zeitstempels, zu dem Sie ausgelöst wurden
  - Liste der ausgelösten Prüfeignisse und des Zeitstempels, zu dem Sie ausgelöst wurden
  - Liste der ausgeführten Jobs sowie Informationen über Erfolg oder Misserfolg für die einzelnen Jobs
  - XClarity Administrator-Metriken, einschließlich Speicherauslastung, Prozessorauslastung und Plattenspeicherplatz
  - Beschränkte Bestandsdaten über alle verwalteten Einheiten
- **Hardwaredaten**

  Durch die Analyse der Hardwaredaten mehrerer Benutzer kann Lenovo Informationen zu Hardwareänderungen erhalten, die regelmäßig vorgenommen werden. Diese Daten können verwendet werden, um die prädiktiven Analysen sowie Ihre Service- und Unterstützungserfahrung zu verbessern, indem die entsprechenden Teile in den richtigen Regionen aufgestockt werden.

  Wenn Sie zustimmen, Hardwaredaten an Lenovo zu senden, werden die folgenden Daten gesammelt und regelmäßig gesendet. Diese Daten sind *nicht anonym*. Zu den Hardwaredaten gehören Attribute, z. B. UUIDs und Seriennummern. IP-Adressen oder Hostnamen fallen nicht darunter.
  - **Tägliche Hardwaredaten**. Jede Bestandsänderung umfasst die folgenden Daten.
    - Ereignis zur Bestandsänderung (FQXHMDM0001I)
    - Änderungen der Bestandsdaten für die Einheit, die diesem Ereignis zugeordnet ist
  - **Wöchentliche Hardwaredaten**. Bestandsdaten sind für alle verwalteten Einheiten inbegriffen.

Wenn Daten an Lenovo gesendet werden, werden sie über HTTPS von der XClarity Administrator-Instanz an die Lenovo Upload-Funktionalität übertragen. REST-APIs werden über diese HTTPS-Verbindung aufgerufen, um die Daten zu senden. Ein bereits vorinstalliertes Zertifikat auf XClarity Administrator wird für die Authentifizierung verwendet. Wenn eine XClarity Administrator-Instanz keinen direkten Zugriff auf das Internet hat, aber ein Proxy für XClarity Administrator konfiguriert ist, werden die Daten über diesen Proxy übertragen.

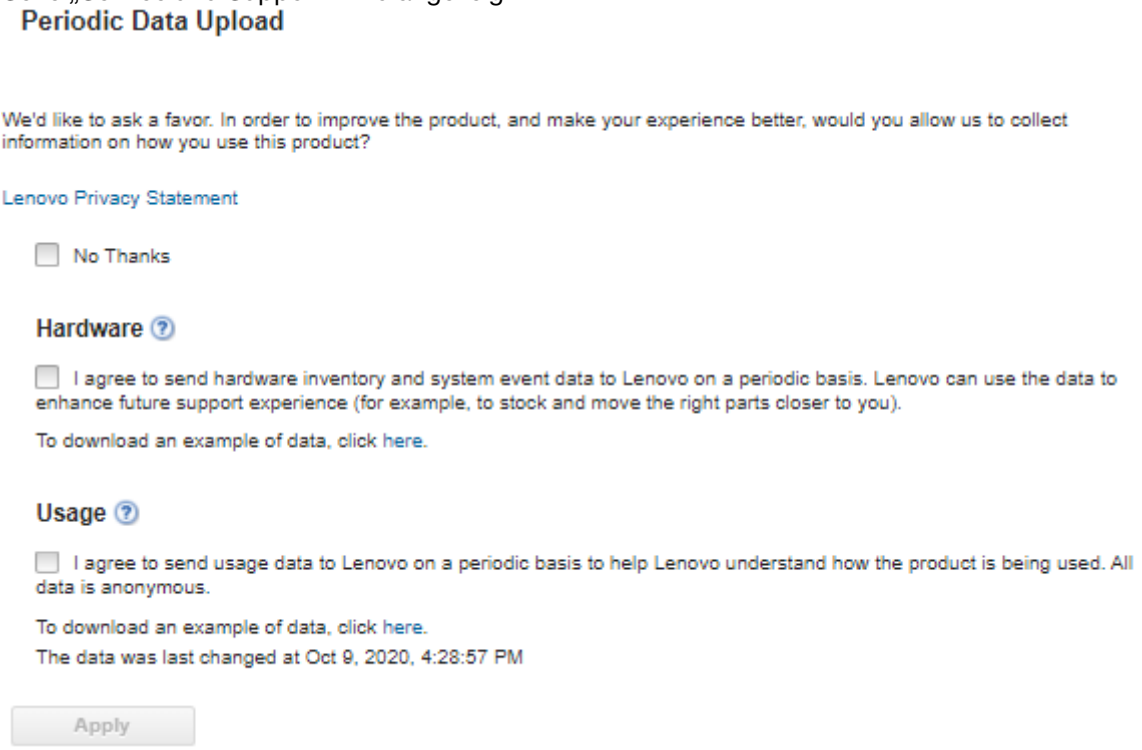
Anschließend werden die Daten in das Lenovo Customer Care-Repository verschoben, wo sie für bis zu 5 Jahre gespeichert werden. Dieses Repository dient der sicheren Aufbewahrung und wird auch für an Lenovo gesendete Debugdaten verwendet, die zur Problembehandlung benötigt werden. Es wird von den meisten Lenovo Server-, Speicher- und Switch-Produkten verwendet.

Im Lenovo Customer Care Repository werden Abfragen für alle Hardware- und Nutzungsdaten ausgeführt und es werden dem Lenovo Produktteam Diagramme zur Analyse zur Verfügung gestellt.

Vorgehensweise

Gehen Sie wie folgt vor, um XClarity Administrator das Sammeln und Senden von Kundendaten an Lenovo zu ermöglichen.

Schritt 1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Service und Support**. Die Seite „Service und Support“ wird angezeigt.



Schritt 2. Klicken Sie im linken Navigationsbereich auf **Regelmäßiges Hochladen von Daten**, um die Seite Regelmäßiges Hochladen von Daten zu öffnen.

Schritt 3. Hier können Sie sich optional damit einverstanden erklären, Hardware- und Nutzungsdaten an Lenovo zu senden.

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

Nach dieser Aufgabe

Wenn Sie zustimmen, Ihre Daten zu senden, können Sie auf dieser Seite die folgenden Aktionen ausführen.

- Den Zeitpunkt der letzten Datenübermittlung ermitteln, indem Sie sich das Datum unter dem entsprechenden Kontrollkästchen ansehen.
- Das zuletzt übermittelte Datenarchiv herunterladen, indem Sie auf den Link unter dem entsprechenden Kontrollkästchen klicken.

Beispiel von Nutzungdaten

Wenn Sie zustimmen, Nutzungsdaten an Lenovo zu senden, werden die folgenden Beispieldaten gesammelt und regelmäßig gesendet.

XClarity Administrator-Metrikdaten

```
Timestamp   cpuLoad  usedSpace  usedRam  usedJavaCpu  usedJavaRam
1497861662  0.99     12.6225    13.3644  71.9         9.4
1497861668  1.23     12.6343    18.5676  0            14.4
1497861674  1.89     12.6371    19.6182  77.9         15.3
1497861679  1.98     12.6442    23.0782  37.9         18.6
1497861685  2.06     12.647     23.2412  77.9         18.6
1497861690  2.14     12.6654    25.3697  10           19
1497861696  2.37     7.75276    25.8952  2            19.4
1497861701  2.34     7.76077    26.0184  24           19.5
1497861056  2.55     7.77003    26.4222  85.9         19.7
1497861061  2.82     7.77877    26.5485  159.9        19.7
1497861067  3        7.7954     27.0066  131.9        20
```

Aktionsdaten

```
/updates/images/userdefined.png={"GET"\:1}
/config/profile={"GET"\:865}
/node/AD9547AB3C8011E79DCC000E1E7D4EE0={"GET"\:1}
/usage/data={"GET"\:12}
/compliancePolicies/persistedResult={"GET"\:3}
/jobs/88={"PUT"\:31}
/osdeployment/rest/internal/event/aicc={"POST"\:186}
/aicc={"GET"\:56}
/updates/images/powerStates.png={"GET"\:2}
/jobs/84={"PUT"\:3}
/updates/images/ActionSprite.png={"GET"\:1}
/nodes/AD9547AB3C8011E79DCC000E1E7D4EE0/lock={"GET"\:1,"PUT"\:2}
/updates/customUI/gridxExtensions/Mark.js={"GET"\:2}
/updates/images/ac22_deleteall_inactive_24.png={"GET"\:1}
/service/forwarders={"GET"\:12}
/nodes/7C64A0A8413811E7A6C6000E1EB35A90/lock={"GET"\:1,"PUT"\:2}
/config/deploy/status={"GET"\:865}
/node/235435543C7D11E7AA13000E1E7D54A0={"GET"\:1}
/updates/ApplyActivateUpdates.js={"GET"\:2}
/discovery={"GET"\:3}
/userAccountSettings={"GET"\:1}
/discoverRequest/jobs/610={"GET"\:9}
/compliancePolicies/events={"POST"\:25}
/events/audit={"GET"\:5}
/updates/images/st22_filterRunning_24.png={"GET"\:2}
/updates/images/st16_running_24.gif={"GET"\:1}
/updates/images/complianceStatus.png={"GET"\:2}
/usage={"GET"\:4}
/updates/json/firmwareRepository/exportPayloads.json={"GET"\:1}
/updates/images/ac22_collapseall_OneUI_24.png={"GET"\:3}
/chassis/0AC502DEFCD6419FB20FB5A9A49D0293={"GET"\:17}
/updates/images/ac22_copy_inactive_24.png={"GET"\:1}
/service/endPoint/collectedArchives={"GET"\:4}
/jobs/lock/88={"DELETE"\:1}
/updates/customUI/gridxModules/IndirectSelect.js={"GET"\:2}
/stgupdates/inventory/events={"POST"\:70}
/electronicDownload={"GET"\:1}
/updates/images/st16_firm_normal_24.png={"GET"\:3}
/updates/images/st16_Empty_24.png={"GET"\:1}
/updates/json/compliancePolicy/getCompByUxsp.json={"GET"\:1}
```

Ereignisdaten

```
{
   "action":100,
```

```
   "commonEventID":"FQXHMSE0203I",
   "cn":"1",
   "eventClass":200,
   "eventID":"FQXHMSE0203I",
   "flags":"",
   "mtm":"",
   "msgID":"",
   "service":100,
   "severity":200},
   "timeStamp":"2017-06-16T15:56:06Z"
}
```


Prüfdaten


```
{
   "action":100,
   "commonEventID":"FQXHMSE0200I",
   "cn":"1",
   "eventClass":200,
   "eventID":"FQXHMSE0200I",
   "flags":"",
   "msgID":"",
   "mtm":"",
   "service":100,
   "severity":200,
   "timeStamp":"2017-06-16T15:56:06Z"
}
```


Bestandsdaten


```
-377665639={
   "firmwareList"\:[{
      "build"\:"2PET41C",
      "date"\:"2017-12-19T05\:00\:00Z",
      "name"\:"CMM firmware",
      "type"\:"CMM firmware",
      "version"\:""
   }],
   "mtm"\:"/",
   "productName"\:"",
   "stillManaged"\:"true",
   "uuid"\:"-377665639"
}
-177044123={
   "firmwareList"\:[{
      "build"\:"A3E117D",
      "date"\:"2018-01-26T00\:00\:00Z",
      "name"\:"UEFI Firmware/BIOS",
      "type"\:"UEFI",
      "version"\:"A3E117D-1.80"
   },{
      "build"\:"A3E113C",
      "date"\:"2016-12-16T00\:00\:00Z",
      "name"\:"UEFI Backup Firmware/BIOS",
      "type"\:"UEFI-Backup",
      "version"\:"A3E113C-1.60"
   },{
      "build"\:"DSALB1Q",
      "date"\:"2018-05-15T00\:00\:00Z",
      "name"\:"DSA Diagnostic Software",
      "type"\:"DSA",
      "version"\:"DSALB1Q-10.3"
```

```
   },{
      "build"\:"TCOO39A",
      "date"\:"2018-01-19T00\:00\:00Z",
      "name"\:"IMM2 Firmware",
      "type"\:"IMM2",
      "version"\:"TCOO39A-4.70"
   },{
      "build"\:"TCOO39A",
      "date"\:"2018-01-19T00\:00\:00Z",
      "name"\:"IMM2 Backup Firmware",
      "type"\:"IMM2-Backup",
      "version"\:"TCOO39A-4.70"
   }],
   "mtm"\:"7162/CC1",
   "productName"\:"Lenovo Flex System x240 Compute Node",
   "stillManaged"\:"true",
   "uuid"\:"-177044123"
}
-734000615={
   "firmwareList"\:[],
   "mtm"\:"8721/HC1",
   "productName"\:"IBM Flex System Enterprise Chassis Midplane Card"},
   "stillManaged"\:"true",
   "uuid"\:"-734000615"
1150304995={
   "firmwareList"\:[{
      "date"\:"06/12/2014",
      "build"\:"",
      "name"\:"Boot ROM",
      "type"\:"Boot ROM",
      "version"\:"7.8.5.0"
   },{
      "date"\:"06/12/2014",
      "build"\:"",
      "name"\:"Main Application 1",
      "type"\:"Main Application 1",
      "version"\:"7.8.5.0"
   },{
      "date"\:"03/29/2013",
      "build"\:"",
      "name"\:"Main Application 2",
      "type"\:"Main Application 2",
      "version"\:"7.5.3.0"
   }],
   "mtm"\:"/",
   "productName"\:"IBM Flex System Fabric EN4093 10Gb Scalable Switch",
   "stillManaged"\:"true",
   "uuid"\:"1150304995"
}
-1050714125={
   "firmwareList"\:[{
      "date"\:"04/19/2016",
      "build"\:"",
      "name"\:"Main Application",
      "type"\:"Main Application",
      "version"\:"7.4.1c"
   }],
   "mtm"\:"/",
   "productName"\:"IBM Flex System FC5022 12-port 16Gb ESB SAN Scalable Switch",
   "stillManaged"\:"true",
   "uuid"\:"-1050714125"
```

}

Beispiel-Hardwaredaten

Wenn Sie zustimmen, Hardwaredaten an Lenovo zu senden, werden die folgenden Beispieldaten gesammelt und regelmäßig gesendet.

Die Daten werden täglich und wöchentlich erfasst.

- „Tägliche Hardwaredaten“ auf Seite 98. Enthält das Bestandsänderungsereignis (FQXHMDM0001I) sowie die Änderungen am Hardwarebestand für die jeweiligen Bestandsänderungen.
- „Wöchentliche Hardwaredaten“ auf Seite 102. Dies umfasst den Bestand für alle Einheiten.

Tägliche Hardwaredaten


```
[{
   "2020-03-23T12:32:24.765": {
      "event": {
         "severity": 200,
         "timeStamp": "2020-03-23T16:32:21Z",
         "eventID": "FQXHMDM0001I",
         "eventClass": 800,
         "service": 100,
         "mtm": "",
         "flags": ["Hidden"],
         "action": 100,
         "msgID": "",
         "commonEventID": "FQXHMDM0001I",
         "cn": ""
      },
      "deviceInventoryChanges": [{
         "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36": [{
            "MODIFIED": [
               { "nodes": [] },
               { "accessState": "Pending" },
               { "powerSupplies": [{
                  "cmmDisplayName": "Power Supply 06",
                  "cmmHealthState": "Non-Critical",
                  "dataHandle": 0,
                  "description": "Power Supply",
                  "excludedHealthState": "Normal",
                  "firmware": [{
                     "build": "",
                     "classifications": [],
                     "date": "",
                     "name": "Power Supply Firmware",
                     "revision": "0",
                     "role": "",
                     "softwareID": "",
                     "status": "",
                     "type": "Power Supply Firmware",
                     "version": ""
                  }],
                  "FRU": "69Y5817",
                  "fruSerialNumber": "ZK125115V0VS",
                  "hardwareRevision": "5.0",
                  "healthState": "NA",
                  "inputVoltageMax": -1,
                  "inputVoltageIsAC": true,
                  "inputVoltageMin": -1,
                  "leds": [{
                     "color": "Green",
```

```
        "location": "Planar",
        "name": "OUT",
        "state": "Off"
    },
    {
        "color": "Amber",
        "location": "Planar",
        "name": "FAULT",
        "state": "Off"
    },
    {
        "color": "Green",
        "location": "Planar",
        "name": "IN",
        "state": "Off"
    }],
    "machineType": "",
    "manufactureDate": "2211",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Power Supply 06",
    "overallHealthState": "Normal",
    "parent": {
        "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
        "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
    },
    "partNumber": "69Y5801",
    "productName": "IBM 2500 W Power Supply",
    "posID": "60",
    "powerAllocation": {
        "totalInputPower": 0,
        "totalOutputPower": 343
    },
    "powerState": "Unknown",
    "productId": "303",
    "serialNumber": "",
    "slots": [6],
    "type": "PowerSupply",
    "userDescription": "",
    "uri": "powerSupply/04382F96885411E00095009500950095",
    "uuid": "04382F96885411E00095009500950095",
    "vpdID": "128"
},
{
    "cmmDisplayName": "Power Supply 04",
    "cmmHealthState": "Normal",
    "dataHandle": 0,
    "description": "Power Supply",
    "excludedHealthState": "Normal",
    "firmware": [{
        "build": "",
        "classifications": [],
        "date": "",
        "name": "Power Supply Firmware",
        "revision": "5",
        "role": "",
        "softwareID": "",
        "status": "",
        "type": "Power Supply Firmware",
        "version": ""
```

```
    }],
    "FRU": "69Y5806",
    "fruSerialNumber": "ZK128116T03B",
    "hardwareRevision": "75.54",
    "healthState": "NA",
    "inputVoltageIsAC": true,
    "inputVoltageMax": 240,
    "inputVoltageMin": 220,
    "leds": [{
       "color": "Green",
       "location": "Planar",
       "name": "OUT",
       "state": "On"
    },
    {
       "color": "Amber",
       "location": "Planar",
       "name": "FAULT",
       "state": "Off"
    },
    {
       "color": "Green",
       "location": "Planar",
       "name": "IN",
       "state": "On"
    }],
    "machineType": "",
    "manufactureDate": "2511",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Power Supply 04",
    "overallHealthState": "Normal",
    "parent": {
       "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
       "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
    },
    "partNumber": "69Y5802",
    "productId": "304",
    "productName": "IBM 2500 W Power Supply",
    "powerAllocation": {
       "totalInputPower": 2505,
       "totalOutputPower": 343
    },
    "powerState": "Unknown",
    "posID": "61",
    "serialNumber": "",
    "slots": [4],
    "type": "PowerSupply",
    "userDescription": "",
    "uri": "powerSupply/FF2D840D7A644BCE91ADC16C78978A03",
    "uuid": "FF2D840D7A644BCE91ADC16C78978A03",
    "vpdID": "128"
}]},
{ "fanMuxes": [{
    "cmmDisplayName": "Fan Logic 01",
    "cmmHealthState": "Non-Critical",
    "dataHandle": 0,
    "description": "Fan Logic Module",
    "excludedHealthState": "Normal",
    "FRU": "81Y2912",
```

```
    "fruSerialNumber": "Y031BG16D00S",
    "hardwareRevision": "4.0",
    "leds": [{
       "color": "Amber",
       "location": "FrontPanel",
       "name": "FAULT",
       "state": "On"
    }],
    "machineType": "",
    "manufacturer": "IBM",
    "manufactureDate": "2511",
    "manufacturerId": "20301",
    "model": "",
    "name": "Fan Logic 01",
    "overallHealthState": "Normal",
    "parent": {
       "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
       "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
    },
    "partNumber": "81Y2990",
    "productId": "338",
    "productName": "IBM Fan Pack Multiplexor Card",
    "status": "Non-Critical",
    "serialNumber": "",
    "slots": [1],
    "type": "FanMux",
    "uri": "fanMux/4247F859984711E08372E99E4175BAB0",
    "uuid": "4247F859984711E08372E99E4175BAB0"
},
{
    "cmmDisplayName": "Fan Logic 02",
    "cmmHealthState": "Non-Critical",
    "dataHandle": 0,
    "description": "Fan Logic Module",
    "excludedHealthState": "Normal",
    "FRU": "81Y2912",
    "fruSerialNumber": "Y031BG16D0CE",
    "hardwareRevision": "4.0",
    "leds": [{
       "color": "Amber",
       "location": "FrontPanel",
       "name": "FAULT",
       "state": "On"
    }],
    "machineType": "",
    "manufactureDate": "2511",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Fan Logic 02",
    "overallHealthState": "Normal",
    "parent": {
       "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
       "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
    },
    "productId": "338",
    "productName": "IBM Fan Pack Multiplexor Card",
    "partNumber": "81Y2990",
    "serialNumber": "",
    "slots": [2],
    "status": "Non-Critical",
```

```
                  "type": "FanMux",
                  "uri": "fanMux/71F72BE3985011E0B5A8E216694D6175",
                  "uuid": "71F72BE3985011E0B5A8E216694D6175"
               }]},
               { "switches": [] },
               { "excludedHealthState": "Normal" },
               { "overallHealthState": "Normal" },
               { "inventoryState": null }
            ]}
         ]
      }]
   }
}]
```


