Lenovo

XClarity Controller mit Intel Xeon SP Prozessoren der 1. und 2. Generation Benutzerhandbuch

Anmerkung: Vor Verwendung dieser Informationen sollten Sie die allgemeinen Informationen in Anhang B „Hinweise“ auf Seite 221 lesen.

Fünfzehnte Ausgabe (Mai 2021)

Inhaltsverzeichnis

Kapitel 1. Einführung

Der Lenovo XClarity Controller (XCC) ist der Management-Controller der nächsten Generation für Lenovo ThinkSystem-Server und ersetzt den Baseboard Management Controller (BMC).

Es handelt sich um die Nachfolgeversion des Serviceprozessors Integrated Management Module II (IMM2), bei dem die Serviceprozessor-Funktionalität sowie die Super E/A-, Videocontroller- und Fernpräsenzfunktion auf einem einzigen Chip auf der Systemplatine des Servers vereint sind. Er bietet unter anderem die folgenden Funktionen:

- Auswahl zwischen einer dedizierten oder einer gemeinsam genutzten Ethernet-Verbindung für das Systemmanagement
- Unterstützung für HTML5
- Unterstützung für den Zugriff über XClarity Mobile
- XClarity Provisioning Manager
- Ferne Konfiguration mithilfe von XClarity Essentials oder XClarity Controller CLI
- Die Möglichkeit für Anwendungen und Tools, um lokal oder über Fernzugriff auf XClarity Controller zuzugreifen
- Erweiterte Remote-Presence-Funktionalität
- REST API-Unterstützung (Redfish-Schema) für zusätzliche webbezogene Services und Softwareanwendungen

  Anmerkung: Der XClarity Controller unterstützt derzeit Redfish Scalable Platforms Management API Specification 1.0.2 und Schema 2016.2

Anmerkungen:

- In der XClarity Controller-Webschnittstelle wird BMC in Bezug auf den XCC verwendet.
- Auf einigen ThinkSystem-Servern ist möglicherweise kein dedizierter Systemmanagement-Netzanschluss verfügbar. Bei diesen Servern ist der Zugriff auf den XClarity Controller nur über einen Netzwerkanschluss verfügbar, der gemeinsam mit dem Serverbetriebssystem verwendet wird.
- Bei Flex-Servern ist das Chassis Management Module (CMM) das primäre Verwaltungsmodul für Systemverwaltungsfunktionen. Der Zugriff auf den XClarity Controller ist über den Netzanschluss auf dem CMM verfügbar.

In diesem Dokument wird erläutert, wie die Funktionen des XClarity Controller in einem ThinkSystem-Server verwendet werden. Der XClarity Controller funktioniert mit dem XClarity Provisioning Manager und UEFI, um Systemverwaltungsfunktionen für ThinkSystem-Server bereitzustellen.

Gehen Sie wie folgt vor, um zu prüfen, ob Firmwareaktualisierungen verfügbar sind.

Anmerkung: Beim ersten Zugriff auf das Support Portal müssen Sie die Produktkategorie, die Produktfamilie und die Modellnummern Ihres Servers auswählen. Wenn Sie das nächste Mal auf das Support Portal zugreifen, werden die Produkte, die Sie beim ersten Mal ausgewählt haben, von der Website erneut geladen, sodass nur die Links für Ihre Produkte angezeigt werden. Um Ihre Produktliste zu ändern oder Elemente zu ihr hinzuzufügen, klicken Sie auf den Link **Meine Produktlisten verwalten**. Die Informationen auf der Website werden in regelmäßigen Abständen aktualisiert. Die tatsächliche Vorgehensweise bei der Suche nach Firmware und Dokumentationen kann deshalb geringfügig von der an dieser Stelle beschriebenen Vorgehensweise abweichen.

1. Wechseln Sie zu http://datacentersupport.lenovo.com.
2. Wählen Sie unter **Support** die Option **Data Center (Rechenzentrum)** aus.

3. Wenn der Inhalt geladen ist, wählen Sie **Servers (Server)** aus.
4. Wählen Sie unter **Select Series (Serie auswählen)** zunächst die entsprechende Serverhardwareserie und dann unter **Select SubSeries (Subserie auswählen)** die Serverprodukt-Subserie und schließlich unter **Select Machine Type (Maschinentyp auswählen)** den Maschinentyp aus.

Merkmale von XClarity Controller Standard, Advanced und XClarity Enterprise Level

Mit dem XClarity Controller werden die Level Standard, Advanced und Enterprise der XClarity Controller-Funktionalität angeboten. Weitere Informationen zu der auf Ihrem Server installierten XClarity Controller-Version finden Sie in der Dokumentation für Ihren Server. Alle Versionen bieten folgende Funktionen:

- Fernzugriff und Fernverwaltung Ihres Servers rund um die Uhr
- Fernverwaltung unabhängig vom Status des verwalteten Servers
- Fernsteuerung der Hardware und der Betriebssysteme

Anmerkung: Einige Merkmale gelten möglicherweise nicht für Flex System-Server.

Im Folgenden sind die Merkmale von XClarity Controller Standard Level aufgeführt:

Funktionen von XClarity Controller Standard Level

Im Folgenden sind die Merkmale von XClarity Controller Standard Level aufgeführt:

Verwaltungsschnittstellen nach Branchenstandard

- IPMI 2.0-Schnittstelle
- Redfish
- CIM-XML
- DCMI 1.5
- SNMPv3
- SNMPv1 (nur Traps) erfordert je nach Servertyp mindestens die XCC Firmwareaktualisierungen v2.10 oder v2.12. Weitere Informationen finden Sie in „XCC-Firmwareaktualisierung – Änderungsdatei“.

Andere Verwaltungsschnittstellen

- Web
- Traditionelle Befehlszeilenschnittstelle
- Vorderseitiger USB-Anschluss – virtuelle Bedienerkonsole über mobiles Gerät

Steuerung von Einschalten/Zurücksetzen

- Einschalten
- Erzwungener/normaler Systemabschluss
- Geplante Stromverbrauchssteuerung
- Systemneustart
- Steuerung der Bootreihenfolge

Ereignisprotokolle

- IPMI SEL
- Protokoll in Klartext

- Prüfprotokoll

Umgebungsüberwachung

- Agentenfreie Überwachung
- Sensorüberwachung
- Lüftersteuerung
- LED-Steuerung
- Chipsatzfehler (Caterr, IERR usw.)
- Anzeige des Systemzustands
- OOB-Leistungsüberwachung für E/A-Adapter
- Bestandsanzeige/-export

RAS

- Virtuelles NMI
- Automatische Firmwarewiederherstellung
- Automatisierte Hochstufung der Sicherungsfirmware
- POST-Watchdog
- Watchdog für BS-Ladeprogramm
- Speicherung der Systemabsturzanzeige (BS-Fehler)
- Integrierte Diagnosetools

Netzwerkkonfiguration

- IPv4
- IPv6
- IP-Adresse, Subnetzmaske, Gateway
- Modi für IP-Adresszuordnung
- Hostname
- Programmierbare MAC-Adresse
- Duale MAC-Auswahl (falls durch Serverhardware unterstützt)
- Neuzuweisungen der Netzanschlüsse
- VLAN-Tagging

Netzwerkprotokolle

- DHCP
- DNS
- DDNS
- HTTP/HTTPS
- SNMPv3
- SNMPv1 (nur Traps)
- SSL
- SSH
- SMTP

- LDAP-Client
- NTP
- SLP
- SSDP

Alerts

- PET-Traps
- CIM-Meldung
- SNMP-Traps
- E-Mail
- Redfish-Ereignisse

Serielle Umleitung

- IPMI-SOL
- Konfiguration des seriellen Anschlusses

Sicherheit

- Core Root of Trust for Measurement (CRTM) von XClarity Controller
- Digital signierte Firmwareaktualisierungen
- Rollenbasierte Zugriffssteuerung (RBAC)
- Lokale Benutzeraccounts
- LDAP/AD-Benutzeraccounts
- Sicheres Rollback der Firmware
- Erkennung von unbefugtem Gehäusezugriff (nur verfügbar bei einigen Servermodellen)
- XCC-Fernbestätigung der physischen Präsenz von UEFI TPM
- Prüfprotokollaufzeichnung der Konfigurationsänderungen und Serveraktionen
- Public-Key-Authentifizierung
- Stilllegung/Umfunktionierung des Systems

Fernpräsenz

- RDOC (Remote Disk on Card): Anhängen virtueller Medien der ISO/IMG-Remotedateien über CIFS, NFS, HTTP, HTTPS, FTP, SFTP und LOCAL

Energieverwaltung

- Echtzeit-Stromzähler

Lizenzverwaltung

- Überprüfung und Repository für Aktivierungsschlüssel

Bereitstellung und Konfiguration

- Remote-Konfiguration
- Bereitstellungs- und Konfigurationstools und Treiberpakete mit dem integrierten XClarity Provisioning Manager
- Sicherung und Wiederherstellung der Konfiguration

Firmwareaktualisierungen

- Agentenfreie Aktualisierung
- Remote-Aktualisierung

Funktionen von XClarity Controller Advanced Level

Im Folgenden sind die Merkmale von XClarity Controller Advanced Level aufgeführt:

Alle Funktionen von XClarity Controller Standard Level plus:

Alerts

- Syslog

Fernpräsenz

- Remote-KVM

Serielle Umleitung

- Serielle Umleitung via SSH

Sicherheit

- Security Key Lifecycle Manager (SKLM)
- Blockierung von IP-Adressen

Energieverwaltung

- Grafische Darstellung der Stromversorgung in Echtzeit
- Historische Stromzähler
- Temperaturgrafiken

Bereitstellung und Konfiguration

- Remote-BS-Implementierung mit dem integrierten XClarity Provisioning Manager mit der XClarity Controller Remote-KVM-Funktion

Funktionen von XClarity Controller Enterprise Level

Im Folgenden sind die Funktionen von XClarity Controller Enterprise Level aufgeführt:

Alle Funktionen von XClarity Controller Standard und XClarity Advanced Level plus:

RAS

- Booterfassung

Fernpräsenz

- Steuerung von Qualität/Bandbreite
- Zusammenarbeit über virtuelle Konsole (sechs Benutzer)
- Chat über virtuelle Konsole
- Virtuelle Datenträger
  - Anhängen von ISO/IMG-Remotedateien über die ferne Konsole

– Anhängen von Dateien aus dem Netzwerk: Anhängen einer ISO- oder IMG-Image-Datei von einem Dateiserver (HTTPS, CIFS, NFS) zum Host als ein DVD- oder USB-Laufwerk

Energieverwaltung

- Energieverbrauchsbegrenzung
- OOB-Leistungsüberwachung – Systemleistungskennzahlen

Bereitstellung und Konfiguration

- Remote-Bereitstellung mit Lenovo XClarity Administrator. Wenn Sie Lenovo XClarity Administrator für die Betriebssystembereitstellung verwenden, finden Sie unter https://pubs.lenovo.com/lxca/supported_operating_system_images ausführliche Informationen zu den unterstützten Betriebssystemen.

XClarity Controller aktualisieren

Wenn Ihr Server über die XClarity Controller-Firmwarefunktionalitätsversion „Standard Level“ oder „Advanced Level“ verfügt, können Sie möglicherweise ein Upgrade für die XClarity Controller-Funktionen auf Ihrem Server durchführen. Weitere Informationen zu den verfügbaren Upgradestufen und wie Sie sie bestellen können, finden Sie in Kapitel 8 „Lizenzverwaltung“ auf Seite 95.

Voraussetzungen – Web-Browser und Betriebssystem

Mithilfe der Informationen in diesem Abschnitt können Sie die Liste unterstützter Browser, Cipher-Suites und Betriebssysteme für Ihren Server anzeigen.

Die XClarity Controller-Webschnittstelle erfordert einen der folgenden Webbrowser:

- Chrome 48.0 oder höher (55.0 oder höher für Ferne Konsole)
- Firefox ESR 38.6.0 oder höher
- Microsoft Edge
- Safari 9.0.2 oder höher (iOS 7 oder höher und OS X)

Anmerkung: Unterstützung für die Funktion der fernen Konsole ist über den Browser auf Betriebssystemen für mobile Geräte nicht verfügbar.

Die oben aufgelisteten Browser stellen die aktuell von der XClarity Controller-Firmware unterstützen Browser dar. Die XClarity Controller-Firmware kann in regelmäßigen Abständen erweitert werden, um Unterstützung für andere Browser bereitzustellen.

Je nachdem, welche Version der Firmware im XClarity Controller verwendet wird, kann sich die Web-Browser-Unterstützung von den in diesem Abschnitt aufgeführten Browsern unterscheiden. Wenn Sie die Liste unterstützter Browser für die Firmware anzeigen möchten, die derzeit auf dem XClarity Controller verwendet wird, klicken Sie auf der XClarity Controller-Anmeldeseite auf die Menüliste **Unterstützte Browser**.

Für eine höhere Sicherheit werden bei der Verwendung von HTTPS nur noch hohe Verschlüsselungsgrade unterstützt. Bei der Verwendung von HTTPS muss die Kombination aus Ihrem Clientbetriebssystem und Browser eine der folgenden Cipher-Suites unterstützen:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256

- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Im Zwischenspeicher Ihres Internet-Browsers werden Informationen zu Webseiten, die Sie besuchen, gespeichert, damit diese zukünftig schneller geladen werden können. Nach einer Flashaktualisierung der XClarity Controller-Firmware verwendet Ihr Browser möglicherweise weiterhin die Informationen aus seinem Zwischenspeicher, anstatt sie aus dem XClarity Controller abzurufen. Nach Aktualisierung der XClarity Controller-Firmware wird empfohlen, dass Sie den Browser-Zwischenspeicher leeren, um sicherzustellen, dass Webseiten, die durch XClarity Controller bereitgestellt werden, ordnungsgemäß angezeigt werden.

Unterstützung für mehrere Sprachen

Mithilfe der Informationen in diesem Abschnitt können Sie die Liste der Sprachen anzeigen, die vom XClarity Controller unterstützt werden.

Standardmäßig ist die ausgewählte Sprache für die XClarity Controller-Webschnittstelle Englisch. In der Schnittstelle können mehrere Sprachen angezeigt werden. Dazu gehören Folgende:

- Französisch
- Deutsch
- Italienisch
- Japanisch
- Koreanisch
- Portugiesisch (Brasilien)
- Russisch
- Vereinfachtes Chinesisch
- Spanisch (international)
- Traditionelles Chinesisch

Klicken Sie auf den Pfeil neben der aktuell ausgewählten Sprache, um die bevorzugte Sprache auszuwählen. Ein Dropdown-Menü wird angezeigt, in dem Sie Ihre bevorzugte Sprache auswählen können.

Die Textzeichenfolgen, die von der XClarity Controller-Firmware generiert werden, werden in der Sprache angezeigt, die vom Browser vorgegeben ist. Wenn der Browser eine andere Sprache als eine der o. g. übersetzten Sprachen vorgibt, wird der Text in Englisch angezeigt. Außerdem werden alle Textzeichenfolgen, die von der XClarity Controller-Firmware angezeigt, aber nicht vom XClarity Controller generiert werden (z. B. von UEFI, PCIe-Adaptern usw. generierte Nachrichten) in Englisch angezeigt.

Die Eingabe sprachspezifischen Textes außer Englisch, wie z. B. der **Trespass-Nachricht**, wird derzeit nicht unterstützt. Nur in Englisch eingegebener Text wird unterstützt.

Einführung zu MIBs

Mithilfe der Informationen in diesem Abschnitt können Sie auf die MIB (Management Information Base) zugreifen.

Die SNMP-MIB kann von https://support.lenovo.com/ heruntergeladen werden (Suche nach Maschinentyp im Portal). Die folgenden vier MIBs sind enthalten.

- In der **SMI MIB** wird die Struktur der Verwaltungsinformationen für die Lenovo Data Center Group (DCG) beschrieben.
- In der **Produkt MIB** werden die Objekt-IDs für Lenovo Produkte beschrieben.
- In der **XCC MIB** sind die Bestands- und Überwachungsinformationen für Lenovo XClarity Controller enthalten.
- In der **XCC Alert MIB** werden Traps für Alert-Bedingungen definiert, die von Lenovo XClarity Controller erkannt wurden.

Anmerkung: Die Importreihenfolge für die vier MIBs ist **SMI MIB** → **Produkt MIB** → **XCC MIB** → **XCC Alert MIB**.

In diesem Dokument verwendete Bemerkungen

Dieser Abschnitt enthält Informationen zu den Bemerkungen, die in diesem Dokument verwendet werden.

In dieser Dokumentation werden die folgenden Bemerkungen verwendet:

- **Anmerkung:** Diese Bemerkungen enthalten wichtige Tipps, Anleitungen oder Ratschläge.
- **Wichtig:** Diese Bemerkungen geben Ihnen Informationen oder Ratschläge, durch die Sie Unannehmlichkeiten oder Fehler vermeiden können.
- **Achtung:** Diese Bemerkungen weisen auf eine mögliche Beschädigung von Programmen, Einheiten oder Daten hin. Eine mit „Achtung“ gekennzeichnete Bemerkung befindet sich direkt vor der Anweisung oder der Beschreibung der Situation, die diese Beschädigung bewirken könnte.

Kapitel 2. XClarity Controller-Webschnittstelle öffnen und verwenden

In diesem Abschnitt werden das Anmeldeverfahren und die Aktionen beschrieben, die Sie über die XClarity Controller-Webschnittstelle ausführen können.

Der XClarity Controller vereint Serviceprozessor-, Videocontroller- und Remote-Presence-Funktionen in einem einzigen Chip. Für den Fernzugriff auf den XClarity Controller über die XClarity Controller-Webschnittstelle müssen Sie sich zuerst anmelden. In diesem Kapitel werden das Anmeldeverfahren und die Aktionen beschrieben, die Sie über die XClarity Controller-Webschnittstelle ausführen können.

Auf die XClarity Controller-Webschnittstelle zugreifen

Die Informationen in diesem Abschnitt befassen sich mit dem Zugriff auf die XClarity Controller-Webschnittstelle.

Der XClarity Controller unterstützt die statische und die Dynamic Host Configuration Protocol(DHCP)-IPv4-Adressierung. Die standardmäßig dem XClarity Controller zugewiesene statische IPv4-Adresse lautet 192.168.70.125. Der XClarity Controller ist anfänglich so konfiguriert, dass er versucht, eine Adresse von einem DHCP-Server abzurufen. Ist dies nicht möglich, verwendet er die statische IPv4-Adresse.

Der XClarity Controller unterstützt auch IPv6, verfügt aber nicht standardmäßig über eine festgelegte statische IPv6-IP-Adresse. Für den Erstzugriff auf den XClarity Controller in einer IPv6-Umgebung können Sie entweder die IPv4-IP-Adresse oder die lokale IPv6-Verbindungsadresse verwenden. Der XClarity Controller generiert mithilfe der IEEE 802 MAC-Adresse eine eindeutige lokale IPv6-Verbindungsadresse, indem zwei Oktette eingefügt werden. Dazu werden die Hexadezimalwerte 0xFF und 0xFE in die Mitte des 48-Bit-MAC wie in RFC4291 beschrieben eingegeben und das zweite Bit von rechts im ersten Oktett der MAC-Adresse umgekehrt. Wenn die MAC-Adresse beispielsweise 08-94-ef-2f-28-af lautet, wäre die lokale Verbindungsadresse:
`fe80::0a94:efff:fe2f:28af`

Beim Zugriff auf den XClarity Controller sind die folgenden IPv6-Bedingungen als Standardwerte definiert:

- Die automatische IPv6-Adresskonfiguration ist aktiviert.
- Die statische IPv6-IP-Adresskonfiguration ist deaktiviert.
- DHCPv6 ist aktiviert.
- Die statusunabhängige automatische Konfiguration ist aktiviert.

Der XClarity Controller ermöglicht die Auswahl einer **dedizierten** Systemmanagement-Netzverbindung (falls vorhanden) oder einer Netzverbindung, die **gemeinsam** mit dem Server verwendet wird. Die Standardverbindung für in einem Gehäuserahmen installierte Server und Turmserver verwendet den **dedizierten** Systemmanagement-Netzanschluss.

Die dedizierte Systemmanagement-Netzverbindung auf den meisten Servern wird mithilfe eines separaten 1-Gbit-Netzwerkschnittstellencontrollers bereitgestellt. Auf einigen Systemen wird die dedizierte Systemmanagement-Netzwerkverbindung jedoch möglicherweise mithilfe des Network Controller Sideband Interface (NCSI) für einen der Netzwerkanschlüsse eines Multi-Port-Netzwerkschnittstellencontrollers bereitgestellt. In diesem Fall ist die dedizierte Systemmanagement-Netzwerkverbindung auf die 10/100-Geschwindigkeit der Seitenbandschnittstelle beschränkt. Informationen zur und Einschränkungen bei der Implementierung des Managementanschlusses auf Ihrem System finden Sie in der Systemdokumentation.

Anmerkung: Möglicherweise hat Ihr Server keinen **dedizierten** Systemmanagement-Netzanschluss. Wenn auf Ihrer Hardware kein **dedizierter** Netzanschluss vorhanden ist, ist die Einstellung **gemeinsam genutzt** die einzige verfügbare XClarity Controller-Einstellung.

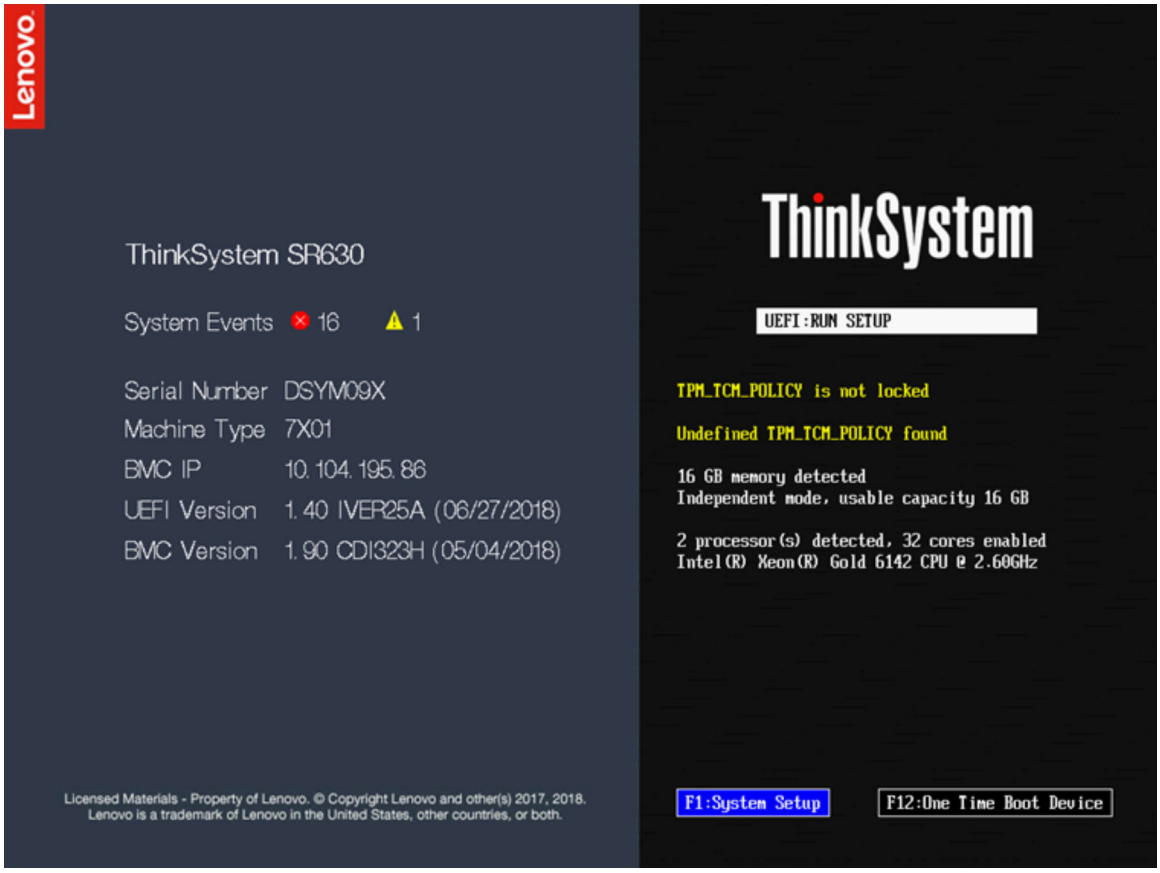
XClarity Controller-Netzwerkverbindung über den XClarity Provisioning Manager einrichten

Mithilfe der Informationen in diesem Abschnitt können Sie eine XClarity Controller-Netzwerkverbindung über den XClarity Provisioning Manager einrichten.

Nachdem Sie den Server gestartet haben, können Sie den XClarity Provisioning Manager verwenden, um die XClarity Controller-Netzwerkverbindung zu konfigurieren. Der Server mit dem XClarity Controller muss mit einem DHCP-Server verbunden sein oder das Servernetz muss so konfiguriert sein, dass er die statische IP-Adresse des XClarity Controller verwendet. Gehen Sie wie folgt vor, um die XClarity Controller-Netzverbindung über das Konfigurationsdienstprogramm herzustellen:

Schritt 1. Schalten Sie den Server ein. Die ThinkSystem-Eingangsanzeige wird angezeigt.

Anmerkung: Es kann bis zu 40 Sekunden dauern, nachdem der Server an die Wechselstromversorgung angeschlossen wurde, bis der Netzschalter aktiviert wird.



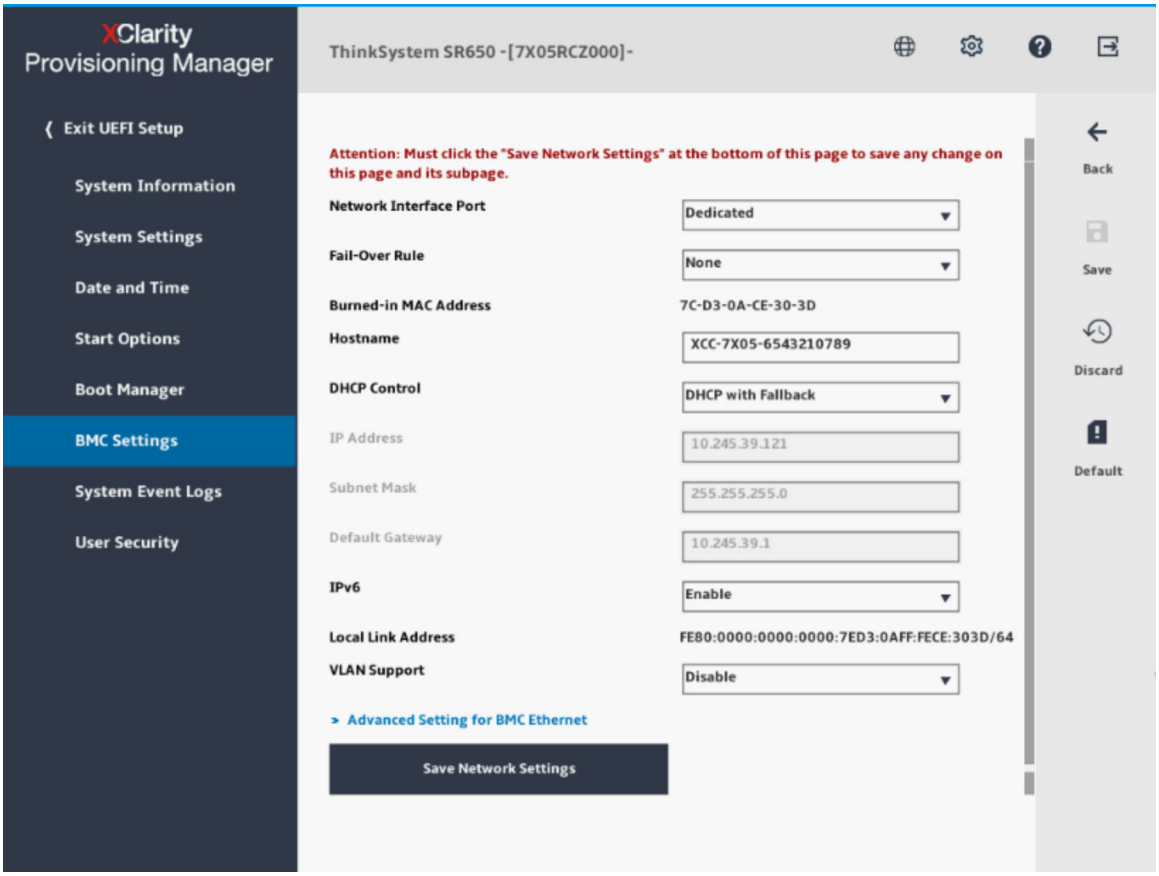
Schritt 2. Wenn die Aufforderung `<F1> System Setup` angezeigt wird, drücken Sie F1. Wenn Sie sowohl ein Startkennwort als auch ein Administratorkennwort festgelegt haben, müssen Sie zum Zugriff auf den XClarity Provisioning Manager das Administratorkennwort eingeben.

Schritt 3. Wählen Sie im Hauptmenü des XClarity Provisioning Manager die Option **UEFI Setup** aus.

Schritt 4. Wählen Sie in der nächsten Anzeige die Option **BMC Settings** und anschließend **Network Settings** aus.

Schritt 5. Im Feld **DHCP Control** stehen drei XClarity Controller-Netzverbindungen zur Auswahl:

- Statische IP
- DHCP aktiviert
- DHCP mit Rückstellung



Schritt 6. Wählen Sie eine der Netzverbindungen.

Schritt 7. Wenn Sie sich dafür entscheiden, eine statische IP-Adresse zu verwenden, müssen Sie die IP-Adresse, die Teilnetzmaske und das Standard-Gateway angeben.

Schritt 8. Sie können den Lenovo XClarity Controller Manager auch dazu verwenden, eine dedizierte Netzverbindung (wenn Ihr Server einen dedizierten Netzanschluss hat) oder eine gemeinsam genutzte XClarity Controller-Netzverbindung auszuwählen.

Anmerkungen:

- Möglicherweise hat Ihr Server keinen Anschluss für dedizierte Systemmanagementnetze. Wenn auf Ihrer Hardware kein dedizierter Netzanschluss vorhanden ist, ist die Einstellung **gemeinsam genutzt** die einzige verfügbare XClarity Controller-Einstellung. Wählen Sie in der Anzeige **Network Configuration** im Feld **Dedicated Shared** (falls zutreffend) oder **Network Interface Port** aus.
- Informationen dazu, wo sich auf Ihrem Server die vom XClarity Controller genutzten Ethernet-Anschlüsse befinden, finden Sie in der Dokumentation zum Server.

Schritt 9. Klicken Sie auf **Speichern**.

Schritt 10. Beenden Sie den XClarity Provisioning Manager.

Anmerkungen:

- Sie müssen etwa eine Minute warten, bis die Änderungen wirksam werden und die Server-Firmware wieder funktioniert.
- Sie können die XClarity Controller-Netzverbindung auch über die XClarity Controller-Webschnittstelle oder die Befehlszeilenschnittstelle konfigurieren. In der XClarity Controller-Webschnittstelle können die Netzwerkverbindungen durch Klicken auf **BMC-Konfiguration** (linker Navigationsbereich) und **Netzwerk** konfiguriert werden. In der XClarity Controller-Befehlszeilenschnittstelle werden die Netzverbindungen mit mehreren Befehlen konfiguriert, je nach der Konfiguration Ihrer Installation.

Am XClarity Controller anmelden

Mithilfe der Informationen in diesem Abschnitt können Sie über die XClarity Controller-Webschnittstelle auf den XClarity Controller zugreifen.

Wichtig: Für den XClarity Controller ist als erster Benutzername `USERID` und als erstes Kennwort `PASSWORD` (mit einer Null anstelle des Buchstabens O) voreingestellt. Bei dieser Standard-Benutzereinstellung haben nur Administratoren Zugriff. Ändern Sie für größere Sicherheit diesen Benutzernamen und das zugehörige Kennwort bei der Erstkonfiguration. Nach der Änderung können Sie `PASSWORD` nicht wieder als Anmeldekennwort festlegen.

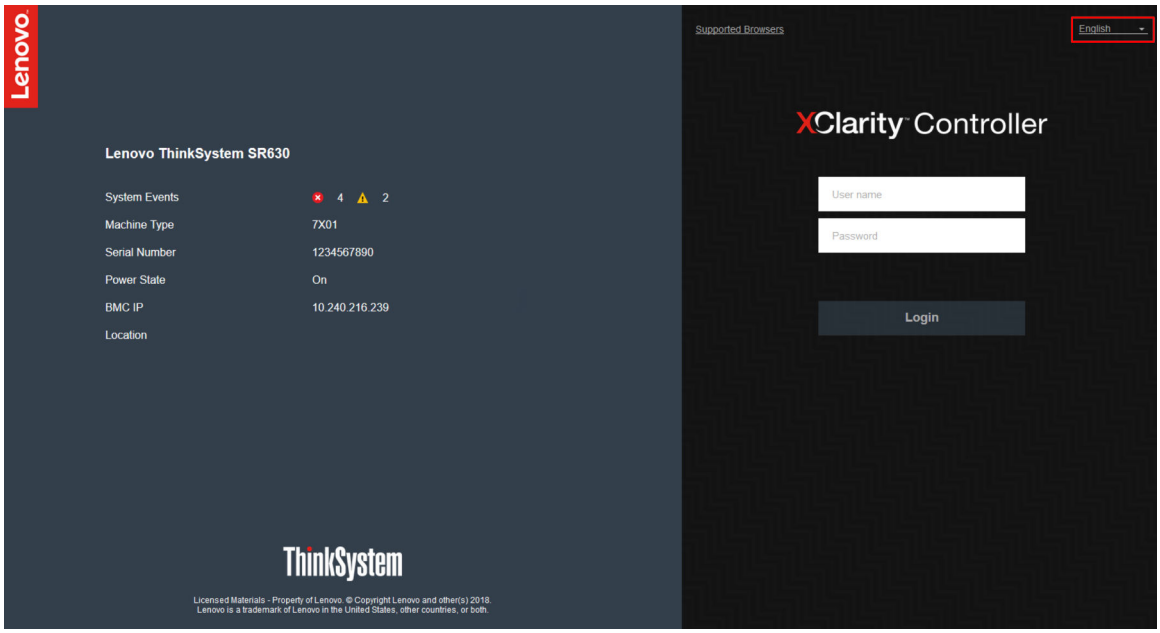
Anmerkung: In einem Flex System können die XClarity Controller-Benutzeraccounts von einem Flex System Chassis Management Module (CMM) verwaltet werden und sich von der oben beschriebenen USERID/PASSW0RD-Kombination unterscheiden.

Führen Sie die folgenden Schritte aus, um über die XClarity Controller-Webschnittstelle auf den XClarity Controller zuzugreifen:

Schritt 1. Öffnen Sie einen Web-Browser. Geben Sie im Feld „Adresse“ oder „URL“ die IP-Adresse oder den Hostnamen des XClarity Controller ein, zu dem Sie eine Verbindung herstellen möchten.

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

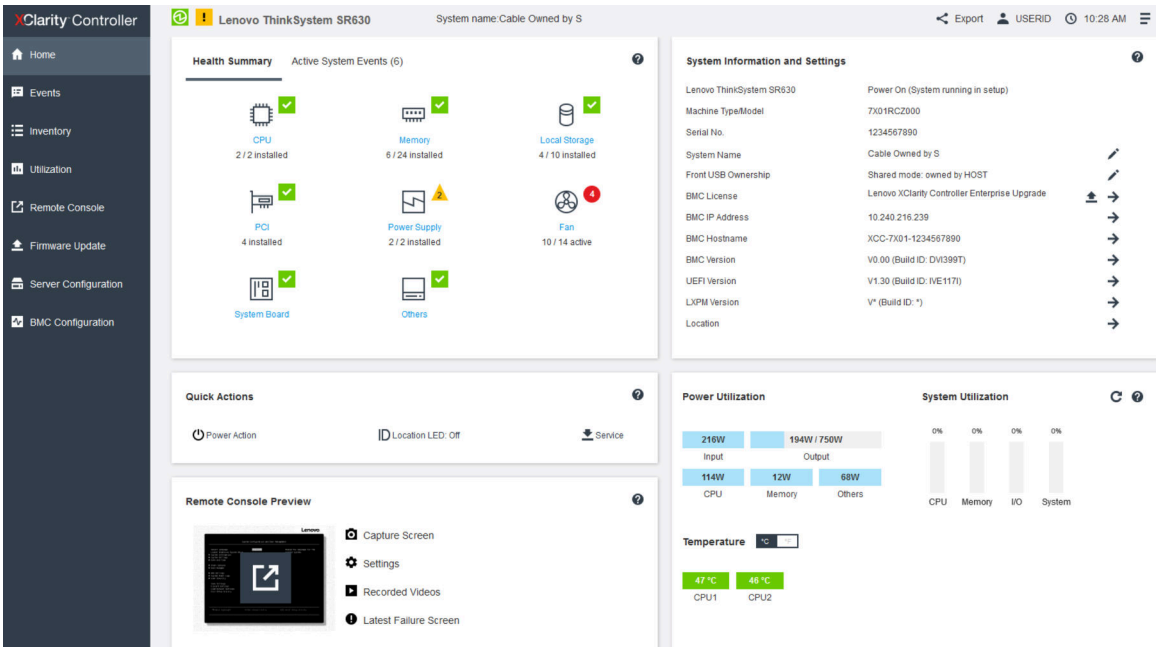
Das Anmeldefenster ist in der folgenden Abbildung dargestellt.



Schritt 3. Geben Sie Ihren Benutzernamen und Ihr Kennwort in das XClarity Controller-Anmeldefenster ein. Wenn Sie den XClarity Controller zum ersten Mal verwenden, können Sie Ihren Benutzernamen

und das Kennwort von Ihrem Systemadministrator anfordern. Alle Anmeldeversuche werden im Ereignisprotokoll erfasst. Je nachdem, wie Ihr Systemadministrator die Benutzer-ID konfiguriert hat, müssen Sie möglicherweise nach der Anmeldung ein neues Kennwort eingeben.

Schritt 4. Klicken Sie auf **Anmelden**, um die Sitzung zu starten. Im Browser wird die Startseite „XClarity Controller“ geöffnet, wie in der folgenden Abbildung dargestellt. Auf der Startseite werden Informationen zum System angezeigt, das vom XClarity Controller verwaltet wird, sowie Symbole, die angeben, wie viele kritische Fehler und wie viele Warnungen derzeit im System vorhanden sind.



Die Startseite ist im Prinzip in zwei Abschnitte unterteilt. Der erste Abschnitt ist der linken Navigationsbereich, in dem ein Satz von Themen angezeigt wird, über die Sie die folgenden Aktionen durchführen können:

- Serverstatus überwachen
- Server konfigurieren
- XClarity Controller oder BMC konfigurieren
- Firmware aktualisieren

Der zweite Abschnitt enthält die grafischen Informationen, die rechts vom Navigationsbereich bereitgestellt werden. Das modulare Format bietet Ihnen einen schnellen Überblick über den Serverstatus sowie einige schnelle Aktionen, die durchgeführt werden können.

Beschreibung der XClarity Controller-Merkmale auf der Webschnittstelle

Nachfolgend sehen Sie eine Tabelle, in der die XClarity Controller-Merkmale im linken Navigationsfenster beschrieben werden.

Anmerkung: Bei der Navigation in der Webschnittstelle können Sie auch auf das Fragezeichensymbol klicken, um die Onlinehilfe anzuzeigen.

Tabelle 1. XClarity Controller-Merkmale

Tabelle mit drei Spalten, die Beschreibungen der Aktionen enthält, die Sie in der XClarity Controller-Webschnittstelle ausführen können.

Tabulatortaste	Auswahl	Beschreibung
Startseite	Zustandszusammenfassung/ Aktive Systemereignisse	Zeigt den aktuellen Status der Haupthardwarekomponenten im System an.
	Systeminformationenen und Einstellungen	Enthält eine Zusammenfassung der allgemeinen Systeminformationen.
	Schnelle Aktionen	Bietet einen Quick Link zur Steuerung der Serverstromversorgung und Positionsanzeige sowie eine Schaltfläche zum Herunterladen der Servicedaten.
	Energieverbrauch/ Systemauslastung/Temperatur	Bietet eine Kurzübersicht über den aktuellen Stromverbrauch, die Systemauslastung und die allgemeine Servertemperatur.
	Ferne Konsolenvorschau	Steuerung des Servers auf Betriebssystemebene. Sie können die Serverkonsole über Ihren Computer anzeigen und bedienen. Der Abschnitt zur fernen Konsole auf der XClarity Controller-Startseite zeigt eine Bildschirmanzeige mit einer Schaltfläche zum Starten an. Die rechte Symbolleiste umfasst die folgenden schnellen Aktionen: • Screenshot erstellen • Einstellungen • Aufgezeichnete Videos • Letzte Fehleranzeige
Ereignisse	Ereignisprotokoll	Bietet eine Liste aller archivierten Hardware- und Verwaltungsereignisse.
	Prüfprotokoll	Bietet eine historische Aufzeichnung aller Benutzeraktionen, z. B. Anmelden an Lenovo XClarity Controller, Erstellen eines neuen Benutzers und Ändern eines Benutzerkennworts. Sie können das Prüfprotokoll verwenden, um Authentifizierung und Kontrollen in IT-Systemen nachzuverfolgen und zu dokumentieren.
	Wartungsverlauf	Zeigt alle Firmwareaktualisierungen, Konfigurations- und Hardwareaustauschprotokolle an.
	Alertempfänger	Verwalten, wer über Systemereignisse benachrichtigt wird. Sie können jeden Empfänger konfigurieren und Einstellungen verwalten, die für alle Ereignisempfänger gelten. Sie können auch ein Testereignis generieren, um die Benachrichtigungs-Konfigurationseinstellungen zu überprüfen.
Bestand		Zeigt alle Komponenten im System an, zusammen mit ihrem Status und wesentlichen Informationen. Sie können auf eine Einheit klicken, um zusätzliche Informationen anzuzeigen. **Anmerkung:** Weitere Details zum Stromversorgungsstatus der Lösung finden Sie in der SMM2-Webschnittstelle.
Auslastung		Zeigt Informationen zu Umgebungs-/Komponententemperatur, Stromverbrauch, Spannungspegel, System-/ Subsystemauslastung und Lüftergeschwindigkeit des Servers und seiner Komponenten in grafischer oder tabellarischer Form an.

Tabelle 1. XClarity Controller-Merkmale (Forts.)

Tabulatortaste	Auswahl	Beschreibung
Speicher	Detail	Zeigt die physische Struktur und die Speicherkonfiguration der Speichereinheiten an.
	RAID-Konfiguration	Rufen Sie die aktuelle RAID-Konfiguration auf, einschließlich Informationen zu virtuellen Platten und physischen Speichereinheiten, oder ändern Sie sie.
Ferne Konsole		Bietet Zugriff auf die Funktionalität der fernen Konsole. Sie können die Funktion „Virtuelle Datenträger“ verwenden, um ISO- oder IMG-Dateien anzuhängen, die sich auf Ihrem System oder an einem Netzwerkstandort befinden, auf den der BMC über CIFS, NFS, HTTPS oder SFTP zugreifen kann. Das angehängte Laufwerk wird als an den Server angeschlossenes USB-Plattenlaufwerk angezeigt.
Firmwareaktualisierung		• Zeigt Firmwareversionen an. • Aktualisieren Sie die XClarity Controller-Firmware und Server-Firmware.
Serverkonfiguration	Adapter	Zeigt Informationen der installierten Netzwerkadapter sowie die Einstellungen an, die über den XClarity Controller konfiguriert werden können.
	Boot-Optionen	• Wählen Sie die Booteinheit für einen einmaligen Bootvorgang während des nächsten Serverneustarts. • Ändern Sie den Bootmodus und die Einstellungen zur Bootreihenfolge.
	Stromversorgungsrichtlinie	• Konfigurieren Sie die redundante Stromversorgung während eines Netzteilausfalls. • Konfigurieren Sie die Richtlinie zur Energieverbrauchsbegrenzung. • Konfigurieren Sie die Richtlinie zum Wiederherstellen der Stromversorgung. **Anmerkung:** Weitere Details zum Stromversorgungsstatus der Lösung finden Sie in der SMM2-Webschnittstelle.
	Servereigenschaften	• Überwachen Sie unterschiedliche Eigenschaften, Statusbedingungen und Einstellungen Ihres Servers. • Verwalten Sie Startzeitlimits für den Server, um Serverblockierungen zu erkennen und zu beheben. • Erstellen Sie die Trespass-Nachricht. Eine Trespass-Nachricht ist eine Meldung, die Sie erstellen können, um Benutzern anzuzeigen, wann sie sich bei XClarity Controller anmelden.
BMC-Konfiguration	Sicherung und Wiederherstellung	Setzen Sie die Konfiguration des XClarity Controller auf die Werkseinstellungen zurück, sichern Sie die aktuelle Konfiguration oder stellen Sie die Konfiguration aus einer Datei wieder her.
	Lizenz	Verwalten Sie Aktivierungsschlüssel für optionale XClarity Controller-Merkmale.
	Netzwerk	Konfigurieren Sie Netzwerkeigenschaften, Statusangaben und Einstellungen für den XClarity Controller.

Tabelle 1. XClarity Controller-Merkmale (Forts.)

Tabulatortaste	Auswahl	Beschreibung
	Sicherheit	Konfigurieren Sie Sicherheitseigenschaften, Statusangaben und Einstellungen für den XClarity Controller.
	Benutzer/LDAP	• Konfigurieren Sie XClarity Controller-Anmeldeprofile und globale Anmeldeeinstellungen. • Zeigen Sie Benutzerkonten an, die derzeit am XClarity Controller angemeldet sind. • Auf der Registerkarte „LDAP“ wird die Benutzerauthentifizierung für die Verwendung mit einem oder mehreren LDAP-Servern konfiguriert. Sie können auch die LDAP-Sicherheit aktivieren oder deaktivieren und deren Zertifikate verwalten.

Kapitel 3. XClarity Controller konfigurieren

Verwenden Sie die Informationen in diesem Kapitel, um mehr über die für XClarity Controller-Konfigurationen verfügbaren Optionen zu erfahren.

Bei der Konfiguration von XClarity Controller sind die folgenden wesentlichen Optionen verfügbar:

- Sicherung und Wiederherstellung
- Lizenz
- Netzwerk
- Sicherheit
- Benutzer/LDAP

Benutzeraccounts/LDAP konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie Benutzeraccounts verwalten.

Klicken Sie unter **BMC-Konfiguration** auf **Benutzer/LDAP**, um Benutzeraccounts zu erstellen, zu ändern oder anzuzeigen und um LDAP-Einstellungen zu konfigurieren.

Auf der Registerkarte **Lokaler Benutzer** werden die Benutzeraccounts angezeigt, die im XClarity Controller konfiguriert und aktuell am XClarity Controller angemeldet sind.

Auf der Registerkarte **LDAP** wird die LDAP-Konfiguration für den Zugriff auf die Benutzeraccounts angezeigt, die auf einem LDAP-Server gespeichert werden.

Benutzerauthentifizierungsverfahren

In diesem Abschnitt werden die Verfahren erläutert, die der XClarity Controller verwenden kann, um Anmeldeversuche zu authentifizieren.

Klicken Sie auf **Anmeldungen erlauben von**, um anzugeben, wie Benutzeranmeldeversuche authentifiziert werden. Wählen Sie eines der folgenden Authentifizierungsverfahren aus:

- **Nur lokal:** Benutzer werden durch eine Suche nach dem lokalen Benutzeraccount authentifiziert, der im XClarity Controller konfiguriert ist. Wenn keine Übereinstimmung für die Benutzer-ID und das Kennwort vorhanden ist, wird der Zugriff verweigert.
- **Nur LDAP:** Der XClarity Controller versucht, den Benutzer mit dem Anmeldeinformationen zu authentifizieren, die auf einem LDAP-Server gespeichert sind. Bei diesem Authentifizierungsverfahren werden die lokalen Benutzeraccounts im XClarity Controller **nicht** durchsucht.
- **Erst lokal, dann LDAP:** Zuerst wird eine lokale Authentifizierung versucht. Falls diese lokale Authentifizierung fehlschlägt, wird eine LDAP-Authentifizierung versucht.
- **Erst LDAP, dann lokaler Benutzer:** Zuerst wird die LDAP-Authentifizierung versucht. Falls die LDAP-Authentifizierung fehlschlägt, wird eine lokale Authentifizierung versucht.

Anmerkungen:

- Nur lokal verwaltete Konten werden für die IPMI- und SNMP-Schnittstellen freigegeben. Diese Schnittstellen unterstützen keine LDAP-Authentifizierung.
- IPMI- und SNMP-Benutzer können sich mithilfe der lokal verwalteten Accounts anmelden, wenn für das Feld **Anmeldungen erlauben von** die Option **Nur LDAP** ausgewählt ist.

Neuen Benutzeraccount erstellen

Mithilfe der Informationen in diesem Abschnitt können Sie einen neuen lokalen Benutzer erstellen.

Benutzer erstellen

Um einen neuen Benutzeraccount zu erstellen, klicken Sie auf **Erstellen**.

Füllen Sie die folgenden Felder aus: **Benutzername**, **Kennwort**, **Kennwort bestätigen** und **Berechtigungsstufe**. Weitere Details zur Berechtigungsstufe finden Sie im folgenden Abschnitt.

Benutzerberechtigungsstufe

Die folgenden Benutzerberechtigungsstufen sind verfügbar:

Supervisor
Für die Benutzerberechtigungsstufe „Supervisor“ gelten keine Einschränkungen.

Nur Lesen
Die Benutzerberechtigungsstufe „Lesezugriff“ verfügt nur über Lesezugriff und kann keine Aktionen wie z. B. Dateiübertragungen, Einschalt- und Neustartaktionen sowie Fernpräsenz-Funktionen ausführen.

Angepasst
Die Benutzerberechtigungsstufe „Angepasst“ ermöglicht ein besser angepasstes Profil für Benutzerberechtigungen mit Einstellungen für die Aktionen, die ein Benutzer ausführen darf.

Wählen Sie mindestens eine der folgenden Benutzerberechtigungsstufen für „Angepasst“ aus:

Adapterkonfiguration – Netzwerkbetrieb und Sicherheit
Benutzer können Konfigurationsparameter auf den Seiten „Sicherheit“, „Netzwerk“ und „Serieller Anschluss“ ändern.

Benutzeraccountverwaltung
Benutzer können andere Benutzer hinzufügen, ändern oder löschen und die globalen Anmeldeeinstellungen ändern.

Zugriff auf ferne Konsole
Benutzer können auf die ferne Konsole zugreifen.

Zugriff auf ferne Konsole und ferne Datenträger
Benutzer können auf die ferne Konsole und auf die Funktion für virtuelle Datenträger zugreifen.

Einschalten/Starten eines fernen Servers
Benutzer können Einschalt- und Neustartfunktionen für den Server ausführen.

Adapterkonfiguration – Allgemein
Benutzer können Konfigurationsparameter auf den Seiten „Servereigenschaften“ und „Ereignisse“ ändern.

Berechtigung zum Löschen von Ereignisprotokollen
Ein Benutzer kann die Ereignisprotokolle löschen. Jeder kann die Ereignisprotokolle einsehen; zum Löschen der Protokolle ist jedoch diese Berechtigungsstufe erforderlich.

Adapterkonfiguration – Erweitert (Firmwareaktualisierung, BMC erneut starten, Konfiguration wiederherstellen)
Für Benutzer gelten keine Einschränkungen beim Konfigurieren des XClarity Controller. Außerdem soll der Benutzer über Verwaltungszugriff auf den XClarity Controller verfügen. Der Verwaltungszugriff umfasst die folgenden erweiterten Funktionen: Firmwareaktualisierungen, PXE-Netzwerkboot, Wiederherstellen von werkseitigen XClarity Controller-Voreinstellungen, Ändern und

Wiederherstellen von XClarity Controller-Einstellungen aus einer Konfigurationsdatei sowie Neustart und Zurücksetzen von XClarity Controller.

Wenn ein Benutzer die Berechtigungsstufe einer XClarity Controller-Anmelde-ID festlegt, wird die daraus resultierende IPMI-Berechtigungsstufe der zugehörigen IPMI-Benutzer-ID entsprechend den folgenden Prioritäten festgelegt:

- Wenn ein Benutzer die Berechtigungsstufe für die XClarity Controller-Anmelde-ID auf **Supervisor** setzt, wird die IPMI-Berechtigungsstufe auf „Administrator“ gesetzt.
- Wenn ein Benutzer die Berechtigungsstufe für die XClarity Controller-Anmelde-ID auf **Lesezugriff** setzt, wird die IPMI-Berechtigungsstufe auf „Benutzer“ gesetzt.
- Wenn ein Benutzer die Berechtigungsstufe für die XClarity Controller-Anmelde-ID auf einen der folgenden Zugriffstypen setzt, wird die IPMI-Berechtigungsstufe auf „Administrator“ gesetzt:
  - Zugriff auf Benutzeraccountverwaltung
  - Zugriff auf ferne Konsole
  - Zugriff auf ferne Konsole und ferne Datenträger
  - Adapterkonfiguration – Netzwerkbetrieb und Sicherheit
  - Adapterkonfiguration – Erweitert
- Wenn ein Benutzer die Berechtigungsstufe für die XClarity Controller-Anmelde-ID auf **Zugriff auf Einschalten/Starten eines fernen Servers** oder auf **Berechtigung zum Löschen von Ereignisprotokollen** setzt, wird die IPMI-Berechtigungsstufe auf „Bediener“ gesetzt.
- Wenn ein Benutzer die Berechtigungsstufe für die XClarity Controller-Anmelde-ID auf **Adapterkonfiguration – Allgemein** setzt, wird die IPMI-Berechtigungsstufe auf „Benutzer“ gesetzt.

SNMPv3-Einstellungen

Um den SNMPv3-Zugriff für einen Benutzer zu aktivieren, aktivieren Sie das Kontrollkästchen neben **SNMPv3-Einstellungen**. Die folgenden Benutzerzugriffsoptionen werden erläutert:

Zugriffstyp
Es werden nur **GET**-Operationen unterstützt. Der XClarity Controller unterstützt keine SNMPv3-**SET**-Operationen. SNMP3 kann nur Abfrageoperationen ausführen.

Adresse für Traps
Geben Sie das Trapziel für den Benutzer an. Das kann eine IP-Adresse oder ein Hostname sein. Mithilfe von Traps benachrichtigt der SNMP-Agent die Verwaltungsstation über Ereignisse (z. B. wenn die Temperatur eines Prozessors den Grenzwert überschreitet).

Authentifizierungsprotokoll
Es wird nur **HMAC-SHA** als Authentifizierungsprotokoll unterstützt. Dieser Algorithmus wird vom SNMPv3-Sicherheitsmodell für die Authentifizierung verwendet.

Datenschutzprotokoll
Die Datenübertragung zwischen dem SNMP-Client und dem Agenten kann mithilfe von Verschlüsselung geschützt werden. Folgende Methoden werden unterstützt: **CBC-DES** und **AES**.

Anmerkungen: Selbst wenn ein SNMPv3-Benutzer sich wiederholende Zeichenfolgen eines Kennworts verwendet, wird dem XClarity Controller dennoch Zugriff gewährt. Nachfolgend werden zwei Referenzbeispiele aufgeführt.

- Wenn das Kennwort auf „**11111111**“ (achtstellige Zahl, die acht Einsen enthält) gesetzt wird, kann der Benutzer dennoch auf den XClarity Controller zugreifen, wenn versehentlich mehr als acht Einsen als Kennwort eingegeben werden. Bei Eingabe von „**1111111111**“ (zehnstellige Zahl, die zehn Einsen enthält)

wird der Zugriff beispielsweise dennoch gewährt. Die sich wiederholende Zeichenfolge wird so behandelt, als ob sie den gleichen Schlüssel hat.

- Wenn das Kennwort auf „**bertbert**“ gesetzt wird, kann der Benutzer auch auf den XClarity Controller zugreifen, wenn das Kennwort versehentlich als „**bertbertbert**“ eingegeben wird. Beide Kennwörter werden so behandelt, als ob sie den gleichen Schlüssel haben.

Weitere Informationen hierzu finden Sie auf Seite 72 in dem Dokument zum Internetstandard RFC 3414 (https://tools.ietf.org/html/rfc3414).

SSH-Schlüssel

Der XClarity Controller unterstützt die SSH-Public-Key-Authentifizierung (RSA-Schlüsseltyp). Um dem lokalen Benutzeraccount einen SSH-Schlüssel hinzuzufügen, aktivieren Sie das Kontrollkästchen neben **SSH-Schlüssel**. Es stehen die folgenden zwei Optionen zur Verfügung:

Schlüsseldatei auswählen
Wählen Sie die SSH-Schlüsseldatei aus, die vom Server in den XClarity Controller importiert werden soll.

Schlüssel in ein Textfeld eingeben
Fügen Sie die Daten von Ihrem SSH-Schlüssel in das Textfeld ein.

Anmerkungen:

- Einige der Tools von Lenovo erstellen möglicherweise einen temporären Benutzeraccount für den Zugriff auf XClarity Controller, wenn das Tool auf dem Serverbetriebssystem ausgeführt wird. Dieser temporäre Account ist nicht sichtbar und verwendet keine der 12 lokalen Benutzeraccountpositionen. Der Account wird mit einem willkürlichen Benutzernamen (z. B. „20luN4SB“) und Kennwort erstellt. Der Account kann nur verwendet werden, um auf den XClarity Controller auf der internen Ethernet-over-USB-Schnittstelle zuzugreifen sowie nur für die CIM-XML- und SFTP-Schnittstellen. Das Erstellen und Entfernen dieses temporären Accounts wird im Prüfprotokoll erfasst, ebenso wie alle Aktionen, die von dem Tool mit diesen Berechtigungen ausgeführt werden.
- Bei der SNMPv3-Engine-ID verwendet der XClarity Controller eine HEX-Zeichenfolge, um die ID anzugeben. Diese HEX-Zeichenfolge wird aus dem XClarity Controller Standard-Hostnamen konvertiert. Siehe folgendes Beispiel:

  Der Hostname „XCC-7X06-S4AHJ300“ wird zunächst in das ASCII-Format konvertiert: 88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

  Die HEX-Zeichenfolge wird unter Verwendung des ASCII-Formats erstellt (Leerzeichen werden ignoriert): 58 43 43 2d 37 58 30 36 2d 53 34 41 48 4a 33 30 30

Benutzeraccount löschen

Mithilfe der Informationen in diesem Abschnitt können Sie einen lokalen Benutzeraccount löschen.

Um einen lokalen Benutzeraccount zu löschen, klicken Sie auf das Papierkorbsymbol in der Zeile des Accounts, den Sie entfernen möchten. Wenn Sie dazu berechtigt sind, können Sie Ihren eigenen Account oder den Account anderer Benutzer entfernen, auch wenn sie derzeit angemeldet sind, es sei denn, dies ist der einzige verbleibende Account mit Berechtigungen zur Verwaltung von Benutzeraccounts. Sitzungen, die beim Löschen von Benutzeraccounts bereits aktiv sind, werden nicht automatisch beendet.

Gehashte Kennwörter für die Authentifizierung verwenden

In diesem Thema wird die Nutzung von gehashten Kennwörtern zur Authentifizierung erläutert.

Neben der Nutzung von Kennwörtern und LDAP/AD-Benutzeraccounts unterstützt der XClarity Controller auch gehashte Drittanbieterkennwörter zur Authentifizierung. Das spezielle Kennwort verwendet ein

einseitiges Hashformat (SHA256) und wird sowohl von der XClarity Controller-Webschnittstelle als auch von der OneCLI- und der Befehlszeilenschnittstelle unterstützt. Beachten Sie jedoch, dass die Authentifizierungen der XCC SNMP-, IPMI- und CIM-Schnittstellen keine gehashten Drittanbieterkennwörter unterstützten. Nur das OneCLI-Tool und die XCC-Befehlszeilenschnittstelle können einen neuen Account mit einem gehashten Kennwort erstellen oder ein gehashtes Kennwort aktualisieren. Der XClarity Controller ermöglicht dem OneCLI-Tool und der XClarity Controller-Befehlszeilenschnittstelle zudem das Abrufen eines gehashten Kennworts, wenn die Funktion zum Lesen gehashter Kennwörter aktiviert ist.

Gehashtes Kennwort über das XClarity Controller-Web festlegen

Klicken Sie unter **BMC-Konfiguration** auf **Sicherheit**. Blättern Sie zum Abschnitt **Security Password Manager**, um die Funktion für Drittanbieterkennwörter zu aktivieren oder zu deaktivieren. Bei aktivierter Funktion wird ein gehashtes Drittanbieterkennwort für die Anmeldeauthentifizierung verwendet. Das Abrufen eines gehashten Drittanbieterkennworts über den XClarity Controller kann auch aktiviert oder deaktiviert werden.

Anmerkung: Standardmäßig sind die Funktionen **Drittanbieterkennwort** und **Drittanbieterkennwort abrufen** deaktiviert.

Um zu überprüfen, ob das Benutzerkennwort **systemeigen** oder ein **Drittanbieterkennwort** ist, können Sie durch Klicken auf **Benutzer/LDAP** unter **BMC-Konfiguration** Details anzeigen. Die Informationen werden in der Spalte **Erweitertes Attribut** angezeigt.

Anmerkungen:

- Benutzer können ein Kennwort nicht ändern, wenn es ein Drittanbieterkennwort ist. Die Felder **Kennwort** und **Kennwort bestätigen** sind abgeblendet.
- Wenn ein Drittanbieterkennwort abgelaufen ist, wird während der Benutzeranmeldung eine Warnung angezeigt.

Ein gehashtes Kennwort über die OneCLI-Funktion festlegen

- Funktion aktivieren

  ```
  $ sudo OneCli config set IMM.ThirdPartyPassword Enabled
  ```

- Gehashtes Kennwort erstellen (kein Salt). Nachfolgend wird ein Beispiel für die Anmeldung beim XClarity Controller mit dem Kennwort **password123** angezeigt.

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

- Benutzer mit gehashtem Kennwort erstellen (mit Salt). Nachfolgend wird ein Beispiel für die Anmeldung beim XClarity Controller mit dem Kennwort **password123** angezeigt. Salt=abc.

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  $ sudo OneCli config set IMM.Loginid.3 Admin

  $ sudo OneCli config set IMM.SHA256Password.3 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
  ```

- Gehashtes Kennwort und salt abrufen.

  ```
  $ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled

  $ sudo OneCli config show IMM.SHA256Password.3

  $ sudo OneCli config show IMM.SHA256PasswordSalt.3
  ```

- Gehashtes Kennwort und salt löschen.

  ```
  $ sudo OneCli config set IMM.SHA256Password.3 ""

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
  ```

- Gehashtes Kennwort für einen bestehenden Account festlegen.

  ```
  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.Password.2 Passw0rd123abc

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

  Anmerkung: Beim Festlegen des gehashten Kennworts wird das Kennwort sofort wirksam. Das ursprüngliche Standardkennwort ist nicht mehr gültig. In diesem Beispiel kann das ursprüngliche Standardkennwort **Passw0rd123abc** nicht mehr verwendet werden, bis das gehashte Kennwort gelöscht wird.

Ein gehashtes Kennwort über die Befehlszeilenschnittstellen-Funktion festlegen

- Funktion aktivieren

  ```
  > hashpw -sw enabled
  ```

- Gehashtes Kennwort erstellen (kein Salt). Nachfolgend wird ein Beispiel für die Anmeldung beim XClarity Controller mit dem Kennwort **password123** angezeigt.

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  > users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a
  super
  ```

- Benutzer mit gehashtem Kennwort erstellen (mit Salt). Nachfolgend wird ein Beispiel für die Anmeldung beim XClarity Controller mit dem Kennwort **password123** angezeigt. Salt=abc.

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  > users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
  -ssalt 'abc' -a super
  ```

- Gehashtes Kennwort und salt abrufen.

  ```
  > hashpw -re enabled

  > users -3 -ghp -gsalt
  ```

- Gehashtes Kennwort und salt löschen.

  ```
  > users -3 -shp "" -ssalt ""
  ```

- Gehashtes Kennwort für einen bestehenden Account festlegen.

```
> users -2 -n admin -p Passw0rd123abc -shp
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

Anmerkung: Beim Festlegen des gehashten Kennworts wird das Kennwort sofort wirksam. Das ursprüngliche Standardkennwort ist nicht mehr gültig. In diesem Beispiel kann das ursprüngliche Standardkennwort **Passw0rd123abc** nicht mehr verwendet werden, bis das gehashte Kennwort gelöscht wird.

Denken Sie nach Festlegung des gehashten Kennworts daran, es nicht für die Anmeldung am XClarity Controller zu verwenden. Bei der Anmeldung müssen Sie das Klartextkennwort verwenden. Im folgenden Beispiel lautet das Klartextkennwort „password123“.

```
$ pwhash = ‘echo –n password123 | openssl dgst –sha256 | awk '{print $NF}''

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

Globale Anmeldeeinstellungen konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie die Einstellungen der Anmelde- und Kennwortrichtlinien konfigurieren, die für alle Benutzer gelten.

Sitzungszeitlimit bei Webinaktivität

Dieser Abschnitt enthält Informationen zur Einstellung der Option „Sitzungszeitlimit bei Webinaktivität“.

Geben Sie im Feld **Sitzungszeitlimit bei Webinaktivität** an, wie lange (in Minuten) XClarity Controller warten soll, bevor er die Verbindung einer inaktiven Websitzung trennt. Die maximale Wartezeit beträgt 1.440 Minuten. Wenn sie auf 0 gesetzt wird, läuft die Websitzung niemals ab.

Die XClarity Controller-Firmware unterstützt bis zu sechs gleichzeitige Websitzungen. Um Sitzungen für andere Benutzer freizugeben, sollten Sie sich von einer Websitzung abmelden, wenn Sie Ihre Arbeit beendet haben, anstatt sich darauf zu verlassen, dass die Sitzung nach dem Inaktivitätszeitlimit automatisch geschlossen wird.

Anmerkung: Wenn Sie das Browserfenster geöffnet lassen, während Sie eine XClarity Controller-Webseite anzeigen, die automatisch aktualisiert wird, wird Ihre Websitzung nicht automatisch aufgrund von Inaktivität geschlossen.

Einstellungen für die Accountsicherheitsrichtlinie

Mithilfe dieser Informationen können Sie sich mit der Accountsicherheitsrichtlinie für Ihren Server vertraut machen und diese festlegen.

Anmerkungen: In einem Flex System werden die Einstellungen für die Accountsicherheitsrichtlinie vom Flex System Chassis Management Module (CMM) verwaltet und können über den XCC nicht geändert werden. Wenn das CMM zur Verwendung der Accountsicherheitsrichtlinie konfiguriert ist, müssen Sie Folgendes beachten:

- Im Gegensatz zum XCC verfügt das CMM nicht über die Einstellung **Warndauer vor Kennwortablauf (in Tagen)**. Wenn die **Kennwortablaufdauer** im CMM mit mehr als 5 Tagen konfiguriert ist, legt der XCC die Warndauer vor Kennwortablauf auf 5 Tage fest. Wenn die Einstellung auf weniger als 5 Tage gesetzt wurde, ist die Warndauer vor Kennwortablauf mit dem unter **Kennwortablaufdauer** eingegebenen Wert identisch.
- Für die Einstellung **Maximale Anzahl fehlgeschlagener Anmeldeversuche** ist im CMM der Bereich 0 bis 100 Mal festgegelegt. Der im XCC definierte Bereich lautet jedoch 0 bis 10 Mal. Bei der Auswahl eines

höheren Werts als 10 Mal im CMM setzt der XCC die maximale Anzahl fehlgeschlagener Anmeldeversuche dennoch weiterhin auf 10 Mal.

- Für die Einstellung **Mindestintervall für Kennwortänderungen (in Stunden)** ist im CMM der Bereich 0 bis 1.440 Stunden festgelegt. Der im XCC definierte Bereich lautet jedoch 0 bis 240 Stunden. Wenn der Benutzer im CMM einen höheren Wert als 240 Stunden auswählt, setzt der XCC das Mindestintervall für Kennwortänderungen dennoch auf 240 Stunden.

Im Folgenden werden die Felder für die Sicherheitseinstellungen beschrieben.

Benutzer zwingen, das Kennwort beim ersten Zugriff zu ändern
Nachdem ein neuer Benutzer mit einem Standardkennwort konfiguriert wurde, erzwingt die Auswahl dieses Kontrollkästchens, dass der betreffende Benutzer sein Kennwort bei der ersten Anmeldung ändern muss. Der Standardwert für dieses Feld ist ein aktiviertes Kontrollkästchen.

Standardaccountkennwort muss bei der nächsten Anmeldung geändert werden
Diese Herstelleroption wird bereitgestellt, um das Zurücksetzen des Standardprofils „USERID“ nach der ersten erfolgreichen Anmeldung zu ermöglichen. Wenn dieses Kontrollkästchen aktiviert ist, muss das Standardkennwort geändert werden, bevor das Konto verwendet werden kann. Für das neue Kennwort gelten alle aktiven Kennwortdurchsetzungsregeln. Der Standardwert für dieses Feld ist ein aktiviertes Kontrollkästchen.

Komplexes Kennwort erforderlich
Das Kontrollkästchen ist standardmäßig aktiviert und das komplexe Kennwort muss den folgenden Regeln entsprechen:

- Darf nur die folgenden Zeichen enthalten (keine Leerraumzeichen zulässig): A-Z, a-z, 0-9, ~`!@#$% ^&*()-+={}[]|:;"'<>,?/._
- Muss mindestens einen Buchstaben enthalten
- Muss mindestens eine Zahl enthalten
- Muss mindestens zwei der folgenden Kombinationen aufweisen:
  - Mindestens ein Großbuchstabe
  - Mindestens ein Kleinbuchstabe
  - Mindestens ein Sonderzeichen
- Keine anderen Zeichen (insbesondere Leerzeichen oder Leerraumzeichen) sind zulässig
- Kennwörter dürfen nicht mehr als zwei aufeinanderfolgende Instanzen desselben Zeichens enthalten (z. B. „aaa“)
- Das Kennwort darf nicht identisch mit dem Benutzernamen, eine mehrfache Wiederholung des Benutzernamens oder der Benutzername in umgekehrter Buchstabenreihenfolge sein
- Kennwörter müssen mindestens 8 und dürfen maximal 32 Zeichen lang sein

Wenn das Kontrollkästchen nicht aktiviert ist, kann die Zahl für die Mindestlänge des Kennworts auf 0 bis 32 Zeichen festgelegt werden. Das Accountkennwort kann leer sein, wenn die Mindestlänge des Kennworts auf 0 festgelegt ist.