Wöchentliche Hardwaredaten


```
{
   "2020-03-23T12:41:28.045": {
      "cabinetList": [{
         "cabinetName": "STANDALONE_OBJECT_NAME",
         "chassisList": [{
            "itemName": "SN#Y010BG57Y01G",
            "itemUUID": "671D5D9EBB4440A49D9DAF08A9EDFB36",
            "itemParentUUID": "",
            "itemLocationRoom": "",
            "itemLocationRack": "",
            "itemLocation": "No Location ConfiguredL",
            "itemLowerUnit": 0,
            "itemType": "CHASSIS",
            "itemHeight": 10,
            "itemSubType": "unknown_type",
            "itemInventory": {
               "accessState": "Online",
               "activationKeys": [],
               "backedBy": "real",
               "bladeSlots": 14,
               "cmmDisplayName": "SN#Y010BG57Y01G",
               "cmmHealthState": "Non-Critical",
               "cmms": [{
                  "accessState": "Online",
                  "backedBy": "real",
                  "cmmDisplayName": "Standby CMM",
                  "dataHandle": 1584981183026,
                  "cmmHealthState": "Normal",
                  "description": "CMM",
                  "firmware": [{
                     "build": "1AON58O",
                     "classifications": [],
                     "date": "2020-03-20T04:00:00Z",
                     "name": "CMM firmware",
                     "revision": "58",
                     "role": "",
                     "status": "",
                     "type": "CMM firmware",
                     "version": "2.5.0"
                  }],
                  "FRU": "68Y7032",
                  "fruSerialNumber": "Y030BG168020",
                  "hostConfig": [],
                  "ipInterfaces": [{
                     "IPv4DHCPmode": "UNKNOWN",
```

```
      "IPv4enabled": false,
      "IPv6DHCPenabled": false,
      "IPv6enabled": false,
      "IPv6statelessEnabled": false,
      "IPv6staticEnabled": false,
      "label": "External",
      "name": "eth0"
   }],
   "errorFields": [],
   "excludedHealthState": "Normal",
   "leds": [{
      "color": "Amber",
      "location": "FrontPanel",
      "name": "FAULT",
      "state": "Off"
   }],
   "machineType": "",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "model": "",
   "name": "Standby CMM",
   "overallHealthState": "Normal",
   "partNumber": "68Y7054",
   "parent": {
      "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
      "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
   },
   "powerAllocation": {
      "maximumAllocatedPower": 20,
      "minimumAllocatedPower": 20
   },
   "productId": "65",
   "role": "backup",
   "serialNumber": "",
   "slots": [2],
   "type": "CMM",
   "uri": "cmm/F1F06BE6946511E089AEB9871E6892B2",
   "userDefinedName": "",
   "userDescription": "",
   "uuid": "F1F06BE6946511E089AEB9871E6892B2"
}],
"complex": [],
"contact": "No Contact Configured",
"dataHandle": 1584981227532,
"description": "Lenovo Flex System Chassis",
"displayName": "SN#Y010BG57Y01G",
"encapsulation": {
   "encapsulationMode": "normal"
},
"energyPolicies": {
   "acousticAttenuationMode": "Off",
   "hotAirRecirculation": {
      "chassisBay": [],
      "isEnabled": false,
      "maxVariation": 9.0
   },
   "powerCappingPolicy": {
      "cappingPolicy": "OFF",
      "currentPowerCap": 0,
      "maxPowerCap": 5010,
      "minPowerCap": 1504,
```

```
      "powerCappingAllocUnit": "watts"
   },
   "powerRedundancyMode": 4
},
"errorFields": [],
"excludedHealthState": "Warning",
"fanSlots": 10,
"fanMuxes": [{
   "cmmDisplayName": "Fan Logic 02",
   "cmmHealthState": "Non-Critical",
   "dataHandle": 0,
   "description": "Fan Logic Module",
   "excludedHealthState": "Warning",
   "FRU": "81Y2912",
   "fruSerialNumber": "Y031BG16D0CE",
   "hardwareRevision": "4.0",
   "leds": [{
      "color": "Amber",
      "location": "FrontPanel",
      "name": "FAULT",
      "state": "On"
   }],
   "machineType": "",
   "manufactureDate": "2511",
   "manufacturer": "IBM",
   "manufacturerId": "20301",
   "model": "",
   "name": "Fan Logic 02",
   "overallHealthState": "Warning",
   "parent": {
      "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
      "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
   },
   "partNumber": "81Y2990",
   "productId": "338",
   "productName": "IBM Fan Pack Multiplexor Card",
   "serialNumber": "",
   "slots": [2],
   "status": "Non-Critical",
   "type": "FanMux",
   "uri": "fanMux/71F72BE3985011E0B5A8E216694D6175",
   "uuid": "71F72BE3985011E0B5A8E216694D6175"
}],
"fanMuxSlots": 2,
"fans": [{
   "cmmDisplayName": "Fan 06",
   "cmmHealthState": "Normal",
   "dataHandle": 0,
   "description": "IBM Fan Pack",
   "errorFields": [],
   "excludedHealthState": "Normal",
   "firmware": [{
      "build": "",
      "classifications": [],
      "date": "",
      "name": "Fan Controller",
      "revision": "226",
      "role": "",
      "status": "",
      "type": "Fan Controller",
      "version": "226"
```

```
    }],
    "FRU": "88Y6685",
    "fruSerialNumber": "YK10JPB69582",
    "hardwareRevision": "4.0",
    "leds": [{
       "color": "Amber",
       "location": "FrontPanel",
       "name": "FAULT",
       "state": "Off"
    }],
    "machineType": "",
    "manufactureDate": "2411",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Fan 06",
    "overallHealthState": "Normal",
    "parent": {
       "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
       "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
    },
    "partNumber": "88Y6691",
    "posID": "11",
    "powerAllocation": {
       "maximumAllocatedPower": 75,
       "minimumAllocatedPower": 75
    },
    "powerState": "Unknown",
    "productId": "342",
    "productName": "80mm Fan Pack for ITE Cooling",
    "serialNumber": "",
    "slots": [6],
    "type": "Fan",
    "userDescription": "",
    "uri": "fan/7293CA21938011E0BC13CB5D330B7C19",
    "uuid": "7293CA21938011E0BC13CB5D330B7C19",
    "vpdID": "373"
}],
"height": 10,
"isConnectionTrusted": "true",
"lastOfflineTimestamp": -1,
"ledCardSlots": 1,
"leds": [{
   "color": "Blue",
   "location": "FrontPanel",
   "name": "Location",
"state": "Off"
}],
"location": {
   "location": "No Location ConfiguredL",
   "lowestRackUnit": 0,
   "rack": "",
   "room": ""
},
"machineType": "8721",
"managerName": "UNKNOWN",
"managerUuid": "UNKNOWN",
"manufacturer": "IBM",
"manufacturerId": "20301",
"mmSlots": 2,
"model": "HC1",
```

```
"name": "SN#Y010BG57Y01G",
"nist": {
   "currentValue": "Compatibility",
   "possibleValues": ["Nist_800_131A_Strict","unsupported","Nist_800_131A_Custom","Compatibility"]
},
"nodes": [{
   "accessState": "Online",
   "activationKeys": [],
   "addinCards": [],
   "addinCardSlots": 0,
   "arch": "Unknown",
   "backedBy": "real",
   "bladeState": 0,
   "bladeState_health": "CRITICAL",
   "bladeState_string": "Init failed",
   "bootMode": {
      "currentValue": "",
      "possibleValues": []
   },
   "bootOrder": {
      "bootOrderList": [],
      "uri": "nodes/DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)/bootOrder"
   },
   "cmmDisplayName": "Node 07",
   "cmmHealthState": "Critical",
   "complexID": -1,
   "contact": "",
   "dataHandle": 1584981175839,
   "description": "",
   "driveBays": 0,
   "drives": [],
   "embeddedHypervisorPresence": false,
   "encapsulation": {
      "encapsulationMode": "notSupported"
   },
   "errorFields": [
      { "HostAndDomain": "NO_CONNECTOR" },
      { "PhysicalAndLocation": "NO_CONNECTOR" },
      { "Encapsulation": "NO_CONNECTOR" },
      { "Memory": "NO_CONNECTOR" },
      { "ServerFirmwareData": "NO_CONNECTOR" },
      { "RackCPU": "NO_CONNECTOR" },
      { "ServerOnboardPciDevices": "NO_CONNECTOR" },
      { "BootMode": "NO_CONNECTOR" },
      { "SecureBootMode": "NO_CONNECTOR" },
      { "BootOrder": "NO_CONNECTOR" },
      { "FlashDimm": "NO_CONNECTOR" },
      { "HostMacAddress": "NO_CONNECTOR" },
      { "VnicMode": "NO_CONNECTOR" },
      { "RemotePresenceEnabled": "NO_CONNECTOR" },
      { "ActivationKey": "NO_CONNECTOR" },
      { "LanOverUsbMode": "NO_CONNECTOR" },
      { "ServerStaticMetrics": "NO_CONNECTOR" },
      { "ScalableComplexPartitionUUIDData": "NO_CONNECTOR" },
      { "ActiveAlerts": "NO_CONNECTOR" },
      { "PFAConfiguration": "NO_CONNECTOR" },
      { "ServerIPaddresses": "NO_CONNECTOR"  },
      { "FaceplateInfo": "NO_CONNECTOR" },
      { "IOCompatibilityData": "NO_CONNECTOR" },
      { "LanOverUsbPortForwardingModes": "NO_CONNECTOR" },
      { "ServerConfigFiles": "NO_CONNECTOR" }
```

```
],
"excludedHealthState": "Normal",
"expansionCards": [],
"expansionCardSlots": 0,
"expansionProducts": [],
"expansionProductType": "",
"faceplateIDs": [],
"firmware": [],
"flashStorage": [],
"FRU": "",
"fruSerialNumber": "",
"hasOS": false,
"hostMacAddresses": "",
"ipInterfaces": [],
"isConnectionTrusted": "true",
"isITME": false
"isRemotePresenceEnabled": false,
"isScalable": false,
"lanOverUsb": "disabled",
"lanOverUsbPortForwardingModes": [],
"leds": [],
"location": {
   "location": "",
   "lowestRackUnit": 0,
   "rack": "",
   "room": ""
},
"logicalID": -1,
"m2Presence": false,
"machineType": "",
"manufacturer": "",
"manufacturerId": "",
"memoryModules": [],
"memorySlots": 0,
"mgmtProcType": "UNKNOWN",
"model": "",
"name": "Node 07",
"nist": {
   "currentValue": "Unknown",
   "possibleValues": ["Nist_800_131A_Strict","unsupported","Compatibility"]
},
"onboardPciDevices": [],
"osInfo": {
   "description": "",
   "storedCredential": ""
},
"overallHealthState": "Normal",
"parent": {
   "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
   "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
},
"partitionID": -1,
"partNumber": "",
"pciCapabilities": [],
"pciDevices": [],
"ports": [],
"posID": "",
"powerAllocation": {
   "maximumAllocatedPower": 0,
   "minimumAllocatedPower": 0
},
```

```
      "powerStatus": 0,
      "powerSupplies": [],
      "primary": false,
      "processors": [],
      "processorSlots": 0,
      "productId": "",
      "productName": "",
      "raidSettings": [],
      "secureBootMode": {
         "currentValue": "",
         "possibleValues": []
      },
      "securityDescriptor": {
         "managedAuthEnabled": false,
         "managedAuthSupported": true,
         "publicAccess": false,
         "roleGroups": ["lxc-supervisor"],
         "storedCredentials": {
            "description": "Credentials for null",
            "id": "1703",
            "userName": "USERID"
         },
         "uri": "nodes/dummy-671d5d9ebb4440a4-chassis(1)-blade(7)"
      },
      "serialNumber": "",
      "slots": [7],
      "status": {
         "message": "managed",
         "name": "MANAGED"
      },
      "subSlots": [],
      "subType": "",
      "tlsVersion": {
         "currentValue": "Unknown",
         "possibleValues": ["unsupported","TLS_12","TLS_11","TLS_10"]
      },
      "type": "ITE",
      "uri": "nodes/DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)",
      "userDefinedName": "",
      "userDescription": "",
      "uuid": "DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)",
      "vnicMode": "disabled",
      "vpdID": ""
   }],
   "overallHealthState": "Warning",
   "parent": {
      "uri": "cabinet/",
      "uuid": ""
   },
   "partNumber": "88Y6660",
   "passThroughModules": [],
   "posID": "14",
   "powerAllocation": {
      "allocatedOutputPower": 1504,
      "midPlaneCardMaximumAllocatedPower": 38,
      "midPlaneCardMinimumAllocatedPower": 38,
      "remainingOutputPower": 3506,
      "totalInputPower": 5445,
      "totalOutputPower": 5010
   },
   "powerSupplies": [{
```

```
    "dataHandle": 0,
    "cmmDisplayName": "Power Supply 06",
    "cmmHealthState": "Non-Critical",
    "description": "Power Supply",
    "excludedHealthState": "Warning",
    "firmware": [{
       "build": "",
       "classifications": [],
       "date": "",
       "name": "Power Supply Firmware",
       "revision": "0",
       "role": "",
       "softwareID": "",
       "status": "",
       "type": "Power Supply Firmware",
       "version": ""
    }                                ],
    "FRU": "69Y5817",
    "fruSerialNumber": "ZK125115V0VS",
    "hardwareRevision": "5.0",
    "healthState": "NA",
    "inputVoltageIsAC": true,
    "inputVoltageMax": -1,
    "inputVoltageMin": -1,
    "leds": [{
       "color": "Green",
       "location": "Planar",
       "name": "OUT",
       "state": "Off"
    }],
    "machineType": "",
    "manufactureDate": "2211",
    "manufacturer": "IBM",
    "manufacturerId": "20301",
    "model": "",
    "name": "Power Supply 06",
    "overallHealthState": "Warning",
    "parent": {
       "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
       "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
    },
    "partNumber": "69Y5801",
    "posID": "60",
    "powerAllocation": {
       "totalInputPower": 0,
       "totalOutputPower": 343
    },
    "powerState": "Unknown",
    "productId": "303",
    "productName": "IBM 2500 W Power Supply",
    "serialNumber": "",
    "slots": [6],
    "type": "PowerSupply",
    "uri": "powerSupply/04382F96885411E00095009500950095",
    "userDescription": "",
    "uuid": "04382F96885411E00095009500950095",
    "vpdID": "128"
}],
"powerSupplySlots": 6,
"productId": "336",
"productName": "IBM Chassis Midplane",
```

```
"securityDescriptor": {
   "managedAuthEnabled": false,
   "managedAuthSupported": true,
   "publicAccess": false,
   "roleGroups": ["lxc-supervisor"],
   "storedCredentials": {
      "description": "Credentials for null",
      "id": "1703",
      "userName": "USERID"
   },
   "uri": "chassis/671d5d9ebb4440a49d9daf08a9edfb36"
},
"SecurityPolicy": {
   "cmmPolicyState": "ACTIVE",
   "cmmPolicyLevel": "SECURE"
},
"serialNumber": "23DVG73",
"status": {
   "message": "MANAGED",
   "name": "MANAGED"
},
"switches": [{
   "accessState": "Online",
   "accessStateRecords": [{
      "health": "OFFLINE",
      "ipAddress": "10.241.53.20",
      "messageBundle": "com.lenovo.lxca.inventory.base.bundle.connections.messages",
      "messageDisplay": "Authentication failed occurred due to HTTP 401 - Unauthorized (OpenPegasus Error: \"U
      "messageID": "0510",
      "messageParameter": "HTTP 401 - Unauthorized (OpenPegasus Error: \"User Unauthorized\")",
      "protocol": "CIM",
      "username": "USERID",
      "timestamp": 1584709239559,
      "trusted": true
   }],
   "attachedNodes": [],
   "backedBy": "real",
   "cmmDisplayName": "IO Module 04",
   "cmmHealthState": "Normal",
   "dataHandle": 1584981209777,
   "description": "FC5022 16Gb SAN Scalable Switch",
   "deviceName": "FC5022",
   "errorFields": [{
      "IOCompatibilityData": "FETCH_FAILED"
   }],
   "excludedHealthState": "Normal",
   "firmware": [{
      "classifications": [],
      "build": "",
      "date": "2016-04-19T04:00:00Z",
      "name": "Main Application",
      "status": "Active",
      "type": "Main Application",
      "version": "7.4.1c"
   }],
   "FRU": "00Y3329",
   "fruSerialNumber": "Y050UZ67D009",
   "ipInterfaces": [{
      "IPv4DHCPmode": "DHCP_THEN_STATIC",
      "IPv4enabled": true,
      "IPv6enabled": true,
```

```
        "IPv6DHCPenabled": true,
        "IPv6statelessEnabled": true,
        "IPv6staticEnabled": false,
        "label": "",
        "name": "ioe0"
     }],
     "leds": [{
        "color": "Amber",
        "location": "FrontPanel",
        "name": "FRU Fault",
        "state": "Off"
     }],
     "machineType": "",
     "manufacturer": "LNV",
     "manufacturerId": "20301",
     "model": "",
     "name": "IO Module 04",
     "ntpPushEnabled": false,
     "ntpPushFrequency": 17,
     "overallHealthState": "Normal",
     "parent": {
        "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
        "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
     },
     "partNumber": "00MM452",
     "ports": [],
     "posID": "17",
     "powerAllocation": {
        "maximumAllocatedPower": -1,
        "minimumAllocatedPower": -1
     },
     "powerState": "On",
     "productId": "329",
     "productName": "Flex System FC5022 24-port 16Gb SAN Scalable Switch",
     "protectedMode": "Not supported",
     "securityDescriptor": {
        "managedAuthEnabled": false,
        "managedAuthSupported": true,
        "publicAccess": false,
        "roleGroups": [],
        "storedCredentials": {
           "description": "Credentials for null",
           "id": "1702",
           "userName": "USERID"
        },
        "uri": "switches/AE986BEC1DD1B201684FC4F57C3B16B6"
     },
     "serialNumber": "",
     "slots": [4],
     "stackMode": "N/A",
     "type": "Switch",
     "uri": "switches/AE986BEC1DD1B201684FC4F57C3B16B6",
     "userDefinedName": "",
     "userDescription": "",
     "uuid": "AE986BEC1DD1B201684FC4F57C3B16B6",
     "vpdID": "309"
  }],
  "switchSlots": 4,
  "tlsVersion": {
     "currentValue": "TLS_12_Server",
     "possibleValues": ["TLS_12_Server","unsupported","TLS_12_Server_Client","SSL_30"]
```

```
                },
                "type": "Chassis",
                "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
                "userDefinedName": "SN#Y010BG57Y01G",
                "userDescription": "",
                "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
                "vpdID": "336"
            }
         }],
         "complexList": [],
         "height": 52,
         "nodeList": [],
         "location": "",
         "placeholderList": [],
         "room": "",
         "storageList": [],
         "switchList": [],
         "UUID": "STANDALONE_OBJECT_UUID"
      }]
   }
}
```

Kapitel 4. Plattenspeicher verwalten

Sie können den von Lenovo XClarity Administrator belegten Festplattenspeicher verwalten, indem Sie große Datendateien verschieben, die nicht unmittelbar für eine Remote-Freigabe erforderlich sind, oder indem Sie nicht mehr benötigte Ressourcen löschen.

Zu dieser Aufgabe

Um festzustellen, wie viel Plattenspeicherplatz derzeit verwendet wird, klicken Sie der Menüleiste von XClarity Administrator auf **Dashboard**. Die Speicherplatzbelegung im Repository und Remote-Freigaben wird im Aktivitätsabschnitt von XClarity Administrator aufgeführt.

Vorgehensweise

Führen Sie einen oder mehrere der folgenden Schritte aus, um Speicherplatz freizugeben, indem Sie Dateien zu einer Remote-Freigabe verschieben und nicht benötigte Ressourcen löschen.

- **Nicht mehr benötigte Ressourcen löschen**

  Sie können Dateien, die nicht mehr benötigt werden, schnell aus dem lokalen Repository löschen, indem Sie die folgenden Schritte ausführen.

  1. Wählen Sie in der XClarity Administrator-Menüleiste **Verwaltung → Datenträger bereinigen** aus, um die Seite Datenträger bereinigen anzuzeigen.
  2. Wählen Sie die Dateien aus, die Sie löschen möchten. Die Überschrift des Abschnitts gibt an, wie viel Speicherplatz freigegeben wird, wenn die Dateien gelöscht werden.
     - **Betriebssystembezogene Dateien**

       Sie können BS-Images, Bootoptionsdateien und Softwaredateien löschen.
     - **Firmwareaktualisierungen**

       Sie können Nutzlastdateien für alle BS-Einheitentreiber löschen, die mit UpdateXpress System Packs (UXSPs) verknüpft sind, sowie einzelne Einheitentreiber, die sich im Status „Heruntergeladen“ befinden.

       Sie können Nutzlastdateien für einzelne Firmwareaktualisierungen löschen, die sich im Status „Heruntergeladen“ befinden und nicht in einer Firmwarekonformitätsrichtlinie verwendet werden.

       Sie können Nutzlastdateien für Verwaltungsserveraktualisierungen löschen, die den Status „Heruntergeladen“ aufweisen.

       Anmerkung: Wenn sich das Repository für Firmwareaktualisierungen auf einer Remote-Freigabe befindet, können Sie die Datenträgerbereinigungsfunktion nicht verwenden, um einzelne Firmwareaktualisierungen und UXSPs zu löschen.
     - **Servicedatendateien**

       Wenn ein Service-Ereignis auf einer Einheit auftritt, werden automatisch Servicedaten für diese Einheit erfasst. Servicedaten werden automatisch immer dann für den Verwaltungsserver erfasst, wenn eine Ausnahme im XClarity Administrator auftritt. Wenn XClarity Administrator und die verwalteten Einheiten ordnungsgemäß funktionieren, sollten Sie diese Archive in regelmäßigen Abständen löschen.

       Wenn Verwaltungsserveraktualisierungen erfolgreich ausgeführt werden, werden die Aktualisierungsdateien automatisch aus dem Repository entfernt.

© Copyright Lenovo 2015, 2025

3. Klicken Sie auf **Ausgewählte löschen**.
4. Überprüfen Sie die Liste der ausgewählten Dateien und klicken Sie auf **Löschen**.

- **Nicht verwendete Firmwareaktualisierungspakete bereinigen**

  Sie können alle nicht verwendeten Firmwarepakete im Aktualisierungs-Repository löschen, indem Sie auf **Bereitstellung → Firmwareaktualisierungen: Repository** in der XClarity Administrator Menüleiste klicken und anschließend auf **Alle Aktionen → Bereinigungs-Repository** klicken.

  Sie können auswählen, ob die neuesten Versionen behalten oder entfernt werden sollen, wenn sie nicht verwendet werden.

  Für das Ausführen dieser Anforderung muss ein Job erstellt werden. Sie können den Jobfortschritt überwachen, indem Sie in der XClarity Administrator-Menüleiste auf **Überwachung → Jobs** klicken.

- **Firmwareaktualisierungspakete zu einem Remote-Repository verschieben**

  Standardmäßig verwendet Lenovo XClarity Administrator ein lokales (internes) Repository zum Speichern von Firmwareaktualisierungen. Sie können Speicherplatz freigeben, der für das lokale XClarity Administrator Repository zur Verfügung steht, indem Sie eine angehängte Remote-Freigabe über das SSH File System (SSHFS) als Remote-Repository verwenden. Sie können dann Firmwareaktualisierungsdateien direkt aus dem Remote-Repository verwenden, um die Firmwarekonformität auf Ihren Einheiten zu erhalten. Weitere Informationen hierzu finden Sie unter Remote-Repository für Firmwareaktualisierungen verwenden in der Onlinedokumentation zu XClarity Administrator.

  Wenn Sie die Position des Firmwareaktualisierungs-Repositorys ändern, können Sie festlegen, dass alle Firmwareaktualisierungen aus dem ursprünglichen Repository in das neue Repository kopiert werden.

  Die Firmwareaktualisierungsdateien im ursprünglichen Repository werden nach dem Wechseln der Positionen *nicht* automatisch gelöscht.

  Tipp: Das Repository für Remote-Aktualisierungen kann von mehreren XClarity Administrator Verwaltungsservern gemeinsam genutzt werden.

  Gehen Sie wie folgt vor, um Firmwareaktualisierungen in ein Remote-Firmwareaktualisierungs-Repository zu verschieben.

  1. Fügen Sie eine Remote-Freigabe zu XClarity Administrator hinzu (siehe Remote-Freigaben verwalten in der Onlinedokumentation zu XClarity Administrator).
  2. Klicken Sie in der XClarity Administrator-Menüleiste auf **Bereitstellung → Firmwareaktualisierungen: Repository**. Die Seite Repository für Firmwareaktualisierungen wird angezeigt.
  3. Klicken Sie auf **Alle Aktionen → Repository-Position wechseln**, um das Dialogfeld „Repository-Position wechseln“ anzuzeigen.
  4. Wählen Sie die gerade erstellte Remote-Freigabe aus der Dropdown-Liste **Repository-Position** aus.
  5. Wählen Sie **Aktualisierungspakete aus aktuellem Repository in neues Repository kopieren** aus, um die Firmwareaktualisierungsdateien in die neue Repository-Position zu kopieren, bevor die Repository-Position gewechselt wird.
  6. Klicken Sie auf **OK**.

     Es wird ein Job erstellt, um Firmwareaktualisierungspakete in das neue Repository zu kopieren. Sie können den Jobfortschritt überwachen, indem Sie in der XClarity Administrator-Menüleiste auf **Überwachung → Jobs** klicken.
  7. Bereinigen Sie die Firmwareaktualisierungsdateien im lokalen Repository.
     a. Wechseln Sie die Position zum lokalen Repository, indem Sie auf **Alle Aktionen → Repository-Position wechseln** klicken und **Lokales Repository** als Repository-Position auswählen. Klicken Sie dann auf **OK**.

b. Klicken Sie auf die Registerkarte **Einzelne Aktualisierungen**, klicken Sie auf das Kontrollkästchen „Alle auswählen“ in der Tabelle, um alle Firmwareaktualisierungen auszuwählen, und klicken Sie dann auf das Symbol **Vollständige Aktualisierungspakete löschen** ( ).

c. Klicken Sie auf die Registerkarte **UpdateXpress System Pack (UXSP)**, klicken Sie auf das Kontrollkästchen „Alle auswählen“ in der Tabelle, um alle UXSPs auszuwählen, und klicken Sie dann auf das Symbol **UXSP und zugehörige Richtlinie löschen** ( ).

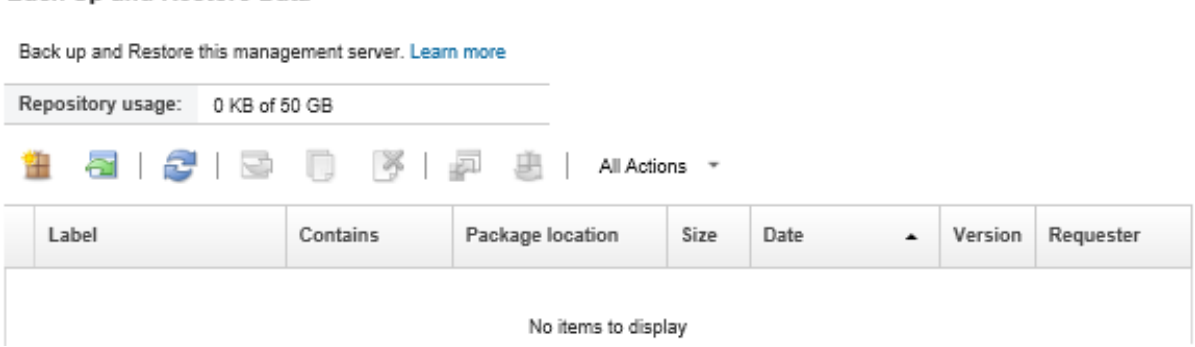
d. Wechseln Sie die Position zurück zum Remote-Repository, indem Sie auf **Alle Aktionen → Repository-Position wechseln** klicken und das neue Remote-Repository als Repository-Position auswählen. Klicken Sie dann auf **OK**.