Kennwortablaufdauer (in Tagen)
Dieses Feld gibt die maximale zulässige Gültigkeitsdauer des Kennworts an, bevor das Kennwort geändert werden muss. Es werden Werte von 0 bis 30 Tagen unterstützt. Der Standardwert für dieses Feld lautet 14 Tage.

Warndauer vor Kennwortablauf (in Tagen)

Dieses Feld gibt die Anzahl der Tage an, die ein Benutzer gewarnt wird, bevor sein Kennwort abläuft. Wenn dieses Feld auf 0 festgelegt ist, werden keine Warnungen ausgegeben. Es werden Werte von 0 bis 30 Tagen unterstützt. Der Standardwert für dieses Feld lautet 14 Tage.

Mindestlänge des Kennworts
Dieses Feld gibt die Mindestlänge des Kennworts an. Für dieses Feld werden 8 bis 32 Zeichen unterstützt. Der Standardwert für dieses Feld ist 10.

Mindestwiederverwendungszyklus des Kennworts
Dieses Feld gibt die Anzahl an vorherigen Kennwörtern an, die nicht wiederverwendet werden dürfen. Es können bis zu zehn vorherige Kennwörter verglichen werden. Wählen Sie 0 aus, um die Wiederverwendung aller vorherigen Kennwörter zuzulassen. Es werden Werte von 0 bis 10 unterstützt. Der Standardwert für dieses Feld lautet 5.

Mindestintervall für Kennwortänderung (in Stunden)
Dieses Feld gibt an, wie lange ein Benutzer von einer Kennwortänderung bis zur nächsten warten muss. Es werden Werte von 0 bis 240 Stunden unterstützt. Der Standardwert für dieses Feld lautet 1 Stunde.

Maximale Anzahl fehlgeschlagener Anmeldeversuche (Male)
Dieses Feld gibt die zulässige Anzahl an fehlgeschlagenen Anmeldeversuchen an, bevor der Benutzer für einen bestimmten Zeitraum gesperrt wird. Es werden Werte von 0 bis 10 unterstützt. Der Standardwert für dieses Feld lautet fünf Anmeldefehler.

Sperrzeitraum nach maximaler Anzahl von fehlgeschlagenen Anmeldeversuchen (in Minuten)
Dieses Feld gibt an, wie viele Minuten das XClarity Controller-Subsystem Fernanmeldeversuche nach Erreichen der maximalen Anzahl fehlgeschlagener Anmeldeversuche deaktiviert. Es werden Werte von 0 bis 2.880 Minuten unterstützt. Der Standardwert für dieses Feld lautet 60 Minuten.

LDAP konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie die LDAP-Einstellungen von XClarity Controller anzeigen oder ändern.

Die LDAP-Unterstützung enthält:

- Unterstützung für das LDAP-Protokoll, Version 3 (RFC-2251)
- Unterstützung für die standardmäßigen LDAP-Client-APIs (RFC-1823)
- Unterstützung für die standardmäßige LDAP-Suchfiltersyntax (RFC-2254)
- Unterstützung für Lightweight Directory Access Protocol (v3), Erweiterung für Transport Layer Security (RFC-2830)

Die LDAP-Implementierung unterstützt die folgenden LDAP-Server:

- Microsoft Active Directory (Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Microsoft Active Directory Application Mode (Windows 2003 Server)
- Microsoft Lightweight Directory Service (Windows 2008, Windows 2012)
- Novell eDirectory Server Version 8.7, 8.8 und 9.4
- OpenLDAP Server 2.1, 2.2, 2.3 und 2.4

Klicken Sie auf die Registerkarte **LDAP**, um die LDAP-Einstellungen für den XClarity Controller anzuzeigen oder zu ändern.

Der XClarity Controller kann den Benutzerzugriff über einen zentralen LDAP-Server anstelle von oder zusätzlich zu den lokalen Benutzeraccounts, die im XClarity Controller selbst gespeichert sind, remote authentifizieren. Für jeden Benutzeraccount können mit der Zeichenfolge „IBMRBSPermissions“ Berechtigungen festgelegt werden. Sie können den LDAP-Server auch dazu verwenden, Benutzern Gruppen zuzuordnen und zusätzlich zu der normalen Benutzerauthentifizierung (Kennwortprüfung) eine Gruppenauthentifizierung durchzuführen. Ein XClarity Controller kann z. B. einer oder mehreren Gruppen zugewiesen werden. In diesem Fall besteht ein Benutzer die Gruppenauthentifizierung nur dann, wenn er zu mindestens einer der Gruppen gehört, die dem XClarity Controller zugeordnet sind.

Gehen Sie zum Konfigurieren eines LDAP-Servers wie folgt vor:

1. Auf der Seite **LDAP-Serverinformationen** stehen in der Elementliste die folgenden Optionen zur Verfügung:

   - **Nur LDAP-Server für Authentifizierung verwenden (mit lokaler Erteilung von Berechtigungen)**: Wenn Sie diese Option wählen, wird XClarity Controller angewiesen, die Anmeldeinformationen nur für die Authentifizierung zum LDAP-Server zu verwenden und Informationen zur Gruppenzugehörigkeit abzurufen. Die Gruppennamen und Berechtigungen können im Abschnitt „Active Directory-Einstellungen“ konfiguriert werden.
   - **LDAP-Server für Authentifizierung und Erteilung von Berechtigungen verwenden**: Wenn Sie diese Option wählen, wird XClarity Controller angewiesen, die Anmeldeinformationen für die Authentifizierung zum LDAP-Server und für die Identifizierung einer Benutzerberechtigung zu verwenden.

   Anmerkung: Die für die Authentifizierung zu verwendenden LDAP-Server können entweder manuell konfiguriert oder mithilfe von DNS-SRV-Datensätzen dynamisch ermittelt werden.

   - **Vorkonfigurierte Server verwenden**: Sie können bis zu vier LDAP-Server konfigurieren, indem Sie die IP-Adresse oder den Hostnamen jedes Servers angeben (vorausgesetzt, DNS ist aktiviert). Die Portnummer für die einzelnen Server ist optional. Wenn in diesem Feld keine Angaben gemacht werden, wird der Standardwert 389 für nicht sichere LDAP-Verbindungen verwendet. Für sichere Verbindungen lautet der Standardportwert 636. Mindestens ein LDAP-Server muss konfiguriert werden.
   - **DNS zum Finden von Servern verwenden**: Sie können angeben, ob die LDAP-Server dynamisch ermittelt werden sollen. Um die LDAP-Server zu ermitteln, werden die in RFC2782 (A DNS RR for specifying the location of services) beschriebenen Verfahren verwendet. Dies wird als DNS SRV bezeichnet. Hierbei ist es erforderlich, einen vollständig qualifizierten Domänennamen (FQDN) zur Verwendung in der DNS-SRV-Anforderung anzugeben.
     - **AD-Gesamtstruktur**: In einer Umgebung mit universellen Gruppen in mehreren Domänen muss der Gesamtstrukturname (Gruppe von Domänen) so konfiguriert werden, dass die erforderlichen globalen Kataloge (GC) ermittelt werden. In einer Umgebung, in der eine domänenübergreifende Gruppenzugehörigkeit nicht zulässig ist, muss dieses Feld nicht ausgefüllt werden.
     - **AD-Domäne**: Sie müssen einen vollständig qualifizierten Domänennamen (FQDN) zur Verwendung in der DNS-SRV-Anforderung angeben.

   Wenn Sie eine sichere LDAP-Verbindung aktivieren möchten, klicken Sie auf das Kontrollkästchen **Sichere LDAP-Verbindung aktivieren**. Beachten Sie, dass zur Unterstützung von sicherem LDAP ein gültiges SSL-Zertifikat vorhanden sein und mindestens ein vertrauenswürdiges SSL-Clientzertifikat in den XClarity Controller importiert werden muss. Ihr LDAP-Server muss Transport Layer Security (TLS) Version 1.2 unterstützen, um mit dem sicheren LDAP-Client von XClarity Controller kompatibel zu sein. Weitere Informationen zur Handhabung von Zertifikaten finden Sie im Abschnitt „Handhabung von SSL-Zertifikaten“ auf Seite 39.
2. Machen Sie Angaben unter **Zusätzliche Parameter**. Unten stehend finden Sie Erläuterungen zu den Parametern.

Bindungsmethode

Bevor eine Suchanfrage oder Abfrage an den LDAP-Server gesendet werden kann, muss eine Bindeanforderung gesendet werden. Mit diesem Feld wird gesteuert, wie diese einleitende Bindung zum LDAP-Server ausgeführt wird. Die folgenden Bindungsmethoden sind verfügbar:

- **Keine Anmeldeinformationen erforderlich**

  Mit dieser Methode wird eine Bindung ohne einen definierten Namen (DN) oder ein Kennwort hergestellt. Diese Methode sollte jedoch nicht verwendet werden, da die meisten Server so konfiguriert sind, dass sie Suchanforderungen für bestimmte Benutzersätze nicht zulassen.

- **Mit konfiguriertem Berechtigungsnachweis**

  Mit dieser Methode wird eine Bindung mit dem konfigurierten definierten Namen und einem Kennwort hergestellt.

- **Anmeldeinformationen verwenden**

  Mit dieser Methode wird eine Bindung mit dem Berechtigungsnachweis hergestellt, der beim Anmeldeprozess angegeben wird. Die Benutzer-ID kann als definierter Name, als Teil eines definierten Namens, als vollständig qualifizierter Domänenname oder über eine Benutzer-ID angegeben werden, die mit dem auf dem XClarity Controller konfigurierten UID-Suchattribut übereinstimmt. Wenn die angegebenen Anmeldeinformationen einem Teil eines DN ähneln (z. B. cn=joe), wird dieser DN-Teil dem konfigurierten definierten Namen des Stammelements vorangestellt, um einen DN zu erstellen, der mit dem Datensatz des Benutzers übereinstimmt. Falls dieser Bindeversuch fehlschlägt, wird ein letzter Bindeversuch unternommen, indem vor den Anmeldeinformationen ein „cn=“ eingefügt und die resultierende Zeichenfolge dem definierten Namen des konfigurierten Stammelements vorangestellt wird.

Wenn der erste Bindeversuch erfolgreich durchgeführt wurde, wird auf dem LDAP-Server nach einem Eintrag zu dem Benutzer gesucht, der sich gerade anmelden möchte Andernfalls wird ein zweiter Bindeversuch unternommen, diesmal mit dem aus dem LDAP-Datensatz des Benutzers abgerufenen DN sowie dem Kennwort, das bei der Anmeldung eingegeben wurde. Wenn der zweite Bindeversuch fehlschlägt, wird dem Benutzer der Zugriff verweigert. Der zweite Bindeversuch wird nur dann durchgeführt, wenn die Bindungsmethoden **Keine Anmeldeinformationen erforderlich** oder **Konfigurierte Anmeldeinformationen verwenden** verwendet werden.

Definierter Name des Stammelements

Der definierte Name (DN) für den Stammeintrag der Verzeichnisstruktur des LDAP-Servers (z. B. dn=mycompany,dc=com). Dieser definierte Name wird als Basisobjekt für alle Suchvorgänge verwendet.

UID-Suchattribut

Wenn als Bindungsmethode **Keine Anmeldeinformationen erforderlich** oder **Konfigurierte Anmeldeinformationen verwenden** festgelegt wurde, folgt der einleitenden Verbindung zum LDAP-Server eine Suchanforderung, die bestimmte Informationen zum Benutzer abruft, einschließlich des definierten Namens (DN), der Anmeldeberechtigungen und der Gruppenmitgliedschaft des Benutzers. Diese Suchanforderung muss den Attributnamen angeben, der für die Benutzer-IDs auf diesem Server steht. Dieser Attributname wird in diesem Feld konfiguriert. Auf Active Directory-Servern lautet der Attributname normalerweise **sAMAccountName**. Auf Novell eDirectory- und OpenLDAP-Servern lautet der Attributname **uid**. Wenn in diesem Feld keine Angaben gemacht werden, lautet der Standardwert **uid**.

Gruppenfilter

Das Feld **Gruppenfilter** wird für die Gruppenauthentifizierung verwendet. Nachdem die Anmeldeinformationen des Benutzers erfolgreich überprüft wurden, wird versucht, die Gruppenauthentifizierung durchzuführen. Wenn die Gruppenauthentifizierung fehlschlägt, wird dem Benutzer die Anmeldung verweigert. Wenn der Gruppenfilter konfiguriert ist, gibt er an, zu welchen

Gruppen der XClarity Controller gehört. Das bedeutet, dass der Benutzer zu mindestens einer der konfigurierten Gruppen gehören muss, damit die Gruppenauthentifizierung erfolgreich durchgeführt werden kann. Wenn das Feld **Gruppenfilter** leer ist, ist die Gruppenauthentifizierung automatisch erfolgreich. Wenn der Gruppenfilter konfiguriert wurde, wird versucht, mindestens eine Gruppe in der Liste zu finden, die mit einer Gruppe übereinstimmt, der der Benutzer angehört. Wenn es keine Übereinstimmung gibt, schlägt die Authentifizierung des Benutzers fehl und der Zugriff wird verweigert. Wenn mindestens eine Übereinstimmung vorhanden ist, ist die Gruppenauthentifizierung erfolgreich.
Beim Abgleich muss die Groß-/Kleinschreibung beachtet werden. Der Filter ist auf 511 Zeichen begrenzt und kann aus einem oder aus mehreren Gruppennamen bestehen. Um mehrere Gruppennamen voneinander abzugrenzen, muss das Doppelpunktzeichen (:) verwendet werden. Vorangestellte und nachgestellte Leerzeichen werden nicht beachtet. Alle anderen Leerzeichen werden als Teil des Gruppennamens behandelt.

Anmerkung: Das Platzhalterzeichen (*) wird nicht mehr als Platzhalter behandelt. Das Platzhalterkonzept wurde eingestellt, um Sicherheitsrisiken vorzubeugen. Ein Gruppenname kann als vollständiger definierter Name oder nur mithilfe des **cn**-Teils angegeben werden. Beispiel: Eine Gruppe mit dem definierten Namen „cn=adminGroup, dc=mycompany, dc=com“ kann mit dem tatsächlichen definierten Namen oder mit „adminGroup“ angegeben werden.

Verschachtelte Gruppenmitgliedschaften werden nur in Active Directory-Umgebungen unterstützt. Wenn ein Benutzer z. B. ein Mitglied von GroupA und GroupB ist und GroupA auch ein Mitglied von GroupC ist, ist der Benutzer (implizit) auch ein Mitglied von GroupC. Verschachtelte Suchprozesse werden nach dem Durchsuchen von 128 Gruppen gestoppt. Zuerst werden alle Gruppen einer Ebene durchsucht, bevor Gruppen einer tieferen Ebene durchsucht werden. Schleifen werden nicht erkannt.

Gruppensuchattribut

In einer Active Directory- oder Novell eDirectory-Umgebung gibt das Feld **Gruppensuchattribut** den Attributnamen an, der die Gruppen bezeichnet, denen ein Benutzer angehört. In einer Active Directory-Umgebung lautet der Attributname **memberOf**. In einer eDirectory-Umgebung lautet der Attributname **groupMembership**. In einer OpenLDAP-Serverumgebung werden Benutzer normalerweise Gruppen zugeordnet, deren „objectClass“ gleich „PosixGroup“ ist. In diesem Kontext gibt dieses Feld den Attributnamen an, der die Mitglieder einer bestimmten PosixGroup bezeichnet. Dieser Attributname lautet **memberUid**. Wenn in diesem Feld keine Angaben gemacht werden, wird für den Attributnamen im Filter standardmäßig **memberOf** verwendet.

Anmeldeberechtigungsattribut

Wenn ein Benutzer erfolgreich über einen LDAP-Server authentifiziert wird, müssen die Anmeldeberechtigungen für den Benutzer abgerufen werden. Um diese Anmeldeberechtigungen abzurufen, muss der an den Server gesendete Suchfilter den Attributnamen angeben, der den Anmeldeberechtigungen zugeordnet wurde. Das Feld **Anmeldeberechtigungsattribut** gibt den Attributnamen an. Wenn in diesem Feld keine Angaben gemacht werden, werden dem Benutzer standardmäßig Leseberechtigungen zugeordnet, vorausgesetzt, der Benutzer besteht die Benutzer- und die Gruppenauthentifizierung.
Der vom LDAP-Server zurückgegebene Attributwert sucht nach der Suchbegriffszeichenfolge „IBMRBSPermissions=“. Auf diese Suchbegriffszeichenfolge muss unmittelbar danach eine Bitfolge (aus bis zu 12 aufeinanderfolgenden Nullen oder Einsen) folgen. Jedes Bit steht für eine Gruppe von Funktionen. Die Bits sind entsprechend ihren Positionen nummeriert. Das Bit ganz links ist Bitposition 0 und das Bit ganz rechts ist Bitposition 11. Durch den Wert 1 an einer bestimmten Position wird die Funktion aktiviert, die mit dieser Bitposition verknüpft ist. Der Wert 0 in einer Bitposition deaktiviert die Funktion, die dieser Bitposition zugeordnet ist.
Ein gültiges Beispiel ist die Zeichenfolge „IBMRBSPermissions=010000000000“. Der Suchbegriff „IBMRBSPermissions=“ wird verwendet, damit er in einer beliebigen Position in diesem Feld platziert werden kann. So kann der LDAP-Administrator ein vorhandenes Attribut wiederverwenden

und eine Erweiterung des LDAP-Schemas verhindern. Außerdem ermöglicht es die Verwendung des Attributs für seine ursprüngliche Bestimmung. Sie können die Suchbegriffszeichenfolge in eine beliebige Position in diesem Feld einfügen. Das verwendete Attribut kann eine frei formatierte Zeichenfolge zulassen. Wenn das Attribut erfolgreich abgerufen werden kann, wird der Wert, der vom LDAP-Server zurückgegeben wird, entsprechend den Informationen in der folgenden Tabelle interpretiert.

Tabelle 2. Berechtigungsbits

Tabelle mit drei Spalten, die Erläuterungen zur Bitposition enthält.

Bitposition	**Funktion**	**Erläuterung**
0	Nie zulassen	Die Authentifizierung eines Benutzers schlägt immer fehl. Diese Funktion kann verwendet werden, um einen oder mehrere bestimmte Benutzer, die einer bestimmten Gruppe zugeordnet sind, zu blockieren.
1	Supervisorzugriff	Einem Benutzer wird die Administratorberechtigung erteilt. Der Benutzer hat Schreib-/Lesezugriff auf jede Funktion. Wenn Sie dieses Bit einstellen, müssen Sie die anderen Bits nicht einzeln einstellen.
2	Schreibgeschützter Zugriff	Ein Benutzer hat Lesezugriff und kann keine Wartungsarbeiten (beispielsweise Neustart, fern ausgeführte Aktionen oder Firmwareaktualisierungen) oder Änderungen (z. B. Funktionen zum Speichern, Löschen oder Wiederherstellen) durchführen. Bitposition 2 und alle anderen Bits schließen sich gegenseitig aus, wobei Bitposition 2 die niedrigste Vorrangstellung hat. Wenn irgendein anderes Bit gesetzt ist, wird dieses Bit ignoriert.
3	Netzwerkbetrieb und Sicherheit	Ein Benutzer kann die Konfiguration für Sicherheit, Netzprotokolle, Netzwerkschnittstelle, Portzuordnungen und serieller Anschluss ändern.
4	Benutzeraccountverwaltung	Ein Benutzer kann andere Benutzer hinzufügen, ändern oder löschen und die globalen Anmeldungseinstellungen im Fenster mit den Anmeldeprofilen ändern.
5	Zugriff auf ferne Konsole	Ein Benutzer kann auf die Remote-Server-Konsole zugreifen.
6	Zugriff auf ferne Konsole und ferne Datenträger	Ein Benutzer kann auf die Remote-Server-Konsole und die Funktionen für ferne Datenträger für den fernen Server zugreifen.
7	Zugriff auf Einschalten/ Starten eines fernen Servers	Ein Benutzer kann auf die Einschalt- und Neustartfunktionen für den fernen Server zugreifen.
8	Basisadapterkonfiguration	Ein Benutzer kann Konfigurationsparameter auf den Seiten „Systemeinstellungen“ und „Alerts“ ändern.
9	Berechtigung zum Löschen von Ereignisprotokollen	Ein Benutzer kann die Ereignisprotokolle löschen. **Anmerkung:** Alle Benutzer können die Ereignisprotokolle einsehen; um jedoch die Protokolle löschen zu können, muss der Benutzer diese Berechtigungsstufe haben.

Tabelle 2. Berechtigungsbits (Forts.)

Bitposition	Funktion	Erläuterung
10	Erweiterte Adapterkonfiguration	Für Benutzer gelten keine Einschränkungen beim Konfigurieren des XClarity Controller. Außerdem verfügt der Benutzer über einen Verwaltungszugriff auf den XClarity Controller. Der Benutzer kann folgende erweiterte Funktionen ausführen: Firmwareaktualisierungen, PXE-Netzboot, werkseitige Voreinstellungen für den XClarity Controller wiederherstellen, die Adapterkonfiguration aus einer Konfigurationsdatei ändern und wiederherstellen und den XClarity Controller erneut starten bzw. zurücksetzen.
11	Reserviert	Diese Bitposition ist für den künftigen Gebrauch reserviert. Wenn keines der Bits gesetzt ist, hat der Benutzer eine Leseberechtigung. Priorität haben die Anmeldeberechtigungen, die direkt aus dem Benutzersatz abgerufen werden. Wenn das Anmeldeberechtigungsattribut nicht im Datensatz des Benutzers enthalten ist, wird versucht, die Berechtigungen von den Gruppen abzurufen, zu denen der Benutzer gehört. Dies wird als Teil der Gruppenauthentifizierungsphase ausgeführt. Dem Benutzer wird das inklusive OR aller Bits für alle Gruppen zugewiesen. Das Bit für den Lesezugriff (Position 2) wird nur gesetzt, wenn alle anderen Bits auf null gesetzt werden. Wenn das Bit für „Nie zulassen“ (Position 0) für eine der Gruppen gesetzt ist, wird dem Benutzer der Zugriff verweigert. Das Bit „Nie zulassen“ (Position 0) hat vor allen anderen Bits Vorrang.

Wenn kein Bit gesetzt ist, wird die Standardeinstellung für den Benutzer auf **Lesezugriff** festgelegt.

Beachten Sie, dass die Anmeldeberechtigungen, die direkt aus dem Benutzerdatensatz abgerufen werden, Priorität haben. Wenn dem Benutzer in seinem Datensatz kein Anmeldeberechtigungsattribut zugeordnet ist, wird versucht, die Berechtigungen aus den Gruppen abzurufen, denen der Benutzer angehört und die mit dem Gruppenfilter übereinstimmen (sofern konfiguriert). In diesem Fall wird dem Benutzer das inklusive ODER aller Bits für alle Gruppen zugewiesen. Analog dazu wird das Bit **Lesezugriff** nur gesetzt, wenn alle anderen Bits null sind. Wenn das Bit **Nie zulassen** für eine seiner Gruppen gesetzt ist, wird dem Benutzer der Zugriff verweigert. Das Bit **Nie zulassen** hat immer Vorrang vor allen anderen Bits.

Anmerkung: Wenn ein Benutzer allgemeine, netzwerk- und/oder sicherheitsbezogene Adapterkonfigurationsparameter ändern darf, sollten Sie erwägen, diesem Benutzer auch die Berechtigung zum Neustarten von XClarity Controller zu erteilen (Bitposition 10). Ohne diese Berechtigung kann der Benutzer zwar Parameter ändern (z. B. die IP-Adresse des Adapters), sie aber nicht in Kraft treten lassen.

3. Geben Sie in den **Active Directory-Einstellungen** (wenn der Modus **LDAP-Server für Authentifizierung und Erteilung von Berechtigungen verwenden** verwendet wird) unter **Erweiterte rollenbasierte Sicherheit für Active Directory-Benutzer aktivieren** an, ob diese Funktion aktiviert werden soll, oder konfigurieren Sie die **Gruppen für lokale Autorisierung** (wenn der Modus **Nur LDAP-Server für Authentifizierung verwenden (mit lokaler Erteilung von Berechtigungen)** verwendet wird).

   - **Erweiterte rollenbasierte Sicherheit für Aktivierung von Active Directory-Benutzern**

     Falls die Einstellung für erweiterte rollenbasierte Sicherheit aktiviert ist, muss ein frei formatierter Servername konfiguriert werden, der als Zielname für diesen bestimmten XClarity Controller dient. Der Zielname kann mithilfe des Snap-In für rollenbasierte Sicherheit (RBS) einer oder mehreren Rollen auf dem Active Directory-Server zugewiesen werden. Hierzu müssen verwaltete Ziele erstellt, mit

spezifischen Namen versehen und dann den entsprechenden Rollen zugewiesen werden. Wenn in diesem Feld ein Name konfiguriert wird, lassen sich somit spezifische Rollen für Benutzer und XClarity Controller (Ziele) definieren, die Mitglieder derselben Rolle sind. Wenn sich ein Benutzer beim XClarity Controller anmeldet und über Active Directory authentifiziert wird, werden aus dem Verzeichnis die Rollen abgerufen, in denen der Benutzer Mitglied ist. Die Berechtigungen für den Benutzer werden aus den Rollen abgeleitet, die als Mitglied ein Ziel haben, das mit einem beliebigen XClarity Controller übereinstimmt oder dessen Name dem hier konfigurierten Namen entspricht. Ein Zielname kann von mehreren XClarity Controllern gemeinsam genutzt werden. Auf diese Weise lassen sich z. B. mehrere XClarity Controller zusammen gruppieren und mithilfe eines einzelnen verwalteten Ziels (d. h. unter einem gemeinsamen Zielnamen) derselben Rolle bzw. denselben Rollen zuweisen. Umgekehrt gilt, dass jeder XClarity Controller einen eindeutigen Namen erhalten kann.

- **Gruppen für lokale Autorisierung**

  Gruppennamen werden konfiguriert, um Spezifikationen für eine lokale Erteilung von Berechtigungen für Benutzergruppen bereitzustellen. Jeder Gruppenname kann Berechtigungen (Rollen) zugewiesen werden, die mit denen in der obigen Tabelle beschriebenen identisch sind. Der LDAP-Server weist Benutzern einen Gruppennamen zu. Wenn sich der Benutzer anmeldet, werden ihm die Berechtigungen zugewiesen, die mit der Gruppe verknüpft sind, zu der er gehört. Sie können weitere Gruppen konfigurieren, indem Sie auf das Symbol „+“ klicken, bzw. Gruppen löschen, indem Sie auf das „x“-Symbol klicken.

Netzwerkprotokolle konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie die Netzwerkeinstellungen von XClarity Controller anzeigen oder festlegen.

Ethernet-Einstellungen konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie anzeigen oder ändern, wie der XClarity Controller über eine Ethernet-Verbindung kommuniziert.

Der XClarity Controller verwendet zwei Netzwerkcontroller. Ein Netzwerkcontroller wird mit dem dedizierten Management-Port verbunden und der andere mit dem gemeinsam genutzten Anschluss. Jeder Netzwerkcontroller wird seiner eigenen MAC-Herstelleradressenkennung zugewiesen. Wenn für die Zuweisung einer IP-Adresse zum XClarity Controller DHCP verwendet wird, ist es möglich, dass dem XClarity Controller vom DHCP-Server eine andere IP-Adresse zugewiesen wird, wenn ein Benutzer zwischen Netzwerkanschlüssen wechselt oder ein Failover vom dedizierten Netzwerkanschluss auf den gemeinsam genutzten Netzwerkanschluss erfolgt. Bei Verwendung von DHCP sollten die Benutzer statt der IP-Adresse den Hostnamen verwenden, um auf den XClarity Controller zuzugreifen. Selbst wenn die XClarity Controller-Netzwerkanschlüsse nicht geändert werden, könnte der DHCP-Server dem XClarity Controller eine andere IP-Adresse zuweisen, wenn die DHCP-Zugangsberechtigung abläuft oder der XClarity Controller neu gestartet wird. Wenn ein Benutzer auf den XClarity Controller mit einer IP-Adresse zugreifen muss, die sich nicht ändert, sollte der XClarity Controller für eine statische IP-Adresse konfiguriert werden, anstatt DHCP zu verwenden.

Klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**, um die Ethernet-Einstellungen für den XClarity Controller zu ändern.

XClarity Controller-Hostnamen konfigurieren

Der standardmäßige XClarity Controller-Hostname setzt sich aus der Zeichenfolge „XCC-“ gefolgt vom Maschinentyp und der Seriennummer des Servers zusammen (z. B. „XCC-7X03-1234567890“). Sie können den XClarity Controller-Hostnamen ändern, indem Sie maximal 63 Zeichen in dieses Feld eingeben. Der Hostname darf keinen Punkt (.) enthalten und darf nur aus Buchstaben, Ziffern, Bindestrichen und Unterstrichen bestehen.

Ethernet-Anschlüsse

Diese Einstellung steuert die Aktivierung von Ethernet-Anschlüssen, die vom Management-Controller verwendet werden, einschließlich der gemeinsam genutzten und dedizierten Anschlüsse.

Wenn die Einstellung **deaktiviert** ist, werden den Ethernet-Anschlüssen keine IPv4- oder IPv6-Adressen zugeordnet und weitere Änderungen an den Ethernet-Konfigurationen werden verhindert.

Anmerkung: Diese Einstellung hat keinen Einfluss auf die USB LAN-Schnittstelle oder den USB-Anschluss zur Verwaltung an der Vorderseite des Servers. Diese Schnittstellen verfügen über eigene dedizierte Aktivierungseinstellungen.

IPv4-Netzwerkeinstellungen konfigurieren

Gehen Sie wie folgt vor, um eine IPv4-Ethernet-Verbindung zu verwenden:

1. Aktivieren Sie die Option **IPv4**.

   Anmerkung: Durch Deaktivieren der Ethernet-Schnittstelle können Sie den Zugriff auf den XClarity Controller vom externen Netzwerk aus verhindern.
2. Wählen Sie im Feld **Methode** eine der folgenden Optionen aus:
   - **IP-Adresse von DHCP abrufen**: Der XClarity Controller erhält seine IPv4-Adresse von einem DHCP-Server.
   - **Statische IP-Adresse verwenden**: Der XClarity Controller verwendet den vom Benutzer angegebenen Wert als IPv4-Adresse.
   - **Erst DHCP, dann statische IP-Adresse**: Der XClarity Controller versucht, die IPv4-Adresse von einem DHCP-Server abzurufen, wenn dieser Versuch aber fehlschlägt, verwendet der XClarity Controller den vom Benutzer angegebenen Wert als IPv4-Adresse.
3. Geben Sie in das Feld **Statische Adresse** die IP-Adresse ein, die Sie dem XClarity Controller zuweisen möchten.

   Anmerkung: Die IP-Adresse muss vier Ganzzahlen von 0 bis 255 enthalten, die durch Punkte voneinander getrennt sind. Sie darf keine Leerzeichen enthalten. Dieses Feld ist nicht konfigurierbar, wenn als Methode **IP-Adresse von DHCP abrufen** angegeben ist.
4. Geben Sie im Feld **Netzwerkmaske** die Subnetzmaske ein, die vom XClarity Controller verwendet wird.

   Anmerkung: Die Subnetzmaske muss vier Ganzzahlen von 0 bis 255 ohne Leerzeichen oder aufeinanderfolgende Punkte enthalten, wobei die Ganzzahlen durch Punkte voneinander getrennt sind. Die Standardeinstellung ist 255.255.255.0. Dieses Feld ist nicht konfigurierbar, wenn als Methode **IP-Adresse von DHCP abrufen** angegeben ist.
5. Geben Sie im Feld **Standard-Gateway** Ihren Netz-Gateway-Router ein.

   Anmerkung: Die Gateway-Adresse muss vier Ganzzahlen von 0 bis 255 ohne Leerzeichen oder aufeinanderfolgende Punkte enthalten, wobei die Ganzzahlen durch Punkte voneinander getrennt sind. Dieses Feld ist nicht konfigurierbar, wenn als Methode **IP-Adresse von DHCP abrufen** angegeben ist.

Erweiterte Ethernet-Einstellungen konfigurieren

Klicken Sie auf die Registerkarte **Erweitertes Ethernet**, um zusätzliche Ethernet-Einstellungen festzulegen.

Anmerkung: In einem Flex System werden die VLAN-Einstellungen von einem Flex System-CMM verwaltet und können auf dem XClarity Controller nicht geändert werden.

Zum Aktivieren von VLAN-Tagging wählen Sie das Kontrollkästchen **VLAN aktivieren** aus. Wenn VLAN aktiviert und eine VLAN-ID konfiguriert ist, nimmt der XClarity Controller nur Pakete mit den angegebenen VLAN-IDs an. Die VLAN-IDs können mit numerischen Werten zwischen 1 und 4094 konfiguriert werden.

Wählen Sie in der Liste **MAC-Auswahl** eine der folgenden Optionen aus:

- Herstellerkennung der MAC-Adresse verwenden

  Die Option „Herstellerkennung der MAC-Adresse“ ist eine eindeutige physische Adresse, die diesem XClarity Controller vom Hersteller zugeordnet wurde. Die Adresse ist ein schreibgeschütztes Feld.

- Angepasste MAC-Adresse verwenden

  Wenn ein Wert angegeben wird, setzt die lokal verwaltete Adresse die Herstellerkennung der MAC-Adresse außer Kraft. Die lokal verwaltete Adresse muss ein Hexadezimalwert von `000000000000` bis `FFFFFFFFFFFF` sein. Dieser Wert muss im Format **xx:xx:xx:xx:xx:xx** angegeben werden, wobei **x** eine Hexadezimalzahl von 0 bis 9 oder „a“ bis „f“ ist. Der XClarity Controller unterstützt nicht die Verwendung einer Multicastadresse. Das erste Byte einer Multicastadresse ist eine ungerade Zahl (das niedrigstwertige Bit hat den Wert 1). Aus diesem Grund muss das erste Byte eine gerade Zahl sein.

Geben Sie im Feld **Maximum Transmission Unit (MTU)** die größte zu übertragende Einheit eines Datenpakets (in Byte) für Ihre Netzwerkschnittstelle an. Der gültige Bereich für die größte zu übertragende Einheit reicht von 60 bis 1500. Der Standardwert für dieses Feld lautet 1500.

Gehen Sie wie folgt vor, um eine IPv6-Ethernet-Verbindung zu verwenden:

IPv6-Netzwerkeinstellungen konfigurieren

1. Aktivieren Sie die Option **IPv6**.
2. Weisen Sie der Schnittstelle mithilfe einer der folgenden Zuordnungsmethoden eine IPv6-Adresse zu:
   - Automatische zustandslose Adresskonfiguration verwenden
   - Statusbehaftete Adresskonfiguration verwenden (DHCPv6)
   - Statisch zugeordnete IP-Adresse verwenden

     Anmerkungen: Wenn **Statisch zugeordnete IP-Adresse verwenden** ausgewählt ist, werden Sie aufgefordert, die folgenden Informationen einzugeben:

     – IPv6-Adresse
     – Präfixlänge
     – Gateway

DNS konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie die DNS-Einstellungen von XClarity Controller anzeigen oder ändern.