- **XClarity Administrator-Sicherungsdateien zu einer Remote-Freigabe verschieben**

  Sie können Festplattenspeicher, der für das lokale Repository von XClarity Administrator zur Verfügung steht, freigeben. Verschieben Sie dazu XClarity Administrator-Sicherungen zu einer Remote-Freigabe. Sie können die Dateien allerdings nicht direkt auf der Remote-Freigabe verwenden. Um die Dateien zu verwenden, müssen Sie sie zurück in das lokale Repository von XClarity Administrator verschieben. Weitere Informationen zu Remote-Freigaben finden Sie unter Remote-Freigaben verwalten in der Onlinedokumentation von XClarity Administrator.

  Wichtig: Es wird empfohlen, Sicherungen vor dem Löschen der Sicherungen in XClarity Administrator auf Ihr lokales System herunterzuladen oder Sicherungen auf eine Remote-Freigabe zu kopieren.

  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Verwaltung → Daten sichern und wiederherstellen**, um die Seite Daten sichern und wiederherstellen anzuzeigen.

     Die Spalte **Paketposition** zeigt an, ob die Sicherung entweder im lokalen Repository von XClarity Administrator oder auf einer Remote-Freigabe gespeichert ist.

  2. Wählen Sie die Sicherung aus und klicken Sie auf das Symbol **Sicherung kopieren** ( ), um das Dialogfeld Sicherung kopieren anzuzeigen.
  3. Wählen Sie die Remote-Freigabe für die Sicherung aus.
  4. Klicken Sie auf **Kopieren**.
  5. Sie können den Kopierfortschritt auf der Seite Jobs überwachen. Wenn der Kopiervorgang abgeschlossen ist, wählen Sie die Sicherung erneut aus und klicken Sie auf das Symbol **Sicherung löschen** ( ), um das Dialogfeld Sicherung löschen anzuzeigen.
  6. Wählen Sie „Lokal“ als Position aus.
  7. Klicken Sie auf **Löschen**.

Kapitel 5. Ermittlungs- und Verwaltungsprobleme

Verwenden Sie diese Informationen, um Probleme mit der Einheitenerkennung und -verwaltung zu beheben.

Einheit kann nicht erkannt werden

Verwenden Sie diese Informationen zur Fehlerbehebung, wenn Probleme bei der Suche nach verwaltbaren Einheiten auftreten.

1. Vergewissern Sie sich, dass die Einheit von Lenovo XClarity Administrator unterstützt wird. Eine Liste der unterstützten Einheiten finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Öffnen Sie die Registerkarte **Kompatibilität** und klicken Sie dann auf den Link für die entsprechenden Einheitentypen.
2. Stellen Sie sicher, dass die Einheit im Netzwerk für XClarity Administrator und XClarity Administrator für die Einheit erreichbar ist.
3. Überprüfen Sie, ob die richtigen Ports in der Firewall geöffnet sind. Informationen zu den Portanforderungen finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.
4. Stellen Sie sicher, dass Unicast- und Multicast-SLP im Netzwerk aktiviert sind.
5. Bei ThinkServer-Servern:
   a. Stellen Sie über die Verwaltungswebschnittstelle für den Server sicher, dass der Hostname des Servers mit einem gültigen Hostnamen oder einer gültigen IP-Adresse konfiguriert ist.
   b. Vergewissern Sie sich, dass SLP aktiviert ist und der Hostname in ThinkServer System Manager (TSM) aktiviert ist.
      - Um zu bestimmen, auf welchen ThinkServer-Servern SLP aktiviert ist, senden Sie mit Ihrem bevorzugten SLP-Tool eine SLP-Anforderung, mit der Sie den WBEM-Service abfragen.
        ```
        $ slptool findsrvs service:wbem
        service:wbem:http://<TSM_IP>:5988,65535
        service:wbem:https://<TSM_IP>:5989,65535
        ```
      - Sie können feststellen, ob SLP auf einem bestimmten ThinkServer aktiviert ist, indem Sie mit Ihrem bevorzugten SLP-Tool eine SLP-Anforderung senden, mit der Sie den WBEM-Service abfragen.
        ```
        $ slptool unicastfindattrs <TSM_IP> service:wbem
        (template-type=wbem),(template-version=2.0),(template-url-syntax=service:URL),
        (service-hi-name=qom),(service-hi-description=Quasi Object Manager 1.0.0),
        (CommunicationMechanism=cim-xml),(CommunicationMechanismsVersion=1.0),
        (MultipleOperationsSupported=false),(AuthenticationMechanismsSupported=Basic),
        (InteropSchemaNamespace=root/interop),(service-id=Lenovo G5 WBEM Service)
        ```
      - Wenn eine Einheit nicht auf die SLP-Anforderung reagiert, starten Sie die TSM-Firmware erneut. Senden Sie dazu einen IPMI-Befehl mit den folgenden Parametern an den TSM. Der Neustart des TSM kann einige Minuten dauern.
        ```
        NetFn = 0x06
        Command = 0x03
        Data = ()
        ```

        Im folgenden Beispiel wird SLP mithilfe des Open-Source-Tools `ipmitool` aktiviert.

        ```
        $ ipmitool -H <TSM_IP> -U <ipmi_user> -P <ipmipassword> raw 0x06 0x03
        ```
6. Überprüfen Sie für RackSwitch-Switches, dass SLP aktiviert und der Hostname in der Switchkonfiguration festgelegt ist.

© Copyright Lenovo 2015, 2025

- Switches der ThinkSystem DB Serie können nicht erkannt werden. Um diese Switches zu verwalten, geben Sie die IP-Adresse des Switches manuell ein, indem Sie auf der Seite Neue Einheiten ermitteln und verwalten auf **Manuelle Eingabe** klicken.
- NVIDIA Mellanox können nicht erkannt werden. Um diese Switches zu verwalten, geben Sie die IP-Adresse des Switches manuell ein, indem Sie auf der Seite Neue Einheiten ermitteln und verwalten auf **Manuelle Eingabe** klicken.
- Überprüfen Sie für andere Switches, dass SLP aktiviert und der Hostname in der Switchkonfiguration festgelegt ist.
  - Senden Sie mit Ihrem bevorzugten SLP-Tool die folgende SLP-Multicast-Anforderung, um zu bestimmen, auf welchen Switches SLP aktiviert ist.

    Anmerkung: Diese Anforderung sucht nur Switches, die sich im gleichen Subnetz befinden, in dem das SLP-Tool ausgeführt wird.

    ```
    $ slptool findsrvs service:io-device.Lenovo:management-module
    service:io-device.Lenovo:management-module://<RackSwitch IP>,64225
    ```
  - Sie können prüfen, ob SLP auf einem bestimmten Switch aktiviert ist, indem Sie mit Ihrem bevorzugten SLP-Tool die folgende SLP-Unicast-Anforderung senden.
    ```
    $ slptool findattrs service:io-device.Lenovo:management-module://<RackSwitch IP>
    (level=1.0),(Type=switch),(data-protocols=ethernet),(serial-number=US7116000D),
    (sysoid=1.3.6.1.4.1.26543.1.7.6),(ipv4-enabled=TRUE),(ipv4-address=<RackSwitch IP>),
    (ipv6-enabled=FALSE),ipv6-addresses,(ipv4-mgmt-protocols=http:80:true,https:443:true,
    telnet:23:true,ssh:22:true,snmpv1v2v3:161:true,snmpv3only:161:false),
    (snmp-engineid=80:00:67:af:03:08:17:f4:33:d3),
    (ssh-fingerprint=8a:43:cb:be:47:d9:31:37:7a:3b:80:f6:dd:00:61:a6),
    (deviceName=<RackSwitch hostname>)
    ```

7. Stellen Sie für Lenovo Storage-Einheiten (außer ThinkSystem DE Serie) sicher, dass SLP aktiviert ist und Ihr Netzwerk keine SLP-Kommunikation zwischen XClarity Administrator und der Speichereinheit blockiert.
   - Um zu bestimmen, auf welchen Speichereinheiten SLP aktiviert ist, senden Sie mit Ihrem bevorzugten SLP-Tool eine SLP-Anforderung, mit der Sie den API-Service abfragen.
     ```
     $ slptool findsrvs service:api
     service:api:https://<CONTROLLER_IP>:443/api,65535
     service:api:https://<CONTROLLER_IP>:443/api,65535
     ```
   - Sie können auch feststellen, ob SLP auf einer bestimmten Speichereinheit aktiviert ist, indem Sie mit Ihrem bevorzugten SLP-Tool eine SLP-Anforderung senden, mit der Sie den API-Service abfragen.
     ```
     $ slptool unicastfindattrs <CONTROLLER_IP> service:api
     (x-system-name=S3200_5.65),(x-system-location=rack\2Crack\2Crack),(x-system-contact=Support contact),
     (x-system-information=S3200_65),(x-vendor-name=Lenovo),(x-product-id=S3200),(x-product-brand=Storage),
     (x-midplane-serial-number=00C0FF2682A8),(x-platform-type=Gallium),(x-bundle-version=""),
     (x-build-date=""),(x-health=OK),(x-wwnn=208000c0ff2682a8),(x-mac-address=00:00:00:00:00:EB)
     ```

   Wenn eine Speichereinheit nicht auf die SLP-Anforderung reagiert:

   - Stellen Sie sicher, dass das Netzwerk die SLP-Kommunikation zwischen den Einheiten zulässt.
   - Stellen Sie sicher, dass der **SMI-S – Storage Management Initiative Specification**-Standard für die Speichereinheiten aktiviert ist. Starten Sie die Speichereinheit über die Verwaltungswebschnittstelle oder die Befehlszeilenschnittstelle erneut.

Einheit kann nicht verwaltet werden

Verwenden Sie diese Informationen, um Fehler beim Verwalten von Einheiten zu beheben.

1. Stellen Sie sicher, dass die Einheit von Lenovo XClarity Administrator unterstützt wird. Weitere Informationen zu unterstützten Einheiten finden Sie unter Support-Website mit

Kompatibilitätsinformationen zu XClarity Administrator. Öffnen Sie die Registerkarte **Kompatibilität** und klicken Sie dann auf den Link für die entsprechenden Einheitentypen.

2. Stellen Sie sicher, dass die Einheit im Netzwerk für XClarity Administrator und XClarity Administrator für die Einheit erreichbar ist.
3. Stellen Sie sicher, dass alle für die Verwaltung geeigneten Ports im Netzwerk und in den Firewalls geöffnet sind. Informationen zu den Portanforderungen finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.
4. Stellen Sie sicher, dass die mindestens erforderliche Firmware auf jedem Server installiert ist, den Sie mit XClarity Administrator verwalten möchten. Die mindestens erforderlichen Firmwareversionen finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Klicken Sie dazu auf die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.
5. Vergewissern Sie sich, dass es keine Probleme mit dem XClarity Administrator-Serverzertifikat gibt.
   a. Stellen Sie sicher, dass das XClarity Administrator-Serverzertifikat nicht abgelaufen ist.
   b. Stellen Sie sicher, dass das XClarity Administrator-Serverzertifikat eine gültige IP-Adresse im SubjectAltName hat (siehe Angepasste Serverzertifikate in XClarity Administrator implementieren in der XClarity Administrator-Onlinedokumentation).
6. Stellen Sie sicher, dass das Datum auf dem Server nicht mit dem LDAP-Zertifikat im Konflikt steht. Wenn das LDAP-Zertifikat beispielsweise vom **03.08.2022** bis zum **03.11.2024** gültig ist, aber das XCC-Datum **15.04.2000** lautet, besteht der Server die TLS-Überprüfung nicht.
7. Stellen Sie sicher, dass CIM over HTTPS auf der Einheit aktiviert ist.
   a. Melden Sie sich bei der Verwaltungswebschnittstelle für den Server mit dem Benutzeraccount `RECOVERY_ID` an.
   b. Klicken Sie auf **IMM-Verwaltung → Sicherheit**.
   c. Klicken Sie auf die Registerkarte **CIM Over HTTPS** und stellen Sie sicher, dass **CIM Over HTTPS aktivieren** ausgewählt ist.
8. Für ThinkSystem SR635- und SR655-Server:
   - Stellen Sie sicher, dass ein Betriebssystem installiert ist und dass der Server mit dem Betriebssystem gestartet wurde, bootfähige Datenträger angehängt sind oder mindestens einmal EFI-Shell ausgeführt wurde, sodass XClarity Administrator Bestandsdaten für diese Server erfassen kann.
   - Vergewissern Sie sich, dass IPMI-über-LAN aktiviert ist. IPMI-over-LAN ist auf diesen Servern standardmäßig deaktiviert und muss manuell aktiviert werden, bevor die Server verwaltet werden können. Um IPMI-over-LAN mithilfe von TSM zu aktivieren, klicken Sie auf **Einstellungen → IPMI-Konfiguration**. Möglicherweise müssen Sie den Server neu starten, damit die Änderung übernommen wird.
9. Wenn das Serverzertifikat der Einheit von einer externen Zertifizierungsstelle signiert ist, müssen Sie sicherstellen, dass das Zertifizierungsstellen und alle Zwischenzertifikate in den XClarity Administrator-Truststore importiert werden (siehe Angepasste Serverzertifikate in verwaltete Einheiten implementieren in der Onlinedokumentation zu XClarity Administrator.
10. Vergewissern Sie sich, dass die Anmeldeinformationen für die Einheit korrekt sind.

    Anmerkung: Stellen Sie sicher, dass das Kennwort den Sicherheits- und Kennwortrichtlinien der Einheit entspricht. Sicherheits- und Kennwortrichtlinien können variieren.

    Wenn die Einheit von XClarity Administrator verwaltet wird, wird der Management-Controller in die zentrale Benutzerverwaltung versetzt. Das bedeutet, dass die im internen oder externen XClarity Administrator-Authentifizierungsserver definierten Benutzeraccounts auch für die Anmeldung beim Management-Controller genutzt werden. Es wird ein neuer, lokaler Benutzeraccount namens RECOVERY_ID erstellt, wobei alle anderen lokalen Accounts auf dem Management-Controller deaktiviert werden.

Bei einem Fehlschlagen des Verwaltungsprozesses während der Konfiguration der zentralen Benutzerverwaltung werden die lokalen Benutzeraccounts auf dem Management-Controller möglicherweise deaktiviert. Führen Sie die folgenden Schritte aus, um die lokalen Benutzeraccounts wiederherzustellen:

- Converged-, NeXtScale- und System x-Server
  a. Melden Sie sich mit dem RECOVERY_ID-Benutzerkonto bei der Verwaltungswebschnittstelle für den Server an.
  b. Klicken Sie auf **IMM-Verwaltung → Benutzer**.
  c. Konfigurieren Sie als Benutzerauthentifizierungsverfahren auf dem Management-Controller die Option **Erst lokal, danach LDAP**.
     1) Klicken Sie auf **Globale Anmeldeeinstellungen**. Das gleichnamige Dialogfenster wird angezeigt.
     2) Klicken Sie auf die Registerkarte **Allgemein**.
     3) Wählen Sie als Benutzerauthentifizierungsverfahren die Option **Erst lokal, danach LDAP** aus und klicken Sie auf **OK**.
  d. Löschen Sie alle lokalen Benutzeraccounts und erstellen Sie sie erneut (außer dem RECOVERY_ ID-Benutzeraccount).
  e. Versuchen Sie, das Gehäuse wieder zu verwalten. Verwenden Sie dazu die Option **Verwaltung erzwingen**, um alle vom vorherigen Verwaltungsversuch verbliebenen CIM-Abonnements zu bereinigen.
- Gehäuse
  a. Melden Sie sich über eine SSH-Sitzung mit dem RECOVERY_ID-Benutzerkonto bei der Verwaltungs-Befehlszeilenschnittstelle für das Gehäuse an.
  b. Führen Sie den folgenden Befehl aus, um die zentrale Benutzerverwaltung zu deaktivieren und eine Authentifizierung mit lokalen Benutzerkonten beim Management-Controller und anderen Gehäusekomponenten zuzulassen.

     Anmerkung: Nach der Ausführung dieses Befehls wird der RECOVERY_ID-Benutzeraccount aus der Benutzerregistrierung entfernt. Die Befehlszeilenschnittstellen-Sitzung wird beendet. Sie können sich jetzt beim Management-Controller und anderen Gehäusekomponenten mit lokalen Benutzeraccounts authentifizieren.

     ```
     fsmcm -off -T mm[p]
     ```
  c. Versuchen Sie, das Gehäuse wieder zu verwalten. Verwenden Sie dazu die Option **Verwaltung erzwingen**, um alle vom vorherigen Verwaltungsversuch verbliebenen CIM-Abonnements zu bereinigen.

11. RackSwitch-Switches:
    - Vergewissern Sie sich, dass SSH auf dem Switch aktiviert ist.
    - Falls festgelegt, überprüfen Sie, ob das „Enable“-Kennwort korrekt ist, mit dem der Privileged Exec-Modus auf dem Switch aktiviert wird.
12. System x3950 X6-Server müssen als zwei 4U-Gehäuse mit jeweils einem eigenen Baseboard Management Controller verwaltet werden.
13. Wenn die Systemplatine in der Einheit ersetzt wurde, wurde für die Einheit eine neue Seriennummer und UUID vergeben. Wenn XClarity Administrator die Einheit als dieselbe Einheit wie vor dem Austausch erkennen soll, müssen Sie die Seriennummer und UUID aktualisieren, damit sie mit der vorherigen übereinstimmt. Anweisungen hierzu finden Sie in der Dokumentation der Einheit.
14. Wenn die Einheit von XClarity Administrator verwaltet wurde, aber keine ordnungsgemäße Aufhebung der Verwaltung stattfand, finden Sie in den folgenden Themen Informationen zu Wiederherstellungsverfahren:

- Gehäuseverwaltung mit einem CMM nach einem Verwaltungsserverausfall wiederherstellen in der XClarity Administrator-Onlinedokumentation
- Serververwaltung nach einem Verwaltungsserverausfall wiederherstellen in der XClarity Administrator-Onlinedokumentation
- RackSwitch-Switch wiederherstellen, für den die Verwaltung nicht ordnungsgemäß aufgehoben wurde in der XClarity Administrator-Onlinedokumentation
- Verwaltung mit einer Lenovo Storage-Einheit nach einem Verwaltungsserverausfall wiederherstellen in der XClarity Administrator-Onlinedokumentation

Speichereinheit kann aufgrund eines ungültigen SSL-/TSL-Zertifikats nicht verwaltet werden

Verwenden Sie diese Informationen, um Fehler beim Verwalten von Speichereinheiten zu beheben.

Jede Einheit hat ein selbst signiertes SSL-Zertifikat, das Lenovo XClarity Administrator verwendet, um über HTTPS mit der Einheit zu kommunizieren. Dieses Zertifikat hat einen allgemeinen Namen (Common Name, CN), der den Hostnamen (oder die IP-Adresse) angibt, der dem Zertifikat zugeordnet wurde. Der allgemeine Name stellt den Namen dar, der durch das SSL-Zertifikat geschützt wird. Das Zertifikat ist nur gültig, wenn der Hostname der Anforderung mit dem allgemeinen Zertifikatsnamen übereinstimmt. Bei einer Änderung der IP-Adresse der Speichereinheit wird das vorhandene Zertifikat folglich ungültig und kann von XClarity Administrator aufgrund eines ungültigen SSL/TSL-Zertifikats nicht verwaltet werden.

Gehen Sie wie folgt vor, um dieses Problem zu lösen:

- Stellen Sie sicher, dass die IP-Adresse im CN-Wert des Zertifikats, das von der DE-Speichereinheit gesendet wurde, das Format IPv4 aufweist.
- Stellen Sie sicher, dass das vorhandene SSL-/TSL-Zertifikat gültig ist.
  - Setzen Sie bei Lenovo ThinkSystem DE-Speichereinheiten das Verwaltungszertifikat der Speichereinheit auf das werkseitige selbst signierte Zertifikat zurück. Weitere Informationen finden Sie unter Verwaltungszertifikate zurücksetzen in der Onlinedokumentation von ThinkSystem Storage DE Serie.
  - Starten Sie bei Lenovo ThinkSystem DS-Speichereinheiten die Management-Controller in der Speichereinheit mithilfe der Verwaltungswebschnittstelle oder der Befehlszeilenschnittstelle neu, um das Zertifikat mit dem richtigen CN und der neuen IP-Adresse oder dem Hostnamen neu zu generieren.

Switch kann aufgrund eines ungültigen SSL-/TSL-Zertifikats nicht verwaltet werden

Mithilfe der Informationen in diesem Abschnitt können Sie Zertifikatsprobleme bei der Verwaltung von Switches beheben, auf denen CNOS ausgeführt wird.

Jede Einheit hat ein selbst signiertes SSL-Zertifikat, das Lenovo XClarity Administrator verwendet, um über HTTPS mit der Einheit zu kommunizieren. Wenn Sie das Zertifikat auf dem Switch löschen oder neu generieren, schlägt die Kommunikation zwischen dem Switch und XClarity Administrator fehl und der Switch wird als offline angezeigt.

Wählen Sie zum Beheben dieses Problems über die Seite „Alle Switches“ den Switch aus und klicken Sie auf **Alle Aktionen → Sicherheit → Nicht vertrauenswürdige Zertifikate auflösen**.

Nach dem Ersetzen der rückseitigen LED-Karte oder Mittelplatinenbaugruppe kann die Konnektivität für ein verwaltetes Flex System-Gehäuse nicht wiederhergestellt werden

Lenovo XClarity Administrator verwaltet Einheiten mithilfe der UUID und einem UUID-basierten vertrauenswürdigen Zertifikat. Bei einem Flex System-Gehäuse wird die UUID wird als Teil der elementaren Produktdaten (LED) auf der rückseitigen LED-Karte gespeichert, die sich auf der Mittelplatinenbaugruppe befindet. Wenn Sie die rückseitige LED-Karte oder Mittelplatinenbaugruppe ersetzen, müssen Sie die UUID der ersetzten rückseitigen LED-Karten auf die neue rückseitige LED-Karte übertragen.

1. Rufen Sie die UUID für das Gehäuse auf. Wenn das Gehäuse nicht funktioniert, können Sie die UUID beziehen, indem Sie sich an den Support wenden und den Maschinentyp sowie die Seriennummer angeben, die sich auf den Gehäuseetiketten befinden.
2. Ändern Sie die UUID für das Gehäuse. Lesen Sie Lenovo Flex System-Onlinedokumentation, um Anweisungen für den Austausch der Mittelplatine/rückseitigen LED-Karte für Ihre Einheit und für die Änderung der UUID zu erhalten.
3. Lösen Sie nicht vertrauenswürdige Zertifikate für das Gehäuse auf.
   a. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Gehäuse**. Die Seite „Alle Gehäuse“ wird angezeigt.
   b. Wählen Sie das Gehäuse mit dem ausgetauschten Teil aus.
   c. Klicken Sie auf **Alle Aktionen → Sicherheit → Nicht vertrauenswürdige Zertifikate auflösen**.
   d. Wählen Sie **Zertifikat installieren** aus.

   XClarity Administrator ruft das aktuelle Zertifikat aus dem Zielgehäuse ab und platziert es im XClarity Administrator Truststore, wodurch das vorherige Zertifikat für das Gehäuse außer Kraft gesetzt wird.
4. Aktualisieren Sie den Bestand für das Gehäuse. Klicken Sie dazu auf **Alle Aktionen → Bestand → Bestand aktualisieren**.

Konnektivität des verwalteten Servers kann nach dem Austausch der Systemplatine nicht wiederhergestellt werden

Lenovo XClarity Administrator verwaltet Einheiten mithilfe der UUID und einem UUID-basierten vertrauenswürdigen Zertifikat. Bei Servern wir die UUID als Teil der elementaren Produktdaten (VPD) auf der Systemplatine gespeichert. Wenn Sie die Systemplatine austauschen, müssen Sie die UUID der ausgetauschten Systemplatine auf die neue Systemplatine übertragen.

Wichtig: Als bewährte Vorgehensweise sollten Sie vor dem Austausch der Systemplatine die Verwaltung des Servers aufheben. Sie können den Server wieder verwalten, nachdem Sie die Systemplatine ersetzt haben.