Anmerkung: In einem Flex System können die DNS-Einstellungen auf dem XClarity Controller nicht geändert werden. DNS-Einstellungen werden vom CMM verwaltet.

Klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**, um die DNS-Einstellungen für den XClarity Controller anzuzeigen oder zu ändern.

Wenn Sie das Kontrollkästchen **Zusätzliche DNS-Server verwenden** aktivieren, können Sie die IP-Adressen von bis zu drei DNS-Servern in Ihrem Netzwerk angeben. Jede IP-Adresse muss vier Ganzzahlen (von 0 bis 255) enthalten, die durch Punkte voneinander getrennt sind. Diese DNS-Serveradressen werden an den Anfang der Suchliste hinzugefügt, sodass die Hostnamensuche auf diesen Servern Vorrang vor der Suche auf einem DNS-Server erhält, der automatisch durch einen DHCP-Server zugeordnet wird.

DDNS konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie das DDNS-Protokoll (Dynamic Domain Name System) auf dem XClarity Controller aktivieren bzw. deaktivieren.

Klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**, um die DDNS-Einstellungen für den XClarity Controller anzuzeigen oder zu ändern.

Aktivieren Sie das Kontrollkästchen **DDNS aktivieren**, um DDNS zu aktivieren. Wenn DDNS aktiviert ist, fordert der XClarity Controller einen DNS-Server auf, die aktive DNS-Konfiguration der konfigurierten Hostnamen, Adressen oder anderer im DNS gespeicherter Informationen in Echtzeit zu ändern.

Wählen Sie eine Option aus der Elementliste aus, um anzugeben, wie der Domänenname von XClarity Controller ausgewählt werden soll.

- **Benutzerdefinierten Domänennamen verwenden**: Sie geben den Domänennamen an, zu dem der XClarity Controller gehört.
- **Den vom DHCP-Server erhaltenen Domänennamen verwenden**: Der Domänenname, zu dem der XClarity Controller gehört, wird vom DHCP-Server angegeben.

Ethernet-over-USB konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie die Ethernet-over-USB-Schnittstelle steuern, die für die In-Band-Kommunikation zwischen Server und XClarity Controller verwendet wird.

Klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**, um die Ethernet-over-USB-Einstellungen für den XClarity Controller anzuzeigen oder zu ändern.

Die Ethernet-over-USB-Schnittstelle wird für die In-Band-Kommunikation zum XClarity Controller verwendet. Aktivieren Sie das Kontrollkästchen, um die Ethernet-over-USB-Schnittstelle zu aktivieren oder zu deaktivieren.

Wichtig: Wenn Sie die Ethernet-over-USB-Schnittstelle deaktivieren, können Sie keine In-Band-Aktualisierung der XClarity Controller- oder Server-Firmware mithilfe der Linux- oder Windows-Flashdienstprogramme durchführen.

Wählen Sie die Methode aus, die der XClarity Controller verwenden soll, um den Endpunkten der Ethernet-over-USB-Schnittstelle Adressen zuzuweisen.

- **IPv6-Link-Local-Adresse für Ethernet-über-USB verwenden**: Diese Methode verwendet IPv6-Adressen basierend auf der MAC-Adresse, die den Endpunkten der Ethernet-over-USB-Schnittstelle zugewiesen wurden. Normalerweise wird die IPv6-Link-Local-Adresse unter Verwendung der MAC-Adresse (RFC 4862) generiert, Windows 2008 und neuere 2016er Betriebssysteme unterstützen aber keine statische IPv6-Link-Local-Adresse am Hostende der Schnittstelle. Stattdessen werden durch das Windows-Standardverhalten bei Ausführung zufällige Link-Local-Adressen neu generiert. Wenn die Ethernet-over-USB-Schnittstelle von XClarity Controller so konfiguriert ist, dass der IPv6-Link-Local-Adressmodus verwendet wird, funktionieren einige Funktionen nicht, die diese Schnittstelle nutzen, da der XClarity Controller nicht weiß, welche Adresse der Schnittstelle von Windows zugewiesen wurde. Wenn auf dem Server Windows ausgeführt wird, verwenden Sie eine der anderen Konfigurationsmethoden für die Ethernet-over-USB-Adresse oder deaktivieren Sie das Standardverhalten von Windows durch Ausführung dieses Befehls: **netsh interface ipv6 set global randomizeidentifiers=disabled**.
- **IPv4-Link-Local-Adresse für Ethernet-over-USB verwenden**: Auf der Seite von XClarity Controller und dem Servers des Netzwerks wird eine IP-Adresse im Bereich 169.254.0.0/16 zugewiesen.
- **IPv4-Einstellungen für Ethernet-over-USB konfigurieren**: Bei dieser Methode werden die IP-Adressen und die Netzwerkmaske angegeben, die der XClarity Controller- und Serverseite der Ethernet-over-USB-Schnittstelle zugewiesen sind.

Anmerkungen:

1. Die Einstellungen der BS-IP-Konfiguration werden nicht verwendet, um die BS-IP-Adresse der Ethernet-over-USB-Schnittstelle zu konfigurieren. Jedoch wird versucht, das BMC zu benachrichtigen, dass die BS-IP-Adresse von Ethernet-over-USB geändert wurde.
2. Bevor Sie die drei IP-Einstellungen für Ethernet-over-USB konfigurieren, müssen Sie die BS-IP-Adresse der Ethernet-over-USB-Schnittstelle manuell in Ihrem lokalen Betriebssystem konfigurieren.

Die Zuordnung von externen Ethernet-Portnummern zu Ethernet-over-USB-Portnummern können Sie durch Klicken auf das Kontrollkästchen **Externe Ethernet-Portweiterleitung für Ethernet zu Ethernet-over-USB aktivieren** steuern. Füllen Sie anschließend die Zuordnungsinformationen für die Ports aus, für die die Weiterleitung von der Verwaltungsnetzwerksschnittstelle zum Server gelten soll.

SNMP konfigurieren

Mithilfe der Informationen in diesem Abschnitt konfigurieren Sie die SNMP-Agenten.

Gehen Sie wie folgt vor, um die SNMP-Alerteinstellungen für den XClarity Controller zu konfigurieren.

1. Klicken Sie auf unter **BMC-Konfiguration** auf **Netzwerk**.
2. Aktivieren Sie das entsprechende Kontrollkästchen, um **SNMPv1-Trap**, **SNMPv2-Trap** und/oder **SNMPv3-Trap** zu aktivieren.
3. Wenn Sie **SNMPv1-Trap** oder **SNMPv2-Trap** aktivieren, füllen Sie die folgenden Felder aus:
   a. Geben Sie im Feld **Community-Name** den Community-Namen ein. Der Name darf nicht leer sein.
   b. Geben Sie im Feld **Host** die Hostadresse ein.
4. Füllen Sie die folgenden Felder aus, wenn Sie den **SNMPv3-Trap** aktiviert haben:
   a. Geben Sie im Feld **Engine-ID** die Engine-ID ein. Engine-ID darf nicht leer sein.
   b. Geben Sie im Feld **Trap-Empfänger-Port** die Portnummer ein. Die Standardportnummer ist 162.
5. Wenn Sie die SNMP-Traps aktivieren, wählen Sie die folgenden Ereignistypen aus, über die Sie benachrichtigt werden möchten:
   - **Kritisch**
   - **Achtung**
   - **System**

   Anmerkung: Klicken Sie auf jede Hauptkategorie, um die entsprechenden Ereignistypen in den Unterkategorien auszuwählen, bei denen Sie Alerts erhalten möchten.

IPMI-Netzwerkzugriff aktivieren oder deaktivieren

Mithilfe der Informationen in diesem Abschnitt können Sie den IPMI-Netzwerkzugriff auf den XClarity Controller steuern.

Klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**, um die IPMI-Einstellungen für den XClarity Controller anzuzeigen oder zu ändern. Füllen Sie die folgenden Felder aus, um IPMI-Einstellungen anzuzeigen oder zu ändern:

IPMI-over-LAN-Zugriff
Klicken Sie auf den Schalter, um den IPMI-Netzwerkzugriff auf den XClarity Controller zu aktivieren oder zu deaktivieren.

Wichtig:

- Wenn Sie keine Werkzeuge oder Anwendungen verwenden, die über das Netzwerk mit dem IPMI-Protokoll auf den XClarity Controller zugreifen, wird dringend empfohlen, den IPMI-Netzwerkzugriff zu deaktivieren, um die Sicherheit zu erhöhen.
- Der IPMI-über-LAN-Zugriff auf XClarity Controller ist standardmäßig deaktiviert.

Netzwerkeinstellungen mit IPMI-Befehlen konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie die Netzwerkeinstellungen mithilfe von IPMI-Befehlen konfigurieren.

Da sämtliche BMC-Netzwerkeinstellungen über separate IPMI-Anforderungen und in keiner bestimmten Reihenfolge konfiguriert werden, verfügt der BMC erst dann über eine vollständige Sicht auf alle Netzwerkeinstellungen, wenn der BMC neu gestartet wurde, um die Netzwerkänderungen zu übernehmen. Die Anforderung zum Ändern einer Netzwerkeinstellung kann zu dem Zeitpunkt erfolgreich sein, zu dem die Anforderung erfolgt, später aber als ungültig eingestuft werden, wenn weitere Änderungen angefordert werden. Wenn die ausstehenden Netzwerkeinstellungen beim Neustart des BMC nicht kompatibel sind, werden die neuen Einstellungen nicht angewendet. Nachdem Sie den BMC erneut gestartet haben, sollten Sie versuchen, mit den neuen Einstellungen auf den BMC zuzugreifen, um sicherzustellen, dass sie wie gewünscht übernommen wurden.

Serviceaktivierung und Portzuordnung

Mithilfe der Informationen in diesem Abschnitt können Sie die Portnummern anzeigen oder ändern, die von einigen Services auf dem XClarity Controller verwendet werden.

Klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**, um die Portzuordnungen für den XClarity Controller anzuzeigen oder zu ändern. Füllen Sie die folgenden Felder aus, um Portzuordnungen anzuzeigen oder zu ändern:

Web
Die Portnummer lautet 80. Dieses Feld ist nicht durch den Benutzer konfigurierbar.

Web over HTTPS
Geben Sie in diesem Feld die Portnummer für Web Over HTTPS an. Der Standardwert ist 443.

REST over HTTPS
Die Portnummer ändert sich automatisch in die Nummer, die im Feld „Web over HTTPS“ angegeben wird. Dieses Feld ist nicht durch den Benutzer konfigurierbar.

CIM over HTTP
Geben Sie in diesem Feld die Portnummer für CIM over HTTP an. Der Standardwert ist 5989.

Anmerkung: CIM ist standardmäßig deaktiviert.

Fernpräsenz
Geben Sie in diesem Feld die Portnummer für Fernpräsenz an. Der Standardwert ist 3900.

IPMI over LAN
Die Portnummer lautet 623. Dieses Feld ist nicht durch den Benutzer konfigurierbar.

Anmerkung: IPMI ist standardmäßig deaktiviert.

SFTP
Geben Sie in diesem Feld die Portnummer an, die für SFTP (SSH File Transfer Protocol) verwendet wird. Die Portnummer lautet 115. Dieses Feld ist nicht durch den Benutzer konfigurierbar.

Anmerkung: IMM.SFTPPortControl=open ist für OneCLI-Inband-Aktualisierungen erforderlich.

SLP
Geben Sie in diesem Feld die Portnummer an, die für SLP verwendet wird. Die Portnummer lautet 427. Dieses Feld ist nicht durch den Benutzer konfigurierbar.

Anmerkungen: XClarity Controller meldet zwei Servicetypen:

- Service: management-hardware.Lenovo:lenovo-xclarity-controller
- Service: wbem

SSDP
Die Portnummer lautet 1900. Dieses Feld ist nicht durch den Benutzer konfigurierbar.

SSH
Geben Sie in diesem Feld die Portnummer an, die für den Zugriff auf die Befehlszeilenschnittstelle über das SSH-Protokoll konfiguriert ist. Der Standardwert ist 22.

SNMP-Agent
Geben Sie in diesem Feld die Portnummer für den SNMP-Agenten an, der auf dem XClarity Controller ausgeführt wird. Der Standardwert lautet 161. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

SNMP-Traps
Geben Sie in diesem Feld die Portnummer an, die für SNMP-Traps verwendet wird. Der Standardwert lautet 162. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

Zugriffsbeschränkung konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie die Einstellungen anzeigen oder ändern, mit denen der Zugriff von IP- oder MAC-Adressen auf den XClarity Controller blockiert wird.

Klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**, um die Einstellungen für die Zugriffssteuerung für XClarity Controller anzuzeigen oder zu ändern.

Sperrliste und Zeitbeschränkung

Mit diesen Optionen können Sie bestimmte IP- und MAC-Adressen für bestimmte Zeiträume sperren.

- **Liste der gesperrten IP-Adressen**
  - Sie können bis zu drei durch Kommas getrennte IPv4-Adressen oder IPv4-Adressbereiche sowie drei IPv6-Adressen oder IPv6-Adressbereiche eingeben, denen der Zugriff auf den XClarity Controller verweigert wird. Beispiele für IPv4:
  - Beispiel einer IPv4-Adresse: 192.168.1.1
  - Beispiel einer Supernet-IPv4-Adresse: 192.168.1.0/24
  - Beispiel eines IPv4-Bereichs: 192.168.1.1–192.168.1.5
- **Liste der blockierten MAC-Adressen**
  - Sie können bis zu drei durch Kommas getrennte MAC-Adressen eingeben, denen der Zugriff auf den XClarity Controller verweigert wird. Beispiel: 11:22:33:44:55:66.
- **Eingeschränkter Zugriff (einmalig)**
  - Sie können einen einmaligen Zeitraum planen, während dem nicht auf den XClarity Controller zugegriffen werden kann. Für den von Ihnen festgelegten Zeitraum:
  - Beginndatum und -uhrzeit müssen nach der aktuellen XCC-Zeit liegen.

  - Enddatum und -uhrzeit müssen nach Beginndatum und -uhrzeit liegen.
- **Eingeschränkter Zugriff (täglich)**
  - Sie können einen oder mehrere tägliche Zeiträume planen, während denen nicht auf den XClarity Controller zugegriffen werden kann. Für jeden von Ihnen festgelegten Zeitraum:
  - Enddatum und -uhrzeit müssen nach Beginndatum und -uhrzeit liegen.

Extern ausgelöste Sperrliste

Mit diesen Optionen können Sie die automatische Sperrung von bestimmten IP-Adressen (IPv4 und IPv6) einrichten, von denen der Client nacheinander versucht hat, sich bei XClarity Controller mit einem anderen falschen Benutzernamen oder Kennwort anzumelden.

Die automatische Sperrung bestimmt dynamisch, wenn vermehrte Anmeldefehler von einer bestimmten IP-Adresse auftreten und sperrt bei dieser Adresse für einen bestimmten Zeitraum den Zugriff auf XClarity Controller.

- **Maximale Anzahl fehlgeschlagener Anmeldeversuche von einer bestimmten IP-Adresse**
  - Diese Zahl gibt an, wie viele Anmeldefehler ein Benutzer mit einem falschen Kennwort von einer bestimmten IP-Adresse haben kann, bevor er gesperrt wird.
  - Wenn dieser Wert auf 0 festgelegt ist, wird die IP-Adresse niemals aufgrund von Anmeldefehlern gesperrt.
  - Der Zähler für Anmeldefehler für die bestimmte IP-Adresse wird nach einer erfolgreichen Anmeldung von dieser IP-Adresse auf Null zurückgesetzt.
- **Sperrzeitraum für eine IP-Sperrung**
  - Die Mindestdauer (in Minuten), die vergehen muss, bevor ein Benutzer sich erneut von einer gesperrten IP-Adresse aus anmelden kann.
  - Wenn dieser Wert auf 0 festgelegt ist, bleibt der Zugriff von der gesperrten IP-Adresse gesperrt, bis der Administrator die Sperre explizit aufhebt.
- **Sperrliste**
  - In der Liste „Sperrliste“ werden alle gesperrten IP-Adressen angezeigt. Sie können eine oder alle IP-Adressen in der Sperrliste entsperren.

Vorderseitigen USB-Anschluss zur Verwaltung konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie den vorderseitigen USB-Anschluss von XClarity Controller zur Verwaltung konfigurieren.

Bei manchen Servern kann der vorderseitige USB-Anschluss umgeschaltet werden, sodass er entweder dem Server oder dem XClarity Controller zugeordnet ist. Die Verbindung zum XClarity Controller wird hauptsächlich mit einem mobilen Gerät genutzt, auf dem die mobile App Lenovo XClarity ausgeführt wird. Wenn zwischen dem mobilen Gerät und der Vorderseite des Servers ein USB-Kabel angeschlossen wurde, wird eine Ethernet-over-USB-Verbindung zwischen der mobilen App auf dem Gerät und dem XClarity Controller hergestellt.

Klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**, um den vorderseitigen USB-Anschluss von XClarity Controller zur Verwaltung anzuzeigen oder zu ändern.

Es gibt vier Arten von Einstellungen, aus denen Sie auswählen können:

Nur-Host-Modus
Der vorderseitige USB-Anschluss ist immer nur mit dem Server verbunden.

Nur-BMC-Modus
Der vorderseitige USB-Anschluss ist immer nur mit dem XClarity Controller verbunden.

Gemeinsam genutzter Modus: Eigentümer BMC
Der vorderseitige USB-Anschluss wird vom Server und dem XClarity Controller gemeinsam genutzt, der Anschluss wird aber zum XClarity Controller umgeschaltet.

Gemeinsam genutzter Modus: Eigentümer Host
Der vorderseitige USB-Anschluss wird vom Server und dem XClarity Controller gemeinsam genutzt, der Anschluss wird aber zum Host umgeschaltet.

Weitere Informationen zur mobilen App finden Sie auf der folgenden Website:

https://pubs.lenovo.com/lxca/lxca_usemobileapp.html

Anmerkungen:

- Ist der vorderseitige USB-Anschluss für den gemeinsamen Modus konfiguriert, wird der Anschluss mit dem XClarity Controller verbunden, wenn es keine Stromversorgung gibt, bzw. mit dem Server, wenn eine Stromversorgung vorhanden ist. Wenn eine Stromversorgung vorhanden ist, kann die Steuerung des vorderseitigen USB-Anschlusses zwischen Server und XClarity Controller hin- und hergeschaltet werden. Im gemeinsamen Modus kann der Anschluss auch zwischen dem Host und dem XClarity Controller umgeschaltet werden, indem die ID-Taste im Bedienfeld drei Sekunden lang gedrückt wird (für Rechenknoten kann dies die USB-Management-Taste sein).
- Wenn der gemeinsame Modus konfiguriert ist und der USB-Anschluss aktuell mit dem Server verbunden ist, kann der XClarity Controller eine Anforderung unterstützen, den vorderseitigen USB-Anschluss zurück zum XClarity Controller zu schalten. Bei Ausführung dieser Anforderung bleibt der vorderseitige USB-Anschluss mit dem XClarity Controller verbunden, bis es auf dem XClarity Controller so lange keine USB-Aktivität gibt, wie vom Inaktivitätszeitlimit vorgegeben.

Sicherheitseinstellungen konfigurieren

Mithilfe der Informationen in diesem Abschnitt konfigurieren Sie Sicherheitsprotokolle.

Anmerkung: Die Mindeststandardeinstellung für die TLS-Version ist TLS 1.2. Sie können aber den XClarity Controller so konfigurieren, dass andere TLS-Versionen verwendet werden, sofern dies Ihr Browser oder Ihre Verwaltungsanwendungen erfordern. Siehe „Befehl „tls““ auf Seite 161 für weitere Informationen.

Klicken Sie unter **BMC-Konfiguration** auf **Sicherheit**, um die Sicherheitseigenschaften, den Sicherheitsstatus und die Sicherheitseinstellungen für Ihren XClarity Controller aufzurufen und zu konfigurieren.

SSL-Übersicht

Dieser Abschnitt enthält eine Übersicht über das SSL-Sicherheitsprotokoll.

SSL ist ein Sicherheitsprotokoll, das eine geschützte Datenübertragung ermöglicht. SSL ermöglicht Client-/Serveranwendungen eine Datenübertragung, die gegen das Ausspionieren, das Manipulieren von Daten während der Übertragung und das Fälschen von Nachrichten geschützt ist. Sie können den XClarity Controller so konfigurieren, dass die SSL-Unterstützung für verschiedene Verbindungsmöglichkeiten, z. B. den sicheren Webserver (HTTPS), die sichere LDAP-Verbindung (LDAPS), CIM over HTTPS oder den SSH-Server, verwendet wird und er die für SSL erforderlichen Zertifikate verwaltet.

Handhabung von SSL-Zertifikaten

Dieser Abschnitt enthält Informationen zur Verwaltung von Zertifikaten, die mit dem SSL-Sicherheitsprotokoll verwendet werden können.

Sie können SSL mit einem selbst signierten Zertifikat oder mit einem von einer unabhängigen Zertifizierungsstelle signierten Zertifikat verwenden. Ein selbst signiertes Zertifikat ist die einfachste Methode für die Verwendung von SSL, allerdings stellt es ein geringes Sicherheitsrisiko dar. Das Risiko besteht darin, dass der SSL-Client keine Möglichkeit hat, beim ersten Verbindungsversuch zwischen Client und Server die Identität des SSL-Servers zu prüfen. Beispielsweise besteht die Möglichkeit, dass ein anderer Anbieter die Identität des XClarity Controller-Webservers vortäuschen und Daten zwischen dem tatsächlichen XClarity Controller-Webserver und dem Webbrowser des Benutzers abfangen könnte. Wenn das selbst signierte Zertifikat beim ersten Verbindungsaufbau zwischen Browser und XClarity Controller in den Zertifikatsspeicher des Browsers importiert wird, sind alle künftigen Datenübertragungen für diesen Browser sicher (vorausgesetzt, dass bei der ersten Verbindung kein Angriff erfolgt ist).

Mehr Sicherheit erhalten Sie, wenn Sie ein Zertifikat verwenden, das von einer Zertifizierungsstelle (CA) signiert ist. Um ein signiertes Zertifikat zu erhalten, müssen Sie **Zertifikatssignieranforderung (CSR) generieren** auswählen. Wählen Sie **Zertifikatssignieranforderung (CSR) herunterladen** aus und senden Sie die Zertifikatssignieranforderung an eine Zertifizierungsstelle, um ein signiertes Zertifikat zu erhalten. Wählen Sie nach Erhalt des signierten Zertifikats die Option **Signiertes Zertifikat importieren**, um es in den XClarity Controller zu importieren.

Die Aufgabe der Zertifizierungsstelle (CA) ist es, die Identität von XClarity Controller zu überprüfen. Ein Zertifikat enthält digitale Signaturen für die Zertifizierungsstelle und den XClarity Controller. Wenn eine anerkannte Zertifizierungsstelle das Zertifikat ausstellt oder wenn das Zertifikat der Zertifizierungsstelle bereits in den Webbrowser importiert wurde, kann der Browser das Zertifikat validieren und den XClarity Controller-Webserver eindeutig identifizieren.

Der XClarity Controller erfordert ein Zertifikat für die Verwendung mit HTTPS-Servern, CIM over HTTPS und sicheren LDAP-Clients. Außerdem müssen für den sicheren LDAP-Client ebenfalls ein oder mehrere vertrauenswürdige Zertifikate importiert werden. Das vertrauenswürdige Zertifikat wird vom sicheren LDAP-Client verwendet, um den LDAP-Server sicher zu identifizieren. Das vertrauenswürdige Zertifikat ist das Zertifikat der Zertifizierungsstelle, die das Zertifikat des LDAP-Servers signiert hat. Wenn der LDAP-Server selbst signierte Zertifikate verwendet, kann das vertrauenswürdige Zertifikat das Zertifikat des LDAP-Servers selbst sein. Sie müssen zusätzliche vertrauenswürdige Zertifikate importieren, wenn Sie in Ihrer Konfiguration mehrere LDAP-Server verwenden.

Verwaltung von SSL-Zertifikaten

Dieser Abschnitt enthält Informationen zu einigen der Aktionen, die für die Verwaltung von Zertifikaten mit dem SSL-Sicherheitsprotokoll ausgewählt werden können.

Klicken Sie unter **BMC-Konfiguration** auf **Sicherheit**, um die SSL-Zertifikatsverwaltung zu konfigurieren.

Wenn Sie XClarity Controller-Zertifikate verwalten, werden die folgenden Aktionen angezeigt:

Signiertes Zertifikat herunterladen
Verwenden Sie diesen Link, um eine Kopie des aktuell installierten Zertifikats herunterzuladen. Das Zertifikat kann im PEM- oder DER-Format heruntergeladen werden. Der Inhalt des Zertifikats kann mithilfe eines Drittanbietertools wie OpenSSL (www.openssl.org) angezeigt werden. Ein Beispiel für die Befehlszeile zum Anzeigen des Inhalts des Zertifikats mithilfe von OpenSSL könnte wie folgt aussehen:

```
openssl x509 -in cert.der -inform DER -text
```

Zertifikatssignieranforderung herunterladen
Verwenden Sie diesen Link, um eine Kopie der Zertifikatssignieranforderung herunterzuladen. Die Zertifikatssignieranforderung kann im PEM- oder DER-Format heruntergeladen werden.

Signiertes Zertifikat generieren

Generieren Sie ein selbst signiertes Zertifikat. Nach Abschluss des Vorgangs kann SSL mithilfe des neuen Zertifikats aktiviert werden.

Anmerkung: Wenn die Aktion **Signiertes Zertifikat generieren** ausgeführt wird, wird das Fenster „Selbst signiertes Zertifikat für HTTPS generieren“ geöffnet. Sie werden aufgefordert, die Pflicht- und Wahlfelder auszufüllen. Sie **müssen** die Pflichtfelder ausfüllen. Klicken Sie nach Angabe Ihrer Informationen auf **Erstellen**, um den Vorgang abzuschließen.

Zertifikatssignieranforderung generieren
Generieren Sie eine Zertifikatssignieranforderung. Nach Abschluss des Vorgangs kann die Zertifikatssignieranforderungsdatei heruntergeladen und zum Signieren an eine Zertifizierungsstelle gesendet werden.

Anmerkung: Wenn die Aktion **Zertifikatssignieranforderung (CSR) generieren** ausgeführt wird, wird das Fenster „Zertifikatssignieranforderung für HTTPS generieren“ geöffnet. Sie werden aufgefordert, die Pflicht- und Wahlfelder auszufüllen. Sie **müssen** die Pflichtfelder ausfüllen. Klicken Sie nach Angabe Ihrer Informationen auf **Erstellen**, um den Vorgang abzuschließen.

Signiertes Zertifikat importieren
Verwenden Sie diese Option, um ein signiertes Zertifikat zu importieren. Um ein signiertes Zertifikat zu erhalten, muss zuerst eine Zertifikatssignieranforderung generiert und an eine Zertifizierungsstelle gesendet werden.

Secure Shell-Server konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie das SSH-Sicherheitsprotokoll verstehen und aktivieren.

Klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**, um den Secure Shell-Server zu konfigurieren.

Damit das SSH-Protokoll verwendet werden kann, muss zuerst ein Schlüssel generiert werden, um den SSH-Server zu aktivieren.

Anmerkungen:

- Für diese Option ist keine Zertifikatsverwaltung erforderlich.
- Der XClarity Controller erstellt anfangs einen SSH-Server-Schlüssel. Wenn Sie einen neuen SSH-Server-Schlüssel generieren möchten, klicken Sie unter **BMC-Konfiguration** auf **Netzwerk** und dann auf **Schlüssel erneut generieren**.
- Nachdem Sie diese Aktion abgeschlossen haben, müssen Sie den XClarity Controller erneut starten, damit Ihre Änderungen wirksam werden.

IPMI-over-Keyboard Controller Style(KCS)-Zugriff

Mithilfe der Informationen in diesem Abschnitt können Sie den IPMI-über-KCS-Zugriff (Keyboard Controller Style) auf den XClarity Controller steuern.

Der XClarity Controller bietet eine IPMI-Schnittstelle über den KCS-Kanal, der keine Authentifizierung erfordert.

Klicken Sie unter **BMC-Konfiguration** auf **Sicherheit**, um den IPMI-über-KCS-Zugriff zu aktivieren oder zu deaktivieren.

Anmerkung: Nachdem Sie die Einstellungen geändert haben, müssen Sie den XClarity Controller erneut starten, damit Ihre Änderungen wirksam werden.

Wichtig: Wenn Sie keine Werkzeuge oder Anwendungen auf dem Server ausführen, die über das IPMI-Protokoll auf den XClarity Controller zugreifen, wird dringend empfohlen, den IPMI-über-KCS-Zugriff zu deaktivieren, um die Sicherheit zu erhöhen. XClarity Essentials verwendet allerdings die IPMI-über-KCS-Schnittstelle zum XClarity Controller. Wenn Sie die IPMI-über-KCS-Schnittstelle deaktiviert haben, aktivieren Sie sie, bevor Sie XClarity Essentials auf dem Server ausführen. Deaktivieren Sie die Schnittstelle dann wieder, wenn Sie fertig sind.

Zurückstufen der Systemfirmware unterbinden –

Mithilfe der Informationen in diesem Abschnitt können Sie verhindern, dass die Systemfirmware auf ältere Firmwareversionen zurückgestuft wird.

Diese Funktion ermöglicht es Ihnen, zu entscheiden, ob die Systemfirmware auf eine ältere Firmwareversion zurückgestuft werden darf oder nicht.

Klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**, um ein Zurückstufen der Systemfirmware zu unterbinden.

Um diese Funktion zu aktivieren oder zu deaktivieren, klicken Sie unter **BMC-Konfiguration** auf **Netzwerk**. Jegliche Änderungen, die Sie vorgenommen haben, werden sofort wirksam, ohne dass der XClarity Controller neu gestartet werden muss.

Physische Präsenz bestätigen

Mithilfe der Informationen in diesem Abschnitt können Sie die physische Präsenz von der XClarity Controller-Webseite bestätigen bzw. diese Bestätigung aufheben, ohne tatsächlich beim Server physisch anwesend zu sein.

Diese Funktion ist nur verfügbar, wenn die **Richtlinie zu physischer Präsenz** über die UEFI aktiviert wurde. Wenn sie aktiviert ist, können Sie auf die Funktion der physischen Präsenz zugreifen, indem Sie unter **BMC-Konfiguration** auf **Sicherheit** klicken.

Sicherheitsschlüsselverwaltung (SKM) konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie Sicherheitsschlüssel erstellen und verwalten.

Diese Funktion verwendet den zentralen Schlüsselverwaltungsserver, um Schlüssel zum Entsperren von Speicherhardware zur Verfügung zu stellen und so Zugriff auf Daten zu erhalten, die auf SEDs in einem ThinkSystem Server gespeichert sind. Der Schlüsselverwaltungsserver umfasst SKLM – IBM SED-Schlüsselverwaltungsserver und KMIP – Thales/Gemalto SED-Schlüsselverwaltungsserver (KeySecure und CipherTrust).

Der XClarity Controller nutzt das Netzwerk, um vom Schlüsselverwaltungsserver Schlüssel abzurufen. Daher muss der Schlüsselverwaltungsserver für den XClarity Controller zugänglich sein. Der XClarity Controller stellt den Kommunikationskanal zwischen dem Schlüsselverwaltungsserver und dem anfordernden ThinkSystem Server bereit. Die XClarity Controller-Firmware versucht, sich mit jedem konfigurierten Schlüsselverwaltungsserver zu verbinden, und wird beendet, sobald eine Verbindung erfolgreich hergestellt wird.

Der XClarity Controller stellt die Kommunikation mit dem Schlüsselverwaltungsserver her, wenn die folgenden Bedingungen erfüllt sind:

- Ein oder mehrere Hostnamen/IP-Adressen des Schlüsselverwaltungsservers sind im XClarity Controller konfiguriert.
- Zwei Zertifikate (Client und Server) sind für die Kommunikation mit dem Schlüsselverwaltungsserver im XClarity Controller installiert.

Anmerkung: Konfigurieren Sie mindestens zwei (einen primären und einen sekundären) Schlüsselverwaltungsserver mit demselben Protokoll für Ihre Einheit. Wenn der primäre Schlüsselverwaltungsserver nicht auf den Verbindungsversuch von XClarity Controller reagiert, werden Verbindungsversuche mit den zusätzlichen Schlüsselverwaltungsservern eingeleitet, bis eine erfolgreiche Verbindung hergestellt werden kann.

Zwischen XClarity Controller und Schlüsselverwaltungsserver muss eine TLS-Verbindung (Transport Layer Security) hergestellt werden. Der XClarity Controller authentifiziert den Schlüsselverwaltungsserver, indem er das Serverzertifikat, das über den Schlüsselverwaltungsserver übermittelt wurde, mit dem Schlüsselverwaltungsserverzertifikat vergleicht, das zuvor in den Truststore von XClarity Controller importiert wurde. Der Schlüsselverwaltungsserver authentifiziert jeden XClarity Controller, der mit ihm kommuniziert, und überprüft, ob der XClarity Controller auf den Schlüsselverwaltungsserver zugreifen darf. Diese Authentifizierung erfolgt durch Vergleichen des Clientzertifikats, das vom XClarity Controller übermittelt wird, mit einer Liste von vertrauenswürdigen Zertifikaten, die auf dem Schlüsselverwaltungsserver gespeichert sind.

Es wird eine Verbindung mit mindestens einem Schlüsselverwaltungsserver hergestellt; die Einheitengruppe gilt als optional. Das Schlüsselverwaltungsserverzertifikat muss importiert und das Clientzertifikat angegeben werden. Standardmäßig wird das HTTPS-Zertifikat verwendet. Wenn Sie es ersetzen möchten, können Sie ein neues generieren.

Anmerkung: Für die Verbindung mit dem KMIP-Server (KeySecure und CipherTrust) muss eine Zertifikatssignieranforderung generiert werden und ihr allgemeiner Name muss mit dem im KMIP-Server definierten Benutzernamen übereinstimmen. Importieren Sie anschließend ein Zertifikat, das von der Zertifizierungsstelle signiert wurde, die vom KMIP-Server für die Zertifikatssignieranforderung als vertrauenswürdig eingestuft wurde.

Schlüsselverwaltungsserver konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie den Hostnamen oder die IP-Adresse und die zugehörigen Portinformationen für den Schlüsselverwaltungsserver erstellen.

Der Abschnitt „Schlüsselverwaltungsserver konfigurieren“ enthält die folgenden Felder:

Hostname oder IP-Adresse
Geben Sie hier den Hostnamen (falls DNS aktiviert und konfiguriert ist) oder die IP-Adresse des Schlüsselverwaltungsservers ein. Es können bis zu vier Server hinzugefügt werden.

Port
Geben Sie hier die Portnummer für den Schlüsselverwaltungsserver ein. Wird das Feld leer gelassen, wird der Standardwert 5696 verwendet. Gültige Werte für Portnummern liegen im Bereich von 1 bis 65535.

Einheitengruppe konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie die Einheitengruppe konfigurieren, die im SKLM-Server verwendet wird.

Bei Verwendung einer Einheitengruppe im SKLM-Server können Benutzer die SED-Schlüssel („Self-Encrypting Drive“ bzw. selbstverschlüsselndes Laufwerk) auf mehreren Servern als Gruppe verwalten. Eine Einheitengruppe mit demselben Namen muss auch auf dem SKLM-Server erstellt werden.