Um die UUID der ausgetauschten Systemplatine an die neue Systemplatine zu übertragen, führen Sie die folgenden Schritte aus.

1. Rufen Sie die UUID für den Server auf. Wenn der Server nicht funktioniert, können Sie die UUID beziehen, indem Sie sich an den Support wenden und den Maschinentyp sowie die Seriennummer angeben, die sich auf den Serveretiketten befinden.
2. Ändern Sie die UUID für den Server. Lesen Sie das Hardwarehandbuch für Ihre Einheit, um Anweisungen für den Austausch von Komponenten und für die Änderung der UUID zu erhalten.
3. Lösen Sie nicht vertrauenswürdige Zertifikate für den Server auf.
   a. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Server**. Die Seite „Alle Gehäuse“ wird angezeigt.

b. Wählen Sie den Server mit dem ausgetauschten Teil aus.

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

d. Wählen Sie **Zertifikat installieren** aus.

XClarity Administrator ruft das aktuelle Zertifikat aus dem Zielserver ab und platziert es im XClarity Administrator Truststore, wodurch das vorherige Zertifikat für den Server außer Kraft gesetzt wird.

4. Aktualisieren Sie den Bestand für den Server. Klicken Sie dazu auf **Alle Aktionen → Bestand → Bestand aktualisieren**.

Kapselung ist nicht deaktiviert, nachdem die Verwaltung eines Servers aufgehoben wurde

Wenn die globale Kapselung aktiviert ist, ändert sich der Kapselungsmodus in den „Kapselung-Lite“-Modus, wenn Sie einen Server verwalten. In der Regel wird bei der Aufhebung der Verwaltung eines Servers der Kapselungsmodus auf „normal“ (deaktiviert) zurückgesetzt.

Wenn der Kapselungsmodus sich nicht in „normal“ ändert, gehen Sie wie folgt vor, um die Kapselung zu deaktivieren:

1. Starten Sie den Baseboard Management Controller neu.
2. Stellen Sie von einem System, das zur Verwendung der IP-Adresse der ausgefallenen virtuellen Lenovo XClarity Administrator-Einheit konfiguriert ist, eine Verbindung zum Zielserver her. Deaktivieren Sie die Kapselung, indem Sie eine SSH-Sitzung zur Einheit öffnen und folgenden Befehl ausführen:
```
encaps lite off
```

Der Rechenknoten wird nach der Verwaltung nicht in der Benutzerschnittstelle angezeigt

Wenn Sie einen ThinkSystem SD530 in einem Gehäuse austauschen, ohne zuvor die Verwaltung des vorhandenen Servers aufzuheben, wird der neue Server möglicherweise nicht in der Benutzerschnittstelle angezeigt.

Um dieses Problem zu beheben, heben Sie die Verwaltung des Gehäuses mit der Option „Erzwingen“ auf und verwalten Sie alle ThinkSystem SD530-Systeme anschließend erneut in einem Gehäuse.

Stromversorgungsstatusstatus ist nicht korrekt

Wenn ein Server ohne Betriebssystem eingeschaltet ist, zeigt Lenovo XClarity Administrator möglicherweise einen falschen Stromversorgungsstatus für diesen Server an.

Führen Sie zum Beheben dieses Problems die folgenden Verfahren aus:

- Stellen Sie sicher, dass die Bare-Metal-Server ausgeschaltet sind.
- Starten Sie bei XClarity Administrator v1.2.2 oder höher das BIOS/UEFI (F1) Setup (siehe Einen Server ein- und ausschalten in der XClarity Administrator Onlinedokumentation).

Kapitel 6. Probleme bei Installation, Entfernung, Aktualisierung und Datenmigration

Verwenden Sie diese Informationen, um Probleme bei der Installation, Entfernung, Aktualisierung und Datenmigration zu beheben.

Keine Videoausgabe, wenn XClarity Administrator in Red Hat KVM installiert wird

Bei der Installation der virtuellen Lenovo XClarity Administrator-Einheit mit der Red Hat KVM-Benutzerschnittstelle erfolgt keine Videoausgabe über die Konsole. Das führt zu einem schwarzen Bildschirm, wenn Sie die XClarity Administrator-VM anstelle des VM-Banners mit der XClarity Administrator-IP-Info eingeschaltet haben.

Damit die Videoausgabe über die Konsole funktioniert, stellen Sie sicher, dass die Bildschirmeinheit auf **Cirrus** festgelegt ist, indem Sie den Bildschirm mit den virtuellen Hardwaredetails für XClarity Administrator öffnen und im linken Navigationsbereich auf **Video** klicken. Standardmäßig wird die Bildschirmeinheit von der Red Hat KVM-Benutzerschnittstelle auf QXL festgelegt.

Adapteränderungen werden nicht erkannt.

Lenovo XClarity Administrator erkennt die Änderungen nicht, nachdem Adapter entfernt, ausgetauscht oder konfiguriert wurden.

Starten Sie die Einheit neu, damit der Baseboard Management Controller (BMC) die Änderungen erkennen kann. Weitere Informationen hierzu finden Sie im Abschnitt System x-Onlinedokumentation.

Konfigurationsassistent kann bei der Erstkonfiguration nicht mit einem Webbrowser erreicht werden

Verwenden Sie diese Informationen, um Probleme bei der Erstkonfiguration von Lenovo XClarity Administrator zu beheben.

1. Stellen Sie sicher, dass Ihr physisches Hostsystem die Mindestsystemanforderungen erfüllt (siehe Unterstützte Hostsysteme in der XClarity Administrator Onlinedokumentation).
2. Stellen Sie sicher, dass Sie ein unterstütztes virtuelles System verwenden, das die Mindestsystemanforderungen erfüllt (siehe Unterstützte Hostsysteme in der XClarity Administrator Onlinedokumentation).
3. Stellen Sie sicher, dass die Webbrowserversion mit XClarity Administrator kompatibel ist. Eine Liste der unterstützten Webbrowser finden Sie unter Auf die XClarity Administrator-Webschnittstelle zugreifen in der XClarity Administrator-Onlinedokumentation.
4. Standardmäßig ist DHCP für Netzwerkkonfigurationen aktiviert. Überprüfen Sie, ob eine gültige IP-Adresse zugewiesen wurde, indem Sie sich lokal bei der virtuellen Maschine anmelden und den Befehl `ifconfig` ausführen. Wenn Sie eine statische Konfiguration verwenden, befolgen Sie die hier genannten Schritte, um Ihre Installation korrekt zu konfigurieren. Weitere Informationen finden Sie unter XClarity Administrator in VMware ESXi-basierten Umgebungen installieren in der Onlinedokumentation von XClarity Administrator.

© Copyright Lenovo 2015, 2025

Implementierung von Lenovo XClarity Administrator schlägt unerwartet fehl.

Verwenden Sie diese Informationen, um Probleme bei der Erstkonfiguration von Lenovo XClarity Administrator zu beheben.

1. Prüfen Sie das Ereignisprotokoll auf Ereignisse, die mit der Implementierung im Zusammenhang stehen, und beheben Sie diese zuerst. Weitere Informationen zum Ereignisprotokoll finden Sie unter Ereignisse handhaben in der Onlinedokumentation von XClarity Administrator.
2. Stellen Sie sicher, dass Ihr physisches Hostsystem die Mindestsystemanforderungen erfüllt.
3. Stellen Sie sicher, dass Ihr System oder virtuelles System die Mindestsystemanforderungen erfüllt.
4. Stellen Sie sicher, dass Sie eine unterstützte Verwaltung virtueller Maschinen verwenden.

Weitere Informationen zu den Anforderungen finden Sie unter Unterstützte Hostsysteme in der Onlinedokumentation von XClarity Administrator.

Lenovo XClarity Administrator-Aktualisierung fehlgeschlagen

Verwenden Sie diese Informationen, um Probleme bei der Aktualisierung von Lenovo XClarity Administrator zu beheben.

1. Stellen Sie sicher, dass Sie alle erforderlichen Aktualisierungen installiert haben.
2. Stellen Sie sicher, dass Sie die Benutzerberechtigungen haben, Aktualisierungen zu installieren.

Weitere Informationen zum Aktualisieren von XClarity Administrator finden Sie unter XClarity Administrator-Verwaltungsserver aktualisieren in der Onlinedokumentation von XClarity Administrator.

Kapitel 7. Verbindungsprobleme

Mithilfe der Informationen in diesem Abschnitt können Sie Konnektivitätsprobleme beheben.

Zugriff auf Lenovo XClarity Administrator nicht möglich

Verwenden Sie diese Informationen, um Probleme beim Zugriff auf Lenovo XClarity Administrator zu beheben.

Wenn das Hostbetriebssystem unerwartet heruntergefahren wurde, stellen Sie XClarity Administrator von der letzten Sicherung wieder her. Weitere Informationen zum Sichern und Wiederherstellen von XClarity Administrator finden Sie unter XClarity Administrator sichern und wiederherstellen in der XClarity Administrator-Onlinedokumentation.

Herstellen einer Verbindung zu Lenovo XClarity Administrator über den Safari-Browser nicht möglich

Verwenden Sie diese Informationen, um Probleme beim Herstellen der Verbindung mit XClarity Administrator über den Safari-Webbrowser zu beheben.

Wenn Sie versuchen, im Webbrowser Safari eine Verbindung mit der XClarity Administrator-Webschnittstelle herzustellen, wird eine Liste mit Clientzertifikaten angezeigt, die Ihrem Benutzeraccount zugeordnet sind. Eines dieser Zertifikate auszuwählen kann den Fehler „Keine Verbindung möglich“ verursachen. Dieses Problem kann u. U. dadurch verursacht werden, dass Safari versucht, ein Clientzertifikat an XClarity Administrator zu senden, dieses aber für den XClarity Administrator-Server ungültig ist. Um das Problem zu beheben, löschen Sie das Clientzertifikat und versuchen Sie erneut, die Verbindung mit der XClarity Administrator-Webschnittstelle herzustellen. Weitere Informationen zu diesem Problem bei Verwendung des Safari-Browsers finden Sie unter Website zu Problemen mit Safari-Clientzertifikaten.

Anmelden nicht möglich

Verwenden Sie diese Informationen, um Probleme mit der Anmeldung bei Lenovo XClarity Administrator, dem CMM und dem Baseboard Management Controller zu beheben.

Anmelden bei Lenovo XClarity Administrator nicht möglich

Verwenden Sie diese Informationen, um Probleme mit der Anmeldung bei Lenovo XClarity Administrator zu beheben.

1. Stellen Sie sicher, dass das Kennwort richtig ist und die Feststelltaste und die Num-Taste nicht aktiviert sind.
2. Vergewissern Sie sich, dass der Benutzeraccount nicht gesperrt ist. Ist dies der Fall, lassen Sie die Sperre durch einen Supervisor aufheben (siehe Einen Benutzer freigeben in der XClarity Administrator-Onlinedokumentation).
3. Stellen Sie sicher, dass der Benutzeraccount nicht deaktiviert ist. Sollte er deaktiviert sein, lassen Sie den Benutzeraccount durch einen Supervisor aktivieren (siehe Einen Benutzer aktivieren oder deaktivieren in der XClarity Administrator-Onlinedokumentation).
4. Wenn Sie einen externen Authentifizierungsserver verwenden:
   a. Stellen Sie sicher, dass die richtigen Rollengruppen in XClarity Administrator konfiguriert sind. Weitere Informationen zu Rollengruppen finden Sie unter Rollengruppe verwalten in der Lenovo XClarity Administrator-Onlinedokumentation.

© Copyright Lenovo 2015, 2025

b. Überzeugen Sie sich davon, dass die Benutzeraccounts auf dem externen Authentifizierungsserver als Mitglieder einer dieser Rollengruppen definiert sind.

c. Wenn Sie das Kennwort für den Client-Account geändert haben, der für die Bindung von XClarity Administrator an den externen Authentifizierungsserver verwendet wird, kontrollieren Sie, ob Sie das neue Kennwort auch in der XClarity Administrator-Webschnittstelle aktualisiert haben:

   1) Melden Sie sich bei XClarity Administrator mit dem derzeit in XClarity Administrator definierten Clientnamen und Kennwort an (siehe Externen Authentifizierungsserver konfigurieren in der XClarity Administrator-Onlinedokumentation).
   2) Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.
   3) Klicken Sie im Abschnitt „Benutzer und Gruppen“ auf **LDAP-Client**, um das Dialogfenster LDAP-Clienteinstellungen anzuzeigen.
   4) Aktualisieren Sie das Kennwort im Feld **Clientkennwort** und klicken Sie auf **Übernehmen**.

   Wenn das Clientkonto aufgrund zu vieler fehlgeschlagener Anmeldeversuche nach der Änderung des Kennworts im externen Authentifizierungsserver gesperrt wurde, können Sie die Accountsperre entweder direkt im externen Authentifizierungsserver aufheben oder warten, bis der Sperrzeitraum abgelaufen ist, bevor Sie versuchen, das Kennwort in XClarity Administrator zu ändern.

d. Wenn das Kennwort für den Client-Account, der für die Bindung von XClarity Administrator an den externen Authentifizierungsserver verwendet wird, abgelaufen ist, führen Sie die folgenden Schritte aus, um das Konto zu entsperren und das Kennwort in XClarity Administrator zu ändern:

   1) Heben Sie die Sperre für den Client-Account auf und ändern Sie das Clientkennwort im externen Authentifizierungsserver.
   2) Melden Sie sich bei XClarity Administrator mit dem derzeit in XClarity Administrator definierten Clientnamen und Kennwort an (siehe Externen Authentifizierungsserver konfigurieren in der XClarity Administrator-Onlinedokumentation).
   3) Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Sicherheit**.
   4) Klicken Sie im Abschnitt „Benutzer und Gruppen“ auf **LDAP-Client**, um das Dialogfenster LDAP-Clienteinstellungen anzuzeigen.
   5) Aktualisieren Sie das Kennwort im Feld **Clientkennwort** und klicken Sie auf **Übernehmen**.

5. Wenn das Hostbetriebssystem unerwartet heruntergefahren wurde und Sie nun einen Authentifizierungsfehler erhalten, stellen Sie XClarity Administrator von der letzten Sicherung wieder her. Weitere Informationen zum Sichern und Wiederherstellen von XClarity Administrator finden Sie unter XClarity Administrator sichern und wiederherstellen in der XClarity Administrator-Onlinedokumentation.

Kennwort für eine lokale Wiederherstellung oder einen Supervisor-Benutzer vergessen

Wenn kein anderes Supervisor-Konto vorhanden ist, können Sie das Kennwort für einen lokalen Benutzer mit der Berechtigung **lxc-recovery** oder **lxc-supervisor** zurücksetzen, indem Sie ein ISO-Image anhängen, das eine Konfigurationsdatei mit dem neuen Kennwort enthält.

Vorbereitende Schritte

Achtung: Dieses Verfahren funktioniert nicht für XClarity Administrator v3.3.x und v3.4.x. Wenn Sie eine dieser Versionen verwenden, wenden Sie sich an den Lenovo Support, um Unterstützung beim Wiederherstellen des Zugriffs auf XClarity Administrator zu erhalten.

Um das Kennwort mit dieser Methode zurückzusetzen, müssen Sie Zugriff auf das XClarity Administrator-Hostsystem haben.

Der Benutzername, der zurückgesetzt wird, muss die Berechtigung **lxc-recovery** oder **lxc-supervisor** besitzen.

Das Kennwort muss die gleichen Überprüfungsregeln befolgen, die von XClarity Administrator erzwungen werden.

Nachdem das Kennwort zurückgesetzt wurde, muss der Benutzer das Kennwort beim ersten Zugriff nicht ändern.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das ISO-Image zu erstellen und anzuhängen.

1. Schalten Sie die virtuelle Maschine aus.
2. Erstellen Sie eine Datei namens `passwordreset.properties`, die die folgenden Parameter enthält.
   ```
   user=
   password=
   ```
   Sie können die Datei mit dem Befehl „echo“ erstellen, z. B.:
   ```
   ECHO user=admin > ./ passwordreset.properties
   ECHO password=New_PasswOrd >> ./ passwordreset.properties
   ```
3. Erstellen Sie ein ISO-Image, das die Datei „passwordreset.properties“ enthält.

   Verwenden Sie die von Ihnen bevorzugte ISO-Software, um ein ISO-Image unter Windows zu erstellen. Verwenden Sie unter Linux den Befehl `mkisofs`, z. B:

   ```
   mkisofs -V passreset -J -o ./passreset.iso ./passwordreset.properties
   ```

   Dabei steht **-V** für den Volumenamen, **-J** ist das Joliet-Format, **-o** gibt den Namen der Ausgabedatei an und **/ passwordreset.properties** ist die Datei, die in das ISO-Image eingebunden werden soll.
4. Laden Sie das ISO-Image mit dem Datastore-Browser an einen geeigneten Speicherort hoch.
5. Stellen Sie das ISO-Image auf der virtuellen Maschine bereit.
   - **Für Citrix**:
     a. Stellen Sie das konfigurierte ISO-Image als physisches CD-Laufwerk auf der virtuellen Maschine bereit.
     b. Wählen Sie in Citrix die virtuelle XClarity Administrator-Maschine aus.
     c. Klicken Sie auf die Registerkarte **Konsole**.
     d. Wählen Sie aus der Laufwerkliste das physische CD-Laufwerk aus.
   - **Für Nutanix AHV-Hosts:**
     a. Klicken Sie auf das Menü **Einstellungen** (⚙) und klicken Sie dann **Image-Konfiguration**, um das Dialogfeld für die Image-Konfiguration anzuzeigen.
     b. Laden Sie das `eth0_config.iso`-Image hoch.
        1) Klicken Sie im Dialogfeld „Image-Konfiguration“ auf **Image hochladen**, um erneut das Dialogfeld zum Erstellen des Image anzuzeigen.
        2) Geben Sie einen Namen für das ISO-Image an.
        3) Wählen Sie ISO für den Image-Typ aus.
        4) Wählen Sie **Eine Datei hochladen** aus, klicken Sie auf **Datei auswählen** und wählen Sie das `eth0_config.iso`-Image aus.
        5) Klicken Sie auf **Speichern**, um die Datei hochzuladen.
        6) Klicken Sie auf **Schließen**, um das Dialogfenster „Image-Konfiguration“ zu schließen.

c. Warten Sie, bis die Hochladeprozesse abgeschlossen sind, bevor Sie mit den Einrichtungsschritten fortfahren. Der Statuskreis im Menü gibt an, wann die Prozesse abgeschlossen sind.

d. Fügen Sie einen Datenträger für das `eth0_config.iso`-Image hinzu.

1) Klicken Sie auf der VM in der unteren Menüleiste auf **Aktualisieren**.

2) Klicken Sie auf das Symbol **Bearbeiten**, damit die CD-ROM das Dialogfeld „Datenträger bearbeiten“ anzeigt.

3) Wählen Sie **Klonen** vom Image-Service für die Operationen aus.

4) Wählen Sie das ISO-Image aus, das Sie zuvor aus der Image-Liste erstellt haben.

5) Klicken Sie auf **Aktualisieren**.

6) Klicken Sie auf **Speichern**.

- **Für RedHat KVM-Hosts:**

a. Wählen Sie im Virtual Machine Manager die virtuelle Maschine aus und klicken Sie dann auf **Hardware hinzufügen**, um das Dialogfenster „Neue virtuelle Hardware hinzufügen“ zu öffnen.

b. Klicken Sie auf die Registerkarte **Speicher**.

c. Wählen Sie **Verwalteten oder anderen vorhandenen Speicher auswählen**, klicken Sie auf **Durchsuchen** und wählen Sie dann das Image `eth0_config.iso` aus.

d. Geben Sie als Einheitentyp **VirtIO** an.

Anmerkung: Für XClarity Administrator bis Version 1.4.0 müssen Sie **IDE** für den Disk-Bus auswählen.

e. Wählen Sie **Kein** als Cachemodus aus.

f. Klicken Sie auf **Fertig stellen**.

- **Für VMware ESXi-Hosts:**

Die ISO-Datei muss im Datenspeicher des ESXi-Hosts sein, damit sie als CD/DVD-Laufwerk auf der virtuellen XClarity Administrator-Maschine bereitgestellt werden kann.

a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Einstellungen bearbeiten**.
b. Klicken Sie auf **Hinzufügen**, um den Assistenten für Hardware hinzufügen aufzurufen.
c. Klicken Sie auf **CD/DVD-Laufwerk** und auf **Weiter**.
d. Wählen Sie **ISO-Image verwenden** aus und klicken Sie auf **Weiter**.
e. Markieren Sie das ISO-Image und klicken Sie auf **Weiter**.
f. Wählen Sie den Knoten mit der virtuellen Einheit aus und klicken Sie auf **Weiter**.
g. Klicken Sie auf **Fertig stellen**.

- **Für Windows Hyper-V-Hosts:**

Wichtig: Die virtuelle Maschine muss vor der ISO-Imagebereitstellung ausgeschaltet sein.

a. Klicken Sie im Fenster „Hyper-V-Manager“ mit der rechten Maustaste auf die virtuelle Einheit und klicken Sie dann auf **Verbinden**, um das Fenster „Verbindung mit virtuellen Computern“ anzuzeigen.

b. Klicken Sie auf **Datenträger → DVD-Laufwerk → Datenträger einlegen**.

c. Markieren Sie das ISO-Image und klicken Sie auf **Öffnen**.

6. Schalten Sie die virtuelle Maschine ein und melden Sie sich bei der XClarity Administrator-Webschnittstelle mit dem Benutzernamen und Kennwort an, die in der Datei `passwordreset.properties` angegeben sind (siehe Auf die XClarity Administrator-Webschnittstelle zugreifen in der Onlinedokumentation von XClarity Administrator).
7. Hängen Sie das Laufwerk ab und löschen Sie das ISO-Image.

- Für Citrix
  a. Wählen Sie bei Citrix Hypervisor die virtuelle XClarity Administrator-Maschine aus.
  b. Klicken Sie auf die Registerkarte **Konsole**.
  c. Löschen Sie die physische CD mit dem konfigurierten ISO-Image aus der Treiberliste.
- **Für Nutanix AHV-Hosts:**
  a. Klicken Sie auf der VM in der unteren Menüleiste auf **Aktualisieren**.
  b. Klicken Sie auf das Symbol **Bearbeiten**, damit die CD-ROM das Dialogfeld „Datenträger bearbeiten“ anzeigt.
  c. Klicken Sie auf das Symbol **Auswerfen**.
  d. Klicken Sie auf **Speichern**.
- **Für VMware ESXi-Hosts:**
  a. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann auf **Einstellungen bearbeiten**.
  b. Wählen Sie das angehängte Laufwerk aus der Liste der Hardware und klicken Sie auf **Entfernen**.
  c. Klicken Sie auf **OK**. Das Laufwerk wird jetzt getrennt.
  d. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie dann erneut auf **Einstellungen bearbeiten**.
  e. Wählen Sie das Laufwerk aus der Liste der Hardware und deaktivieren Sie das Kontrollkästchen **Beim Einschalten verbinden**.
  f. Klicken Sie auf **OK**.
  g. Löschen Sie das ISO-Image aus dem Datenspeicher.
- **Für Windows Hyper-V-Hosts:**
  a. Klicken Sie im Fenster „Hyper-V-Manager“ mit der rechten Maustaste auf die virtuelle Einheit und klicken Sie dann auf **Verbinden**, um das Fenster „Verbindung mit virtuellen Computern“ anzuzeigen.
  b. Klicken Sie auf **Datenträger → DVD-Laufwerk →** *iso_image_name*.**iso auswerfen**.
  c. Löschen Sie das ISO-Image aus dem Datenspeicher.

Direkte Anmeldung beim verwalteten CMM nicht möglich

Verwenden Sie diese Informationen, um Probleme mit der direkten Anmeldung bei einem verwalteten CMM zu beheben.

1. Stellen Sie sicher, dass das Kennwort richtig ist und die Feststelltaste und die Num-Taste nicht aktiviert sind.
2. Stellen Sie sicher, dass die Anmeldeinformationen mit denen übereinstimmen, die in Lenovo XClarity Administrator gespeichert sind. Wenn das CMM von XClarity Administrator verwaltet wird, können Sie sich nicht mit lokalen CMM-Accounts anmelden. Weitere Informationen über die zentrale und dezentrale Benutzerverwaltung in XClarity Administrator finden Sie unter Authentifizierungsserver verwalten in der Onlinedokumentation von XClarity Administrator.

Direkte Anmeldung beim Management-Controller nicht möglich

Verwenden Sie diese Informationen, um Probleme mit der direkten Anmeldung bei einem Management-Controller zu beheben.

1. Stellen Sie sicher, dass das Kennwort richtig ist und die Feststelltaste und die Num-Taste nicht aktiviert sind.

2. Stellen Sie sicher, dass die Anmeldeinformationen mit denen übereinstimmen, die in Lenovo XClarity Administrator gespeichert sind.
3. Überprüfen Sie, ob die Management-Controller-Version mit XClarity Administrator kompatibel ist.
4. Stellen Sie sicher, dass nur ein XClarity Administrator-Server den Management-Controller verwaltet.

Anmelden bei Flex Power System-Servern nicht möglich

Verwenden Sie diese Informationen, um Fehler zu beheben, wenn Sie sich direkt bei einem verwalteten Flex Power System-Server anmelden – Lenovo XClarity Administrator

Falls ein Gehäuse sowohl Flex System- als auch Flex Power System-Server enthält, können Sie sich u. U. aufgrund von Authentifizierungsproblemen nicht direkt an den Flex Power System-Server anmelden.

Bei einer Verwaltung des Gehäuses durch XClarity Administrator wird das CMM in den zentralen Verwaltungsmodus versetzt. Das bedeutet, dass die im internen oder externen Authentifizierungsserver definierten Benutzeraccounts auch für die Anmeldung beim Chassis Management Module (CMM) genutzt werden und lokale CMM-Benutzeraccounts deaktiviert werden.

Verwenden Sie für die Anmeldung bei der Management-Controller-Webschnittstelle eines verwalteten Flex Power System-Server den RECOVERY_ID-Account, der bei der Verwaltung des Gehäuses durch XClarity Administrator erstellt wurde. Melden Sie sich beim CMM mit diesem Account an und ändern Sie das Kennwort. (Das Kennwort muss beim ersten Zugriff geändert werden.) Danach können Sie sich bei der Management-Controller-Webschnittstelle des Power System-Knotens mit dem RECOVERY_ID-Account anmelden.

Wenn Sie einen Flex Power System-Knoten über eine HMC (Hardware Management Console) verwalten möchten, gehen Sie wie folgt vor:

1. Verwenden Sie SSH, um sich bei der Verwaltungs-Befehlszeilenschnittstelle anzumelden.
2. Führen Sie die folgenden Befehle aus, um als Benutzerauthentifizierungsverfahren für das CMM die Option **Erst lokale, danach externe Authentifizierung** zu konfigurieren und den USERID-Account zu löschen und erneut zu erstellen.
```
env -T mm[p]
accseccfg –am localldap
users -n USERID –clear
users -add -n USERID -p <password> -g Supervisor -ms 0
```

Plötzlicher Verbindungsausfall bei einer Einheit

Verwenden Sie diese Informationen, um Probleme beim Herstellen der Verbindung mit einer einzelnen Einheit zu beheben.

1. Wenn die Einheit, die gespeicherte Anmeldeinformationen verwendet, offline ist, prüfen Sie, ob die gespeicherten Anmeldeinformationen abgelaufen oder ungültig sind. Falls sie abgelaufen oder ungültig sind, gehen Sie wie folgt vor:
   a. Wählen Sie über die Seite „Alle Einheiten“ die Einheit aus, die aufgelöst werden soll.
   b. Klicken Sie auf **Alle Aktionen → Sicherheit → Gespeicherte Anmeldeinformationen auflösen**.
   c. Ändern Sie das Kennwort für gespeicherte Anmeldeinformationen oder wählen Sie andere gespeicherte Anmeldeinformationen aus, um diese für die verwaltete Einheit zu verwenden.
2. Prüfen Sie das Ereignisprotokoll auf Netzwerkereignisse für die Einheit und beheben Sie diese zuerst. Weitere Informationen zum Ereignisprotokoll finden Sie unter Ereignisse handhaben in der Onlinedokumentation von Lenovo XClarity Administrator.

3. Stellen Sie sicher, dass die Netzwerkhardware für den Verbindungspfad zur Einheit ordnungsgemäß funktioniert.
4. Stellen Sie sicher, dass die richtigen Switch- und Firewallanschlüsse für die Einheit aktiviert sind. Informationen zu erforderlichen Anschlüssen finden Sie unter Portverfügbarkeit in der Onlinedokumentation von XClarity Administrator.
5. Stellen Sie sicher, dass die Einheit über eine gültige Netzwerkkonfiguration verfügt, indem Sie sich bei der Einheit anmelden und prüfen, ob die IP-Adresse für das Netzwerk gültig ist. Sie können für die Einheit auch einen Pingtest durchführen, um zu testen, ob sie im Netzwerk sichtbar ist.
6. Versuchen Sie, sich direkt bei der Einheit anzumelden.

Kapitel 8. Lenovo XClarity Administrator-Konfigurationsprobleme

Verwenden Sie diese Informationen, um Probleme mit der Konfiguration von Lenovo XClarity Administrator zu beheben.

Externe LDAP-Konfigurationsprobleme

Verwenden Sie diese Informationen, um Fehler beim Konfigurieren eines externen Authentifizierungsservers zu beheben.

1. Stellen Sie sicher, dass der definierte Name des Stammelements richtig ist.
2. Überprüfen Sie, ob der Lenovo XClarity Administrator-Benutzeraccount Mitglied von mindestens einer Rollengruppe ist. Weitere Informationen zu Rollengruppen finden Sie unter Rollengruppe verwalten in der XClarity Administrator-Onlinedokumentation.
3. Stellen Sie sicher, dass die XClarity Administrator-Rollengruppe mindestens einer Rollengruppe auf dem LDAP-Server entspricht.
4. Wenn Sie vorkonfigurierte Serveradressen verwenden, müssen Sie kontrollieren, ob die IP-Adresse und die Portnummer des Servers korrekt sind.
5. Stellen Sie sicher, dass die DNS-Konfigurationseinstellungen korrekt sind.
6. Wenn Sie DNS für die Serverermittlung nutzen, müssen Sie sich vergewissern, dass der Domänenname und der Gesamtstrukturname richtig sind.
7. Stellen Sie sicher, dass der definierte Clientname und das Kennwort richtig sind.

Informationen zur Installation des externen Authentifizierungsservers finden Sie unter Externen Authentifizierungsserver konfigurieren in der Onlinedokumentation von XClarity Administrator.

Benutzer hat keine ausreichende Berechtigung zum Konfigurieren des Servers.

Verwenden Sie diese Informationen, um Probleme bei der Konfiguration verwalteter Server zu beheben.

1. Stellen Sie sicher, dass Sie bei einem Benutzeraccount angemeldet sind, der zu einer Supervisor- oder Administrator-Rollengruppe gehört. Weitere Informationen zu Benutzerrollen finden Sie unter Rollengruppe verwalten in der Onlinedokumentation von Lenovo XClarity Administrator.
2. Wenden Sie sich an Ihren Systemadministrator, um Ihre Berechtigungen zu aktualisieren.

Aktivierungsprobleme bei Features on Demand

Verwenden Sie diese Informationen, um Fehler beim Aktivieren von Features zu beheben.

Stellen Sie sicher, dass Sie die Anleitung für das Tool befolgen, das Sie verwenden, um den FoD-Schlüssel (FoD – Features on Demand) zu übernehmen. Weitere Informationen zu FoD-Schlüsseln finden Sie unter FoD-Schlüssel (Feature on Demand) anzeigen in der Lenovo XClarity Administrator-Onlinedokumentation.

VMware warnt davor, dass der VMXNET 3-Treiber nicht unterstützt wird.

Möglicherweise wird eine Warnung angezeigt, dass der VMXNET 3-Treiber nicht unterstützt wird, wenn sie Lenovo XClarity Administrator installieren, die Einstellungen für die virtuelle Maschine der XClarity

© Copyright Lenovo 2015, 2025

Administrator-Einheit bearbeiten, vmotion von XClarity Administrator ausführen oder innerhalb der mit VMware verknüpften Management- und Überwachungsinfrastruktur.

Die XClarity Administrator-Einheit enthält den VMXNET 3-Treiber. Sie können alle VMware-Fehler ignorieren, die besagen, dass der Treiber nicht unterstützt wird.

Kapitel 9. Leistungsprobleme

Verwenden Sie diese Informationen, um Leistungsprobleme zu beheben.

Leistungsprobleme mit Lenovo XClarity Administrator

Verwenden Sie diese Informationen, um Leistungsprobleme mit Lenovo XClarity Administrator zu beheben.

Wenn Sie eine Umgebung mit vielen Einheiten und vielen gleichzeitigen Benutzersitzungen betreiben und Sie eine herabgesetzte Systemleistung feststellen, verringern Sie die Anzahl der gleichzeitigen Benutzersitzungen zur XClarity Administrator-Webschnittstelle oder erhöhen Sie die virtuellen CPU-Ressourcen, die der virtuellen Einheit zugeordnet sind.

Stellen Sie sicher, dass die Ressourcen, die für die virtuelle Maschine verfügbar sind (Hauptspeicher, Festplattengröße, Prozessor), für die Anzahl der verwalteten Einheiten geeignet sind. Weitere Informationen zu den Anforderungen an virtuelle Maschinen finden Sie unter Unterstützte Hostsysteme in der Onlinedokumentation von XClarity Administrator.

Zusätzliche Leistungsaspekte und Tipps finden Sie im Whitepaper zur Leistung von XClarity Administrator.

Schlechte oder langsame Netzwerkleistung

Mithilfe der Informationen in diesem Abschnitt können Sie Probleme mit einer schlechten oder langsamen Netzwerkleistung beheben.

1. Stellen Sie sicher, dass keine größeren Netzwerkvorgänge ausgeführt werden, z. B. Systemerkennungen, Betriebssystembereitstellungen oder rollierende Firmwareaktualisierungen.
2. Stellen Sie sicher, dass das restliche Netzwerk mit einer nominalen Nutzung in Betrieb ist.
3. Wenn Sie Servicequalität (QoS) implementiert haben, stellen Sie sicher, dass diese so konfiguriert wurde, dass eine optimale Konnektivität zu Lenovo XClarity Administrator möglich ist.
4. Stellen Sie sicher, dass Ihre Netzwerktopologie für Konnektivität und Leistung von XClarity Administrator optimiert sind.

© Copyright Lenovo 2015, 2025

Kapitel 10. Sicherheitsprobleme

Verwenden Sie diese Informationen, um Sicherheitsprobleme zu beheben, einschließlich Benutzerverwaltung und Authentifizierung.

SSL-Zertifikat ist nicht vertrauenswürdig

Die Zertifikatskette enthält möglicherweise eine Signatur, die selbst signiert ist oder nicht von einer bekannten Zertifizierungsstelle stammt.

Ports 443, 3888, 9090, 50636, 50637

Jedes Lenovo XClarity Administrator-Instanz hat eine eindeutige, intern generierte Zertifizierungsstelle. Standardmäßig verwenden diese Ports (für die Kommunikation zwischen Benutzer und virtueller Einheit oder zwischen verwalteten Einheiten und virtueller Einheit) ein Zertifikat, das von dieser Zertifizierungsstelle signiert ist. Wenn das SSL-Zertifikat nicht vertrauenswürdig ist, generieren und implementieren Sie ein angepasstes, extern signiertes Serverzertifikat auf XClarity Administrator. Weitere Informationen finden Sie unter Angepasste Serverzertifikate in XClarity Administrator implementieren in der Onlinedokumentation von XClarity Administrator.

Port 8443

Jede XClarity Administrator-Instanz hat eine eindeutige Zertifizierungsstelle, die nur für die BS-Implementierung verwendet wird. Diese Zertifizierungsstelle signiert ein Zertifikat, das für den Zielserver an Port 8443 verwendet wird. Wenn die BS-Implementierung gestartet wird, ist das Zertifizierungsstellenzertifikat im BS-Image enthalten, das an den Zielserver weitergeleitet wird. Beim Implementierungsprozess stellt dieser Server wieder eine Verbindung mit Port 8443 her und überprüft das Zertifikat, das Port 8443 beim Handshake bereitstellen, da sie das Zertifizierungsstellenzertifikat haben.

Serverzertifizierungsüberprüfung fehlgeschlagen

Verwenden Sie diese Informationen, wenn Sie versuchen, ein Serverzertifikat in Lenovo XClarity Administrator zu installieren, aber die Überprüfung des Zertifikats fehlschlägt.

Zu dieser Aufgabe

Die Überprüfung des Serverzertifikats kann fehlschlagen, wenn XClarity Administrator Folgendes versucht:

- Verbindung zu den verwalteten Einheiten mithilfe von CIM-XML über HTTPS
- Erreichen eines externen Authentifizierungsservers mit sicherem LDAP (wenn Sie eine sichere LDAP-Verbindung konfiguriert haben)
- Erreichen eines externen SAML-Identity Providers mit einer sicheren Verbindung (wenn Sie SAML konfiguriert haben)
- Verbindung zu den Remote-Dateiservern zum Importieren von Betriebssystem-Images (wenn Sie einen HTTPS-Imageserver konfiguriert haben)
- Verbindung mit Lenovo, um Informationen zum Garantiestatus des Herstellers zu erhalten
- Verbindung mit Apple- und Google-Push-Benachrichtigungsservern (wenn Lenovo XClarity Mobile-Push-Benachrichtigungen für eine iOS- oder Android-Einheit aktiviert sind)

Vorgehensweise

Führen Sie zur Lösung des Problems die folgenden Schritte aus.

© Copyright Lenovo 2015, 2025

- Stellen Sie sicher, dass das Zertifikat oder sein Signaturzertifikat im Truststore für vertrauenswürdige Zertifikate oder im Truststore für Zertifikate für externe Dienste in XClarity Administrator vorhanden ist. Weitere Informationen zu vertrauenswürdigen Zertifikaten und Zertifikaten für externe Dienste finden Sie unter Mit Sicherheitszertifikaten arbeiten in der Onlinedokumentation von XClarity Administrator
- Stellen Sie sicher, dass das Zertifikat nicht widerrufen wurde (siehe Eine Zertifikatswiderrufliste hinzufügen und ersetzen in der Onlinedokumentation von XClarity Administrator).
- Stellen Sie sicher, dass die IP-Adresse oder der Hostname des Servers mit einem der alternativen Namen oder dem allgemeinen Namen (falls SAN nicht vorhanden) im Zertifikat übereinstimmt.
- Stellen Sie sicher, dass das heutige Datum zwischen den Angaben unter „Not valid before“ und „Not valid after“ im Zertifikat liegt.
- Stellen Sie sicher, dass das Zertifikat mit einem unterstützten Algorithmus signiert wird, entweder SHA1 oder stärker im traditionellen Modus oder SHA256 oder stärker im NIST Strict Mode (siehe Verschlüsselungsmodus und Kommunikationsprotokolle festlegen in der Onlinedokumentation von XClarity Administrator).

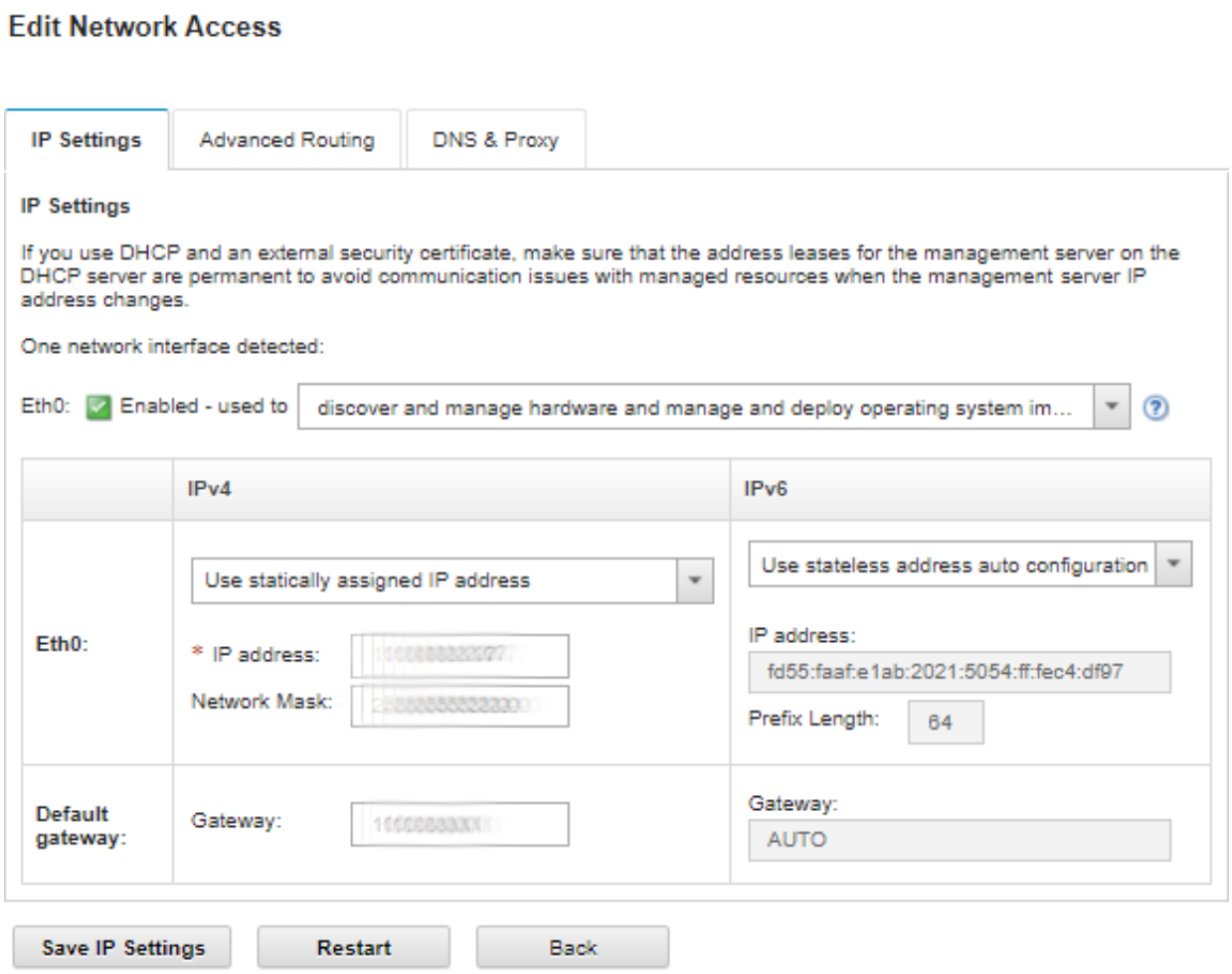
Sicherheitsrisiken bei Samba und Apache

Lenovo XClarity Administrator verwendet Samba- und Apache-Server bei der Implementierung von Betriebssystemen und der Aktualisierung von BS-Einheitentreibern als Remote-Freigabe mit Schreibschutz. Wenn Sie nicht beabsichtigen, XClarity Administrator zur Verwaltung von Betriebssystemen zu verwenden, können Sie die Samba- und Apache-Server deaktivieren, indem Sie die XClarity Administrator-Netzwerkrolle nur auf die Ermittlung und Verwaltung von Hardware festlegen.

Vorgehensweise

Gehen Sie wie folgt vor, um Samba- und Apache-Server zu deaktivieren.

1. Klicken Sie in der XClarity Administrator-Menüleiste auf **Verwaltung → Netzwerkzugriff**. Die aktuell definierten Netzwerkeinstellungen werden angezeigt.
2. Klicken Sie auf **Netzwerkzugriff bearbeiten**, um die Seite „Netzwerkzugriff bearbeiten“ anzuzeigen.



3. Wählen Sie die Option **Nur Hardware ermitteln und verwalten** für die Netzwerkschnittstelle.
4. Klicken Sie auf **IP-Einstellungen speichern**.
5. Klicken Sie auf **Neu starten**, um den Verwaltungsserver neu zu starten.

Kapitel 11. Fehlerbehebung bei Problemen mit Sicherung und Wiederherstellung

Verwenden Sie diese Informationen, um Probleme bei Sicherung und Wiederherstellung zu beheben.

Sicherungsvorgang scheint beim Neustart des Verwaltungsservers nicht mehr zu reagieren

Das Erstellen einer Lenovo XClarity Administrator-Sicherung kann eine Weile dauern. Eine Fortschrittsleiste zeigt den Status der Jobs an.

Vorgehensweise

Wenn der Sicherungsvorgang nicht mehr reagiert, gehen Sie wie folgt vor.

- Wenn die Schaltfläche **Abbrechen** angezeigt wird, können Sie den Sicherungsprozess abbrechen.
- Wenn die Schaltfläche **Abbrechen** nicht angezeigt wird, öffnen Sie eine neue Registerkarte, um festzustellen, ob die Schaltfläche **Abbrechen** erscheint.
- Wenn sich dadurch das Problem nicht beheben lässt, starten Sie die virtuelle Maschine neu.

Anmerkung: Wenn Sie den Sicherungsvorgang abbrechen oder die virtuelle Maschine neu starten, wird unter Umständen keine Sicherung erstellt.

XClarity Administrator Fenster ist nach einer Aktualisierung während der Sicherung leer

Lenovo XClarity Administrator ist während des Vorgangs stillgelegt, um zu verhindern, dass Daten geändert werden. Wenn Sie XClarity Administrator aktualisieren oder schließen, bevor der Sicherungsvorgang abgeschlossen ist und der Verwaltungsserver neu gestartet wurde, ist das XClarity Administrator Fenster möglicherweise leer, wenn sich der Verwaltungsserver noch im Stillstand befindet.

Vorgehensweise

Führen Sie zur Lösung des Problems die folgenden Schritte aus.

1. Aktualisieren Sie die Seite regelmäßig, um zu überprüfen, ob sie geladen wird.
2. Wenn das Fenster nach einer geraumen Zeit leer bleibt, starten Sie die virtuelle Maschine neu.
3. Wenn sie weiterhin nicht geladen wird, löschen Sie die Datei `/opt/lenovo/lxca/bin/QUIESCE_MODE_FLAG` manuell.

   Anmerkung: Dieser Schritt erfordert Rootzugriff. Wenden Sie sich an den Support, bevor Sie diesen Schritt ausführen.
4. Starten Sie die virtuelle Maschine von XClarity Administrator neu.

© Copyright Lenovo 2015, 2025

Kapitel 12. Ereignisüberwachungs- und weiterleitungsprobleme

Verwenden Sie diese Informationen, um Probleme bei der Ereignisüberwachung und -weiterleitung zu beheben.

Ereignisse werden nicht weitergeleitet.

Verwenden Sie diese Informationen, um Fehler beim Weiterleiten von Ereignissen zu beheben.

- Wenn ein Plan für die Ereignisweiterleitung erstellt wurde, werden nur Ereignisse weitergeleitet, die innerhalb des festgelegten Zeitfensters auftreten. Stellen Sie sicher, dass die geplante Zeit nicht abgelaufen ist.
- Bei E-Mail-basierten Webservices:
  - Wenn ein sicherer Verbindungstyp für die Ereignisweiterleitung ausgewählt ist, versucht Lenovo XClarity Administrator, das Zertifikat des SMTP-Servers herunterzuladen und in seinen Truststore zu importieren. Sie werden aufgefordert, das Hinzufügen dieses Zertifikat zum Truststore zu akzeptieren. Schlägt dies fehl, ist keine Verbindung mit dem SMTP-Server möglich.

    Beheben Sie diesen Fehler, indem Sie das Zertifikat manuell in den XClarity Administrator-Truststore importieren. Klicken Sie dazu auf **Verwaltung → Sicherheit → Vertrauenswürdige Zertifikate** und das Symbol **Erstellen** ( ).
  - Überprüfen Sie, ob der SMTP-Server nur E-Mails akzeptiert, die von einem registrierten Benutzer gesendet wurden. Wenn dies der Fall ist, wird die Standardabsenderadresse (`LXCA.`*<source_identifier>*`@`*<smtp_host>*) abgelehnt. Um dieses Problem zu beheben, müssen Sie in der Ereignisweiterleitung im Feld **Absender** mindestens einen Domänennamen angeben.
  - Stellen Sie bei Verwendung der OAUTH2-Authentifizierung sicher, dass das Sicherheitstoken nicht abgelaufen ist. Ist dies der Fall, können Sie das Python-Script oauth2.py und das Aktualisierungstoken verwenden, um ein neues Sicherheitstoken zu generieren. Anschließend aktualisieren Sie die Ereignisweiterleitung in XClarity Administrator mit dem neuen Sicherheitstoken. Siehe Ereignisweiterleitung an einen SMTP-Service für Gmail einrichten für weitere Informationen.