Der Bereich „Einheitengruppe“ umfasst das folgende Feld:

Einheitengruppe

Bei Verwendung einer Einheitengruppe können Benutzer die Schlüssel für SEDs auf mehreren Servern als Gruppe verwalten. Eine Einheitengruppe mit demselben Namen muss auch auf dem SKLM-Server erstellt werden. Der Standardwert für dieses Feld lautet IBM_SYSTEM_X_SED.

Zertifikatsverwaltung einrichten

In diesem Abschnitt sind Informationen zur Verwaltung von Client- und Serverzertifikaten enthalten.

Client- und Serverzertifikate werden verwendet, um die Kommunikation zwischen SKLM-Server und XClarity Controller im ThinkSystem-Server zu authentifizieren. Die Client- und Serverzertifikatsverwaltung wird in diesem Abschnitt erläutert.

Clientzertifikate verwalten

In diesem Abschnitt sind Informationen zum Verwalten von Clientzertifikaten enthalten.

Clientzertifikate werden wie folgt klassifiziert:

- Ein von XClarity Controller selbst zugewiesenes Zertifikat.
- Ein Zertifikat, das von einer XClarity Controller-Zertifikatssignieranforderung (CSR) generiert und (extern) von einer dritten Zertifizierungsstelle signiert wurde.

Ein Clientzertifikat ist für die Kommunikation mit dem SKLM-Server erforderlich. Das Clientzertifikat enthält digitale Signaturen für die Zertifizierungsstelle und den XClarity Controller.

Anmerkungen:

- Zertifikate werden bei Firmwareaktualisierungen beibehalten.
- Wenn für die Kommunikation mit dem SKLM-Server kein Clientzertifikat erstellt wird, wird das HTTPS-Serverzertifikat von XClarity Controller verwendet.
- Die Aufgabe der Zertifizierungsstelle (CA) ist es, die Identität von XClarity Controller zu überprüfen.

Um ein Clientzertifikat zu erstellen, klicken Sie auf das Plus-Symbol ( ) und wählen Sie eines der folgenden Elemente:

- Neuen Schlüssel und selbst signiertes Zertifikat generieren
- Neuen Schlüssel und Zertifikatssignieranforderung (CSR) generieren

Das Aktionselement **Neuen Schlüssel und selbst signiertes Zertifikat generieren** generiert einen neuen Chiffrierschlüssel und ein selbst signiertes Zertifikat. Geben Sie im Fenster „Neuen Schlüssel und selbst signiertes Zertifikat generieren“ die Informationen in die erforderlichen und optionalen Felder ein, die für Ihre Konfiguration gelten (siehe folgende Tabelle). Klicken Sie auf **OK**, um den Chiffrierschlüssel und das Zertifikat zu generieren. Während das selbstsignierte Zertifikat generiert wird, erscheint ein Statusfenster. Wenn das Zertifikat erfolgreich installiert wurde, wird ein Bestätigungsfenster angezeigt.

Anmerkung: Der neue Chiffrierschlüssel und das Zertifikat ersetzen alle vorhandenen Schlüssel und Zertifikate.

Tabelle 3. Neuen Schlüssel und selbst signiertes Zertifikat generieren

In einer Tabelle aus zwei Spalten sind die erforderlichen und optionalen Felder für die Aktion „Neuen Schlüssel und selbst signiertes Zertifikat generieren“ aufgeführt. Die unterste Zeile erstreckt sich auf beide Spalten.

Tabelle 3. Neuen Schlüssel und selbst signiertes Zertifikat generieren (Forts.)

Feld	Beschreibung
Land[1]	Wählen Sie aus der Liste das Land aus, in dem sich der BMC physisch befindet.
Staat oder Bundesland[1]	Geben Sie den Staat oder das Bundesland an, in dem sich der BMC physisch befindet.
Ort oder Standort[1]	Geben Sie den Ort oder Standort an, in dem sich der BMC physisch befindet.
Name des Unternehmens[1]	Geben Sie den Namen des Unternehmen oder der Organisation ein, dem bzw. der der BMC gehört.
BMC-Hostname[1]	Geben Sie den BMC-Hostnamen ein, der in der Webadressleiste angezeigt wird.
Ansprechpartner	Geben Sie den Namen des Ansprechpartners ein, der für den BMC verantwortlich ist.
E-Mail-Adresse	Geben Sie die E-Mail-Adresse des Ansprechpartners ein, der für den BMC verantwortlich ist.
Organisationseinheit	Geben Sie die Einheit innerhalb des Unternehmens ein, zu der der BMC gehört.
Nachname	Geben Sie den Nachnamen des Ansprechpartners ein, der für den BMC verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.
Vorname	Geben Sie den Vornamen des Ansprechpartners ein, der für den BMC verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.
Initialen	Geben Sie die Initialen des Ansprechpartners ein, der für den BMC verantwortlich ist. Dieses Feld ist auf maximal 20 Zeichen begrenzt.
Qualifikationsmerkmal eines definierten Namens	Geben Sie das Qualifikationsmerkmal eines definierten Namens für den BMC ein. Dieses Feld ist auf maximal 60 Zeichen begrenzt.
1. Dies ist ein erforderliches Feld.	

Nachdem das Clientzertifikat generiert wurde, können Sie das Zertifikat in den Speicher von Ihrem XClarity Controller herunterladen, indem Sie das Aktionselement **Zertifikat herunterladen** auswählen.

Das Aktionselement **Neuen Schlüssel und Zertifikatssignieranforderung (CSR) generieren** generiert einen neuen Chiffrierschlüssel und eine Zertifikatssignieranforderung. Geben Sie im Fenster „Neuen Schlüssel und Zertifikatssignieranforderung (CSR) generieren“ die Informationen in die erforderlichen und optionalen Felder ein, die für Ihre Konfiguration gelten (siehe folgende Tabelle). Klicken Sie auf **OK**, um den neuen Chiffrierschlüssel und die Zertifikatssignieranforderung zu generieren.

Während die Zertifikatssignieranforderung generiert wird, erscheint ein Statusfenster. Nach erfolgreichem Abschluss wird ein Bestätigungsfenster angezeigt. Nachdem die Zertifikatssignieranforderung generiert wurde, müssen Sie sie zur digitalen Signierung an eine Zertifizierungsstelle senden. Wählen Sie das Aktionselement **Zertifikatssignieranforderung (CSR) herunterladen** aus und klicken Sie auf **OK**, um die Zertifikatssignieranforderung auf Ihrem Server zu sichern. Sie können die Zertifikatssignieranforderung dann zum Signieren an Ihre Zertifizierungsstelle senden.

Tabelle 4. Neuen Schlüssel und Zertifikatssignieranforderung (CSR) generieren

In einer Tabelle aus zwei Spalten sind die erforderlichen und optionalen Felder für die Aktion „Neuen Schlüssel und Zertifikatssignieranforderung (CSR) generieren“ aufgeführt. Die unterste Zeile erstreckt sich auf beide Spalten.

Tabelle 4. Neuen Schlüssel und Zertifikatssignieranforderung (CSR) generieren (Forts.)

Feld	Beschreibung
Land[1]	Wählen Sie aus der Liste das Land aus, in dem sich der BMC physisch befindet.
Staat oder Bundesland[1]	Geben Sie den Staat oder das Bundesland an, in dem sich der BMC physisch befindet.
Ort oder Standort[1]	Geben Sie den Ort oder Standort an, in dem sich der BMC physisch befindet.
Name des Unternehmens[1]	Geben Sie den Namen des Unternehmen oder der Organisation ein, dem bzw. der der BMC gehört.
BMC-Hostname[1]	Geben Sie den BMC-Hostnamen ein, der in der Webadressleiste angezeigt wird.
Ansprechpartner	Geben Sie den Namen des Ansprechpartners ein, der für den BMC verantwortlich ist.
E-Mail-Adresse	Geben Sie die E-Mail-Adresse des Ansprechpartners ein, der für den BMC verantwortlich ist.
Organisationseinheit	Geben Sie die Einheit innerhalb des Unternehmens ein, zu der der BMC gehört.
Nachname	Geben Sie den Nachnamen des Ansprechpartners ein, der für den BMC verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.
Vorname	Geben Sie den Vornamen des Ansprechpartners ein, der für den BMC verantwortlich ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.
Initialen	Geben Sie die Initialen des Ansprechpartners ein, der für den BMC verantwortlich ist. Dieses Feld ist auf maximal 20 Zeichen begrenzt.
Qualifikationsmerkmal eines definierten Namens	Geben Sie das Qualifikationsmerkmal eines definierten Namens für den BMC ein. Dieses Feld ist auf maximal 60 Zeichen begrenzt.
Kennwort abfragen	Geben Sie das Kennwort für die Zertifikatssignieranforderung ein. Dieses Feld ist auf maximal 30 Zeichen begrenzt.
Unstrukturierter Name	Geben Sie zusätzliche Informationen an, etwa einen unstrukturierten Namen, der dem BMC zugewiesen ist. Dieses Feld ist auf maximal 60 Zeichen begrenzt.
1. Dies ist ein erforderliches Feld.	

Die Zertifikatssignieranforderung wird von der Zertifizierungsstelle mithilfe des Zertifikatverarbeitungstools des Benutzers, z. B. **OpenSSL** oder das Befehlszeilentool **Certutil**, digital signiert. Alle Clientzertifikate, die mithilfe des Zertifikatverarbeitungstools des Benutzers signiert werden, verfügen über das gleiche **Basiszertifikat**. Dieses **Basiszertifikat** muss ebenfalls auf den SKLM-Server importiert werden, sodass alle Server, die vom Benutzer digital signiert wurden, vom SKLM-Server akzeptiert werden.

Nachdem das Zertifikat von der Zertifizierungsstelle signiert wurde, müssen Sie es in den BMC importieren. Klicken Sie auf das Aktionselement **Signiertes Zertifikat importieren** und wählen Sie die Datei aus, die als Clientzertifikat hochgeladen werden soll. Klicken Sie dann auf **OK**. Während das von der Zertifizierungsstelle signierte Zertifikat hochgeladen wird, erscheint ein Statusfenster. Wenn dieser Vorgang erfolgreich war, wird

das Fenster „Zertifikat hochladen“ angezeigt. Wenn das Hochladen nicht erfolgreich war, wird in einem Fenster darauf hingewiesen, dass beim Hochladen ein Fehler aufgetreten ist.

Anmerkungen:

- Um die Sicherheit zu erhöhen, verwenden Sie ein Zertifikat, das von einer Zertifizierungsstelle digital signiert wird.
- Das Zertifikat, das in XClarity Controller importiert wird, muss der Zertifikatssignieranforderung entsprechen, die zuvor generiert wurde.

Nachdem ein von einer Zertifizierungsstelle signiertes Zertifikat in den BMC importiert wurde, wählen Sie das Aktionselement **Zertifikat herunterladen** aus. Wenn Sie dieses Aktionselement auswählen, wird das von der Zertifizierungsstelle signierte Zertifikat von XClarity Controller heruntergeladen und in Ihrem System gespeichert.

Serverzertifikate verwalten

Dieser Abschnitt enthält Informationen zur Verwaltung von Serverzertifikaten.

Das Serverzertifikat wird im SKLM-Server generiert und muss in den XClarity Controller importiert werden, bevor die Funktionalität für den sicheren Laufwerkszugriff funktioniert. Um das Zertifikat zu importieren, das den SKLM-Server zum BMC authentifiziert, klicken Sie im Abschnitt zum Serverzertifikatstatus auf der Seite „Laufwerkszugriff“ auf **Zertifikat importieren**. Während die Datei in den Speicher von XClarity Controller übertragen wird, wird eine Statusanzeige angezeigt.

Nachdem das Serverzertifikat erfolgreich zum XClarity Controller übertragen wurde, wird der Bereich mit dem Status des Serverzertifikats mit folgendem Inhalt angezeigt: `A server certificate is installed.`

Wenn Sie ein vertrauenswürdiges Zertifikat entfernen möchten, klicken Sie auf die entsprechende Schaltfläche **Entfernen**.

Erweitertes Prüfprotokoll

Mithilfe der Informationen in diesem Abschnitt können Sie das erweiterte Prüfprotokoll steuern.

Mit dieser Funktion können Sie entscheiden, ob die Protokolleinträge des IPMI-Befehls „set“ (Rohdaten) aus LAN- und KCS-Kanälen in das Prüfprotokoll aufgenommen werden sollen.

Klicken Sie in der XCC-Webschnittstelle unter **BMC-Konfiguration** auf **Sicherheit**, um das erweiterte Prüfprotokoll zu aktivieren/deaktivieren.

Anmerkung: Wenn der IPMI-Befehl „set“ aus dem LAN-Kanal stammt, sind Benutzername und Quell-IP-Adresse in der Protokollnachricht enthalten. Alle IPMI-Befehle mit sensiblen Sicherheitsinformationen (z. B. Kennwort) werden ausgeschlossen.

Verschlüsselungseinstellung

In diesem Thema werden die verschiedenen Verschlüsselungseinstellungen erläutert.

Hochsicherheitsmodus

- Nur moderne und starke Verschlüsselungscodes werden unterstützt
- NIST-konform
- PFS-konform (Perfect Forward Secrecy)

Kompatibilitätsmodus

- Unterstützt eine Vielzahl unterschiedlicher Cipher-Suites für maximale Kompatibilität
- Nicht PFS- und nicht NIST-konform

NIST-konformer Modus

- Unterstützt eine Vielzahl unterschiedlicher Cipher-Suites für maximale Kompatibilität
- NIST-konform
- PFS-konform

Unterstützung für TLS-Versionen

- TLS 1.0 und höher
- TLS 1.1 und höher
- TLS 1.2 und höher
- TLS 1.3

Die TLS-Verschlüsselungseinstellung dient dazu, die unterstützten TLS-Cipher-Suites auf BMC-Services zu beschränken.

Die verschiedenen von TLS Cipher-Suites unterstützten Einstellungen finden Sie in der folgenden Tabelle.

Sicherheits-modus	TLS-Version	TLS-Cipher-Suites
Hochsicher-heitsmodus	TLS 1.3 und niedriger	• TLS_AES_256_GCM_SHA384
Hochsicher-heitsmodus	TLS 1.2 und niedriger	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
NIST-konformer Modus	TLS 1.3 und niedriger	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256
NIST-konformer Modus	TLS 1.2 und niedriger	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

Sicherheits-modus	TLS-Version	TLS-Cipher-Suites
Kompatibilitätsmodus	TLS 1.3 und niedriger	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256
Kompatibilitätsmodus	TLS 1.2 und niedriger	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
Kompatibilitätsmodus	TLS 1.1 und niedriger	• TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

BMC-Konfiguration sichern und wiederherstellen

In diesem Abschnitt wird beschrieben, wie Sie die BMC-Konfiguration wiederherstellen oder ändern.

Wählen Sie **Sicherung und Wiederherstellung** unter **BMC-Konfiguration**, um die folgenden Aktionen auszuführen:

- Anzeigen einer Zusammenfassung der Management-Controller-Konfiguration
- Sichern oder Wiederherstellen der Management-Controller-Konfiguration
- Anzeigen des Sicherungs- oder Wiederherstellungsstatus
- Zurücksetzen der Management-Controller-Konfiguration auf die Werkseinstellungen
- Aufrufen des Assistenten für die Management-Controller-Erstkonfiguration

BMC-Konfiguration sichern

In diesem Abschnitt wird beschrieben, wie Sie Ihre BMC-Konfiguration sichern.

Wählen Sie **Sicherung und Wiederherstellung** unter **BMC-Konfiguration**. Ganz oben sehen Sie den Abschnitt **BMC-Konfiguration sichern**.

Wenn zuvor eine Sicherung erstellt wurde, werden die zugehörigen Details im Feld **Letzte Sicherung** angezeigt.

Um die aktuelle BMC-Konfiguration zu sichern, führen Sie die folgenden Schritte aus:

1. Legen Sie das Kennwort für die BMC-Sicherungsdatei fest.
2. Geben Sie an, ob die ganze Datei oder nur sensible Daten verschlüsselt werden sollen.
3. Starten Sie den Sicherungsvorgang durch Klicken auf **Sicherung starten**. Während des Vorgangs können Sie keine Aktionen zum Wiederherstellen/Zurücksetzen ausführen.
4. Wenn der Vorgang abgeschlossen ist, wird eine Schaltfläche angezeigt, über die Sie die Datei herunterladen und speichern können.

Anmerkung: Wenn der Benutzer einen neuen XClarity Controller-Benutzer sowie das zugehörige Kennwort einrichtet und eine Sicherung der Konfiguration erstellt, werden Standardaccount und -kennwort (`USERID/PASSWORD`) ebenfalls aufgenommen. Wenn anschließend Standardaccount und -kennwort aus der Sicherung gelöscht werden, zeigt das System eine Meldung mit dem Hinweis an, dass bei der Wiederherstellung des XClarity Controller-Accounts und -Kennworts ein Fehler aufgetreten ist. Benutzer können diese Meldung ignorieren.

BMC-Konfiguration wiederherstellen

In diesem Abschnitt wird beschrieben, wie Sie die BMC-Konfiguration wiederherstellen.

Wählen Sie **Sicherung und Wiederherstellung** unter **BMC-Konfiguration**. Unter **BMC-Konfiguration sichern** befindet sich der Abschnitt **BMC aus Konfigurationsdatei wiederherstellen**.

Um den BMC auf eine zuvor gespeicherte Konfiguration wiederherzustellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Backup-Datei aus und geben Sie das Kennwort ein, wenn Sie dazu aufgefordert werden.
2. Überprüfen Sie die Datei durch Klicken auf **Inhalt anzeigen**, um die Details anzuzeigen.
3. Nachdem Sie den Inhalt überprüft haben, klicken Sie auf **Wiederherstellung starten**.

BMC auf werkseitige Voreinstellungen zurücksetzen

In diesem Abschnitt wird beschrieben, wie der BMC auf die Werkseinstellungen zurückgesetzt wird.

Wählen Sie **Sicherung und Wiederherstellung** unter **BMC-Konfiguration**. Unter **BMC aus Konfigurationsdatei wiederherstellen** befindet sich der Abschnitt **BMC auf Werkseinstellungen zurücksetzen**.

Um den BMC auf die Werkseinstellungen zurückzusetzen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Zurücksetzen des BMC auf werkseitige Voreinstellungen starten**.

   Anmerkungen:

   - Nur Benutzer mit der Benutzerberechtigungsstufe „Supervisor“ können diese Aktion ausführen.
   - Die Ethernet-Verbindung wird vorübergehend getrennt. Sie müssen sich erneut bei der XClarity Controller-Webschnittstelle anmelden, nachdem das Zurücksetzen abgeschlossen ist.
   - Wenn Sie auf **Zurücksetzen des BMC auf werkseitige Voreinstellungen starten** klicken, gehen alle vorherigen Konfigurationsänderungen verloren. Wenn Sie LDAP bei der Wiederherstellung der BMC-Konfiguration aktivieren möchten, müssen Sie zuerst ein vertrauenswürdigen Sicherheitszertifikat importieren.
   - Nach Abschluss des Vorgangs wird der XClarity Controller neu gestartet. Wenn es sich um einen lokalen Server handelt, wird Ihre TCP/IP-Verbindung unterbrochen und Sie müssen die Netzwerkschnittstelle möglicherweise erneut konfigurieren, um wieder eine funktionsfähige Verbindung herzustellen.

- Das Zurücksetzen des BMC auf werkseitige Voreinstellungen wirkt sich nicht auf die UEFI-Einstellungen aus.

XClarity Controller neu starten

In diesem Abschnitt wird erläutert, wie Sie den XClarity Controller neu starten.

Weitere Informationen zum Neustart vom XClarity Controller finden Sie unter „Stromversorgungsaktionen“ auf Seite 66.

Kapitel 4. Serverstatus überwachen

Mithilfe der Informationen in diesem Abschnitt erfahren Sie, wie Sie Informationen zum Server, auf den Sie zugreifen, anzeigen und überwachen können.

Nachdem Sie sich beim XClarity Controller angemeldet haben, wird eine Systemstatusseite angezeigt. Auf dieser Seite können Sie den Server-Hardwarestatus, Ereignis- und Prüfprotokolle, den Systemstatus, den Wartungsverlauf und Alertempfänger anzeigen.

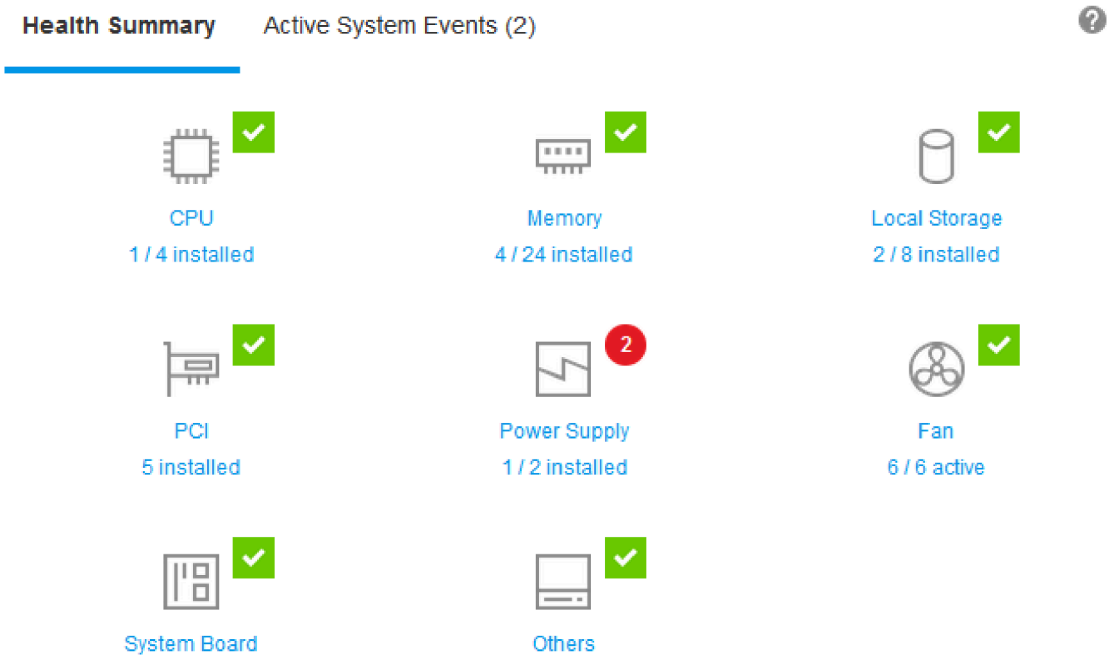
Hardwarezustand/aktive Systemereignisse anzeigen

Verwenden Sie die Informationen in diesem Abschnitt, um zu erfahren, wie Sie den Hardwarezustand bzw. aktive Systemereignisse anzeigen.

Wenn Sie die XClarity Controller-Startseite aufrufen, wird standardmäßig eine **Zustandszusammenfassung** angezeigt. In einer grafischen Darstellung wird die Anzahl der installierten Hardwarekomponenten mit ihrem jeweiligen Zustand angezeigt. Es werden folgende Hardwarekomponenten überwacht:

- Prozessor (CPU)
- Speicher
- Lokaler Speicher
- PCI-Adapter
- Netzteil
- Lüfter
- Systemplatine
- Sonstiges

Anmerkung: Lokaler Speicher zeigt bei Systemen mit einer Simple-Swap-Rückwandplatinen-Konfiguration auf dem Statussymbol möglicherweise „nicht verfügbar“ an.



Wenn eine der Hardwarekomponenten nicht ordnungsgemäß funktioniert, wird sie durch entsprechende Symbole (Kritisch oder Warnung) gekennzeichnet. Ein kritischer Zustand wird durch einen roten Kreis angegeben und eine Warnungsbedingung durch ein gelbes Dreieck. Wenn Sie mit der Maus über das Symbol für den kritischen oder Warnzustand fahren, werden bis zu drei aktuell aktive Ereignisse für die jeweilige Komponente angezeigt.

Um die anderen Ereignisse anzuzeigen, klicken Sie auf die Registerkarte **Aktive Systemereignisse**. In einem Fenster werden die Ereignisse angezeigt, die derzeit im System aktiv sind. Klicken Sie auf **Alle Ereignisprotokolle anzeigen**, um den gesamten Ereignisverlauf anzuzeigen.

Wenn die Hardwarekomponente durch ein grünes Häkchen gekennzeichnet ist, funktioniert sie ordnungsgemäß und es liegen keine aktiven Ereignisse vor.

Im Text unter den Zuständen der Hardwarekomponenten wird die Anzahl der installierten Komponenten angezeigt. Wenn Sie auf den Text klicken, werden Sie zur Seite **Bestand** geleitet.

Systeminformationen anzeigen

In diesem Abschnitt wird erläutert, wie Sie eine Zusammenfassung allgemeiner Serverinformationen abrufen.

Der Bereich **Systeminformationen und Einstellungen** links auf der Startseite enthält eine Zusammenfassung allgemeiner Serverinformationen wie z. B.:

- Maschinenname, Stromversorgungs- und Betriebssystemstatus
- Maschinentyp/-modell
- Seriennummer
- Systemname
- Eigentumsrecht vorderer USB-Anschluss
- BMC-Lizenz
- BMC-IP-Adresse
- BMC-Hostname
- UEFI-Version
- BMC-Version
- LXPM-Version
- Position

Der Server kann sich in einem der Systemstatus befinden, die in der folgenden Tabelle aufgeführt sind.

Tabelle 5. Systemstatusbeschreibungen

Zweispaltige Tabelle mit Überschriften, die den Systemstatus des Servers dokumentieren.

Status	**Beschreibung**
Stromversorgung des Systems ausgeschaltet/Status unbekannt	Der Server ist ausgeschaltet.
System eingeschaltet/UEFI wird gestartet	Der Server ist eingeschaltet, aber die UEFI wird noch nicht ausgeführt.
System wird in UEFI ausgeführt	Der Server ist eingeschaltet und die UEFI wird ausgeführt.
System wurde in UEFI gestoppt	Der Server ist eingeschaltet; die UEFI hat einen Fehler erkannt und ihre Ausführung wurde beendet.
Betriebssystem wird gestartet oder Betriebssystem wird nicht unterstützt	Der Server kann sich aus einem der folgenden Gründe in diesem Status befinden: • Das Ladeprogramm des Betriebssystems wurde gestartet, aber das Betriebssystem wird nicht ausgeführt. • Die Ethernet-over-USB-Schnittstelle des BMC ist deaktiviert. • Das Betriebssystem hat die Treiber, die die Ethernet-over-USB-Schnittstelle unterstützen, nicht geladen.
Betriebssystem gestartet	Das Serverbetriebssystem wird ausgeführt.
Aussetzen in RAM	Der Server wurde in den Bereitschafts- oder Ruhemodus versetzt.
System wird im Hauptspeichertest ausgeführt	Der Server ist eingeschaltet und Speicherdiagnosetools werden ausgeführt.
System wird in der Konfiguration ausgeführt	Der Server ist eingeschaltet und das System wurde im UEFI-F1-Konfigurationsmenü oder im LXPM-Menü gestartet.
System wird im LXPM-Wartungsmodus ausgeführt	Der Server ist eingeschaltet und das System wurde im LXPM-Wartungsmodus gestartet, in dem Benutzer nicht im LXPM-Menü navigieren können.

Wenn Sie den Systemnamen ändern möchten, klicken Sie auf das Stiftssymbol. Geben Sie den Systemnamen ein, den Sie verwenden möchten, und klicken Sie dann auf das grüne Häkchen.

Wenn Sie das Eigentumsrecht am vorderen USB-Anschluss ändern möchten, klicken Sie auf das Stiftssymbol und wählen Sie den gewünschten Modus für **Eigentumsrecht vorderer USB-Anschluss** aus dem Dropdown-Menü aus. Klicken Sie anschließend auf das grüne Häkchen.

Wenn Ihr Server über eine andere Lizenz verfügt als die XClarity Controller Enterprise-Lizenz, können Sie möglicherweise ein Lizenzupgrade erwerben, um von erweiterten Funktionen zu profitieren. Um die Upgradelizenz nach Erhalt zu installieren, klicken Sie auf den nach oben zeigenden Pfeil.

Um eine Lizenz hinzuzufügen, zu löschen oder zu exportieren, klicken Sie auf den nach rechts zeigenden Pfeil.

Um die relevanten Einstellungen für die IP-Adresse des BMC, den BMC-Hostnamen, die UEFI-Version, die BMC-Version und die Positionselemente zu ändern, klicken Sie auf den nach rechts zeigenden Pfeil.

- Für die IP-Adresse und den Hostnamen werden Sie zum Abschnitt **Ethernet-Konfiguration** unter **Netzwerk** geleitet.
- Für die UEFI- und BMC-Versionen werden Sie zur Seite **Firmwareaktualisierung** geleitet.
- Für die Positionselemente werden Sie zum Abschnitt **Servereigenschaften** auf der Seite **Serverkonfiguration** geleitet.

Systemauslastung anzeigen

Wenn Sie im linken Bereich auf **Auslastung** klicken, wird eine Zusammenfassung der allgemeinen Serverauslastungsinformationen angezeigt.

Die Systemauslastung ist eine zusammengefasste Metrik auf Grundlage der Echtzeitauslastung von Prozessor, Speicher und E/A-Subsystemen. Die Auslastungsdaten stammen alle von der ME-Seite (Node Manager), die Folgendes umfasst:

- **CPU-Auslastung**
  - Aggregierter C-State
  - Gemessene Zeit in C0 als Prozentsatz des verwendeten und maximalen C0-State-Werts (pro Sekunde).
- **Hauptspeichernutzung**

  - Aggregierter R/W-Umfang aller Speicherkanäle.
  - Gemessene Bandbreite, berechnet als Prozentsatz der verwendeten und maximal verfügbaren Speicherbandbreite (pro Sekunde).
- **E/A-Auslastung**
  - Aggregierter R/W-Umfang der Rootanschlüsse beim PCIe*-Bus.
  - Gemessene Bandbreite, berechnet als Prozentsatz der verwendeten und maximal verfügbaren E/A-Bandbreite (pro Sekunde).

Ereignisprotokolle anzeigen

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

Wählen Sie auf der Registerkarte **Events** die Option **Ereignisprotokoll** aus, um die Seite **Ereignisprotokoll** anzuzeigen. Alle Ereignisse im Protokoll haben eine Zeitmarke, für die die XClarity Controller-Einstellungen für Datum und Uhrzeit verwendet wurden. Einige Ereignisse generieren beim Auftreten außerdem Alerts, falls dies im **Alarmempfänger** so konfiguriert wurde. Sie können Ereignisse im Ereignisprotokoll sortieren und filtern.

Im Folgenden finden Sie eine Beschreibung der Aktionen, die auf der Seite **Ereignisprotokoll** durchgeführt werden können.

- **Tabelle anpassen**: Wählen Sie dieses Aktionselement aus, um den Typ der Informationen auszuwählen, der in der Tabelle angezeigt werden soll. Eine Folgenummer kann angezeigt werden, um die Reihenfolge von Ereignissen zu ermitteln, wenn mehr als ein Ereignis denselben Zeitstempel hat.

  Anmerkung: Einige Folgenummern werden von internen BMC-Prozessen verwendet, es ist also normal, dass es möglicherweise Lücken in den Folgenummern gibt, wenn die Ereignisse durch Folgenummern sortiert werden.
- **Protokolle löschen**: Wählen Sie dieses Aktionselement aus, um die Ereignisprotokolle zu löschen.
- **Aktualisieren**: Wählen Sie dieses Aktionselement aus, um die Anzeige mit Ereignisprotokolleinträgen zu aktualisieren, die möglicherweise seit der letzten Anzeige der Seite aufgetreten sind.
- **Typ**: Wählen Sie aus, welcher Ereignistyp angezeigt werden soll. Zu den Ereignistypen gehören:

   zeigt Fehlereinträge im Protokoll an

   zeigt Warnungseinträge im Protokoll an

   zeigt Informationseinträge im Protokoll an

  Klicken Sie auf das jeweilige Symbol, um die Fehlertypen, die angezeigt werden sollen, ein- oder auszuschalten. Wenn Sie hintereinander auf das Symbol klicken, werden die Ereignisse angezeigt bzw. nicht angezeigt. Ein blauer Kasten um das Symbol gibt an, dass der Ereignistyp angezeigt wird.
- **Quelltypfilter**: Wählen Sie ein Element aus dem Dropdown-Menü aus, um nur den Typ der Ereignisprotokolleinträge anzuzeigen, die angezeigt werden sollen.
- **Zeitfilter**: Wählen Sie dieses Aktionselement aus, um das Intervall der Ereignisse anzugeben, die Sie anzeigen möchten.

- **Suchen**: Um nach bestimmten Ereignistypen oder Suchbegriffen zu suchen, klicken Sie auf das Lupensymbol, und geben Sie in das Feld **Suchen** das zu suchende Wort ein. Beachten Sie, dass bei der Eingabe die Groß-/Kleinschreibung beachtet wird.

Anmerkung: Die maximale Anzahl an Einträgen im Ereignisprotokoll ist 1024. Wenn die Ereignisprotokolle voll sind, überschreibt der neue Protokolleintrag automatisch den ältesten.

Prüfprotokolle anzeigen

Das **Prüfprotokoll** stellt eine historische Aufzeichnung aller Benutzeraktionen bereit, z. B. das Anmelden bei XClarity Controller, Erstellen eines neuen Benutzers und Ändern eines Benutzerkennworts.

Sie können das Prüfprotokoll verwenden, um die Authentifizierung, Änderungen und Systemaktionen zu dokumentieren.

Das Ereignisprotokoll und das Prüfprotokoll unterstützen ähnliche Wartungs- und Anzeigeaktionen. Eine Beschreibung der Anzeige- und Filteraktionen, die auf der Seite „Prüfprotokoll“ durchgeführt werden können, finden Sie unter „Ereignisprotokolle anzeigen“ auf Seite 57.

Anmerkungen:

- Nach Ausführung der Lenovo Tools auf dem Serverbetriebssystem kann es sein, dass das Prüfprotokoll Datensätze enthält, die durch einen Benutzernamen (z. B. Benutzer „20luN4SB“) ausgeführte Aktionen darstellen, die Sie eventuell nicht erkennen. Wenn einige dieser Tools auf dem Serverbetriebssystem ausgeführt werden, erstellen sie möglicherweise einen temporären Benutzeraccount für den Zugriff auf XClarity Controller. Der Account wird mit einem willkürlichen Benutzernamen und Kennwort erstellt und kann nur für den Zugriff auf XClarity Controller auf der internen Ethernet-over-USB-Schnittstelle verwendet werden. Der Account kann nur verwendet werden, um auf die CIM-XML- und SFTP-Schnittstellen von XClarity Controller zuzugreifen. Das Erstellen und Entfernen dieses temporären Accounts wird im Prüfprotokoll erfasst, ebenso wie alle Aktionen, die von dem Tool mit diesen Berechtigungen ausgeführt werden.
- Die maximale Anzahl an Einträgen im Prüfprotokoll ist 1024. Wenn die Prüfprotokolle voll sind, überschreibt der neue Protokolleintrag automatisch den ältesten.

Wartungsverlauf anzeigen

Die Seite **Wartungsverlauf** enthält Informationen über die Firmwareaktualisierung, Konfigurations- und Hardwareaustauschprotokolle.

Die Inhalte des Wartungsverlauf können gefiltert werden, um bestimmte Ereignistypen oder bestimmte Zeitintervalle anzuzeigen.