© Copyright Lenovo 2015, 2025

Kapitel 13. Probleme bei der Einheitenverwaltung

Verwenden Sie diese Informationen zur Fehlerbehebung bei Problemen mit der Einheitenverwaltung.

Daten auf blockierten Laufwerken können nicht sicher gelöscht werden

Verwenden Sie diese Informationen, um Probleme zu beheben, bei denen das sichere Löschen auf SATA-Festplatten fehlschlägt und die Fehlermeldung `Festplatten sind blockiert und können nicht gelöscht werden` angezeigt wird.

Integrierte SATA-Festplatten befinden sich standardmäßig im blockierten Zustand. Wenn der Server ein blockiertes Laufwerk hat, hebt Lenovo XClarity Administrator das Blockieren des Laufwerks vorübergehend auf und bootet dann zur Bare-Metal-Aktualisierung (Bare Metal Update, BMU), um das Laufwerk zu löschen. Wenn die Bare-Metal-Aktualisierung von XClarity Administrator beendet wird und der Server das Betriebssystem startet, wird das Laufwerk automatisch wieder blockiert.

Wenn ein Server unter XClarity Administrator im Modus *Verwaltete Authentifizierung* verwaltet wird, erstellt XClarity Administrator das LDAP-Konto SYSMGR_xxx zur Verwaltung und Überwachung des Servers anstelle lokaler Anmeldeinformationen (siehe Authentifizierungsserver verwalten in der Onlinedokumentation für XClarity Administrator). Das LDAP-Konto SYSMGR_xxx verfügt nicht über eine IPMI-Berechtigung, so dass XClarity Administrator das Blockieren des Datenträgers nicht aufheben kann. Dadurch schlägt der Vorgang des sicheren Löschens auf diesem Server fehl.

Um dieses Problem zu beheben, verwalten Sie den Server im Modus *Lokale Authentifizierung* und versuchen Sie dann, die Laufwerke sicher zu löschen.

SATA-SDD-Datenträger können nicht sicher gelöscht werden, wenn sie mit Marvell RAID verbunden sind

Verwenden Sie diese Informationen zur Fehlerbehebung bei Problemen mit dem sicheren Löschen von SATA-SDDs, wenn diese mit Marvell RAID-Controllern verbunden sind.

Sie können keine SATA-SDD-Datenträger sicher löschen, die mit Marvell RAID-Controllern verbunden sind. Ziehen Sie stattdessen die folgenden Empfehlungen in Betracht.

- Für 7mm-SATA-SSDs verbinden Sie diese mit Broadcom RAID-Controllern, um ein sicheres Löschen durchzuführen.
- Verbinden Sie M.2 SATA SSDs mit Marvell Nicht-RAID-Controllern (z. B. ThinkSystem M.2 SATA/NVMe Einrichtungssatz für zwei Positionen), um eine sichere Löschung durchzuführen.

Die Marvell RAID-Firmware verfügt über einen internen Timeout (9 Sekunden). Wenn die SSD nicht rechtzeitig auf den Befehl reagiert (die Löschung nicht beendet), setzt die Marvell RAID-Firmware die SDD zurück, wodurch sie gesperrt wird und die sichere Löschung fehlschlägt. Führen Sie den folgenden Befehl aus, um den SDD zu entsperren.

```
hdparm --user-master u --security-unlock user123 %diskName%
```

Bestandsdaten sind nach dem Hinzufügen oder Austauschen von Karten nicht auf dem neuesten Stand

Bei AMD1P- und TSM-basierten Einheiten zeigt Lenovo XClarity Administrator möglicherweise nicht die richtigen Bestandsdaten für neu eingesetzte PCIe-Karten ein, z. B. FRU und Firmware.

© Copyright Lenovo 2015, 2025

Nach dem Wechsel einer PCIe-Karte müssen Sie die verwaltete Einheit neu starten und mehrere Minuten warten, bis der Baseboard Management Controller den Bestand aktualisiert hat.

XClarity Administrator ruft alle 24 Stunden automatisch die Bestandsdaten von verwalteten Einheiten ab. Sie können entweder auf die nächste Bestandserfassung warten oder die Bestandsdaten manuell erfassen, indem Sie den Server auf der Seite „Server“ auswählen und dann zu **Aktionen → Bestand → Bestand aktualisieren** klicken.

Kapitel 14. Serverkonfigurationsprobleme

Verwenden Sie diese Informationen, um Probleme mit der Konfiguration von Servermustern und -profilen zu beheben.

Beim Erstellen eines Musters von einem vorhandenen Server ist ein Fehler aufgetreten.

Verwenden Sie diese Informationen, um Probleme bei der Erstellung von Servermustern von einem vorhandenen verwalteten Server zu beheben.

1. Stellen Sie sicher, dass der Serverstatus nicht „Offline“ lautet. Weitere Informationen zu Servermustern finden Sie unter Ein Servermuster erstellen in der Onlinedokumentation von Lenovo XClarity Administrator.
2. Wiederholen Sie den Vorgang.

Beim Implementieren eines Musters in einer Einheit ist ein Aktivierungsfehler aufgetreten.

Ein Aktivierungsfehler weist darauf hin, dass beim Implementieren des Servermusters auf einer verwalteten Einheit ein Fehler aufgetreten ist. Ein Aktivierungsfehler kann verschiedene Gründe haben. Verwenden Sie diese Informationen, um diese Arten von Problemen zu beheben.

Überprüfen Sie die Details des Jobs auf der Seite „Jobs“, indem Sie den Aktivierungsjob für das Serverprofil mit dem Status „Gestoppt mit Fehlern“ suchen und dann auf den Job klicken. Um das Problem zu identifizieren, prüfen Sie die Fehlernachrichten.

- Konnektivitäts- oder Netzwerkweiterleitungsprobleme zwischen Lenovo XClarity Administrator und der verwalteten Einheit.

  Diese Probleme werden in den Jobnachrichten als LDAP-Fehler dargestellt. Dies weist darauf hin, dass im Zusammenhang mit der Verbindung der Einheit zur virtuellen Einheit über eine der konfigurierten Netzwerkschnittstellen ein Fehler aufgetreten ist.

  Stellen Sie sicher, dass die Netzwerkverbindung zwischen der virtuellen XClarity Administrator-Einheit und der Einheit betriebsbereit ist. Wenn sich diese in verschiedenen Netzwerksegmenten befinden, stellen Sie sicher, dass zwischen den beiden Segmenten Netzwerkweiterleitbarkeit besteht.
- Mindestens eine Konfigurationseinstellung im Servermuster führt dazu, dass sich eine Einstellung ändert, die auf der ausgewählten verwalteten Einheit nicht gültig ist. Beachten Sie die folgenden Beispiele.
  - Das ausgewählte erweiterte UEFI-Muster ist nicht mit der ausgewählten Einheit kompatibel.

    Wenn beispielsweise ein UEFI-Muster, das mit XClarity Administrator für einen X6-basierten Server (z. B. System x3950 X6) bereitgestellt wird, ausgewählt und auf einem System x3650 M4-Server implementiert wird, können die Unterschiede bei den Prozessoreinstellungen zwischen den beiden Servern dazu führen, dass die Profilaktivierung fehlschlägt. Um das Problem zu beheben, stellen Sie sicher, dass das ausgewählte erweiterte UEFI-Muster mit dem ausgewählten Server kompatibel ist.
  - Ein Anschlussmuster für einen Ethernet-Adapter-Anschluss wird einem Anschluss zugewiesen, der die ausgewählten Einstellungen nicht unterstützt.

    Beispielsweise gibt es auf Emulex-basierten Adaptern Einstellungen, die nur auf dem ersten Anschluss des Adapters angezeigt werden, insbesondere der erweiterte Modus und die Porteinstellungen, über die ein Anschluss deaktiviert wird. Wenn diese Einstellungen dem zweiten Anschluss des Adapters

© Copyright Lenovo 2015, 2025

zugewiesen werden, kann ein Aktivierungsfehler auftreten. Diese Probleme werden möglicherweise in den Jobnachrichten als `Erweiterter Modus ist keine Einstellung` oder `Anschluss1 ist keine Einstellung` dargestellt. Um dieses Problem zu beheben, stellen Sie sicher, dass das Anschlussmuster, das diese erweiterten Anschlussmustereinstellungen für den erweiterten Modus oder die Anschlussaktivierung enthält, nur dem ersten Anschluss des Adapters zugewiesen wird.

– Einige Einstellungen werden nach einer Firmwareaktualisierung nicht auf den ausgewählten verwalteten Einheiten unterstützt.

  Beispielsweise können nach der Firmwareaktualisierung eines E/A-Adapters einige Einstellungen durch die neue Firmware entfernt oder umbenannt werden, daher ist die Einstellung im Servermuster auf dem Zielserver nicht gültig. Diese Probleme werden in der Jobmeldung mit „xxx ist keine Einstellung“ angegeben. Zum Beheben dieses Problems übernehmen Sie ein neues Servermuster vom Server, damit das neue Muster alle von der neuen Firmware unterstützten Einstellungen enthält. Falls das alte Muster weiterhin verwendet werden soll, müssen Sie die ungültigen Einstellungen manuell aus dem Servermuster entfernen.

- Beim Einschalten oder Neustart des Server tritt ein Fehler auf, wenn die vollständige Aktivierung für die Implementierung des Musters oder Profils ausgewählt ist.

  Stellen Sie sicher, dass der Einheit-Stromversorgungsstatus ordnungsgemäß in XClarity Administrator angegeben ist. Wenn nicht, aktualisieren Sie den Bestand, um den Stromversorgungsstatus zu synchronisieren:

  1. Klicken Sie in der Menüleiste von XClarity Administrator auf **Hardware → Server**. Die Seite Server zeigt eine tabellarische Ansicht aller verwalteten Server an (Rackserver und Rechenknoten).
  2. Wählen Sie den Server aus und klicken Sie auf **Alle Aktionen → Bestand aktualisieren**.

Auf einem Switch ist eine ungültige Konfiguration implementiert

Verwenden Sie diese Informationen, um Probleme zu beheben, die auftreten, wenn auf einem Switch eine ungültige Konfiguration implementiert wird.

VLAN-IDs müssen erstellt werden, bevor Sie einen Anschluss zu einem bestimmten VLAN hinzufügen. Wenn ein Anschlussmuster interne Switch-VLAN-Einstellungen mit VLAN-IDs enthält, die für den Switch nicht vorkonfiguriert wurden, ist die Profilaktivierung zwar möglicherweise erfolgreich, die nicht angewandte und ungültige Konfiguration auf dem Switch aber muss repariert werden.

Um dieses Problem zu beheben, melden Sie sich beim Switch an und konfigurieren Sie die Voraussetzungen manuell oder umgehen Sie die Änderungen, indem Sie ein Muster mit gültigen Einstellungen implementieren.

Kapitel 15. Probleme bei Firmwareaktualisierung und Repository

Verwenden Sie diese Informationen, um Probleme bei Firmwareaktualisierungen zu beheben.

Es konnte keine Verbindung mit dem Lenovo Repository hergestellt werden.

Bei Lenovo XClarity Administrator v2.8 und früheren Versionen wurde eine HTTP-Verbindung zum Lenovo Support verwendet, um den Firmware-Update-Katalog zu aktualisieren und Aktualisierungspakete herunterzuladen. Jetzt erfordert der Lenovo Support jedoch eine HTTPS-Verbindung.

Installieren Sie das neuestes GAFix auf Ihrer XClarity Administrator-Instanz oder führen Sie ein Upgrade auf XClarity Administrator v3.0.0 oder höher durch.

Nach erfolgreicher Firmwareaktualisierung wird auf der Seite „Übernehmen/Aktivieren“ nicht die aktualisierte Firmwareversion angezeigt

Verwenden Sie diese Informationen, um Probleme mit der Seite Firmwareaktualisierungen: anwenden/aktivieren zu beheben.

Stellen Sie sicher, dass der neueste Bestand verglichen wird, indem Sie auf das Symbol **Aktualisieren** ( ) auf der Seite Firmwareaktualisierungen: anwenden/aktivieren klicken, um eine Synchronisation mit den Lenovo XClarity Administrator-Einheitendaten anzufordern.

Firmware kann auf einer Einheit nicht aktualisiert werden

Verwenden Sie diese Informationen zur Fehlerbehebung, wenn Probleme bei der Firmwareaktualisierung bei verwalteten Einheiten auftreten.

- Lesen Sie Hinweise zur Firmwareaktualisierung in der Onlinedokumentation von XClarity Administrator und folgen Sie den angezeigten Empfehlungen.
- Stellen Sie sicher, dass der Serverstatus nicht offline ist und der Server von Lenovo XClarity Administrator über das Netzwerk erreicht werden kann.
- Falls bei der Firmware-Aktualisierung von einem FC5022-Switch mit FOS v7.4.x und früher ein Fehler auftritt, führen Sie folgenden Befehl in der Befehlszeilenschnittstelle aus. Siehe Tech-Tipp HT507915 für weitere Informationen.
  ```
  Seccrypto -- default -type SSH -force
  ```

Blockierungen des CMM-Firmwareaktualisierung

Verwenden Sie diese Informationen zur Fehlerbehebung bei der Aktualisierung der CMM-Firmware, Flex-Stackversion 1.3.2.1 2PET12K bis 2PET12Q, die länger als drei Wochen ausgeführt wurde und Teil einer dualen CMM-Konfiguration ist.

1. Setzen Sie den CMM virtuell erneut ein. Wenn Sie zwei CMMs im selben Gehäuse haben, setzen Sie die beiden CMMs gleichzeitig virtuell erneut ein. Die mindestens erforderlichen Firmwareversionen finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Klicken Sie dazu auf

© Copyright Lenovo 2015, 2025

die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.

2. Wiederholen Sie die Aktualisierung von XClarity Administrator.

Firmware ist auf dem neuesten Stand, besteht aber die Konformitätsprüfung nicht.

Verwenden Sie diese Informationen, um Konformitätsprobleme nach Firmwareaktualisierungen zu beheben.

Setzen Sie die Einheit erneut virtuell ein oder führen Sie eine zusätzliche Aktualisierung (z. B. des Festplattenlaufwerks) durch.

Firmwareaktualisierungen der Flex System-Switches schlagen unerwartet fehl.

In den folgenden Abschnitten werden Fehler beschrieben, die im Jobprotokoll vorhanden sind.

Um die Meldungen zu finden, klicken Sie auf **Überwachung → Jobs** im Menü von Lenovo XClarity Administrator. Sie finden die Fehlernachricht, indem Sie auf den Link für den Job in der Spalte **Jobs** klicken, um das Dialogfenster mit der Jobzusammenfassung und den Jobergebnissen anzuzeigen. Unter dem Abschnitt „Zielergebnisse“ werden die Meldungen in der Spalte **Meldung** aufgelistet; sie beginnen mit `"***FEHLER***`.

Target Results: With Errors: 1 Running: 0 Completed: 0

Target	Message
VDI-5K_CH4-VS: IO Module 03: I/O Module Bay 3: IOM	Failed

Timestamp	Message
April 18, 2016 at 11:47:50	TaskMaanger: IO Module 03 bay 3 (172.16.25.153): IOM: Starting new process for task_id 9.
April 18, 2016 at 11:47:50	IO Module 03 bay 3 (172.16.25.153): IOM TaskType is: IOM : ues = CMMDelay=0, immDelay=0, pciCheck=true
April 18, 2016 at 11:56:19	IO Module 03 bay 3 (172.16.25.153): IOM Reported *** ERROR ***. Firmware download operation failed.
April 18, 2016 at 11:56:21	TaskManager: IO Module 3 bay 3 (172.16.25.153): IOM: Task_id 9 failed. rc=68
April 18, 2016 at 11:56:21	TaskManager: IO Module 03 bay 3 (172.16.25.153): IOM: StopOnError: Canceling the remaining non-required tasks in the job...

Wichtig: Bei der Aktualisierung der Flex-Switch-Firmware mit XClarity Administrator können sporadisch Fehler auftreten. Wenn Sie auf Fehler stoßen, führen Sie die Vorschläge in den folgenden Abschnitten aus. Wenn bei der Aktualisierung der Flex-Switch-Firmware mit XClarity Administrator weiterhin Fehler auftreten, aktualisieren Sie die Flex-Switches direkt über die Flex-Switch-Schnittstelle.

Anmerkung: Firmwareaktualisierungen eines Flex System-Switches können unerwartet fehlschlagen, wenn auf dem Switch nicht EHCM L3 ausgeführt wird. Weitere Informationen finden Sie unter Hinweise zur Firmwareaktualisierung in der Onlinedokumentation von XClarity Administrator.

Firmwareaktualisierung des Flex-Switches mit folgender Fehlernachricht fehlgeschlagen: „Firmwaredownload fehlgeschlagen.“

Verwenden Sie diese Informationen zur Problembehebung bei folgender Fehlernachricht im Jobprotokoll: `IOM: Firmwaredownload fehlgeschlagen ***FEHLER*** gemeldet`. Bei EN4023- und FC5022-Switches könnte dies geschehen, wenn Sie versuchen, eine Aktualisierung mit Systemunterbrechung durchzuführen, bei der eine frühere Firmwareaktualisierungsversion übersprungen und direkt mit der neuesten Version fortgefahren wird.

Um dieses Problem zu umgehen, aktualisieren Sie den Flex-Switch direkt aus der Flex-Switch-Befehlszeilenschnittstelle oder -Webschnittstelle.

Bei FC5022 ist die Migration von FOS v7.3 zu FOS v8.0.1-pha ein Update, das mit Systemunterbrechung erfolgt. Die Migration von FOS v7.4 zu FOS v8.0.1-pha kann ohne Systemunterbrechung durchgeführt werden.

Die mindestens erforderlichen Firmwareversionen finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator. Klicken Sie dazu auf die Registerkarte **Compatibility** (Kompatibilität) und dann auf den Link für die entsprechenden Einheitentypen.

Firmwareaktualisierung des Flex-Switches mit folgender Fehlernachricht fehlgeschlagen: „DCSS_RC_CDT_FAIL“

Verwenden Sie diese Informationen zur Problembehebung bei folgender Fehlernachricht im Jobprotokoll: `IOM: DCSS_RC_CDT_FAIL ***FEHLER*** gemeldet`. Bei dieser Meldung ist der Flex-Switch möglicherweise ausgeschaltet oder es liegt ein anderes Kommunikationsproblem vor.

Führen Sie die folgenden Aktionen in der angegebenen Reihenfolge aus. Versuchen Sie nach jedem Schritt erneut, die Firmware zu aktualisieren.

1. Stellen Sie sicher, dass der Flex-Switch eingeschaltet ist.
2. Überprüfen Sie, ob die IP-Adresse des Flex-Switches gültig ist.
3. Setzen Sie den Flex-Switch zurück.
4. Setzen Sie das CMM zurück oder starten Sie es neu.

Firmwareaktualisierung des Flex-Switches mit folgender Fehlernachricht fehlgeschlagen: „Zeitlimitüberschreitung“

Verwenden Sie diese Informationen zur Problembehebung bei folgender Fehlernachricht im Jobprotokoll: `IOM: Zeitlimitüberschreitung ***FEHLER*** gemeldet`. Dieser Fehler kann auftreten, wenn die IP-Adresse des Switches von Lenovo XClarity Administrator nicht über das Netzwerk erreichbar ist.

Führen Sie die folgenden Aktionen in der angegebenen Reihenfolge aus. Versuchen Sie nach jedem Schritt erneut, die Firmware zu aktualisieren.

1. Stellen Sie sicher, dass der Flex-Switch eine gültige IP-Adresse hat und XClarity Administrator über das Netzwerk auf den Switch zugreifen kann.
2. Setzen Sie den Flex-Switch zurück.
3. Setzen Sie das CMM zurück oder starten Sie es neu.

Firmwareaktualisierung des Flex-Switch mit folgender Fehlermeldung fehlgeschlagen: „Es kann nicht die gleiche Firmwareversion heruntergeladen werden. Laden Sie eine andere Firmware herunter.“

Verwenden Sie diese Informationen, um Fehlernachrichten des Typs `IOM: Gemeldeter ***FEHLER*** Es kann nicht die gleiche Firmwareversion heruntergeladen werden. Laden Sie eine andere Firmware herunter.` Fehlernachricht im Jobprotokoll. Dieser Fehler kann auftreten, wenn Sie versuchen, den EN4023-Switch mit derselben Version zu aktualisieren.

Es ist nicht möglich, die Firmware des EN4023-Switches auf die Version zu aktualisieren, die bereits ausgeführt wird.

Firmwareaktualisierung des Flex-Switch mit folgender Fehlernachricht fehlgeschlagen: Host konnte nicht kontaktiert werden

Verwenden Sie diese Informationen zur Problembehebung bei folgender Fehlernachricht im Jobprotokoll: IOM: Host konnte nicht kontaktiert werden ***FEHLER*** gemeldet. Dieser Fehler kann auftreten, wenn die IP-Adresse des Switches von Lenovo XClarity Administrator nicht über das Netzwerk erreichbar ist.

Führen Sie die folgenden Aktionen in der angegebenen Reihenfolge aus. Versuchen Sie nach jedem Schritt erneut, die Firmware zu aktualisieren.

1. Stellen Sie sicher, dass der Switch eine gültige IP-Adresse hat und XClarity Administrator über das Netzwerk auf den Switch zugreifen kann.
2. Starten Sie den Switch neu.
3. Starten Sie das CMM neu.

Firmwareaktualisierung des Flex-Switch mit folgender Fehlernachricht fehlgeschlagen: „Datei ist nicht vorhanden“

Verwenden Sie diese Informationen zur Problembehebung bei folgender Fehlernachricht im Jobprotokoll: `IOM: Datei ist nicht vorhanden ***FEHLER*** gemeldet`. Dieser Fehler kann auftreten, wenn die IP-Adresse des Switches von Lenovo XClarity Administrator nicht über das Netzwerk erreichbar ist.

Führen Sie die folgenden Aktionen in der angegebenen Reihenfolge aus. Versuchen Sie nach jedem Schritt erneut, die Firmware zu aktualisieren.

1. Stellen Sie sicher, dass der Switch eine gültige IP-Adresse hat und XClarity Administrator über das Netzwerk auf den Switch zugreifen kann.
2. Setzen Sie den Switch zurück.
3. Setzen Sie das CMM zurück oder starten Sie es neu.

Firmwareaktualisierung des Flex-Switches mit folgender Fehlernachricht fehlgeschlagen: „Flashen mit Fehler beendet“

Verwenden Sie diese Informationen zur Problembehebung bei folgender Fehlernachricht im Jobprotokoll: `IOM: Flashen mit Fehler beendet ***FEHLER*** gemeldet`. Dies kann vorkommen, wenn der Switch über keine gültige IP-Adresse verfügt.

Stellen Sie sicher, dass der Switch eine gültige IP-Adresse hat und Lenovo XClarity Administrator über das Netzwerk auf den Switch zugreifen kann.

Firmwareaktualisierung des EN6131 40 Gb Ethernet Switch oder IB6131 Infiniband Switch unerwartet fehlgeschlagen

Verwenden Sie diese Informationen, um einen unerwarteten Fehler zu beheben, wenn Sie die Firmware für den EN6131 40 Gb Ethernet Switch oder IB6131 InfiniBand Switch aktualisieren.

1. Überprüfen Sie das Jobprotokoll für eine Fehlernachricht vom Switch, wie z. B. `Nicht genügend Speicherplatz verfügbar, um das Image herunterzuladen.`

   Anmerkung: Möglicherweise sind zusätzliche Informationen im Jobprotokoll vorhanden. Oft liegen die Meldungen im Format `IOM: msg *** FEHLER *** gemeldet` vor, wobei *msg* den spezifischen Fehler für dieses Modul angibt.
2. Überprüfen Sie die Netzwerkgeschwindigkeit und -stabilität. Die Firmwareaktualisierung kann fehlschlagen, wenn die Aktualisierung nicht innerhalb von 30 Minuten abgeschlossen ist.
3. Geben Sie ausreichend Plattenspeicherplatz auf dem Switch für die Aktualisierungsdatei frei. Der Speicherplatz wird verwendet, wenn Aktualisierungsdateien auf den Switch kopiert werden. Anweisungen zum Verwalten des Plattenspeicherplatzes finden Sie unter Lenovo Flex System EN6131 40Gb Ethernet Switch in der Flex Systems-Onlinedokumentation.
4. Wiederholen Sie die Aktualisierung von Lenovo XClarity Administrator.

Firmwareaktualisierung des Lenovo EN4091 Pass-through-Moduls schlägt fehl.

Verwenden Sie diese Informationen, um einen unerwarteten Fehler bei der Aktualisierung des Lenovo EN4091 Pass-through-Moduls zu beheben.

1. Prüfen Sie das Jobprotokoll auf eine Fehlernachricht vom Pass-through-Modul, wie z. B. `Firmware-Image besteht Datenintegritätstest nicht` oder `Host konnte nicht kontaktiert werden.`

   Anmerkung: Möglicherweise sind zusätzliche Informationen im Jobprotokoll vorhanden. Oft liegen die Meldungen im Format `IOM: msg *** FEHLER *** gemeldet` vor, wobei *msg* den spezifischen Fehler für dieses Modul angibt.
2. Setzen Sie den Lenovo EN4091 virtuell erneut ein.
3. Wiederholen Sie die Aktualisierung von Lenovo XClarity Administrator.

Firmwareaktualisierung des Flex System-Switches mit folgender Fehlernachricht fehlgeschlagen: „Authentifizierung des Hostschlüssels fehlgeschlagen“

Es wird eine Fehlernachricht im Jobprotokoll im Format „IOM: Authentifizierung des Hostschlüssels fehlgeschlagen ***FEHLER*** gemeldet“ angezeigt. Dieser Fehler tritt auf, wenn der SFTP-Schlüssel auf einem SFTP-Server geändert wurde, der zuvor für die Aktualisierung des Flex System-Switches verwendet wurde. Betroffene Switches: CN4093 EN2092, EN4091, EN4093, EN4093R, SI4093.

In Lenovo XClarity Administrator kann dieser Fehler auftreten, wenn die Firmware auf einem Flex System-Switch bereits aktualisiert wurde und Sie dann eine neuere Version von XClarity Administrator installieren oder XClarity Administrator neu starten und danach versuchen, den Switch zu aktualisieren. Dies liegt daran, dass durch die Installation einer neuen Version von XClarity Administrator oder durch den Neustart von XClarity Administrator möglicherweise ein neuer SFTP-Schlüssel generiert wird.

Um dieses Problem zu lösen, geben Sie den folgenden Befehl über die Befehlszeilenschnittstelle für einen Flex System-Switch oder einen Lenovo Flex System-Switch ein, um die SSH-Schlüssel zu löschen. Beachten Sie dabei Folgendes: Wenn der Switch die ISCLI verwendet, müssen Sie sich im Terminalmodus

der Konfiguration befinden, um diesen Befehl auszuführen. Sie können zum Terminalmodus der Konfiguration wechseln, indem Sie den Befehl `enable` und dann den Befehl `configure terminal` ausführen.
`clear ssh-clienthostkey all`

Anmerkung: Wenn sich der Flex System-Switch im IBMNOS-CLI-Modus befindet, geben Sie die folgenden Befehle von der Switch-CLI ein, um die SSH-Schlüssel zu löschen:
```
maint
clssh
all
exit
```

Bei der Durchführung einer Aktualisierung wird das System nicht in den Wartungsmodus versetzt.

Verwenden Sie diese Informationen, um Probleme bei Firmwareaktualisierungen und dem Wartungsmodus zu beheben.

Wiederholen Sie die Firmwareaktualisierung.

Beim Neustart eines Servers aus dem Betriebssystem wird der Wartungsmodus nicht aktiviert.

Bei der Aktualisierung von Firmware mit verzögerter Aktivierung auf einem der folgenden Server wird für den Aktualisierungsstatus „Ausstehender Wartungsmodus“ angezeigt, selbst nachdem der Server aus dem Betriebssystem neu gestartet wurde.

- Flex System x240 M5 Typ 2591 und 9532
- NeXtScale nx360 M5 Typ 5465
- System x3250 M6 Typ 3633 und 3943
- System x3550 M5 Typ 5463
- System x3500 M5 Typ 5464
- System x3550 M5 Typ 8869
- System x3650 M5 Typ 5462
- System x3650 M5 Typ 8871

Um dieses Problem zu beheben, starten Sie den Server von der Management-Controller-Webschnittstelle neu. Wenn der Server wieder online ist, wird der Aktivierungsvorgang für die Aktualisierung fortgesetzt.

Server, auf dem Red Hat Enterprise Linux (RHEL) ausgeführt wird, wird nicht neu gestartet

Bei Red Hat® Enterprise Linux (RHEL) v7 und höher setzt ein Neustart des Betriebssystems über einen grafischen Modus den Server standardmäßig aus.

Sie müssen bei RHEL manuell das Ausschalteverhalten des Netzschalters konfigurieren. Anweisungen hierzu finden Sie unter Red Hat-Handbuch zur Datenmigration und -Verwaltung: Ändern des Verhaltens beim Drücken des Netzschalters im grafischen Zielmodus.

Kapitel 16. Probleme mit der Aktualisierung von BS-Einheitentreibern und Repository

Verwenden Sie diese Informationen, um Probleme bei BS-Einheitentreiberaktualisierungen zu beheben.

Verbindung mit der Lenovo Support-Website zum Herunterladen von Einheitentreiberaktualisierungen nicht möglich

Verwenden Sie diese Informationen, um Probleme beim Download von UpdateXpress System Packs (UXSPs) und Einheitentreiber von der Lenovo Support-Website zu beheben.

- Stellen Sie sicher, dass der Lenovo XClarity Administrator-Einheitenport (eth0 oder eth1), der für die Verwaltung konfiguriert ist, über Internetzugriff verfügt. Weitere Informationen zum Netzwerkbetrieb finden Sie unter Hinweise zum Netzwerkbetrieb in der Onlinedokumentation von XClarity Administrator.
- Stellen Sie vor dem Versuch einer Aktualisierung der Einheitentreiber auf einem verwalteten Server sicher, dass alle erforderlichen Ports und Internetadressen verfügbar sind. Weitere Informationen über Ports finden Sie unter Portverfügbarkeit und Firewalls und Proxy-Server in der Onlinedokumentation von XClarity Administrator.

Aktualisierung von Einheitentreiber auf einem Server nicht möglich

Verwenden Sie diese Informationen zur Fehlerbehebung, wenn Probleme bei der Aktualisierung von Einheitentreibern bei einem verwalteten Server auftreten.

- Stellen Sie sicher, dass der Server online ist und Lenovo XClarity Administrator über das Netzwerk darauf zugreifen kann.
- Lesen Sie die Hinweise zur Aktualisierung von Einheitentreibern (siehe Hinweise zum Aktualisieren von BS-Einheitentreibern in der Onlinedokumentation von XClarity Administrator).

© Copyright Lenovo 2015, 2025

Kapitel 17. Probleme bei der Betriebssystembereitstellung

Verwenden Sie diese Informationen, um Probleme zu beheben, auf die Sie möglicherweise bei dem Versuch stoßen, Betriebssysteme auf verwalteten Servern von Lenovo XClarity Administrator zu implementieren.

Informationen zu allgemeinen Problemen im Zusammenhang mit der Betriebssystembereitstellung finden Sie unter Betriebssystem kann nicht implementiert werden.

Probleme bei der Statusmeldung während der BS-Implementierung

Verwenden Sie diese Informationen, um Probleme mit der Statusmeldung von Lenovo XClarity Administrator zu beheben, die während der Betriebssystemimplementierung auftreten.

- Bei der Implementierung von VMware 6.5 oder höher mit XClarity Administrator bis Version 1.4.0 besagt der Jobstatus möglicherweise, dass die Implementierung abgeschlossen ist, bevor das Betriebssystem bereit ist.

  Werden Skripts für die Überwachung des Abschlusses der BS-Implementierung verwendet, fügen Sie dem Skript eine Verzögerung von 10 Minuten hinzu, nachdem der Jobstatus über die Implementierung eingegangen ist, der besagt, dass die BS-Implementierung abgeschlossen ist.
- Bei der Implementierung von Windows über ein Netzwerk, das VLAN-Tagging verwendet, werden möglicherweise Statusfehler während der Konfigurationsphase *specialize* der Implementierung gemeldet.

  Sie können diese Fehler ignorieren.

Betriebssystem kann nicht implementiert werden.

Verwenden Sie diese Informationen, um allgemeine Probleme zu beheben, auf die Sie möglicherweise bei dem Versuch stoßen, ein Betriebssystem auf einem verwalteten Server von Lenovo XClarity Administrator zu implementieren.

In langsamen Netzwerkumgebungen kann die Betriebssystemimplementierung von SLES 12 und 12.1 im statischen IP-Modus fehlschlagen, weil der Netzwerkverzögerungs-Startparameter in diesem Modus nicht wirksam wird. DiesesProblem wird in SLES 12.2 behoben.

Führen Sie zur Lösung des Problems die folgenden Schritte aus:

1. Stellen Sie bei ThinkSystem V3 und V4 Server (mit XCC2 oder XCC3) mi aktiviertem Systemschutz und der festgelegten Aktion **BS-Start verhindern** sicher, dass der Systemschutz auf der Einheit konform ist. Wenn der Systemschutz nicht konform ist, werden die Einheiten daran gehindert, den Bootvorgang abzuschließen, wodurch die BS-Implementierung fehlschlägt. Damit Sie diese Einheit bereitstellen können, reagieren Sie manuell auf die Systemschutz-Bootaufforderung, damit die Einheiten normal booten können.
2. Wenn Ihnen die Nachricht `https://<management_server_IP>/osdeployment/connection/... Erlaubnis nicht erteilt` angezeigt wird, aktualisieren Sie das BIOS auf dem Server und bearbeiten Sie die Datums- und Uhrzeiteinstellung, damit sie das aktuelle Datum und die aktuelle Uhrzeit anzeigt.
3. Überprüfen Sie alle Anforderungen für das Betriebssystem, das implementiert wird. Weitere Informationen finden Sie unter Unterstützte Betriebssysteme in der Onlinedokumentation von XClarity Administrator.Beispiele:
   - Bei der Implementierung von VMware ESXi kann ein Problem auftreten, wenn der Memory Mapped I/O (MMIO)-Platz nicht auf mindestens 3 GB festgelegt wird.

© Copyright Lenovo 2015, 2025

- Wenn Sie Microsoft Windows implementieren und eine Active Director-Domäne verknüpfen, folgen Sie den Hinweisen unter In Windows Active Directory integrieren in der Onlinedokumentation von XClarity Administrator.

4. Überprüfen Sie die Beschränkungen bezüglich der Unterstützung der Betriebssystembereitstellung für bestimmte E/A-Adapter. Informationen zur Unterstützung für E/A-Adapter finden Sie unter Support-Website mit Kompatibilitätsinformationen zu XClarity Administrator.
5. Stellen Sie sicher, dass Sie über eine stabile Netzwerkverbindung zwischen XClarity Administrator und der Einheit (verwalteter Server) verfügen, auf der das Betriebssystem installiert wird.

   Anmerkung: Bei Implementierung von SLES 11 SP4 könnte die Implementierung beendet und nicht neu gestartet werden, wenn die Netzwerkverbindung zwischen XClarity Administrator und der Einheit unterbrochen wird. Überprüfen Sie in diesem Fall die Netzwerkumgebung und implementieren Sie das Betriebssystem erneut.
6. Stellen Sie sicher, dass mindestens ein Netzwerkanschluss auf XClarity Administrator für die Verwaltung und Bereitstellung von Betriebssystem-Images eingerichtet ist.Sie können die Netzwerktopologie von XClarity Administrator auf der Seite „Netzwerkzugriff“ konfigurieren. Weitere Informationen zur Seite „Netzwerkzugriff“ finden Sie unter Netzwerkzugriff konfigurieren in der Onlinedokumentation von XClarity Administrator.
7. Stellen Sie sicher, dass der zur Verbindung mit dem Datennetzwerk verwendete Netzwerkanschluss von XClarity Administrator für das gleiche Netzwerk konfiguriert ist, das auch für die Datennetzwerkanschlüsse des verwalteten Servers konfiguriert ist. Der Anschluss des Servers wird durch die MAC-Adresse angegeben und kann über die Seite Betriebssysteme -> Netzwerkeinstellungen konfiguriert werden. Weitere Informationen zur Bearbeitung der Netzwerkeinstellungen finden Sie unter Netzwerkeinstellungen für verwaltete Server konfigurieren in der Onlinedokumentation von XClarity Administrator.
8. Stellen Sie sicher, dass auf dem Zielserver kein verzögertes oder teilweise aktiviertes Servermuster vorhanden ist. Wenn ein Servermuster auf dem Zielserver verzögert oder teilweise aktiviert wurde, starten Sie den Server neu, damit alle Konfigurationseinstellungen übernommen werden.
9. Zeigen Sie sich den Status des Servers auf der Seite BS-Images implementieren an, um sicherzugehen, dass der Bereitstellungsstatus „Bereit“ lautet. Wenn der Status „Nicht bereit“ lautet, klicken Sie auf den Statuslink, um festzustellen, warum der Server für die Betriebssystembereitstellung nicht bereit ist. Weitere Informationen zur Implementierung von Betriebssystemen finden Sie unter Ein Betriebssystem-Image implementieren in der Onlinedokumentation von XClarity Administrator.
10. Stellen Sie sicher, dass die Einheit für die Speicherposition, die für die Betriebssystembereitstellung ausgewählt wurde, sichtbar ist.

    Tipp: Um sicherzustellen, dass ein Betriebssystem erfolgreich implementiert wurde, trennen Sie alle Speichereinheiten (bis auf den Speicher, der für die Betriebssystembereitstellung ausgewählt wurde) vom Server.

Datei kann nicht in das BS-Images-Repository importiert werden

Verwenden Sie die Informationen in diesem Abschnitt, um Probleme zu beheben, auf die Sie möglicherweise beim Importieren von Dateien in das Image-Repository von Lenovo XClarity Administrator stoßen.

Führen Sie zur Lösung des Problems die folgenden Schritte aus:

- Stellen Sie sicher, dass die zu importierende Datei über den Prüfsummentest überprüft wurde.
- Stellen Sie sicher, dass das Basisbetriebssystem von XClarity Administrator unterstützt wird. Weitere Informationen finden Sie unter Unterstützte Betriebssysteme in der Onlinedokumentation von XClarity Administrator.
- Wenn Sie vom lokalen System importieren:

  - Für Internet Explorer sowie Microsoft Edge-Webbrowser besteht ein Upload-Limit von 4 GB. Wenn die Datei, die Sie importieren, größer als 4 GB ist, können Sie einen anderen Webbrowser verwenden (z. B. Chrome oder Firefox)
- Wenn Sie von einem Remote-Dateiserver importieren:
  - Stellen Sie sicher, dass der gesamte Pfad zur Datei mit dem tatsächlichen Pfad auf dem Remote-Dateiserver übereinstimmt.
  - Stellen Sie sicher, dass der gesamte Pfad zur Datei abhängig vom Betriebssystem, das den Remote-Dateiserver hostet, die richtigen Schrägstriche oder umgekehrten Schrägstriche enthält.
  - Stellen Sie sicher, dass die erforderlichen Berechtigungen für das Verzeichnis auf dem Remote-Dateiserver erteilt wurden.
  - Stellen Sie sicher, dass ausreichend Speicherplatz im BS-Image-Repository existiert, um die Datei speichern zu können (siehe Plattenspeicher verwalten in der Onlinedokumentation von XClarity Administrator).
  - Stellen Sie sicher, dass Sie sich mit den richtigen Anmeldeinformationen beim Remote-Dateiserver angemeldet haben.
  - Stellen Sie sicher, dass eine stabile Netzwerkverbindung zwischen XClarity Administrator und dem Remote-Dateiserver besteht.
  - Stellen Sie sicher, dass die korrekten vertrauenswürdigen Zertifikate importiert wurden und dass die Zertifikate nicht widerrufen wurden (siehe Mit Sicherheitszertifikaten arbeiten in der Onlinedokumentation von XClarity Administrator).
  - Stellen Sie sicher, dass der Remote-Dateiserver mindestens einen Algorithmus unterstützt, der von XClarity Administrator für jeden Algorithmustyp unterstützt wird, der von SSH angefordert wird (siehe Eine sichere Umgebung implementieren in der Onlinedokumentation von XClarity Administrator).

Betriebssystem-Installationsprogramm kann das Plattenlaufwerk nicht finden, auf dem Sie installieren möchten.

Bei Servern mit Software-RAID-Adaptern (wie 110i AnyRAID-Adapter, ServeRAID C100- oder C105-Adapter und Intel RSTe SATA Software RAID-Adapter) muss der SATA-Modus, wenn der SATA-Adapter im Management-Controller aktiviert ist, auf „AHCI.“ festgelegt sein. Die anderen Modi (wie „RAID“ und „IDE“) werden für Software-RAID von RHEL, SUSE, VMware oder Windows-Betriebssystemen nicht unterstützt.

Anmerkung: Auf jedem Server muss ein Hardware-RAID-Adapter installiert und konfiguriert sein. Der Software-RAID, der in der Regel im integrierten Intel SATA-Speicheradapter vorhanden ist, wird nicht unterstützt. Wenn jedoch kein Hardware-RAID-Adapter vorhanden ist, kann die Betriebssystemimplementierung in manchen Fällen funktionieren, indem Sie für den SATA-Adapter den AHCI-SATA-Modus festlegen.

Gehen Sie wie folgt vor, um den SATA-Modus für ThinkServer zu ändern.
1. Wählen Sie vom AMI Setup Utility das Menü **Advanced Settings**.
2. Verwenden Sie die Pfeiltasten, um den **SATA Mode** auszuwählen.
3. Drücken Sie die Schaltfläche **+**, um den Wert von `AHCI` zu ändern.
4. Drücken Sie **F10**, um die Änderung zu speichern.

Gehen Sie wie folgt vor, um den SATA-Modus für andere Server zu ändern.
1. Wählen Sie über das F1 Setup Utility das Menü **System Settings → Devices and I/O Ports → Onboard SATA Mode** aus.
2. Drücken Sie die Schaltfläche **+**, um den Wert von `AHCI` zu ändern.
3. Drücken Sie **F10**, um die Änderung zu speichern.

Betriebssystem-Installationsprogramm kann auf einem ThinkServer-Server nicht starten

Für ThinkServer-Server muss die Speicher-OpROM-Richtlinie auf dem ThinkServer Management Module auf „UEFI Only“ festgelegt sein, damit das Image des Betriebssystem-Installationsprogramms ordnungsgemäß startet. Wenn die Richtlinie auf „Legacy Only“ festgelegt ist, wird das Betriebssystem-Installationsprogramm nicht gestartet.

Gehen Sie wie folgt vor, um die Speicher-OpROM-Richtlinie zu ändern.

1. Wählen Sie im AMI Setup Utility das Menü **Boot Manager → Miscellaneous Boot Settings** aus.
2. Verwenden Sie die Pfeiltasten, um **Speicher-OpROM-Richtlinie** auszuwählen.
3. Drücken Sie die Schaltfläche **+**, um den Wert von `UEFI Only` zu ändern.
4. Drücken Sie **F10**, um die Änderung zu speichern.

Weitere Informationen hierzu finden Sie in der ThinkServer-Dokumentation.

Probleme bei der Implementierung von VMware ESXi

Verwenden Sie diese Informationen, um Probleme zu beheben, auf die Sie möglicherweise bei der Implementierung von VMware ESXi-Betriebssystemen auf verwalteten Servern von Lenovo XClarity Administrator stoßen.

VMware-Bereitstellung verursacht Blockierung des Systems oder Neustart

Während der Installation von VMware 5.1u1, 5.1u2, 5.1u3 oder 5.5 (beliebige Aktualisierung) auf einem verwalteten Server kann der Server blockieren oder neu starten.

Die Blockierung oder der Neustart kann kurz nach folgender Fehlernachricht auftreten:
`Loading image.pld`

VMware 5.5 erfordert, dass im Speicher abgebildeter E/A-Platz (MMIO, memory-mapped I/O) innerhalb der ursprünglichen 4 GB des Servers konfiguriert wird. Je nach Konfiguration versuchen bestimmte Systeme, mehr Hauptspeicher als 4 GB zu verwenden, was Fehler verursachen kann.

Führen Sie zur Lösung des Problems die folgenden Schritte aus:

Tipp: Sie können ein für die Virtualisierung bestimmtes, vordefiniertes, erweitertes UEFI-Muster verwenden, statt **MM Config** über das Setup Utility für jeden Server zu definieren. Mit diesem Muster wird die MM Config-Option auf 3 GB festgelegt und die PCI-64-Bit-Ressourcenzuordnung deaktiviert. Weitere Informationen zu diesen Mustern finden Sie unter Erweiterte UEFI-Einstellungen definieren in der Onlinedokumentation von XClarity Administrator.

1. Starten Sie das System neu. Wenn `Press <F1> Setup` angezeigt wird, drücken Sie F1.
2. Wählen Sie **Systemeinstellungen → Einheiten und E/A-Anschlüsse**.
3. Ändern Sie die Einstellung für **MM Config** von 2 GB in 3 GB.
4. Stellen Sie sicher, dass die Einstellung für **PCI 64-Bit Resource** auf „Deaktivieren“ festgelegt ist.
5. Versuchen Sie, das VMware-Image erneut zu installieren.

VMware-Implementierung schlägt mit Laufwerksfehlern fehl

Während der Installation von VMware ESXi wird möglicherweise ein Laufwerksfehler zurückgegeben und die Implementierung schlägt fehl.

Möglicherweise ähnelt die Fehlernachricht dem folgenden Beispiel:

```
error:/tmp/partitioning:line 2: install requires --disk
or --firstdisk
error:/tmp/partitioning:line 1: clearpart requires
one of the following arguments: --alldrives, --firstdisk,
--ignoredrives=, --drives=
```

Dieser Fehler kann auftreten, wenn das ESXi-Installationsprogramm keine SAS-Konfiguration erkennt, die zur Formatierung und Installation verfügbar ist. In der Regel bedeutet dies, dass die RAID-Konfiguration auf dem Server entweder deaktiv oder falsch konfiguriert ist. Der Fehler kann auch darauf zurückzuführen sein, dass ein Servermuster über Lenovo XClarity Administrator implementiert wurde und **Lokale Festplatte deaktivieren** für das Muster ausgewählt wurde.

Führen Sie zur Lösung des Problems die folgenden Schritte aus:

- Wenn ein Servermuster auf diesem Server implementiert wurde und **Lokale Festplatte deaktivieren** ausgewählt wurde, aktualisieren Sie das Servermuster und implementieren Sie es erneut. Weitere Informationen zum Konfigurieren von lokalem Speicher über Servermuster finden Sie unter Lokalen Speicher definieren in der Onlinedokumentation von XClarity Administrator.
- Überprüfen Sie, ob die RAID-Konfiguration auf dem Server korrekt ist:
  1. Starten Sie den Server neu und versuchen Sie, in einer älteren Option zu starten, indem Sie F12 drücken (wählen Sie etwas wie HD0).
  2. Wenn während des Startvorgangs Informationen zum LSI SAS-Adapter angezeigt werden, drücken Sie die Tastenkombination Strg+C, um die Konfiguration zu ändern.
  3. Wenn die Benutzerschnittstelle angezeigt wird, wählen Sie **RAID-Eigenschaften** und **Bestehende Konfiguration anzeigen** aus.
     - Wenn **Bestehende Konfiguration anzeigen** nicht angezeigt wird, wurde der RAID nicht konfiguriert.
     - Wenn für die vorhandene Konfiguration der Status „Deaktiv“ angezeigt wird, stellen Sie sicher, dass der RAID ordnungsgemäß konfiguriert ist.

Betriebssystem startet nicht neu, um die ESXi-Implementierung auf einem ThinkServer-Server abzuschließen

Verwenden Sie diese Informationen, um Fehler zu beheben, auf die Sie möglicherweise beim Implementieren von VMware ESXi- Betriebssystemen auf verwalteten Server von Lenovo XClarity Administrator stoßen, wenn PXE auf einer Netzwerkkarte aktiviert ist oder sich eine bootfähige Einheit (außer dem Laufwerk mit der Installation) in der Bootreihenfolge befindet.

Wenn Sie ESXi auf einem ThinkServer-Server implementieren, verschiebt das Betriebssystem das Laufwerk, auf dem das Betriebssystem installiert ist, nicht explizit an den Anfang der Bootreihenfolge. Wenn eine Booteinheit mit einem bootfähigen Betriebssystem oder PXE-Server vor der ESXi-Booteinheit angegeben ist, startet ESXi nicht. Für die Implementierung von ESXi aktualisiert XClarity Administrator die Bootreihenfolge für die meisten Server, um sicherzustellen, dass die ESXi-Booteinheit oben auf der Liste steht. ThinkServer-Server bieten jedoch keine Möglichkeit, damit XClarity Administrator die Bootreihenfolge dahingehend aktualisieren kann.