Anmerkung: Die maximale Anzahl an Einträgen im Wartungsverlauf ist 250. Wenn die Wartungsverlaufsprotokolle voll sind, überschreibt der neue Protokolleintrag automatisch den ältesten.

Alertempfänger konfigurieren

Verwenden Sie die Informationen in diesem Abschnitt, um E-Mail- und Syslog-Benachrichtigungen oder SNMP TRAP-Empfänger hinzuzufügen und zu ändern.

Im Folgenden finden Sie eine Beschreibung der Aktionen, die auf der Registerkarte **Alarmempfänger** durchgeführt werden können.

Die folgenden Aktionselemente können im Empfängerabschnitt **E-Mail/Syslog** ausgeführt werden.

- **Erstellen**: Wählen Sie dieses Aktionselement aus, um weitere neue E-Mail-Empfänger und Syslog-Empfänger zu erstellen. Es können bis zu 12 E-Mail- und Syslog-Empfänger konfiguriert werden.
  - **E-Mail-Empfänger erstellen**: Wählen Sie dieses Aktionselement aus, um einen E-Mail-Empfänger zu erstellen.
    - Geben Sie den Namen und die E-Mail-Adresse des Empfängers ein.
    - Wählen Sie diese Option aus, um die Ereignisbenachrichtigung zu aktivieren oder deaktivieren. Wenn die Option deaktiviert ist, bleibt der Account konfiguriert, es werden aber keine E-Mails gesendet.
    - Wählen Sie die Ereignistypen aus, über die der Empfänger benachrichtigt wird. Wenn Sie auf das Dropdown-Menü neben den Kategoriebezeichnungen „Critical“, „Attention“ oder „System“ klicken, können Sie Benachrichtigungen für bestimmte Komponenten in der Kategorie auswählen bzw. die Auswahl aufheben.
    - Sie können auswählen, ob die Ereignisprotokollinhalte im E-Mail-Alert enthalten sein sollen oder nicht.
    - Der Index gibt an, welcher der 12 Empfängerslots zugeordnet ist.
    - Sie können den E-Mail-Server, an den die Ereignisse weitergeleitet werden, hier oder durch Klicken auf die SMTP-Server-Aktion oben im Abschnitt konfigurieren. Konfigurationsdetails finden Sie unter SMTP-Server.
  - **Syslog-Empfänger erstellen**: Wählen Sie dieses Aktionselement aus, um einen Syslog-Empfänger zu erstellen.
    - Geben Sie den Namen und die IP-Adresse oder den Hostnamen des Syslog-Servers an.
    - Wählen Sie diese Option aus, um die Ereignisbenachrichtigung zu aktivieren oder deaktivieren. Wenn die Option deaktiviert ist, bleibt der Account konfiguriert, es werden aber keine E-Mails gesendet.
    - Der Index gibt an, welcher der 12 Empfängerslots zugeordnet ist.
    - Wählen Sie die Ereignistypen aus, die an den Syslog-Server gesendet werden. Wenn Sie auf das Dropdown-Menü neben den Kategoriebezeichnungen „Critical“, „Attention“ oder „System“ klicken, können Sie Benachrichtigungen für bestimmte Komponenten in der Kategorie auswählen bzw. die Auswahl aufheben.
- **SMTP-Server**: Wählen Sie dieses Aktionselement aus, um die relevanten Einstellungen für den SMTP-E-Mail-Server zu konfigurieren. Es kann nur ein E-Mail-Server konfiguriert werden. Dieselbe E-Mail-Konfiguration wird verwendet, wenn Alerts an alle konfigurierten E-Mail-Empfänger gesendet werden. Der BMC schaltet automatisch über den STARTTLS-Befehl gleichmäßig über Port 587 von einer sicheren Verbindung zu einer verschlüsselten Verbindung für die E-Mail-Übertragung um, wenn der Ziel-Mailserver dies unterstützt.
  - Geben Sie den Hostnamen oder die IP-Adresse und die Netzwerkanschlussnummer des E-Mail-Servers an.
  - Wenn der E-Mail-Server eine Authentifizierung erfordert, aktivieren Sie das Kontrollkästchen **Authentifizierung erforderlich** und geben Sie den Benutzernamen und das Kennwort ein. Wählen Sie den Typ der Authentifizierung aus, die vom E-Mail-Server benötigt wird: entweder eine Challenge/Response-Methode (**CRAM-MD5**) oder einfache Anmeldeinformationen (**LOGIN**).
  - Einige Netzwerke blockieren möglicherweise ausgehende E-Mails, wenn der Wert des umgekehrten Pfads nicht wie erwartet lautet. Standardmäßig verwendet der XClarity Controller alertmgr@domain, wobei der Domänenname wie im DDNS-Abschnitt der XClarity Controller-Netzwerkwebseite lautet. Sie können Ihre eigenen Absenderinformationen anstelle des Standards angeben.
  - Sie können die Verbindung zum E-Mail-Server testen, um sicherzustellen, dass die E-Mail-Einstellungen ordnungsgemäß konfiguriert wurden. Der XClarity Controller zeigt eine Nachricht an, in der angegeben wird, ob die Verbindung erfolgreich ist.

- **Wiederholung und Verzögerung**: Wählen Sie dieses Aktionselement aus, um die relevanten Einstellungen für die Optionen „Wiederholung“ und „Verzögerung“ zu konfigurieren.
  - Das Wiederholungslimit gibt an, wie oft der XClarity Controller versucht, einen Alert zu senden, wenn der ursprüngliche Versuch nicht erfolgreich war.
  - Die Verzögerung zwischen Einträgen gibt an, wie lange der XClarity Controller wartet, nachdem ein Alert an einen Empfänger gesendet wurde, bevor ein Alert an den nächsten Empfänger gesendet wird.
  - Die Verzögerung zwischen den Versuchen gibt an, wie lange der XClarity Controller nach einem misslungenen Versuch wartet, bevor er erneut versucht, den Alert zu senden.
- **Protokoll**: Wählen Sie dieses Aktionselement aus, um die relevanten Einstellungen für das Verbindungsprotokoll zu konfigurieren.
  - Sie können **TCP-Protokoll** und **UDP-Protokoll** auswählen. Beachten Sie, dass diese Einstellung für alle syslog-Empfänger angewendet wird.
- Wenn E-Mail- oder Syslog-Empfänger erstellt wurden, werden sie in diesem Abschnitt aufgelistet.
  - Um die Einstellungen für einen E-Mail- oder Syslog-Empfänger zu bearbeiten, klicken Sie auf das Stiftsymbol unter der Aktionsüberschrift auf der Zeile neben dem Empfänger, den Sie konfigurieren möchten.
  - Klicken Sie auf das Papierkorbsymbol, um einen E-Mail- oder Syslog-Empfänger zu löschen.
  - Klicken Sie auf das Papierflugzeugsymbol, um einen Test-Alert an einen E-Mail- oder Syslog-Empfänger zu senden.

Die folgenden Aktionen können im Benutzersegment **SNMPv3** durchgeführt werden.

- **Erstellen**: Wählen Sie dieses Aktionselement aus, um SNMPv3 TRAP-Empfänger zu erstellen.
  - Wählen Sie den Benutzeraccount aus, der den SNMPv3-Traps zugeordnet werden soll. Der Benutzeraccount muss einer der zwölf lokalen Benutzeraccounts sein.
  - Geben Sie den Hostnamen oder die IP-Adresse des SNMPv3-Managers an, der die SNMPv3-Traps empfangen wird.
  - Der XClarity Controller verwendet den HMAC-SHA-Hashalgorithmus, um eine Authentifizierung mit dem SNMPv3-Manager durchzuführen. Dies ist der einzige unterstützte Algorithmus.
  - Das Datenschutzkennwort wird mit dem Datenschutzprotokoll verwendet, um die SNMP-Daten zu verschlüsseln.
  - Die **globale SNMPv3-Einstellungen** gilt für alle SNMPv3 TRAP-Empfänger. Diese Einstellungen können beim Erstellen eines SNMPv3 TRAP-Empfängers oder durch Klicken auf die Aktion „SNMPv3-Einstellungen“ oben im Benutzersegment **SNMPv3** konfiguriert werden.
    - Wählen Sie die Einstellung aus, um SNMPv3 Traps zu aktivieren oder zu deaktivieren. Wenn die Einstellungen deaktiviert sind, bleiben sie konfiguriert, es werden aber keine SNMPv3-Traps gesendet.
    - Die Informationen zum BMC-Kontakt und Standort sind erforderlich und werden auf der Webseite „Serverkonfiguration“ konfiguriert. Weitere Informationen hierzu finden Sie im Abschnitt „Position und Kontakt festlegen“ auf Seite 85.
    - Wählen Sie die Ereignistypen aus, die dafür sorgen, dass TRAPs an den SNMPv3-Manager gesendet werden. Wenn Sie auf das Dropdown-Menü neben den Kategoriebezeichnungen „Critical“, „Attention“ oder „System“ klicken, können Sie Benachrichtigungen für bestimmte Komponenten in der Kategorie auswählen bzw. die Auswahl aufheben.

  Anmerkung: Die Datenübertragung zwischen dem SNMP-Client und dem -Agenten kann mithilfe von Verschlüsselung geschützt werden. Die unterstützten Methoden für das **Datenschutzprotokoll** sind CBC-DES und AES.

- Wenn SNMPv3-Trap-Empfänger erstellt wurden, werden sie in diesem Abschnitt aufgelistet.
  - Um die Einstellungen für einen SNMPv3-Empfänger zu bearbeiten, klicken Sie auf das Stiftsymbol unter der Aktionsüberschrift auf der Zeile neben dem Empfänger, den Sie konfigurieren möchten.
  - Klicken Sie auf das Papierkorbsymbol, um einen SNMPv3-Empfänger zu löschen.

Daten der letzten Betriebssystem-Fehleranzeige erfassen

Mithilfe der Informationen in diesem Abschnitt können Sie eine Betriebssystem-Fehleranzeige erfassen und anzeigen.

Die Betriebssystemanzeige wird automatisch erfasst, wenn das Zeitlimit des BS-Watchdogs erreicht ist. Wenn ein Ereignis eintritt, das zum Beenden des Betriebssystems führt, wird der BS-Watchdog ausgelöst und die Bildschirminhalte werden erfasst. XClarity Controller speichert nur einen Screenshot. Wenn das Zeitlimit des BS-Watchdogs erreicht ist, wird der vorherige Screenshot durch einen neuen Screenshot überschrieben. Die Funktion des Betriebssystem-Watchdogs muss aktiviert sein, damit Sie die Betriebssystem-Fehleranzeige erfassen können. Informationen zum Festlegen der BS-Watchdog-Zeit finden Sie unter „Serverzeitlimits festlegen“ auf Seite 86. Die Betriebssystem-Fehleranzeige steht nur mit XClarity Controller Advanced oder Enterprise Level zur Verfügung. Weitere Informationen zu der auf Ihrem Server installierten XClarity Controller-Funktionalität finden Sie in der Dokumentation für Ihren Server.

Klicken Sie im Abschnitt **Ferne Konsole** der XClarity Controller-Startseite auf **Letzte Fehleranzeige**, um ein Bild der Betriebssystemanzeige anzuzeigen, das aufgezeichnet wurde, als das Zeitlimit des BS-Watchdogs erreicht wurde. Sie können den Screenshot auch anzeigen, indem Sie auf **Service** und dann auf **Letzte Fehleranzeige** im Abschnitt **Schnelle Aktion** der Startseite klicken. Wenn im System noch keine Zeitlimitüberschreitung des BS-Watchdogs aufgetreten ist und es die Betriebssystemanzeige erfasst hat, wird in einer Nachricht gemeldet, dass die Fehleranzeige nicht erstellt wurde.

Kapitel 5. Server konfigurieren

Verwenden Sie die Informationen in diesem Kapitel, um mehr über die für Serverkonfigurationen verfügbaren Optionen zu erfahren.

Bei der Konfiguration des Servers sind die folgenden Optionen verfügbar:

- Adapter
- Boot-Optionen
- Stromversorgungsrichtlinie
- Servereigenschaften

Adapterinformationen und Konfigurationseinstellungen anzeigen

Mithilfe der Informationen in diesem Abschnitt können Sie Informationen zu Adaptern anzeigen, die im Server installiert sind.

Klicken Sie unter **Serverkonfiguration** auf **Adapter**, um Informationen zu den im Server installierten Adaptern anzuzeigen.

Anmerkungen:

- Wenn der Adapter keine Statusüberwachung unterstützt, ist er für die Überwachung oder Konfiguration nicht sichtbar. Bestandsinformationen zu allen installierten PCI-Adaptern finden Sie auf der Seite **Bestand**.

Bootmodus und Bootreihenfolge des Systems konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie den Bootmodus und die Bootreihenfolge des Systems konfigurieren.

Wenn Sie unter **Serverkonfiguration** die Option **Bootoptionen** auswählen, können Sie den Systembootmodus und die Bootreihenfolge konfigurieren.

Anmerkung: Keine nicht authentifizierte Inband-Methode ist berechtigt, die sicherheitsbezogenen Systemeinstellungen zu ändern. „Sicherer Start“ darf beispielsweise NICHT über nicht authentifizierte Inband-APIs aus der Betriebssystem- oder UEFI-Shell konfiguriert werden können. Dazu gehören auch OneCLI mit Inband-Ausführung und das Abrufen temporärer Anmeldeinformationen mittels IPMI, oder Tools und APIs zur Konfiguration von „Sicherer Start“, TPM und kennwortbezogenen Einstellungen in der UEFI-Konfiguration. Für alle sicherheitsbezogenen Einstellungen muss eine ordnungsgemäße Authentifizierung mit ausreichenden Berechtigungen vorhanden sein.

Für den Systembootmodus stehen die folgenden zwei Optionen zur Verfügung:

UEFI-Boot
Wählen Sie diese Option aus, um einen Server zu konfigurieren, der Unified Extensible Firmware Interface (UEFI) unterstützt. Wenn Sie UEFI-aktivierte Betriebssysteme starten, kann diese Option die Startzeit durch Deaktivieren älterer ROMs für Zusatzeinrichtungen deaktivieren.

Legacy-Boot
Wählen Sie diese Option aus, wenn Sie einen Server für den Start eines Betriebssystems konfigurieren, das traditionelle Firmware (BIOS) erfordert. Wählen Sie diese Option nur aus, wenn Sie nicht UEFI-aktivierte Betriebssysteme starten.

Um die Systembootreihenfolge zu konfigurieren, wählen Sie eine Einheit aus der Liste unter **Verfügbare Einheiten** aus und klicken Sie auf den Rechtspfeil, um die Einheit der Bootreihenfolge hinzuzufügen. Um eine Einheit aus der Bootreihenfolge zu entfernen, wählen Sie eine Einheit aus der Liste der Bootreihenfolge aus und klicken Sie auf den Linkspfeil, um die Einheit zurück zur Liste der verfügbaren Einheiten zu verschieben. Um die Bootreihenfolge zu ändern, wählen Sie eine Einheit aus und klicken Sie auf den Pfeil nach oben oder unten, um die Einheit je nach Priorität nach oben oder unten zu verschieben.

Wenn Sie eine Änderung an der Bootreihenfolge vornehmen, müssen Sie eine Neustartoption wählen, bevor Sie die Änderungen übernehmen. Die folgenden Optionen stehen zur Verfügung.

- **Server sofort neu starten**: Die Änderung der Bootreihenfolge wird gespeichert und der Server wird sofort neu gestartet, ohne das Betriebssystem herunterzufahren.
- **Server normal neu starten**: Die Änderung der Bootreihenfolge wird gespeichert und das Betriebssystem wird vor dem Neustart des Servers heruntergefahren.
- **Später manuell neu starten**: Die Änderung der Bootreihenfolge wird gespeichert, aber erst beim nächsten Neustart des Servers wirksam.

Einmaligen Bootvorgang konfigurieren

Um den konfigurierten Start vorübergehend zu ignorieren und stattdessen einmalig auf eine angegebene Einheit zu booten, verwenden Sie die Informationen in diesem Abschnitt.

Klicken Sie unter **Serverkonfiguration** auf **Bootoptionen** und wählen Sie eine Einheit aus dem Dropdown-Menü aus, auf die das System beim nächsten Neustart des Servers booten soll. Die folgenden Optionen sind verfügbar:

PXE-Netzwerk
Ihr Server wird so konfiguriert, dass er versucht, einen PXE-Netzwerkboot (Preboot Execution Environment) auszuführen.

Primärer Wechseldatenträger
Der Server wird von der Standard-USB-Einheit gestartet.

Standard-CD/-DVD
Der Server wird von der Standard-CD/DVD-Einheit gestartet.

Systemeinrichtung F1
Der Server wird in den Lenovo XClarity Provisioning Manager gestartet.

Diagnosepartition
Der Server wird in den Diagnoseabschnitt von Lenovo XClarity Provisioning Manager gestartet.

Standardfestplatte
Der Server wird vom Standardplattenlaufwerk gestartet.

Primäre ferne Medien
Der Server wird von den angehängten virtuellen Datenträgern gebootet.

Kein einmaliger Bootvorgang
Es wird die konfigurierte Bootreihenfolge verwendet. Die konfigurierte Bootreihenfolge wird nicht durch einmaliges Booten außer Kraft gesetzt.

Wenn Sie die Art des Bootens für die einmalige Booteinheit ändern, können Sie auch angeben, dass ein Legacy- oder UEFI-Boot ausgeführt werden soll. Aktivieren Sie das Kontrollkästchen **Legacy-Boot bevorzugen**, wenn Sie möchten, dass der Boot ein Legacy-BIOS-Boot ist. Deaktivieren Sie das Kontrollkästchen, wenn Sie einen UEFI-Boot wünschen. Wenn Sie eine einmalige Änderung der Bootreihenfolge auswählen, müssen Sie eine Neustartoption wählen, bevor Sie die Änderungen übernehmen.

- **Server sofort neu starten**: Die Änderung der Bootreihenfolge wird gespeichert und der Server wird sofort neu gestartet, ohne das Betriebssystem herunterzufahren.
- **Server normal neu starten**: Die Änderung der Bootreihenfolge wird gespeichert und das Betriebssystem wird vor dem Neustart des Servers heruntergefahren.
- **Später manuell neu starten**: Die Änderung der Bootreihenfolge wird gespeichert, aber erst beim nächsten Neustart des Servers wirksam.

Serverstromversorgung verwalten

Mit den Informationen in diesem Abschnitt können Sie Informationen zur Stromverbrauchssteuerung anzeigen und Funktionen zur Stromverbrauchssteuerung ausführen.

Wählen Sie die Option **Stromversorgungsrichtlinie** unter **Serverkonfiguration** aus, um Informationen zur Stromverbrauchssteuerung anzuzeigen und Funktionen zur Stromverbrauchssteuerung auszuführen.

Anmerkung: In einem Gehäuse, das Blade- oder Serverknoten mit hoher Dichte enthält, wird die Gehäusekühlung und -stromversorgung vom Gehäusemanagementcontroller und nicht vom XClarity Controller gesteuert.

Stromversorgungsredundanz konfigurieren

Um die Stromversorgungsredundanz zu konfigurieren, verwenden Sie die Informationen in diesem Abschnitt.

Folgende Felder sind im Abschnitt zur Stromversorgungsredundanz enthalten:

- **Redundant (N+N)**: In diesem Modus bleibt der Server bei Ausfall eines Netzteils funktionsfähig.
  - **Nullausgabemodus**: Wenn diese Option in der redundanten Konfiguration aktiviert ist, werden bei Geringlastbedingungen einige Netzteile automatisch in den Standby-Modus versetzt. Auf diese Weise liefert das verbleibende Netzteil die gesamte Stromversorgung, um die Effizienz zu erhöhen.
- **Redundant (N+1)**: In diesem Modus bleibt der Server bei Ausfall eines Netzteils funktionsfähig, wenn vier Netzteile installiert wurden.
- **Nicht redundanter Modus**: In diesem Modus ist nicht sichergestellt, dass der Server bei Ausfall eines Netzteils funktionsfähig bleibt. Der Server wird gedrosselt, wenn ein Netzteil beim Versuch, den Betrieb eines Netzteils aufrechtzuerhalten, ausfällt.

Nachdem Sie die Konfigurationsänderungen vorgenommen haben, klicken Sie auf **Übernehmen**.

Richtlinie zur Energieverbrauchsbegrenzung konfigurieren

Um die Richtlinie zur Energieverbrauchsbegrenzung zu konfigurieren, verwenden Sie die Informationen in diesem Abschnitt.

Sie können die Energieverbrauchsbegrenzung aktivieren oder deaktivieren. Wenn die Energieverbrauchsbegrenzung aktiviert ist, können Sie die Obergrenze der vom Server genutzten Energie auswählen. Wenn die Energieverbrauchsbegrenzung deaktiviert ist, wird die Obergrenze für den Stromverbrauch durch den Server von der Stromversorgungsredundanz-Richtlinie bestimmt. Um die Einstellung zu ändern, klicken Sie zuerst auf **Zurücksetzen**. Wählen Sie die bevorzugte Einstellung aus, und klicken Sie dann auf **Übernehmen**.

Die Energieverbrauchsbegrenzung kann mithilfe von Wechsel- oder Gleichstromverbrauchsmessungen aktiviert werden. Wählen Sie aus dem Dropdown-Menü die Art der Messungen aus, die verwendet werden sollen, um die maximale Energieverbrauchsbegrenzung zu bestimmen. Beim Umschalten zwischen Wechsel- und Gleichstrom wird die Zahl auf dem Schieberegler entsprechend geändert.

Es gibt zwei Möglichkeiten zum Ändern des Werts für die Energieverbrauchsbegrenzung:

- **Methode 1**: Bewegen Sie die Schiebereglermarke auf die gewünschte Wattzahl, um die allgemeine Strombegrenzung für den Server festzulegen.
- **Methode 2**: Geben Sie den Wert im Eingabefeld ein. Die Schiebereglermarke verschiebt sich automatisch zur entsprechenden Position.

Nachdem Sie die Konfigurationsänderungen vorgenommen haben, klicken Sie auf **Übernehmen**.

Anmerkung: Die Option **Stromversorgungsrichtlinien** ist nicht verfügbar, wenn sich der XClarity Controller in einem Gehäuse befindet, der Blade- oder Serverknoten mit hoher Dichte enthält. Die Stromversorgungsrichtlinie wird vom Gehäusemanagementcontroller und nicht vom XClarity Controller gesteuert.

Richtlinie zum Wiederherstellen der Stromversorgung konfigurieren

Um zu konfigurieren, wie der Server reagiert, wenn die Stromversorgung nach einem Stromausfall wiederhergestellt wird, verwenden Sie die Informationen in diesem Abschnitt.

Bei der Konfiguration der Richtlinie zum Wiederherstellen der Stromversorgung stehen Ihnen die folgenden drei Optionen zur Verfügung:

Immer aus
Der Server bleibt ausgeschaltet, selbst wenn die Stromversorgung wiederhergestellt ist.

Wiederherstellen
Der Server wird automatisch eingeschaltet, sobald die Stromversorgung wiederhergestellt ist, sofern der Server zu dem Zeitpunkt, als der Stromausfall eintrat, eingeschaltet war. Andernfalls bleibt der Server ausgeschaltet, wenn die Stromversorgung wiederhergestellt ist.

Immer an
Der Server wird automatisch eingeschaltet, sobald die Stromversorgung wiederhergestellt ist.

Nachdem Sie die Konfigurationsänderungen vorgenommen haben, klicken Sie auf **Übernehmen**.

Anmerkung: Die Option **Richtlinie zum Wiederherstellen der Stromversorgung** ist nicht in einem Gehäuse verfügbar, der Blade- oder Serverknoten mit hoher Dichte enthält. Die Richtlinie zum Wiederherstellen der Stromversorgung wird vom Gehäusemanagementcontroller und nicht vom XClarity Controller gesteuert.

Stromversorgungsaktionen

Mit den Informationen in diesem Abschnitt lernen Sie die Stromversorgungsaktionen kennen, die für den Server ausgeführt werden können.

Klicken Sie im Abschnitt **Schnelle Aktion** auf der Startseite von XClarity Controller auf **Stromversorgungsaktion**.

Die folgende Tabelle enthält eine Beschreibung der Stromversorgungs- und Neustartaktionen, die auf dem Server ausgeführt werden können.

Tabelle 6. Stromversorgungsaktionen und Beschreibungen

Diese Tabelle mit zwei Spalten enthält Beschreibungen der Stromversorgungs- und Neustartaktionen.

Tabelle 6. Stromversorgungsaktionen und Beschreibungen (Forts.)

Stromversorgungsaktion	Beschreibung
Server einschalten	Wählen Sie dieses Aktionselement aus, um den Server einzuschalten und das Betriebssystem zu booten.
Server normal ausschalten	Wählen Sie dieses Aktionselement aus, um das Betriebssystem herunterzufahren und den Server anschließend auszuschalten.
Server sofort ausschalten	Wählen Sie dieses Aktionselement aus, um den Server auszuschalten, ohne zuerst das Betriebssystem herunterzufahren.
Server normal neu starten	Wählen Sie dieses Aktionselement aus, um das Betriebssystem herunterzufahren und den Server anschließend aus- und wieder einzuschalten.
Server sofort neu starten	Wählen Sie dieses Aktionselement aus, um den Server sofort aus- und anschließend wieder einzuschalten, ohne zuerst das Betriebssystem herunterzufahren.
Server zur Systemkonfiguration booten	Wählen Sie diese Option, um den Server einzuschalten bzw. neu zu starten und automatisch in das Systemsetup zu booten, ohne dass während des Bootvorgangs F1 gedrückt werden muss.
Non-Maskable Interrupt (NMI) auslösen	Wählen Sie dieses Aktionselement aus, um ein Non-Maskable Interrupt (NMI) für ein blockiertes System zu erzwingen. Die Auswahl dieses Aktionselements ermöglicht es dem Plattformbetriebssystem, einen Hauptspeicherauszug zu erstellen, der für die Fehlerbehebung des blockierten Systems verwendet werden kann. Der automatische Neustart der NMI-Einstellung vom Menü „F1-Systemkonfiguration“ bestimmt, ob XClarity Controller den Server nach dem NMI neu startet.
Stromversorgungsaktionen planen	Wählen Sie dieses Aktionselement aus, um tägliche oder wöchentliche Aktionen zum Einschalten und zum Neustarten für den Server zu planen.
Management-Controller neu starten	Wählen Sie dieses Aktionselement aus, um den XClarity Controller neu zu starten.
Server aus- und wieder einschalten	Wählen Sie diese Aktion aus, um den Server aus- und wieder einzuschalten.
Anmerkung: Falls sich das Betriebssystem im Bildschirmschoner- oder gesperrten Modus befindet, wenn das Herunterfahren des Betriebssystems versucht wird, kann der XClarity Controller möglicherweise keinen ordnungsgemäßen Systemabschluss einleiten. Der XClarity Controller führt dann einen Kaltstart oder einen Systemabschluss nach Ablaufen des Ausschaltverzögerungsintervalls durch, während das Betriebssystem möglicherweise noch ausgeführt wird.	

Stromverbrauch mit IPMI-Befehlen steuern und überwachen

Mithilfe der Informationen in diesem Abschnitt können Sie den Stromverbrauch mithilfe von IPMI-Befehlen steuern und überwachen.

In diesem Abschnitt wird beschrieben, wie Sie mit dem Intel Intelligent Power Node Manager und der Data Center Manageability Interface (DCMI) eine Überwachung der Stromversorgung und Thermik sowie eine richtlinienbasierte Stromverbrauchssteuerung für einen Server mit den Stromverbrauchssteuerungsbefehlen über die Intelligent Platform Management Interface (IPMI) bereitstellen.

Für Server mit Intel Node Manager SPS 3.0 können XClarity Controller-Benutzer die IPMI-Stromverbrauchssteuerungsbefehle verwenden, die von der Management Engine (ME) von Intel bereitgestellt werden, um die Funktionen des Node Managers zu steuern und den Energieverbrauch des Servers zu überwachen. Die Stromverbrauchssteuerung kann auch über die entsprechenden DCMI-Befehle ausgeführt werden. In diesem Abschnitt finden Sie Beispiele für Node Manager- und DCMI-Stromverbrauchssteuerungsbefehle.

Serverstromversorgung mit Node Manager-Befehlen steuern

Mithilfe der Informationen in diesem Abschnitt können Sie die Serverstromversorgung mit dem Node Manager steuern.

Die Node Manager-Firmware von Intel hat keine externe Schnittstelle. Daher müssen die Node Manager-Befehle zuerst vom XClarity Controller empfangen und dann an den Intel Node Manager gesendet werden. Der XClarity Controller fungiert als Relay und Transporteinheit für die IPMI-Befehle unter Verwendung von IPMI-Standardbridging.

Anmerkung: Änderungen an den Richtlinien des Node Managers über die IPMI-Befehle des Node Managers können zu Konflikten mit der Stromverbrauchssteuerungsfunktionalität von XClarity Controller führen. Standardmäßig ist das Bridging der Node Manager-Befehle deaktiviert, um Konflikte zu vermeiden.

Für Benutzer, die die Serverstromversorgung mithilfe des Node Managers anstelle von XClarity Controller verwalten möchten, steht ein OEM-IPMI-Befehl zur Verfügung, der sich aus (Netzwerkfunktion: **0x3A**) und (Befehl: **0xC7**) zusammensetzt.

So aktivieren Sie die nativen IPMI-Befehle von Node Manager: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x3a 0xc7 0x01**

So deaktivieren Sie die nativen IPMI-Befehle von Node Manager: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x3a 0xc7 0x00**

Die folgenden Informationen sind Beispiele für die Stromverbrauchssteuerungsbefehle von Node Manager.

Anmerkungen:

- Wenn Sie den IPMI-Kanal **0** und die Zieladresse **0x2c** angeben, können Sie das IPMITOOL verwenden, um Befehle zum Intel Node Manager zur Verarbeitung zu senden. Eine Anforderungsnachricht wird verwendet, um eine Aktion zu initiieren; eine Antwortnachricht wird an den Anforderer zurückgesendet.
- Die Befehle werden aufgrund von Platzbeschränkungen in den folgenden Formaten angezeigt.

Überwachung des Stromverbrauchs durch Abrufen der Statistik zum globalen Systemenergieverbrauch (Befehlscode 0xC8): Anforderung: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00** Antwort: 57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

Energieverbrauchsbegrenzung durch Festlegen der Intel Node Manager-Richtlinie, (Befehlscode 0xC1): Anforderung: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**Antwort: 57 01 00

Energieeinsparung durch Festlegen der Intel Node Manager-Richtlinie, (Befehlscode 0xC1): Anforderung: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**

Funktion zum Abrufen der Einheiten-ID durch Abrufen der Einheiten-ID der Intel Management Engine: Anforderung: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x06 0x01**Antwort: 50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

Weitere Befehle des Intel Node Manager finden Sie in der neuesten Version der **Intel Intelligent Power Node Manager, External Interface Specification Using IPMI** unter https://businessportal.intel.com.

Serverstromversorgung mit DCMI-Befehlen steuern

Mithilfe der Informationen in diesem Abschnitt können Sie die Serverstromversorgung mithilfe von DCMI-Befehlen steuern.

Die DCMI bietet Überwachungs- und Kontrollfunktionen, die über Standardverwaltungssoftwareschnittstellen verfügbar gemacht werden können. Funktionen zur Stromverbrauchssteuerung können ebenfalls über DCMI-Befehle ausgeführt werden.

Die folgenden Informationen sind Beispiele für häufig verwendete DCMI-Stromverbrauchssteuerungsfunktionen und -befehle. Eine Anforderungsnachricht wird verwendet, um eine Aktion zu initiieren; eine Antwortnachricht wird an den Anforderer zurückgesendet.

Anmerkung: Die Befehle werden aufgrund von Platzbeschränkungen in den folgenden Formaten angezeigt.

Energiewert abrufen: Anforderung: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x02 0xdc 0x01 0x00 0x00** Antwort: `dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40`

Energielimit festlegen: Anforderung: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **PASSW0RD** `raw` **0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03** Antwort: `dc`

Energieverbrauchsbegrenzung abrufen: Anforderung: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x03 0xdc 0x00 0x00** Antwort: `dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00`

Energielimit aktivieren: Anforderung: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x01 0x00 0x00** Antwort: `dc`

Energielimit deaktivieren: Anforderung: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x00 0x00 0x00** Antwort: `dc`

Anmerkung: Auf manchen Servern werden die Ausnahmeaktionen für den Befehl **Energielimit festlegen** möglicherweise nicht unterstützt. So wird beispielsweise der Parameter **Hard Power Off system and log events to SEL** eventuell nicht unterstützt.

Eine vollständige Liste der Befehle, die von der DCMI-Spezifikation unterstützt werden, finden Sie in der aktuellen Version der **Spezifikation der Data Center Manageability Interface** unter https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf.

Funktionalität „Ferne Konsole“

Verwenden Sie die Informationen in diesem Abschnitt, um zu erfahren, wie Sie per Fernzugriff die Serverkonsole anzeigen und mit ihr interagieren.

Sie können die Funktionalität der fernen Konsole in der XClarity Controller-Webschnittstelle zum Anzeigen und Interagieren mit der Serverkonsole verwenden. Sie können ein Datenträger-Image (ISO- oder IMG-Datei) als virtuelles Laufwerk auf dem Server zuweisen. Die Funktionalität der fernen Konsole steht nur mit den

Features XClarity Controller Advanced und XClarity Controller Enterprise zur Verfügung und ist nur über die Webschnittstelle verfügbar. Sie müssen sich am XClarity Controller mit einer Benutzer-ID anmelden, die über Administratorzugriff oder Zugriff auf die ferne Konsole verfügt, um die Funktionen der fernen Konsole verwenden zu können. Weitere Informationen zum Upgrade von XClarity Controller Standard auf XClarity Controller Advanced oder XClarity Controller Enterprise finden Sie unter „XClarity Controller aktualisieren“ auf Seite 6.

Verwenden Sie die Funktionen der fernen Konsole, um folgende Aktionen auszuführen:

- Zeigen Sie, unabhängig vom Serverzustand, über Fernzugriff Videos mit einer Grafikauflösung von bis zu 1.280 x 1.024 bei 72 Hz oder 75 Hz an.
- Greifen Sie mithilfe der Tastatur und der Maus eines fernen Clients über Fernzugriff auf den Server zu.
- Hängen Sie ISO- und IMG-Dateien, die sich auf Ihrem lokalen System oder auf einem fernen System befinden, als virtuelle Laufwerke an, die vom Server genutzt werden können.
- Laden Sie ein IMG- oder ISO-Image in den XClarity Controller-Speicher hoch und hängen Sie es dem Server als virtuelles Laufwerk an. Es können bis zu zwei Dateien mit einer maximalen Gesamtgröße von 50 MB in den XClarity Controller-Speicher hochgeladen werden.

Anmerkungen:

- Wenn die Funktion der fernen Konsole im Mehrbenutzermodus gestartet wird (ein XClarity Controller mit Enterprise-Funktionsumfang unterstützt bis zu sechs gleichzeitige Sitzungen), kann die Funktion für ferne Datenträger jeweils nur von einer Sitzung ausgeführt werden.
- Die ferne Konsole kann nur das vom Videocontroller auf der Systemplatine generierte Video anzeigen. Wenn ein separater Videocontroller installiert und anstelle des Systemvideocontrollers verwendet wird, kann die ferne Konsole von XClarity Controller den Videoinhalt aus dem hinzugefügten Adapter nicht anzeigen.
- Wenn Sie in Ihrem Netzwerk mit Firewalls arbeiten, muss ein Netzwerkanschluss geöffnet sein, um diese Funktion der fernen Konsole zu unterstützen. Informationen dazu, wie Sie die Netzwerkanschlusszahl anzeigen oder ändern, die von der Funktion der fernen Konsole verwendet wird, finden Sie unter „Serviceaktivierung und Portzuordnung“ auf Seite 36.
- Die Funktion der fernen Konsole verwendet HTML5 zum Anzeigen des Servervideos auf Webseiten. Um diese Funktion zu verwenden, muss Ihr Browser das Anzeigen von Videoinhalten mit HTML5-Elementen unterstützen.
- Wenn Sie selbst signierte Zertifikate und eine IPv6-Adresse verwenden, um auf den BMC via Internet Explorer zuzugreifen, kann die Sitzung der fernen Konsole aufgrund eines Zertifikatsfehlers möglicherweise nicht gestartet werden. Um dieses Problem zu vermeiden, kann das selbst signierte Zertifikat den Stellen zum Vertrauen von Stammzertifikaten von Internet Explorer hinzugefügt werden:
  - Wählen Sie unter **BMC-Konfiguration** die Option **Sicherheit** und laden das selbst signierte Zertifikat herunter.
  - Ändern Sie die Erweiterung der Zertifikatsdatei in „*.crt“ und doppelklicken Sie auf die Web-Zertifikatsdatei.
  - Löschen Sie den Cache des IE11-Browsers.
  - Klicken Sie auf **Zertifikat installieren**, um das Zertifikat im Zertifikatspeicher zu installieren, indem Sie den Schritten des Assistenten zum Importieren von Zertifikaten folgen.

Funktionalität „Ferne Konsole“ aktivieren

Dieser Abschnitt enthält Informationen zur Funktionalität der fernen Konsole.

Wie zuvor erwähnt ist die Funktionalität der fernen Konsole von XClarity Controller nur in den Features XClarity Controller Advanced und XClarity Controller Enterprise verfügbar. Wenn Sie nicht über die Berechtigung zur Bedienung der fernen Konsole verfügen, erscheint ein Schlosssymbol.

Nachdem Sie den Aktivierungsschlüssel für das Upgrade von XClarity Controller Advanced erworben und erhalten haben, installieren Sie es mithilfe der Anweisungen unter „Aktivierungsschlüssel installieren“ auf Seite 95.

Um die Funktionalität der fernen Konsole zu verwenden, führen Sie die folgenden Schritte aus:

1. Klicken Sie im Abschnitt „Ferne Konsole“ der XClarity Controller-Startseite oder der Website der fernen Konsole auf das Bild, das einen weißen in die Diagonale zeigenden Pfeil darstellt.
2. Wählen Sie einen der folgenden Modi aus:
   - Ferne Konsole im Einzelbenutzermodus starten
   - Ferne Konsole im Mehrbenutzermodus starten

   Anmerkung: XClarity Controller mit dem Feature XClarity Controller Enterprise unterstützt bis zu sechs gleichzeitige Videositzungen im Mehrbenutzermodus.
3. Geben Sie an, ob es anderen Benutzern erlaubt sein soll, eine Anforderung zur Trennung der Verbindung mit einem Benutzer der fernen Konsole zu senden, wenn jemand die Funktion der fernen Konsole verwenden möchte und diese bereits im Einzelbenutzermodus verwendet wird bzw. wenn die maximale Anzahl Benutzer die Funktion der fernen Konsole im Mehrbenutzermodus verwendet. Die Option **Zeitintervall, in dem keine Antwort erfolgt** gibt an, wie lange XClarity Controller wartet, bevor der Benutzer automatisch getrennt wird, wenn auf die Anforderung zur Trennung der Verbindung keine Antwort eingeht.
4. Geben Sie an, ob die letzten drei Videos zum Serverboot aufgezeichnet werden dürfen.
5. Geben Sie an, ob die letzten drei Videos zum Serverabsturz aufgezeichnet werden dürfen.
6. Wählen Sie aus, ob Screenshots von Betriebssystemabstürzen mit HW-Fehler erfasst werden dürfen.
7. Klicken Sie auf **Ferne Konsole starten**, um die Seite der fernen Konsole in einer anderen Registerkarte zu öffnen. Wenn alle verfügbaren Sitzungen der fernen Konsole verwendet werden, wird ein Dialogfeld angezeigt. In diesem Dialogfenster kann der Benutzer eine Anforderung zum Trennen der Verbindung an einen Benutzer der fernen Konsole senden, der die Einstellung **Anforderungen zum Trennen der Verbindung meiner fernen Sitzung durch andere Benutzer zulassen** aktiviert hat. Der Benutzer kann die Anforderung zur Verbindungstrennung akzeptieren oder ablehnen. Wenn der Benutzer nicht innerhalb des über die Einstellung **Zeitintervall, in dem keine Antwort erfolgt** angegebenen Intervalls antwortet, wird die Benutzersitzung von XClarity Controller automatisch beendet.

Fernsteuerung der Stromversorgung

In diesem Abschnitt wird erläutert, wie Befehle zur Stromversorgung und zum Neustart des Servers aus dem Fenster der fernen Konsole gesendet werden.

Über das Fenster der fernen Konsole können Sie Befehle zur Stromversorgung und zum Neustart an den Server senden, ohne zur Hauptwebseite zurückzukehren. Um die Stromversorgung des Servers über die ferne Konsole zu steuern, klicken Sie auf **Stromversorgung** und wählen Sie einen der folgenden Befehle aus:

Server einschalten
Wählen Sie dieses Aktionselement aus, um den Server einzuschalten und das Betriebssystem zu booten.

Server normal ausschalten
Wählen Sie dieses Aktionselement aus, um das Betriebssystem herunterzufahren und den Server anschließend auszuschalten.

Server sofort ausschalten
Wählen Sie dieses Aktionselement aus, um den Server auszuschalten, ohne zuerst das Betriebssystem herunterzufahren.

Server normal neu starten
Wählen Sie dieses Aktionselement aus, um das Betriebssystem herunterzufahren und den Server anschließend aus- und wieder einzuschalten.

Server sofort neu starten
Wählen Sie dieses Aktionselement aus, um den Server sofort aus- und anschließend wieder einzuschalten, ohne zuerst das Betriebssystem herunterzufahren.

Server zur Systemkonfiguration booten
Wählen Sie diese Option, um den Server einzuschalten bzw. neu zu starten und automatisch in das Systemsetup zu booten, ohne dass während des Bootvorgangs F1 gedrückt werden muss.

Screenshot-Funktion der fernen Konsole

Anhand der Informationen in diesem Abschnitt wird Ihnen vermittelt, wie Sie die Screenshot-Funktion der fernen Konsole verwenden.

Die Screenshot-Funktion im Fenster der fernen Konsole erfasst die Inhalte der Videoanzeige auf dem Server. Gehen Sie wie folgt vor, um eine Bildschirmanzeige zu erfassen und zu speichern:

Schritt 1. Klicken Sie im Fenster der fernen Konsole auf **Bildschirm erfassen**.

Schritt 2. Klicken Sie im Dialogfenster auf **Datei speichern** und dann auf **OK**. Die Datei wird „rpviewer.png“ genannt und in Ihrem Standardordner für Downloads gespeichert.

Anmerkung: Der Screenshot wird als Dateityp PNG gespeichert.

Tastaturunterstützung der fernen Konsole

Im Fenster der fernen Konsole werden unter **Tastatur** die folgenden Optionselemente angezeigt:

- Klicken Sie auf **Virtuelle Tastatur**, um die virtuelle Tastatur zu starten. Diese Funktion ist hilfreich, wenn Sie ein Tablet verwenden, das über keine physische Tastatur verfügt. Die folgenden Optionen können verwendet werden, um Makros und Tastenkombinationen zu erstellen, die an den Server gesendet werden können. Das Betriebssystem auf dem Clientsystem, das Sie verwenden, kann bestimmte Tastenkombinationen abfangen, etwa „Strg + Alt + Entf“, anstatt sie an den Server zu übertragen. Andere Tasten, wie die F1- oder ESC-Taste, können vom verwendeten Programm oder Browser abgefangen werden. Makros bieten einen Mechanismus, Tastatureingaben an den Server zu senden, die der Benutzer möglicherweise nicht senden kann.
- Klicken Sie auf **Servermakros**, um die vom Server definierten Makros zu verwenden. Einige Servermakros sind durch die XClarity Controller-Firmware vordefiniert. Andere serverdefinierte Makros können mithilfe von Lenovo XClarity Essentials definiert und vom XClarity Controller heruntergeladen werden. Diese Makros werden für alle Benutzer der fernen Konsole definiert.
- Klicken Sie auf **Konfigurieren**, um benutzerdefinierte Makros hinzuzufügen oder zu entfernen. Die benutzerdefinierten Makros werden nur für den aktuellen Benutzer der fernen Konsole definiert. Andere Benutzer der fernen Konsole sehen die benutzerdefinierte Makros des jeweils anderen nicht.
  - Klicken Sie auf das Symbol „Makros hinzufügen“ und drücken Sie die gewünschten Tastenkombinationen. Klicken Sie dann auf **Hinzufügen**, um ein neues Makro hinzuzufügen.
  - Um ein benutzerdefiniertes Makro zu entfernen, wählen Sie das Makro aus der Liste aus und klicken Sie auf das Papierkorbsymbol.
  - Um ein benutzerdefiniertes Makro an den Server zu senden, wählen Sie die Option **Benutzerdefinierte Makros** aus und klicken Sie auf das gewünschte Makro.

Mausunterstützung über ferne Konsole

Dieser Abschnitt enthält Informationen zu den Optionen für die Fernsteuerung der Maus.

Das Fenster der fernen Konsole bietet verschiedene Möglichkeiten für die Maussteuerung, z. B. die absolute Maussteuerung, relative Maussteuerung (keine Beschleunigung) und Maussteuerung (RHEL, älteres Linux).

Absolute und relative Maussteuerung

Mithilfe dieser Informationen können Sie auf die absoluten und relativen Optionen zum Steuern der Maus zugreifen.

Gehen Sie wie folgt vor, um auf die absoluten und relativen Optionen zur Maussteuerung zuzugreifen:

Schritt 1. Klicken Sie im Fenster der fernen Konsole auf **Maus**.

Schritt 2. Klicken Sie im Dropdown-Menü auf **Mauseinstellungen**.

Schritt 3. Wählen Sie einen der folgenden Modi für **Mausbeschleunigung** aus:

Absolute Positionierung (Windows, neueres Linux und Mac OS X)
Der Client sendet Mauspositionsnachrichten an den Server, die relativ zum Ursprung (oberer linker Bereich) des Anzeigebereichs sind.

Relative Positionierung, keine Beschleunigung
Der Client sendet die Mausposition als relative Position im Hinblick auf die vorherige Position.

Relative Positionierung (älteres Linux)
Dieser Modus wendet einen Beschleunigungsfaktor an, um die Maus besser auf einige Linux-Ziele abzustimmen. Die Beschleunigungseinstellungen wurden ausgewählt, um die Kompatibilität mit älteren Linux-Distributionen zu maximieren.

Bildschirmvideo aufzeichnen/wiedergeben

Verwenden Sie die Informationen in diesem Abschnitt, um Fernpräsenz-Bildschirmvideos aufzuzeichnen oder wiederzugeben.

Die XClarity Controller-Webschnittstelle bietet eine DVR-ähnliche Funktion, um die Aufzeichnung und Wiedergabe von Fernpräsenz-Bildschirmvideos zu unterstützen. Diese Funktion unterstützt nur die Videoaufzeichnung in einen Netzwerkordner. Derzeit werden NFS- und CIFS-Protokolle unterstützt. Gehen Sie bei der Verwendung der Aufzeichnungs- und Wiedergabefunktion wie folgt vor:

1. Klicken Sie auf der Webseite der fernen Konsole auf **Bildschirmaufzeichnung**, um das Einstellungsfenster zu öffnen.
2. Im Einstellungsfenster müssen Sie möglicherweise die folgenden Informationen angeben:
   - Wenn der Anhängetyp „CIFS“ ausgewählt ist, geben Sie die Parameter für **Ferner Ordner**, **Benutzername** und **Kennwort** an. Das Format für den fernen CIFS-Ordner ist **//<Remote-IP-Adresse>/<Ordnername>**. Beispiel: //xxx.xxx.xxx.xxx/Ordner
   - Wenn der Anhängetyp „NFS“ ausgewählt ist, geben Sie den Parameter für **Ferner Ordner** an. Das Format für den fernen NFS-Ordner ist **<Remote-IP-Adresse>:/<Ordnername>**. Beispiel: xxx.xxx.xxx.xxx:/Ordner
   - Geben Sie ggf. den Namen der Videodatei an. Wenn bereits ein Dateiname angegeben wurde, wird eine Fehlernachricht angezeigt. Wählen Sie „Dateinamen überschreiben“ aus, um den vorhandenen Dateinamen zu überschreiben. Wenn das Kontrollkästchen „Auto“ aktiviert ist, wird der Name der Videodatei automatisch generiert.
   - „Max. Dateigröße“ gibt die maximale Größe der Videodatei an, bei der die Videoaufzeichnung automatisch gestoppt wird.

- „Max. Aufzeichnungsdauer“ gibt die maximale Aufzeichnungsdauer des Videos an, bei der die Videoaufzeichnung automatisch gestoppt wird.

3. Klicken Sie auf **Aufzeichnung starten**, um die Videoaufzeichnung zu starten.
4. Klicken Sie auf **Aufzeichnung stoppen**, um die Videoaufzeichnung zu stoppen. Ein Popup-Fenster mit der Meldung „Videoaufzeichnung abgeschlossen“ mit relevanten Informationen zur Videoaufzeichnung wird angezeigt.
5. Laden Sie die aufgezeichneten Videos von NFS oder CIFS in Ihren lokalen Ordner herunter. Klicken Sie im Abschnitt „Ferne Konsolenvorschau“ der XClarity Controller-Homepage auf **Aufgezeichnete Videos** und wählen Sie die Videodatei aus, die Sie wiedergeben möchten.

Anzeigemodi der fernen Konsole

Mithilfe der Informationen in diesem Abschnitt können Sie die Anzeigemodi der fernen Konsole konfigurieren.

Um die Anzeigemodi der fernen Konsole zu konfigurieren, klicken Sie auf **Anzeigemodus**.

Die folgenden Menüoptionen sind verfügbar:

Vollbildmodus
Bei diesem Modus wird der gesamte Client-Desktop für die Videoanzeige verwendet. Durch Drücken der ESC-Taste in diesem Modus wird der Vollbildmodus beendet. Da das Menü der fernen Konsole nicht im Vollbildmodus sichtbar ist, müssen Sie den Vollbildmodus erst beenden, bevor Sie die anderen Funktionen im Menü der fernen Konsole nutzen können, wie z. B. die Tastaturmakros.

Anpassen
Dies ist die Standardeinstellung beim Starten der fernen Konsole. Bei dieser Einstellung wird der Ziel-Desktop vollständig ohne Bildlaufleisten angezeigt. Das Seitenverhältnis wird beibehalten.

Bildschirm skalieren
Wenn die Skalierung aktiviert ist, füllt das Videobild das gesamte Konsolenfenster aus.

Ursprünglicher Bildschirm
Das Videobild hat dieselben Abmessungen wie auf Serverseite. Bei Bedarf werden Bildlaufleisten eingeblendet, damit Videobildbereiche angezeigt werden können, die nicht in das Fenster passen.

Farbmodus
Passt die Farbtiefe des Fensters der fernen Konsole an. Es gibt zwei Farbmodi zur Auswahl:

- Farbe: 7, 9, 12, 15 und 23 Bit
- Grauskala: 16, 32, 64 und 128 Grautöne

Anmerkung: Farbmodusanpassungen werden normalerweise vorgenommen, wenn Ihre Verbindung zum fernen Server eine begrenzte Bandbreite hat und Sie den Bandbreitenbedarf reduzieren möchten.

Methoden zum Anhängen von Datenträgern

Mithilfe der Informationen in diesem Abschnitt erfahren Sie, wie Sie Datenträger anhängen.

Es stehen drei Methoden zum Anhängen von ISO- und IMG-Dateien als virtuelle Laufwerke zur Verfügung.

- Sie können dem Server virtuelle Laufwerke von der Sitzung der fernen Konsole aus hinzufügen, indem Sie auf **Datenträger** klicken.
- Sie können sie direkt von der Webseite der fernen Konsole hinzufügen, ohne eine Sitzung der fernen Konsole herzustellen.
- Eigenständiges Tool

Die Benutzer benötigen die Berechtigungen **Zugriff auf ferne Konsole und ferne Datenträger**, um die Funktionen für virtuelle Medien zu nutzen.

Die Dateien können als virtuelle Datenträger vom lokalen System oder von einem fernen Server angehängt werden. Sie können über das Netzwerk abgerufen oder mit der RDOC-Funktion in den XClarity Controller-Speicher hochgeladen werden. Diese Mechanismen werden unten beschrieben.

- Lokale Datenträger sind ISO- oder IMG-Dateien, die sich in dem System befinden, das Sie verwenden, um auf den XClarity Controller zuzugreifen. Dieser Mechanismus ist nur über die Sitzung der fernen Konsole verfügbar, nicht direkt von der Webseite der fernen Konsole aus. Er ist außerdem nur mit den Features von XClarity Controller- Enterprise verfügbar. Um lokale Datenträger anzuhängen, klicken Sie im Bereich **Lokale Datenträger anhängen** auf **Aktivieren**. Es können bis zu vier Dateien gleichzeitig an den Server angehängt werden.

  Anmerkungen:

  – Bei Verwendung des Browsers Google Chrome ist eine zusätzliche Anhängeoption namens **Dateien/ Ordner anhängen** verfügbar, mit der Sie Dateien/Ordner durch Ziehen und Ablegen anhängen können.
  – Wenn mit einem XClarity Controller mehrere gleichzeitige Sitzungen der fernen Konsole aktiv sind, kann diese Funktion nur von einer der Sitzungen aktiviert werden.
- Dateien, die sich auf einem fernen System befinden, können ebenfalls als virtuelle Datenträger angehängt werden. Es ist möglich, bis zu vier Dateien gleichzeitig als virtuelle Laufwerke anzuhängen. Der XClarity Controller unterstützt folgende Filesharing-Protokolle:
  – **CIFS – Common Internet File System**:
    – Geben Sie die URL ein, die die Datei auf dem fernen System lokalisiert.
    – Wenn Sie möchten, dass die Datei dem Server als schreibgeschützter virtueller Datenträger bereitgestellt wird, aktivieren Sie das Kontrollkästchen.
    – Geben Sie die Anmeldeinformationen ein, die der XClarity Controller benötigt, um auf die Datei auf dem fernen System zuzugreifen.

      Anmerkung: Der XClarity Controller unterstützt keine Leerzeichen im Benutzernamen, im Kennwort oder in der URL. Stellen Sie sicher, dass die Anmeldeinformationen für den CIFS-Server mit keinem Leerzeichen im Benutzernamen oder Kennwort konfiguriert sind und auch die URL kein Leerzeichen enthält.
    – Die Anhängeoptionen sind optional und werden durch das CIFS-Protokoll definiert.
    – Wenn der ferne Server zu einer Sammlung von Servern gehört und die Sicherheit zentral verwaltet wird, geben Sie den Domänennamen ein, zu dem der ferne Server gehört.
  – **NFS – Network File System**:
    – Geben Sie die URL ein, die die Datei auf dem fernen System lokalisiert.
    – Wenn Sie möchten, dass die Datei dem Server als schreibgeschützter virtueller Datenträger bereitgestellt wird, aktivieren Sie das Kontrollkästchen.
    – Die Anhängeoptionen sind optional und werden durch das NFS-Protokoll definiert. NFSv3 und NFSv4 werden unterstützt. Beispielsweise müssen Sie zur Verwendung von NFSv3 die Option „nfsvers=3“ angeben. Wenn der NFS-Server die Sicherheitsoption AUTH_SYS zur Authentifizierung von NFS-Vorgängen verwendet, müssen Sie die Option „sec=sys“ angeben.
  – **HTTPFS – HTTP Fuse-based File System**:
    – Geben Sie die URL ein, die die Datei auf dem fernen System lokalisiert.
    – Wenn Sie möchten, dass die Datei dem Server als schreibgeschützter virtueller Datenträger bereitgestellt wird, aktivieren Sie das Kontrollkästchen.

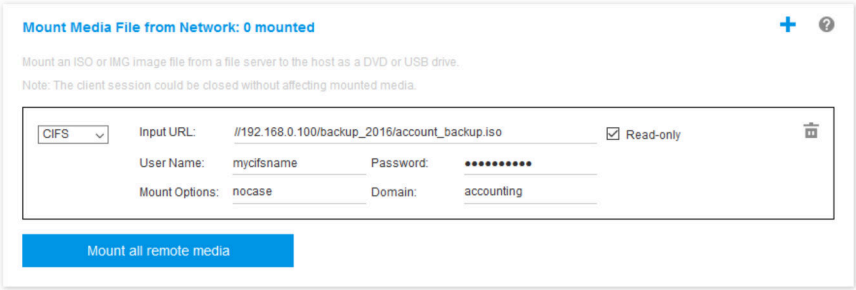
Anmerkung: Beim Anhängevorgang für von Microsoft IIS generierten Sicherheitszertifikaten können Fehler auftreten. Lesen Sie in diesem Fall unter „Fehler beim Anhängen von Datenträgern“ auf Seite 84 nach.

Klicken Sie auf **Alle fernen Medien anhängen**, um die Datei als virtuellen Datenträger anzuhängen. Um den virtuellen Datenträger zu entfernen, klicken Sie auf das Papierkorbsymbol auf der rechten Seite des angehängten Datenträgers.

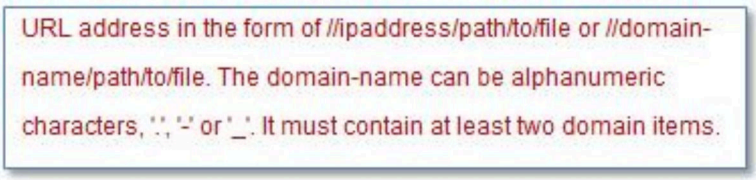
- Es können bis zu zwei Dateien in den XClarity Controller-Speicher hochgeladen und als virtuelle Datenträger mithilfe der RDOC-Funktion von XClarity Controller angehängt werden. Die Gesamtgröße beider Dateien darf 50 MB nicht überschreiten. Diese Dateien verbleiben im XClarity Controller-Speicher, bis sie entfernt werden, selbst dann, wenn die Sitzung der fernen Konsole beendet wurde. Die RDOC-Funktion unterstützt die folgenden Mechanismen beim Hochladen der Dateien:
  - **CIFS – Common Internet File System**: Siehe Beschreibung oben.

    Beispiel:

    Um eine ISO-Datei mit dem Namen „account_backup.iso“, die sich im Verzeichnis „backup_2016“ eines CIFS-Servers unter der IP-Adresse 192.168.0.100 befindet, als schreibgeschütztes virtuelles Laufwerk auf dem Server anzuhängen, würden Sie die Felder wie in der folgenden Abbildung dargestellt füllen. In diesem Beispiel gehört der Server unter der Adresse 192.168.0.100 zu einer Sammlung von Servern in der Domäne „Accounting“. Der Domänenname ist optional. Wenn Ihr CIFS-Server keiner Domäne angehört, lassen Sie das Feld **Domäne** leer. Die CIFS-Anhängeoption für „Keine Groß-/Kleinschreibung“ wird im Feld **Anhängeoptionen** angegeben. In diesem Beispiel weist es den CIFS-Server darauf hin, dass die Überprüfung von Groß-/Kleinschreibung des Dateinamens ignoriert werden soll. Das Feld **Anhängeoptionen** ist optional. Die vom Benutzer in diesem Feld eingegebenen Informationen werden vom BMC nicht verwendet, sondern bei der Anforderung zum Anhängen einfach an den CIFS-Server übergeben. Lesen Sie die Dokumentation für die Implementierung Ihres CIFS-Servers, um festzustellen, welche Optionen von Ihrem CIFS-Server unterstützt werden.



Der BMC bietet bei Angabe der URL Unterstützung. Wenn die eingegebene URL ungültig ist, wird die Schaltfläche „Anhängen“ abgeblendet und unter dem URL-Feld, das das erwartete URL-Format zeigt, erscheint roter Text.

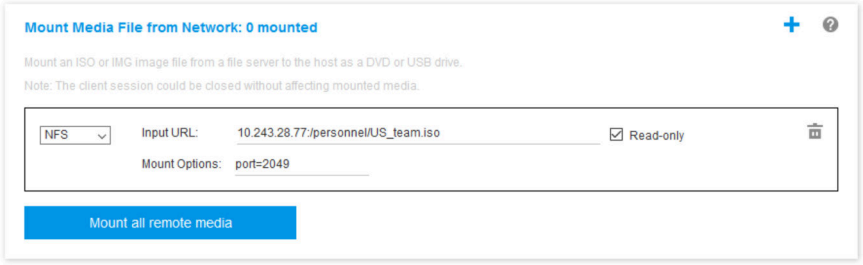


  - **NFS – Network File System**: Siehe Beschreibung oben.

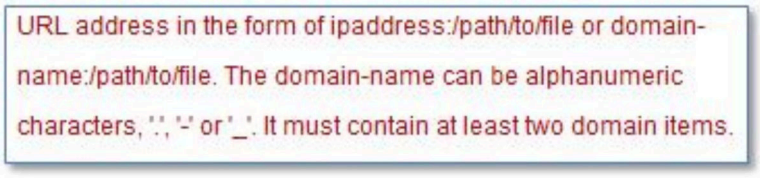
    Beispiel:

    Um eine ISO-Datei mit dem Namen „US_team.iso“, die sich im Verzeichnis „personnel“ eines NFS-Servers unter der IP-Adresse 10.243.28.77 befindet, als schreibgeschütztes virtuelles Laufwerk auf dem Server anzuhängen, würden Sie die Felder wie in der folgenden Abbildung dargestellt füllen. Die

NFS-Anhängeoption „Port = 2049“ gibt an, dass Netzwerkanschluss 2049 zum Übertragen der Daten verwendet werden soll. Das Feld **Anhängeoptionen** ist optional. Die vom Benutzer in diesem Feld eingegebenen Informationen werden bei der Anforderung zum Anhängen an den NFS-Server übergeben. Lesen Sie die Dokumentation für die Implementierung Ihres NFS-Servers, um festzustellen, welche Optionen von Ihrem NFS-Server unterstützt werden.



Der BMC bietet bei Angabe der URL Unterstützung. Wenn die eingegebene URL ungültig ist, wird die Schaltfläche „Anhängen“ abgeblendet und unter dem URL-Feld, das das erwartete URL-Format zeigt, erscheint roter Text.

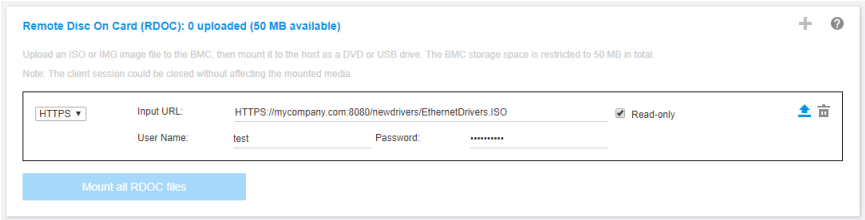


- **HTTPS – Hypertext Transfer Protocol Secure**:
  - Geben Sie die URL ein, die die Datei auf dem fernen System lokalisiert.
  - Wenn Sie möchten, dass die Datei dem Server als schreibgeschützter virtueller Datenträger bereitgestellt wird, aktivieren Sie das Kontrollkästchen.
  - Geben Sie die Anmeldeinformationen ein, die der XClarity Controller benötigt, um auf die Datei auf dem fernen System zuzugreifen.

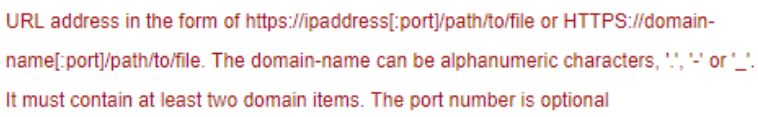
  Anmerkungen:

  - Beim Anhängevorgang für von Microsoft IIS generierten Sicherheitszertifikaten können Fehler auftreten. Lesen Sie in diesem Fall unter „Fehler beim Anhängen von Datenträgern“ auf Seite 84 nach.
  - Der XClarity Controller unterstützt keine Leerzeichen im Benutzernamen, im Kennwort oder in der URL. Stellen Sie sicher, dass die Anmeldeinformationen für den CIFS-Server mit keinem Leerzeichen im Benutzernamen oder Kennwort konfiguriert sind und auch die URL kein Leerzeichen enthält.
    Beispiel:

    Um eine ISO-Datei mit dem Namen „EthernetDrivers.iso“, die sich im Verzeichnis „newdrivers“ eines HTTPS-Servers mit dem Domänennamen „mycompany.com“ unter Netzwerkanschluss 8080 befindet, als schreibgeschütztes virtuelles Laufwerk auf dem Server anzuhängen, würden Sie die Felder wie in der folgenden Abbildung dargestellt füllen.



Der BMC bietet bei Angabe der URL Unterstützung. Wenn die eingegebene URL ungültig ist, wird die Schaltfläche „Anhängen“ abgeblendet und unter dem URL-Feld, das das erwartete URL-Format zeigt, erscheint roter Text.



- **SFTP – SSH File Transfer Protocol**
  - Geben Sie die URL ein, die die Datei auf dem fernen System lokalisiert.
  - Wenn Sie möchten, dass die Datei dem Server als schreibgeschützter virtueller Datenträger bereitgestellt wird, aktivieren Sie das Kontrollkästchen.
  - Geben Sie die Anmeldeinformationen ein, die der XClarity Controller benötigt, um auf die Datei auf dem fernen System zuzugreifen.

  Anmerkungen:

  - Der XClarity Controller unterstützt keine Leerzeichen im Benutzernamen, im Kennwort oder in der URL. Stellen Sie sicher, dass die Anmeldeinformationen für den CIFS-Server mit keinem Leerzeichen im Benutzernamen oder Kennwort konfiguriert sind und auch die URL kein Leerzeichen enthält.
  - Wenn sich der XClarity Controller mit einem HTTPS-Server verbindet, wird ein Dialogfenster mit Informationen zum Sicherheitszertifikat angezeigt, das vom HTTPS-Server verwendet wird. Der XClarity Controller ist nicht in der Lage, die Echtzeit des Sicherheitszertifikats zu überprüfen.
- **LOCAL – Common Internet File System**:
  - Durchsuchen Sie Ihr System nach der ISO- oder IMG-Datei, die Sie anhängen möchten.
  - Wenn Sie möchten, dass die Datei dem Server als schreibgeschützter virtueller Datenträger bereitgestellt wird, aktivieren Sie das Kontrollkästchen.

Klicken Sie auf **Alle RDOC-Dateien anhängen**, um die Datei als virtuellen Datenträger anzuhängen. Um den virtuellen Datenträger zu entfernen, klicken Sie auf das Papierkorbsymbol rechts neben dem angehängten Datenträger.

Eigenständiges Tool

Benutzer, welche die Einheiten oder Images (.iso/.img) mit dem XClarity Controller anhängen müssen, können den eigenständigen Codeteil „rdmount“ des OneCLI-Pakets verwenden. Insbesondere öffnet „rdmount“ eine Verbindung zum XClarity Controller und hängt die Einheit oder die Images an den Host an.

„rdmount“ hat die folgende Syntax:

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

Beispiel für das Anhängen einer ISO-Datei:

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

Remote-Datenträger mit Java-Client

In diesem Abschnitt wird beschrieben, wie Sie lokale Datenträger mit dem Java-Client anhängen.

Mit dem Java-Client können Sie dem Server ein CD- oder DVD-Laufwerk, ein Diskettenlaufwerk oder ein USB-Flashlaufwerk zuordnen oder Sie können ein Datenträgerimage auf Ihrem Computer angeben, das der Server verwenden kann. Sie können das Laufwerk für verschiedene Funktionen verwenden, z. B. zum

Neustarten (Booten) des Servers, Installieren neuer Software auf dem Server und Installieren oder Aktualisieren des Betriebssystems auf dem Server. Sie haben Zugriff auf den fernen Datenträger. Die Laufwerke und Datenträgerimages werden auf dem Server als USB-Laufwerke angezeigt.

Anmerkungen: Die ferne Konsole von Java unterstützt eine der folgenden Java-Umgebungen und kann nur geöffnet werden, wenn der HTML5-Client nicht ausgeführt wird.

1. Oracle Java-Laufzeitumgebung 1.8/Java SE 8 oder neuere Versionen
2. OpenJDK 8. Die Verteilung von AdoptOpenJDK mit HotSpot JVM wird unterstützt.

Wenn Sie AdoptOpenJDK verwenden, müssen Sie https://openwebstart.com/ unter OS X, Windows und Linux verwenden.

Image-Datei erstellen

Gehen Sie wie folgt vor, um eine neue Image-Datei aus einem angegebenen Quellordner zu erstellen:

1. Klicken Sie im Fenster „Virtuelle Datenträger“ von Java-Client unter der Registerkarte **Virtuelle Datenträger** auf die Option **Image erstellen**. Das Fenster „Image aus Ordner erstellen“ wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Durchsuchen** neben dem Feld **Quellordner**, um den entsprechenden Quellordner auszuwählen.
3. Klicken Sie auf die Schaltfläche **Durchsuchen** neben dem Feld **Neue Image-Datei**, um die gewünschte Image-Datei auszuwählen.
4. Klicken Sie auf die Schaltfläche **Image erstellen**.

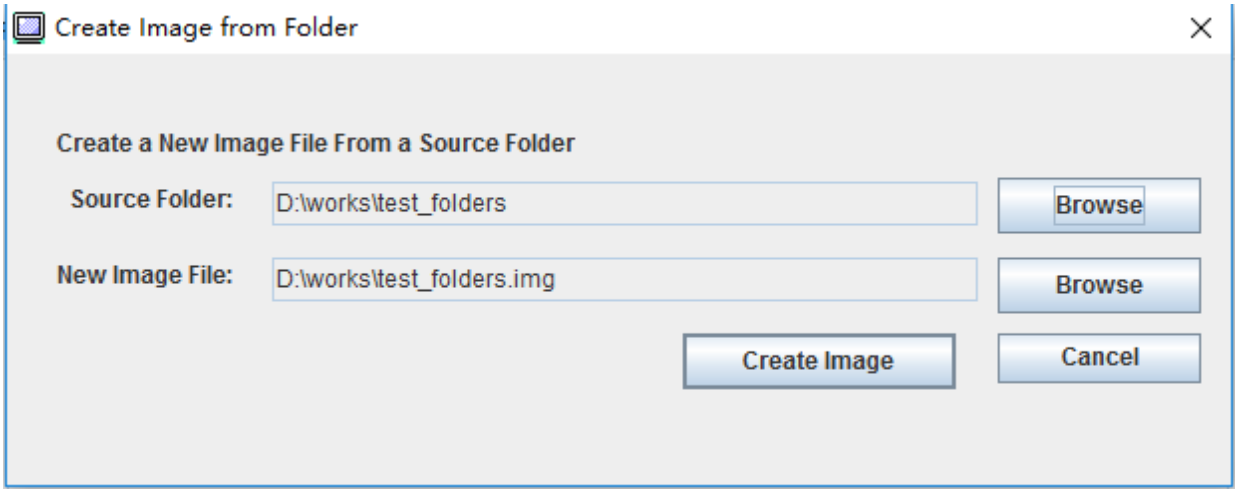


Abbildung 1. Image-Datei erstellen

Einheiten zum Anhängen auswählen

Gehen Sie wie folgt vor, um ein lokales Image, einen Ordner oder ein CD-/DVD-/USB-Laufwerk anzuhängen:

Klicken Sie im Fenster „Virtuelle Datenträger“ von Java-Client unter der Registerkarte **Virtuelle Datenträger** auf die Option **Einheiten zum Anhängen auswählen**. Das Fenster „Einheiten zum Anhängen auswählen“ wird angezeigt.