Wenn der ThinkServer-Server über PXE-bootfähige Netzwerkadapter verfügt, deaktivieren Sie die PXE-Unterstützung auf den Netzwerkadaptern, implementieren Sie das Betriebssystem erneut und aktivieren Sie anschließend wieder die PXE-Unterstützung. Drücken Sie die Taste F12, um den Bootvorgang zu

unterbrechen und die PXE-Einstellungen zu öffnen. Weitere Informationen zum Ändern der PXE-Booteinstellungen finden Sie in der Dokumentation des Netzwerkadapters.

Wenn der ThinkServer-Server abgesehen vom Laufwerk, auf dem das Betriebssystem installiert werden soll, über weitere bootfähige Einheiten in der Bootreihenfolge verfügt, entfernen Sie die bootfähigen Einheiten aus der Bootreihenfolge, implementieren Sie das Betriebssystem erneut und fügen Sie die bootfähigen Einheiten anschließend wieder zur Bootreihenfolge hinzu. Stellen Sie sicher, dass das installierte Laufwerk ganz oben in der Liste steht. Weitere Informationen zum Ändern der Bootreihenfolge finden Sie in der ThinkServer-Dokumentation.

Probleme bei der Implementierung von Red Hat und SUSE Linux

Verwenden Sie diese Informationen, um Probleme zu beheben, auf die Sie möglicherweise bei der Implementierung von Red Hat und SUSE Linux-Betriebssystemen auf verwalteten Servern von Lenovo XClarity Administratorstoßen.

Redhat 6.x kann nicht auf Rack-basierten Servern mit statischer IP implementiert werden

Es kann ein Problem bei dem Versuch auftreten, Redhat 6.x auf einem verwalteten Server zu implementieren, wenn dieser Server mit einem Top of Rack-Switch (TOR) verbunden ist. Wenn für den TOR-Switch das **Spanning-Tree-Protokoll** aktiviert und die **standardmäßige Weiterleitung** deaktiviert ist, kann das Redhat-Image möglicherweise nicht auf den Server heruntergeladen werden.

Führen Sie zur Lösung des Problems die folgenden Schritte aus:

- Stellen Sie sicher, dass der Server so konfiguriert ist, dass DHCP (und keine statische IP-Adresse) verwendet wird. Versuchen Sie dann erneut, das Betriebssystem zu implementieren.
- Ändern Sie die Konfiguration auf dem Top of Rack-Switch (TOR), um das Spanning-Tree-Protokoll zu deaktivieren *oder* die standardmäßige Paketweiterleitung zu aktivieren.

BS-Implementierung schlägt wegen fehlender Treiber fehl

Bei der Implementierung von Red Hat® Enterprise Linux (RHEL) Server oder SUSE® Linux Enterprise Server (SLES) auf einem Server wird möglicherweise eine Fehlernachricht angezeigt, die die Implementierung stoppt und nach einer gewissen Zeit ist das Zeitlimit für den Implementierungsjob überschritten.

Dieses Problem kann auftreten, wenn das Betriebssystem-Image keine Treiber enthält, um alle auf dem verwalteten Server installierten Adapter zu unterstützen.

Out-of-Box-Treiber sind in Lenovo XClarity Administrator für bestimmte Mellanox IB-Adapter nicht vorab geladen. Daher wird die Implementierung von RHEL oder SLES auf einem Server mit diesen Mellanox Adaptern nicht unterstützt. Weitere Informationen zu Einschränkungen bei Mellanox Adaptern finden Sie im Abschnitt Lenovo XClarity Administrator Unterstützungswebsite für Mellanox Adapter.

Probleme bei der Implementierung von Microsoft Windows

Verwenden Sie diese Informationen, um Probleme zu beheben, auf die Sie möglicherweise bei der Implementierung von Microsoft Windows auf verwalteten Servern von Lenovo XClarity Administrator stoßen.

BS-Implementierung schlägt wegen vorhandener Systempartitionen auf angeschlossenem Plattenlaufwerk fehl

Wenn Sie Microsoft Windows auf einem Server implementieren, dürfen auf den angeschlossenen Plattenlaufwerken keine Systempartitionen vorhanden sein. Wenn eine Partition erkannt wird, schlägt die Betriebssystemimplementierung fehl.

Führen Sie zum Beheben dieses Problems einen der folgenden Schritte aus:

- Trennen Sie die Verbindung zum angeschlossenen Plattenlaufwerk.
- Löschen Sie die Systempartition auf dem angeschlossenen Plattenlaufwerk manuell.

  Achtung: Das Löschen von Partitionen auf einem Plattenlaufwerk führt zu Datenverlust. Stellen Sie sicher, dass Sie alle Daten auf dem Plattenlaufwerk gesichert haben, bevor Sie Partitionen löschen.

  1. Führen Sie mit einer Windows-Eingabeaufforderung das Dienstprogramm `diskpart` aus (siehe Website „DiskPart Commands“).
  2. Wählen Sie den Datenträger aus, indem Sie `select disk` <*number*> eingeben, wobei <*number*> die Nummer des Datenträgers mit der Partition ist, die Sie löschen möchten (siehe Website „Select disk“).
  3. Wählen Sie zu löschende Partition aus, indem Sie `select partition` <*number*> eingeben, wobei <*number*> die Partitionsnummer auf dem ausgewählten Datenträger ist (siehe Website „Select partition“).
  4. Löschen Sie die Partition, indem Sie `delete partition override` eingeben. Die Platten- und Partitionsnummern sind in der WinPE-Fehlernachricht enthalten, die angezeigt wird, wenn eine Systempartition erkannt wird und sich im Jobprotokoll befindet (siehe Website „Delete partition“).

Kapitel 18. Fernsteuerungsprobleme

Verwenden Sie diese Informationen, um Fehler zu beheben, die beim Einsatz der Fernsteuerungsanwendung in Lenovo XClarity Administrator auftreten können.

Fernsteuerungssitzung startet nicht.

Verwenden Sie diese Information zur Problembehebung, wenn sich die Fernsteuerungssitzung nicht über die Lenovo XClarity Administrator-Webschnittstelle oder über die Verknüpfung auf Ihrem System starten lässt.

Führen Sie zur Lösung des Problems die folgenden Schritte aus.

1. Vergewissern Sie sich, dass der Server, mit dem Sie die Verbindung herstellen möchten, durch XClarity Administrator verwaltet wird und sich im Betriebszustand „Online“ oder „Normal“ befindet. Weitere Informationen zum Serverstatus finden Sie im Abschnitt „Den Status eines verwalteten Servers anzeigen“ in der XClarity Administrator-Onlinedokumentation.
2. Stellen Sie sicher, dass Popups in Ihrem Webbrowser während dieser Sitzung nicht deaktiviert sind.
3. Überprüfen Sie, ob Ihr Webbrowser Sicherheitszertifikate von XClarity Administrator akzeptiert hat. Normalerweise werden Sie zum Akzeptieren des Zertifikats aufgefordert, wenn Sie erstmals mit Ihrem Browser auf XClarity Administrator zugreifen.
4. Klicken Sie im Fenster „Fernsteuerung“ auf **Einstellungen → Allgemein → Mit Verwaltungsserver synchronisieren** und warten Sie eine Minute. Öffnen Sie anschließend die Fernsteuerungssitzung erneut.
5. Überzeugen Sie sich, dass Sie zum Starten der Anwendung die unterstützte JRE verwenden.
   - Internet Explorer: Klicken Sie auf **Extras → Internetoptionen → Erweitert**. Vergewissern Sie sich, dass die richtige JRE ausgewählt ist (JRE-Version 7.0, Update 18 oder höher).
   - Firefox: Klicken Sie auf **Extras → Einstellungen → Anwendungen**. Vergewissern Sie sich, dass Java Web Start Launcher dem JNLP-Inhaltstyp zugeordnet ist.

   Anmerkung: Stellen Sie sicher, dass die Option **SSL 2.0-kompatibles ClientHello-Format verwenden** *nicht* in der Java-Systemsteuerung ausgewählt ist.

   Wenn Sie die Anwendung über die Verknüpfung auf Ihrem Desktop starten, stellen Sie sicher, dass Ihr lokales System Konnektivität zu XClarity Administrator besitzt. Die Anwendung überprüft Ihre Benutzer-ID beim XClarity Administrator-Authentifizierungsserver.
6. Löschen Sie den Inhalt des Java Web Start-Cachespeichers auf dem lokalen System. Zum Löschen des Java Web Start-Cachespeichers unter einem Windows-Betriebssystem führen Sie den Befehl `javaws -uninstall` aus. Dies kann auch in der Windows-Systemsteuerung im Menü „Java“ geschehen.
7. Für die Fernsteuerung ist es erforderlich, dass ein Features on Demand-Schlüssel für ThinkServer System Manager Premium Upgrade auf den ThinkServer-Servern installiert ist. Weitere Informationen zu den auf Ihren Servern installierten FoD-Schlüsseln finden Sie unter FoD-Schlüssel (Feature on Demand) anzeigen in der Onlinedokumentation von XClarity Administrator.

Fernsteuerungssitzung nach der Anmeldung blockiert

Verwenden Sie diese Informationen zur Problembehebung, wenn die Fernsteuerungssitzung nach dem Anmelden nicht mehr reagiert.

Wenn Sie keine unterstützte Java Runtime Environment (JRE) verwenden, kann die Fernsteuerungssitzung nach dem Anmelden blockieren. Wenn die Fernsteuerungssitzung nach dem Anmelden anscheinend nicht mehr reagiert, vergewissern Sie sich, dass Sie zum Starten der Anwendung die unterstützte JRE verwenden:

© Copyright Lenovo 2015, 2025

- Oracle JRE Version 6.18 oder höher

Es wird keine Verbindung zu einem Server hergestellt.

Verwenden Sie diese Informationen zur Problembehebung, wenn keine Fernsteuerungssitzung zu einem Server hergestellt werden kann.

Führen Sie zur Lösung des Problems die folgenden Schritte aus.

- Stellen Sie sicher, dass Sie über die folgenden Berechtigungen verfügen: **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin** oder **lxc-hw-manager**.
- Vergewissern Sie sich, dass Ihr lokales System über Netzwerkkonnektivität verfügt und eine Verbindung zu Lenovo XClarity Administrator herstellen kann.
- Stellen Sie sicher, dass der Server durch XClarity Administrator verwaltet wird, indem Sie auf der Menüleiste von XClarity Administrator auf **Hardware → Server** klicken.
- Wenn auf Ihrem lokalen System eine Firewall installiert ist, stellen Sie sicher, dass sie Verbindungen zur IP-Adresse des verwalteten Servers zulässt.
- Senden Sie ein Ping-Signal an die IP-Adresse des verwalteten Servers, um zu überprüfen, ob Ihr lokales System Konnektivität zum verwalteten Server besitzt. Wenn Sie versuchen, auf einen verwalteten Server von einem System aus zuzugreifen, das eine IP-Adresse aus einem externen Netzwerk besitzt, muss auch die IP-Adresse des verwalteten Servers von außen erreichbar sein.
- Vergewissern Sie sich, dass XClarity Administrator-Tunnelung nicht deaktiviert wurde, sodass XClarity Administrator Ihre Fernsteuerungsanfragen per Tunnel an den verwalteten Server übertragen kann, der nur im privaten Verwaltungsnetzwerk adressierbar ist. Die Tunnelung ist standardmäßig aktiviert.Andernfalls können Sie die XClarity Administrator-Tunnelung im Dialogfeld Einstellungen für die Fernunterstützung auf der Registerkarte **Sicherheit** aktivieren. Siehe Fernbedienungseinstellungen festlegen für weitere Informationen.

Kann nicht mit einem Flex System-Switch nach dem Start einer Fernsteuerungssitzung kommunizieren

Verwenden Sie diese Informationen, um das Problem zu beheben, wenn Lenovo XClarity Administrator nicht mehr mit einem Cisco Nexus B22 Fabric Extender-Netzwerk-Switch nach dem Start einer Fernsteuerungssitzung kommuniziert.

Wenn das CMM zur Verwendung der automatischen Erkennung konfiguriert ist, stellen Sie sicher, dass der Netzwerkanschluss am Cisco Nexus B22 Fabric Extender-Netzwerk-Switch zur Verwendung des Modus zur automatischen Aushandlung konfiguriert ist.

Im Einzelbenutzermodus kann keine Verbindung zu einem Server hergestellt werden.

Verwenden Sie diese Informationen zur Problembehebung, wenn keine Serververbindung im Einzelbenutzermodus hergestellt werden kann.

Wenn Sie eine Verbindung zu einem Server im Einzelbenutzermodus herstellen, kann immer nur eine Fernsteuerungssitzung eingerichtet werden.

Führen Sie zur Lösung des Problems die folgenden Schritte aus.

1. Versuchen Sie, im Mehrbenutzermodus auf den verwalteten Server zuzugreifen (sofern laut Sicherheitsanforderungen zulässig).

2. Erkundigen Sie sich bei den anderen Benutzern, ob bereits jemand eine Fernsteuerungssitzung mit dem verwalteten Server eingerichtet hat. Wenn dies so ist, warten Sie, bis der Benutzer die Fernsteuerungssitzung mit dem verwalteten Server beendet hat.
3. Versuchen Sie erneut, im Einzelbenutzermodus eine Verbindung mit dem verwalteten Server herzustellen.

Fernsteuerung kann eine Verbindung mit einem Server herstellen, doch es ist kein Video verfügbar

Verwenden Sie diese Informationen zur Problembehebung, wenn Sie in einer Fernsteuerungssitzung mit einem Server verbunden sind, aber die Nachricht `No video available` angezeigt wird.

Stellen Sie sicher, dass der Server eingeschaltet ist und das Betriebssystem mit einer unterstützten Auflösung und Bildwiederholrate ausgeführt wird.

In der folgenden Tabelle sind die unterstützten Auflösungen und Bildwiederholraten aufgeführt.

Tabelle 1. Unterstützte Auflösungen und Aktualisierungsraten

Auflösung	Aktualisierungsrate
640 x 480	60, 72, 75 und 85 Hz
800 x 600	60, 72, 75 und 85 Hz
1024 x 768	60, 72, 75 und 85 Hz
1440 x 900	60 Hz
1280 x 1024	60 und 75 Hz
1680 x 1050	60 Hz
1600 x 1200	60 und 75 Hz

Ein Server wird nicht in der Liste zum Hinzufügen einer neuen Sitzung angezeigt

Mithilfe der Informationen in diesem Abschnitt können Sie Probleme mit nicht in der Liste für das Hinzufügen einer neuen Sitzung angezeigten Servern oder nicht mehr im Miniaturansichtsbereich angezeigten Servern beheben.

Führen Sie zur Lösung des Problems die folgenden Schritte aus.

1. Stellen Sie sicher, dass der verwaltete Server durch Lenovo XClarity Administrator verwaltet wird, indem Sie auf der Menüleiste von XClarity Administrator auf **Hardware → Server** klicken.
2. Synchronisieren Sie den Bestand, indem Sie auf die Registerkarte **Allgemein** im Menü Fernbedienungseinstellungen und dann auf **Mit Verwaltungsserver synchronisieren** klicken. Weitere Informationen zu Fernbedienungseinstellungen finden Sie unter Fernbedienungseinstellungen festlegen in der XClarity Administrator-Onlinedokumentation.

Serverstatus in Fernsteuerungssitzung stimmt nicht mit Status in Lenovo XClarity Administrator überein

Mithilfe der Informationen in diesem Abschnitt können Sie Probleme mit einem abweichenden Status für einen verwalteten Server in einer Fernsteuerungssitzung und in Lenovo XClarity Administrator beheben.

Führen Sie zur Lösung des Problems die folgenden Schritte aus.

1. Stellen Sie sicher, dass der Server durch XClarity Administrator verwaltet wird, indem Sie auf der Menüleiste von XClarity Administrator auf **Hardware → Server** klicken.
2. Synchronisieren Sie den Bestand, indem Sie auf die Registerkarte **Allgemein** im Menü Fernbedienungseinstellungen und dann auf **Mit Verwaltungsserver synchronisieren** klicken. Weitere Informationen zu Fernbedienungseinstellungen finden Sie unter Fernbedienungseinstellungen festlegen in der XClarity Administrator-Onlinedokumentation.

Laufwerk oder Image kann nicht an einen Server angehängt werden

Verwenden Sie diese Informationen zur Problembehebung, wenn ein Laufwerk oder Image nicht mit der Funktion „Ferne Medien“ angehängt werden kann.

Führen Sie zur Lösung des Problems die folgenden Schritte aus.

1. Stoppen Sie die Fernsteuerungssitzung und starten Sie sie neu.
2. Setzen Sie den Debugmodus für die Fernsteuerungssitzung auf „Vollständig“. Sie können den Debugmodus über „Einstellungen“ auf der Seite **Allgemein** festlegen. Wenn Sie den Debugmodus auf „Vollständig“ setzen, werden Protokolldateien für die Fernsteuerungssitzung generiert. Weitere Informationen zum Debugmodus finden Sie unter Fernbedienungseinstellungen festlegen.
3. Senden Sie die Protokolldateien an den Lenovo-Support. Weitere Informationen zum Senden von Diagnosedaten an den Lenovo-Support erhalten Sie in Mit Service und Unterstützung arbeiten.

Das optionale Speichermedium wird in der Liste der fernen Medieneinheiten, die zum Anhängen verfügbar sind, nicht angezeigt

Mithilfe der Informationen in diesem Abschnitt können Sie Probleme Speichermedien beheben, die nicht in der Liste der fernen Medieneinheiten zum Anhängen verfügbaren sind.

Wenn eine CD-, DVD- oder USB-Einheit nicht in der Liste der zum Anhängen verfügbaren fernen Medieneinheiten angezeigt wird, klicken Sie im Bereich „Ferne Medien“ auf **Mit Administratoraccount erneut starten**, um auf weitere lokale Einheiten zuzugreifen.

Stromversorgungsoption kann nicht ausgeführt werden.

Verwenden Sie diese Informationen zur Fehlerbehebung, wenn in einer Fernsteuerungssitzung eine Stromversorgungsoperation auf einem verwalteten Server nicht ausgeführt werden kann.

Wenn Sie versuchen, in einer Fernsteuerungssitzung eine Stromversorgungsoperation auf einem verwalteten Server auszuführen, erhalten Sie möglicherweise eine Meldung, dass die Stromversorgungsoperation fehlgeschlagen oder im aktuellen Betriebszustand des verwalteten Servers nicht ausführbar ist.

Führen Sie zur Lösung des Problems die folgenden Schritte aus:

1. Vergewissern Sie sich, dass der Server durch Lenovo XClarity Administrator verwaltet wird. Weitere Informationen finden Sie unter Den Status eines verwalteten Servers anzeigen in der Onlinedokumentation von XClarity Administrator.
2. Überprüfen Sie auf der Seite „Server“, ob der Status des Servers gültig ist.
3. Vergewissern Sie sich, dass die Stromversorgungsoperation im aktuellen Betriebszustand des Servers anwendbar ist. Beispiel: Wenn der Server bereits ausgeschaltet ist, kann keine Ausschaltoperation ausgeführt werden.
4. Prüfen Sie im Jobprotokoll nach, ob die Stromversorgungsoperation ausgeführt wurde. Abhängig von der aktuellen Auslastung von XClarity Administrator kann es einige Zeit dauern, bis die Operation

abgeschlossen ist. Weitere Informationen zum Anzeigen des Jobstatus finden Sie unter Jobs überwachen.

Videoübertragung bei Verbindung mit Flex System x280 X6-, x480 X6- und x880 X6-Server nicht verfügbar

Mithilfe der Informationen in diesem Abschnitt können Sie Probleme beim Start einer Fernsteuerungssitzung für ein Flex System x280 X6-, x480 X6- und x880 X6-Server-System mit mehreren Knoten oder bei einer fehlenden Videoübertragung auf der neuen Registerkarte beheben.

Führen Sie zur Lösung des Problems die folgenden Schritte aus.

1. Beenden Sie die gerade gestartete Verbindung (falls diese noch aktiv ist), indem Sie die neue Registerkarte schließen.
2. Starten Sie eine Remoteverbindung mit dem *primären* Server in der Konfiguration mit mehreren Knoten.

Kapitel 19. Benutzerschnittstellenprobleme

Verwenden Sie diese Informationen, um Probleme mit der Benutzerschnittstelle zu beheben.

Menüelemente, Symbolleistensymbole und Schaltflächen sind deaktiviert (ausgegraut)

Verwenden Sie diese Informationen zur Problembehandlung, wenn bestimmte Aktionen in der Benutzerschnittstelle deaktiviert sind.

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

Stellen Sie sicher, dass Ihr Benutzeraccount einer Rollengruppe mit Berechtigungen zugewiesen ist, die für die Ausführung der Aktion erforderlich sind. Weitere Informationen erhalten Sie von Ihrem System Administrator.

Der Webbrowser reagiert nicht, wenn mehrere Registerkarten geöffnet sind

Wenn mehrere Registerkarten mit Lenovo XClarity Administrator Seiten geöffnet sind, stürzt der Webbrowser möglicherweise ab oder reagiert nicht

XClarity Administrator verwendet JavaScripts vom Client, die große Mengen an Daten mit dem Verwaltungsserver austauschen. Wenn mehrere Registerkarten geöffnet sind, verbraucht der Webbrowser mehr Speicher, Prozessorzyklen und Netzwerkbandbreiten. Mehrere geöffnete Registerkarten können ein Grund dafür sein, dass einige Browser abstürzen oder nicht mehr reagieren. Die Auswirkungen variieren je nach Typ und Version des Webbrowsers.

Um dieses Problem zu beheben, verringern Sie die Anzahl der Registerkarten des Webbrowsers mit XClarity Administrator Seiten.

Weitere Informationen erhalten Sie unter Tipp HT504133

JSON-Antwort fehlgeschlagen, Parsing-Fehler und andere unerwartete Fehler

Mithilfe der Informationen in diesem Abschnitt können Sie Probleme mit der JSON-Antwort beheben.

Melden Sie sich vom Lenovo XClarity Administrator ab und versuchen Sie, sich wieder anzumelden.

Die Benutzeroberfläche ist nicht in der bevorzugten Sprache

Verwenden Sie diese Informationen, um Probleme mit den Spracheinstellungen zu beheben.

1. Stellen Sie sicher, dass der Webbrowser die Ländereinstellung Ihrer bevorzugte Sprache verwendet.

© Copyright Lenovo 2015, 2025

2. Klicken Sie in der Lenovo XClarity Administrator-Titelleiste auf das Benutzeraktionen-Menü (

) und anschließend auf **Sprache ändern**. Wählen Sie die Sprache aus, die Sie anzeigen möchten, und klicken Sie dann auf **Schließen**.

Ladezeiten langsam oder scheinbar inaktiv, lange Wartezeit für Aktualisierung, falsches Rendering

Verwenden Sie diese Informationen, um Probleme mit der Benutzerschnittstelle zu beheben.

1. Aktualisieren Sie die Seite mit der Schaltfläche **Aktualisieren** in Ihrem Webbrowser.
2. Leeren Sie den Browsercache und aktualisieren Sie die Seite.

Unerwarteter Datenverlust

Verwenden Sie diese Informationen, um Datenverlust in Lenovo XClarity Administrator zu beheben.

Wenn das Hostbetriebssystem unerwartet heruntergefahren wurde, stellen Sie XClarity Administrator von der letzten Sicherung wieder her (siehe XClarity Administrator sichern und wiederherstellen in der Onlinedokumentation von XClarity Administrator).

Änderungen der Einheitenposition werden nicht in der Rack-Ansicht angezeigt.

Verwenden Sie diese Informationen, um Probleme mit der Rack-Ansicht in Lenovo XClarity Administrator zu beheben.

Wenn Sie die Position einer Einheit mithilfe einer der folgenden REST-APIs oder unter Verwendung des Baseboard Management Controllers ändern, nachdem die Einheit von XClarity Administrator verwaltet wurde, werden die Änderungen nicht in der Rack-Ansicht auf der Benutzerschnittstelle von XClarity Administrator angezeigt. Bearbeiten Sie die Eigenschaften der Einheit oder das Rack auf der Benutzerschnittstelle, um die in der API oder im Management Controller vorgenommenen Änderungen anzuzeigen (siehe Systemeigenschaften für einen Server ändern, Die Details eines verwalteten Gehäuses anzeigen und Racks verwalten in der Onlinedokumentation von XClarity Administrator).

- PUT /canisters/*<UUID>*
- PUT /chassis/*<UUID>*
- PUT /nodes/*<UUID>*