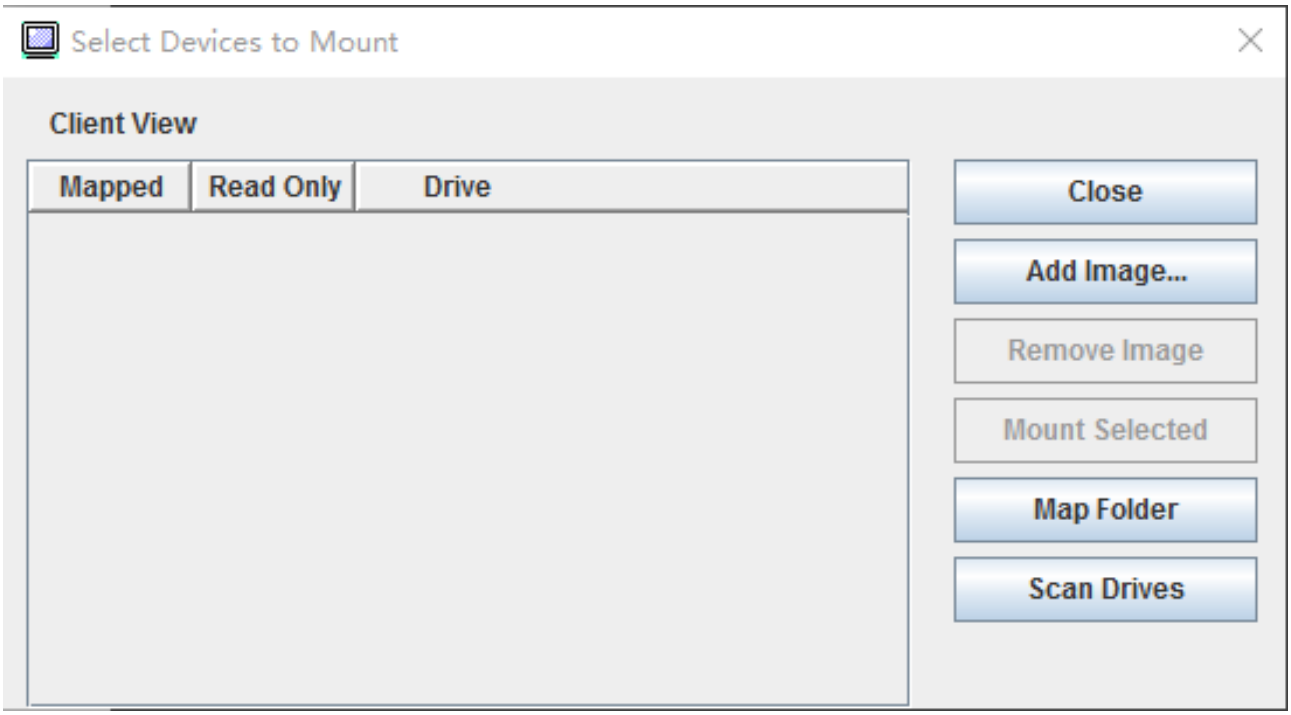


Abbildung 2. Fenster „Einheiten zum Anhängen auswählen“

Gehen Sie wie folgt vor, um ein lokales Image, einen Ordner oder ein CD-/DVD-/USB-Laufwerk anzuhängen:

- **Lokales Image anhängen**:
  1. Klicken Sie auf die Schaltfläche **Image hinzufügen**, um das Image auszuwählen, das Sie anhängen möchten.
  2. Aktivieren Sie das Kontrollkästchen der Option **Zugeordnet**.
  3. Aktivieren Sie ggf. das Kontrollkästchen der Option **Schreibgeschützt**.
  4. Klicken Sie auf die Schaltfläche **Auswahl anhängen**, um das lokale Image erfolgreich anzuhängen.

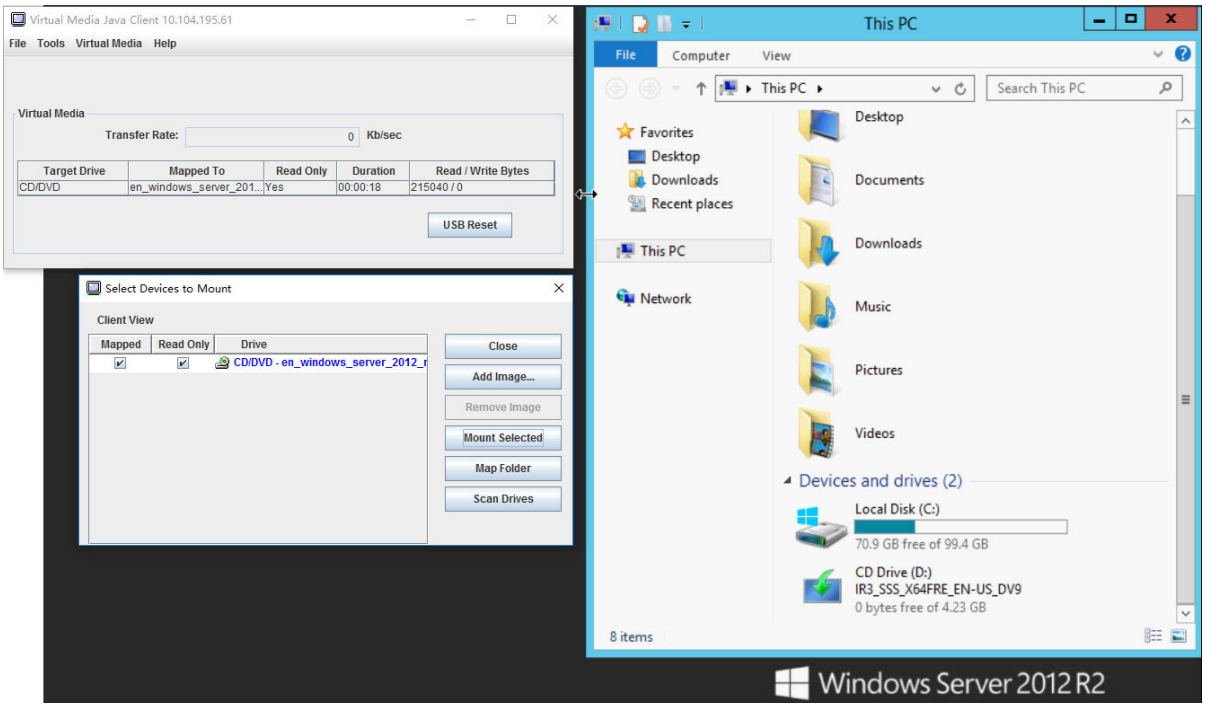


Abbildung 3. Lokales Image anhängen

- **Lokalen Ordner anhängen**:
  1. Klicken Sie auf die Schaltfläche **Ordner zuordnen**, um den lokalen Ordner auszuwählen, den Sie anhängen möchten.
  2. Klicken Sie auf die Schaltfläche **Auswahl anhängen**, um den lokalen Ordner erfolgreich anzuhängen.

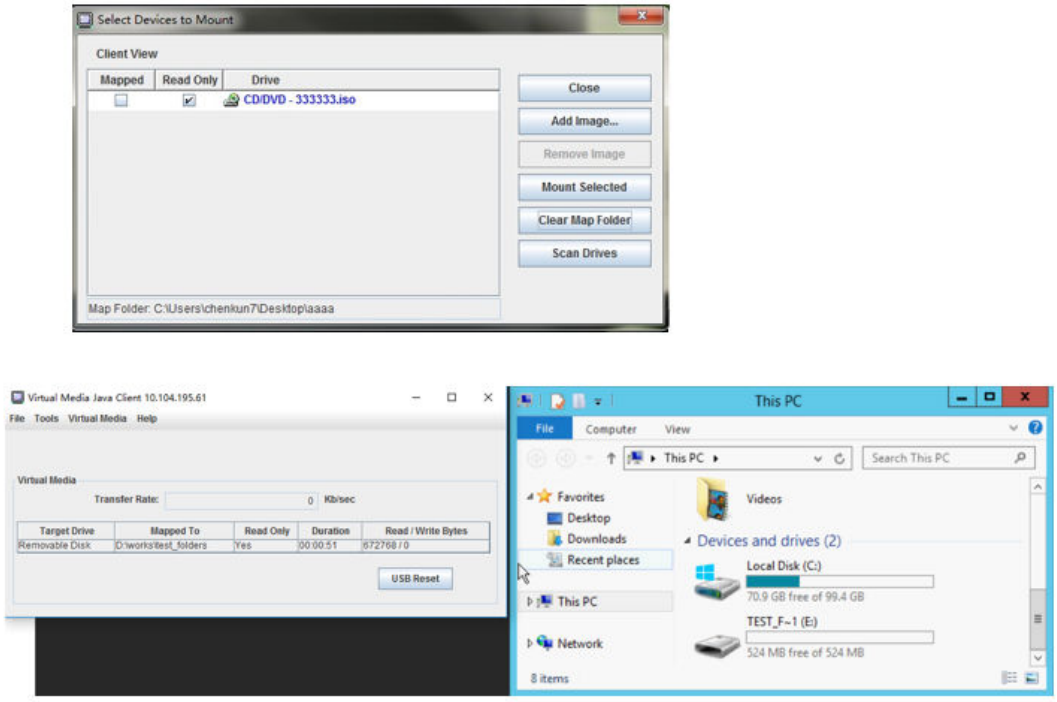


Abbildung 4. Lokalen Ordner anhängen

- **CD-/DVD- oder USB-Laufwerk anhängen**:
  1. Klicken Sie auf die Schaltfläche **Laufwerke scannen**, um ein angeschlossenes CD-/DVD- oder USB-Laufwerk zu ermitteln.
  2. Aktivieren Sie das Kontrollkästchen der Option **Zugeordnet**.
  3. Aktivieren Sie ggf. das Kontrollkästchen der Option **Schreibgeschützt**.
  4. Klicken Sie auf die Schaltfläche **Auswahl anhängen**, um das lokale Image erfolgreich anzuhängen.

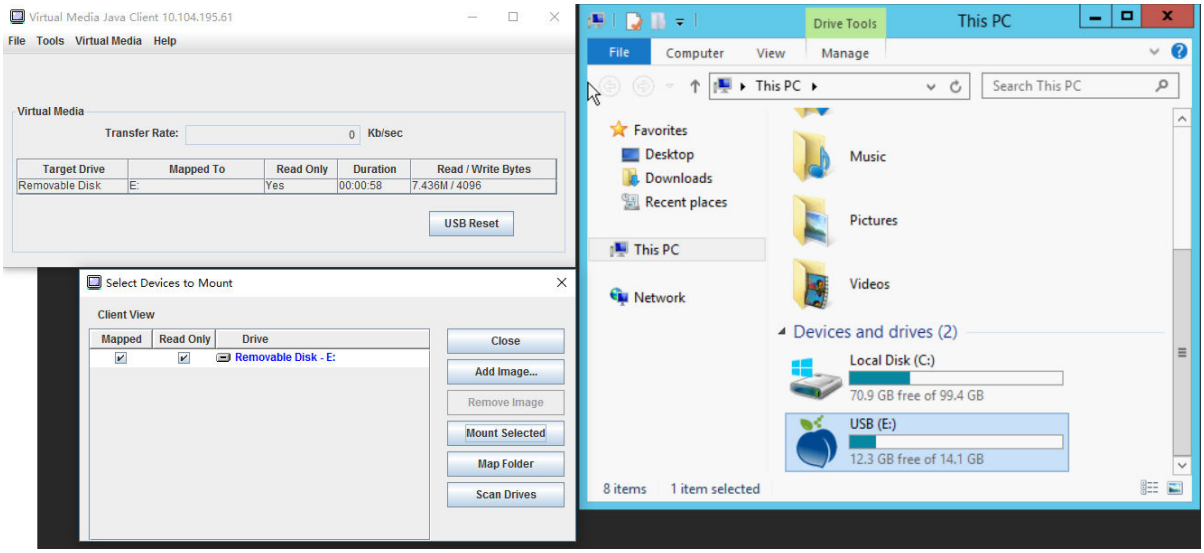


Abbildung 5. CD-/DVD- oder USB-Laufwerk anhängen

Das Fenster „Einheiten zum Anhängen auswählen“ enthält eine aktuelle Liste der lokalen Einheiten, die angehängt werden können. Dieses Fenster enthält die folgenden Felder und Schaltflächen:

- Das Feld **Zugeordnet** enthält das Kontrollkästchen, mit dem Sie die Einheiten auswählen können, die Sie anhängen oder zuordnen möchten.
- Das Feld **Schreibgeschützt** enthält das Kontrollkästchen, mit dem Sie die zugeordneten oder angehängten Einheiten auswählen können, die auf dem Hostserver **schreibgeschützt** sind.
- Das Feld **Laufwerk** enthält den Einheitenpfad auf dem lokalen Computer.
- Klicken Sie auf die Schaltfläche **Schließen**, um das Fenster „Einheiten zum Anhängen auswählen“ zu schließen.
- Klicken Sie auf die Schaltfläche **Image hinzufügen**, um nach dem Diskettenimage und der ISO-Image-Datei in Ihrem lokalen Dateisystem zu suchen, die Sie zur Liste der Einheiten hinzufügen möchten.
- Klicken Sie auf die Schaltfläche **Image entfernen**, um ein Image zu entfernen, das zur Liste der Einheiten hinzugefügt wurde.
- Klicken Sie auf die Schaltfläche **Auswahl anhängen**, um alle Einheiten, die zum Anhängen oder Zuordnen im Feld **Zugeordnet** angekreuzt wurden, anzuhängen oder zuzuordnen.

  Anmerkung: Der Ordner wird schreibgeschützt angehängt.
- Klicken Sie auf die Schaltfläche **Laufwerke scannen**, um die Liste der lokalen Einheiten zu aktualisieren.

Einheiten zum Abhängen auswählen

Gehen Sie wie folgt vor, um Hostserver-Einheiten abzuhängen:

1. Klicken Sie im Fenster „Virtuelle Datenträger“ von Java-Client unter der Registerkarte **Virtuelle Datenträger** auf die Option **Alle abhängen**.
2. Nachdem Sie die Option **Alle abhängen** ausgewählt haben, wird ein Bestätigungsfenster zum Abhängen aller Einheiten angezeigt. Wenn Sie akzeptieren, werden **alle** Hostserver-Einheiten vom Server abgehängt.

   Anmerkung: Sie können Laufwerke nicht einzeln abhängen.

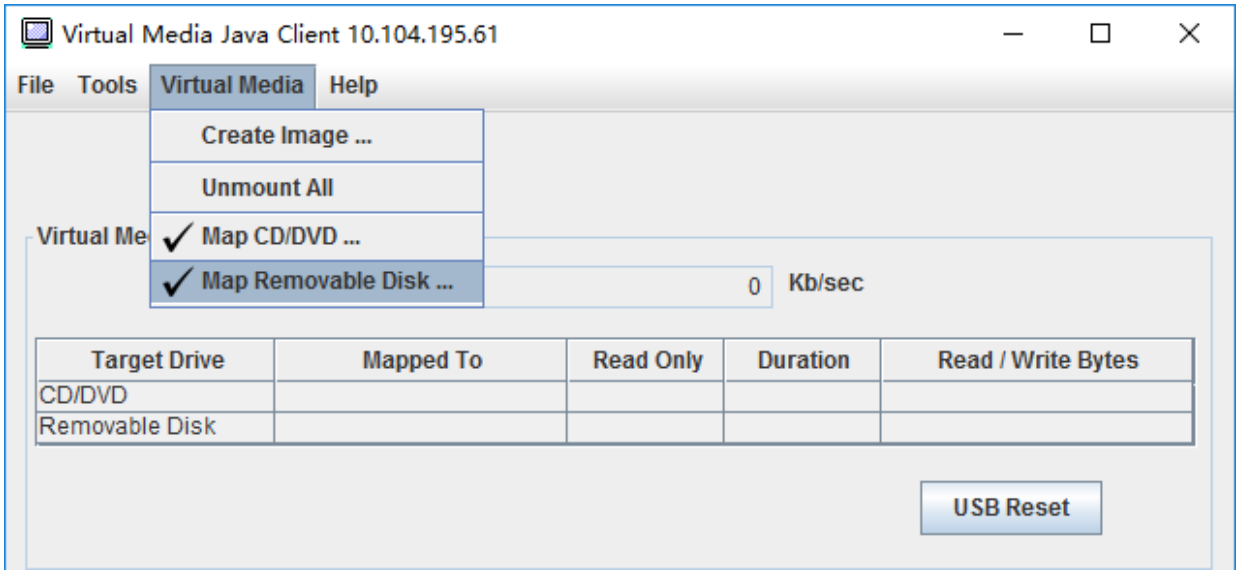


Abbildung 6. Alle abhängen

Fehler beim Anhängen von Datenträgern

Mithilfe der Informationen in diesem Abschnitt können Sie Probleme beim Anhängen von Datenträgern beheben.

Beim Anhängevorgang für von Microsoft IIS generierten Sicherheitszertifikaten können Fehler auftreten. Ist dies der Fall, ersetzen Sie das Sicherheitszertifikat durch ein neues, das von openssl generiert wurde. Die neu erstellte pfx-Datei wird auf den Microsoft IIS-Server geladen.

Das folgende Beispiel zeigt, wie das neue Sicherheitszertifikat über openssl beim Linux-Betriebssystem generiert wird.

```
$ openssl
OpenSSL>

$ openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)

$ openssl req -new -key server.key > server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:HD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo
Organizational Unit Name (eg, section) []:Lenovo
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:LNV

$ ls
server.csr  server.key

$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV
Organizational Unit Name (eg, section) []:LNV
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

$ ls
server.crt  server.csr  server.key

$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
```

```
Enter Export Password:
Verifying - Enter Export Password:

$ ls
server.crt  server.csr  server.key  server.pfx
```

Sitzung der fernen Konsole beenden

In diesem Abschnitt wird erläutert, wie Sie die Sitzung der fernen Konsole beenden.

Schließen Sie zum Beenden Ihrer Konsolensitzung die Fenster „Ferne Konsole“ und „Sitzung mit virtuellen Datenträgern“.

Servicedaten herunterladen

Mithilfe der Informationen in diesem Abschnitt können Sie Serviceinformationen über Ihren Server sammeln. Dies erfolgt normalerweise nur auf Anforderung von Servicetechnikern, die bei der Lösung eines Serverproblems helfen.

Klicken Sie auf der XClarity Controller-Startseite auf die Option **Service** im Abschnitt **Schnelle Aktion** und wählen Sie **Servicedaten herunterladen** aus. Klicken Sie auf **OK**, um die Servicedateien herunterzuladen.

Das Sammeln der Service- und Supportdaten dauert einige Minuten, um die Servicedaten zu generieren. Die Datei wird in Ihrem Standarddownloadordner gespeichert. Die Namenskonvention für die Servicedatendatei lautet wie folgt:`<machine type and model>_<serial number>_xcc_<date>-<time>.tgz`

Beispiel: 7X2106Z01A_2345678_xcc_170511-175656.tgz.

Zusätzlich zum tgz-Format können die Servicedaten auch im tzz-Format heruntergeladen werden. Tzz verwendet einen anderen Komprimierungsalgorithmus und kann mit einem Dienstprogramm wie „lzop“ extrahiert werden.

Servereigenschaften

Mithilfe der Informationen in diesem Abschnitt können Sie die relevanten Servereigenschaften anzeigen oder ändern.

Position und Kontakt festlegen

Mithilfe der Informationen in diesem Abschnitt können Sie verschiedene Parameter festlegen, die Ihnen dabei helfen, das System gegenüber Bedien- und Supportpersonal zu identifizieren.

Wählen Sie unter **Serverkonfiguration** die Option **Servereigenschaften**, um **Standort und Kontakt** zu definieren.

Kontakt
Ermöglicht es Ihnen, den Namen und die Telefonnummer der Person anzugeben, die im Falle eines Problems mit diesem System kontaktiert werden soll.

Anmerkung: Dieses Feld ist mit dem Feld „Kontakt“ in der SNMPv3-Konfiguration identisch. Es ist erforderlich, damit SNMPv3 aktiviert werden kann.

Rack-Name
Ermöglicht es Ihnen, den Server durch Angabe des Racks, in dem er sich befindet, leichter zu finden.

Anmerkung: Das Feld ist optional und lässt sich nicht in einem Flex-Knoten konfigurieren.

Raumnummer
Ermöglicht es Ihnen, den Server durch Angabe des Raums, in dem er sich befindet, leichter zu finden.

Gebäude
Ermöglicht es Ihnen, den Server durch Angabe des Gebäudes, in dem er sich befindet, leichter zu finden.

Niedrigste U
Ermöglicht es Ihnen, den Server durch Angabe der Position im Rack leichter zu finden.

Anmerkung: Das Feld ist optional und lässt sich nicht in einem Flex-Knoten konfigurieren.

Adresse
Ermöglicht die Angabe der vollständigen Postanschrift, unter der sich der Server befindet.

Anmerkung: Wenn die erforderlichen Informationen eingegeben wurden, werden sie auf der XClarity Controller-Startseite im Abschnitt „SNMPv3“ in einer einzigen Zeile im Feld **Position** angezeigt.

Serverzeitlimits festlegen

Mithilfe der Informationen in diesem Abschnitt können Sie Zeitlimits für den Server festlegen.

Diese Zeitlimits werden zur Wiederherstellung von Vorgängen auf einem Server verwendet, der blockiert ist.

Wählen Sie unter **Serverkonfiguration** die Option **Servereigenschaften** aus, um die Serverzeitlimits zu konfigurieren. Es stehen folgende Serverzeitlimits zur Auswahl:

BS-Watchdog
Mit dem BS-Watchdog wird das Betriebssystem überwacht, um sicherzustellen, dass es nicht blockiert ist. Die Ethernet-over-USB-Schnittstelle muss für diese Funktion aktiviert sein. Details hierzu finden Sie im Abschnitt „Ethernet-over-USB konfigurieren“ auf Seite 34. Der XClarity Controller kontaktiert das Betriebssystem in einem Intervall, das in der Auswahl **BS-Watchdog-Zeit** konfiguriert ist. Wenn das Betriebssystem nicht reagiert, bevor es Zeit für die nächste Prüfung ist, geht der XClarity Controller davon aus, dass das Betriebssystem blockiert ist. Der XClarity Controller erfasst die Inhalte der Serveranzeige und startet anschließend den Server neu, um den Betrieb wiederherzustellen. Der XClarity Controller startet den Server nur einmal neu. Wenn das Betriebssystem nach dem Neustart weiterhin blockiert ist, verbleibt der Server in diesem blockierten Zustand, anstatt dass er immer wieder neu gestartet wird, sodass das Problem untersucht und behoben werden kann. Zum Zurücksetzen des BS-Watchdogs schalten Sie den Server aus und wieder ein. Um den BS-Watchdog zu aktivieren, wählen Sie ein Intervall aus der Dropdown-Liste **BS-Watchdog-Zeit** aus und klicken Sie auf „Übernehmen“. Um den BS-Watchdog zu deaktivieren, wählen in der Dropdown-Liste **BS-Watchdog-Zeit** die Option „Keine“ aus.

Watchdog für das Ladeprogramm
Der Watchdog für das Ladeprogramm überwacht das Intervall zwischen der Fertigstellung von POST und dem Beginn der Ausführung des Betriebssystems. Die Ethernet-over-USB-Schnittstelle muss für diese Funktion aktiviert sein. Details hierzu finden Sie im Abschnitt „Ethernet-over-USB konfigurieren“ auf Seite 34. Wenn POST beendet ist, startet der XClarity Controller einen Zeitgeber und beginnt, mit dem Betriebssystem Kontakt aufzunehmen. Wenn das Betriebssystem nicht innerhalb des in der Auswahl des Watchdogs für das Ladeprogramm konfigurierten Zeitraums reagiert, geht der XClarity Controller davon aus, dass der Bootvorgang des Betriebssystems blockiert ist. Der XClarity Controller startet dann den Server in dem Versuch neu, den Betrieb wiederherzustellen. Der XClarity Controller startet den Server nur einmal neu. Wenn das Booten des Betriebssystems nach dem Neustart weiterhin blockiert ist, verbleibt der Server in diesem blockierten Zustand, anstatt dass er immer wieder neu gestartet wird, sodass das Problem untersucht und behoben werden kann. Der Watchdog für das Ladeprogramm wird zurückgesetzt, wenn der Server aus- und wiedereingeschaltet wird oder wenn der

Server erfolgreich in das Betriebssystem bootet. Um den Watchdog für das Ladeprogramm zu aktivieren, wählen Sie ein Intervall aus der Dropdown-Liste **Watchdog für das Ladeprogramm** aus und klicken Sie auf „Übernehmen“. Um den Watchdog für das Ladeprogramm zu deaktivieren, wählen in der Dropdown-Liste **Watchdog für das Ladeprogramm** die Option „Keine“ aus.

Ausschaltverzögerung aktivieren

Verwenden Sie das Feld „Ausschaltverzögerung“, um anzugeben, wie viele Minuten das XClarity Controller-Subsystem auf das Herunterfahren des Betriebssystems warten soll, bevor es das Abschalten erzwingt. Um den Wert für die Ausschaltverzögerung festzulegen, wählen Sie das Zeitintervall aus der Dropdown-Liste aus und klicken Sie auf **Übernehmen**. Um den XClarity Controller für das Erzwingen des Ausschaltens zu deaktivieren, wählen Sie in der Dropdown-Liste **Keine** aus.

Überschreitungsnachricht

Um die Meldung zu erstellen, die angezeigt wird, wenn sich ein Benutzer beim XClarity Controller anmeldet, verwenden Sie die Informationen in diesem Abschnitt.

Wählen Sie **Servereigenschaften** unter **Serverkonfiguration** aus. Verwenden Sie die Option **Trespass-Meldung**, um eine Meldung zu konfigurieren, die dem Benutzer angezeigt werden soll. Klicken Sie abschließend auf **Übernehmen**.

Der Meldungstext wird im Nachrichtenbereich der XClarity Controller-Anmeldeseite angezeigt, wenn sich ein Benutzer anmeldet.

Datum und Uhrzeit für XClarity Controller einstellen

Dieser Abschnitt enthält Informationen zu den Datums- und Zeiteinstellungen von XClarity Controller. Sie finden hier Anweisungen für die Konfiguration von Datum und Uhrzeit von XClarity Controller. Das Datum und die Uhrzeit von XClarity Controller werden verwendet, um alle Ereignisse mit Zeitstempel zu versehen, die im Ereignisprotokoll aufgezeichnet werden, sowie alle Alerts, die versendet werden.

Klicken Sie auf der XClarity Controller-Startseite auf das Uhrensymbol in der rechten oberen Ecke, um Datum und Uhrzeit von XClarity Controller anzuzeigen oder zu ändern. Der XClarity Controller hat keine eigene Echtzeituhr. Sie können den XClarity Controller so konfigurieren, dass seine Uhrzeit und sein Datum mit einem Network Time Protocol-Server oder mit der Echtzeituhr-Hardware des Servers synchronisiert werden.

Synchronisation mit NTP

Gehen Sie wie folgt vor, um die Uhr von XClarity Controller mit dem NTP-Server zu synchronisieren:

- Wählen Sie **Zeit synchronisieren mit NTP** aus und geben die NTP-Serveradresse an.
- Sie können weitere NTP-Server angeben, indem Sie auf das Symbol „+“ klicken.
- Geben Sie an, wie häufig der XClarity Controller mit dem NTP-Server synchronisiert werden soll.
- Die Zeit, die vom NTP-Server abgerufen wird, liegt im UTC-Format (Coordinated Universal Time) vor.
  - Wenn Sie möchten, dass der XClarity Controller seine Uhrzeit und sein Datum für Ihre lokale Region anpasst, wählen Sie die Zeitzonenverschiebung für Ihr Gebietsschema aus dem Dropdown-Menü aus.
  - Wenn für Ihr Standort die Sommerzeit gilt, aktivieren Sie das Kontrollkästchen **Automatisch an Sommerzeit anpassen**.
- Wenn die Konfigurationsänderungen abgeschlossen sind, klicken Sie auf **Übernehmen**.

Synchronisation mit dem Host

Die Zeit, die in der Echtzeituhr-Hardware des Servers gespeichert ist, kann im UTC-Format vorliegen oder bereits an die Ortszeit angepasst und in diesem Format gespeichert worden sein. Einige Betriebssysteme speichern die Echtzeituhr im UTC-Format, andere wiederum als Ortszeit. Die Echtzeituhr des Servers gibt

nicht an, in welchem Format die Uhrzeit vorliegt. Wenn also der XClarity Controller so konfiguriert ist, dass er sich mit der Echtzeituhr des Hosts synchronisiert, kann der Benutzer angeben, wie der XClarity Controller die Uhrzeit und das Datum von der Echtzeituhr verwenden soll.

- Lokal (Beispiel: Windows): In diesem Modus behandelt der XClarity Controller die Uhrzeit und das Datum, die von der Echtzeituhr abgerufen werden, als Ortszeit mit den jeweils gültigen Zeitzonen- und Sommerzeitverschiebungen.
- UTC (Beispiel: Linux): In diesem Modus behandelt der XClarity Controller die Uhrzeit und das Datum, die von der Echtzeituhr abgerufen werden, als UTC-Zeit ohne die jeweils gültigen Zeitzonen- und Sommerzeitverschiebungen. In diesem Modus können Sie angeben, dass die Uhrzeit und das Datum für Ihre lokale Region angepasst werden soll, indem Sie die Zeitzonenverschiebung für Ihr Gebietsschema aus dem Dropdown-Menü auswählen. Wenn für Ihren Standort die Sommerzeit gilt, können Sie auch das Kontrollkästchen **Automatisch an Sommerzeit anpassen** aktivieren.
- Wenn die Konfigurationsänderungen abgeschlossen sind, klicken Sie auf **Übernehmen**

Anmerkungen:

- Bei Eintreten der Sommerzeit werden alle Aktionen, die für den XClarity Controller für den Zeitraum terminiert wurden, in dem die Uhr vorgestellt wird, nicht ausgeführt. Wenn beispielsweise der Beginn für die Sommerzeit in den USA für den 12. März auf 2:00 Uhr morgens festgelegt ist und für 2:10 Uhr am selben Tag eine Aktion eingeplant ist, wird diese nicht ausgeführt. Sobald 2.00 Uhr erreicht ist, liest der XClarity Controller die Uhrzeit als 3.00 Uhr.
- Die Datums- und Zeiteinstellungen von XClarity Controller können in einem Flex System nicht geändert werden.

Kapitel 6. Speicher konfigurieren

Verwenden Sie die Informationen in diesem Kapitel, um mehr über die für Speicherkonfigurationen verfügbaren Optionen zu erfahren.

Bei der Speicherkonfiguration sind die folgenden Optionen verfügbar:

- Detail
- RAID-Konfiguration

RAID-Detail

Mithilfe der Informationen in diesem Abschnitt können Sie die Funktion „RAID-Detail“ verwenden.

Diese Funktion zeigt die physische Struktur und Speicherkonfiguration der Speichereinheiten zusammen mit Details wie Standort, Hersteller, Produktname, Status, Kapazität, Schnittstelle, Medien, Formfaktor und anderen Informationen an.

RAID-Konfiguration

Mithilfe der Informationen in diesem Abschnitt können Sie RAID konfigurieren.

Verwenden Sie die Informationen in diesem Abschnitt, um Speicherpools, zugehörige virtuelle Platten und Laufwerke für den RAID-Controller anzuzeigen und zu konfigurieren. Wenn das System ausgeschaltet ist, schalten Sie es ein, um die RAID-Informationen anzuzeigen.

Virtuelle Laufwerke anzeigen und konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie virtuelle Laufwerke anzeigen und konfigurieren.

Wenn Sie unter **Serverkonfiguration** die Option **RAID-Konfiguration** auswählen, wird die Registerkarte **Konfiguration für die Einheit** ausgewählt. Standardmäßig werden die vorhandenen virtuellen Platten angezeigt. Die logischen Laufwerke sind nach Platteneinheiten und Controllern sortiert. Außerdem werden detaillierte Informationen zu den virtuellen Platten angezeigt, wie z. B. die Stripgröße und die Bootfähigkeit des Datenträgers.

Um die RAID-Einstellungen zu konfigurieren, klicken Sie auf **Bearbeitungsmodus aktivieren**.

Im Bearbeitungsmodus können Sie auf das Controller-Aktionsmenü klicken, die aktuellen virtuellen RAID-Platten anzeigen und neue virtuelle RAID-Platten erstellen.

Im Menü „Controlleraktionen“ können Sie die folgenden Aktionen ausführen:

RAID-Konfiguration löschen
Löscht die gesamte Konfiguration und alle Daten auf dem ausgewählten Controller.

Fremde Konfiguration verwalten
Sie können alle erkannten fremden Laufwerke importieren. Ein fremdes Laufwerk ist ein Laufwerk, das von einer anderen RAID-Konfiguration in den aktuellen RAID-Controller verschoben wurde.

Anmerkung: Sie werden benachrichtigt, wenn keine fremden Laufwerke erkannt wurden.

Die Informationen zu den aktuellen virtuellen RAID-Platten für einen bestimmten Controller werden jeweils als „Karten der virtuellen Platte“ angezeigt. Jede Karte enthält Informationen wie Name, Status, Kapazität und Aktionen der virtuellen Platte. Das Stiftssymbol ermöglicht es Ihnen, die Informationen zu bearbeiten. Über das Papierkorbsymbol können Sie die Karte der virtuellen Platte löschen.

Anmerkung: Die Kapazität und die RAID-Stufe können nicht geändert werden.

Wenn Sie auf den Namen der virtuellen Platte klicken, wird das Fenster mit den Eigenschaften der virtuellen Platte angezeigt.

Wenn Sie eine neue virtuelle RAID-Platte erstellen möchten, führen Sie die folgenden Schritte aus:

Anmerkung: Wenn keine verbleibende Speicherkapazität vorhanden ist, können Sie keine neue virtuelle Platte erstellen.

1. **Laufwerke oder Platteneinheit mit freier Speicherkapazität auswählen**
   a. Wenn Sie eine virtuelle Platte in einer neuen Platteneinheit erstellen, müssen Sie die RAID-Stufe angeben. Wenn es nicht genügend Laufwerke zum Auswählen gibt und Sie auf **Weiter** klicken, wird eine Fehlernachricht unter dem Feld mit der RAID-Stufe angezeigt.

      Bei einigen RAID-Stufen ist ein Bereich erforderlich. Zudem muss eine Mindestanzahl Laufwerke im Bereich verfügbar sein.

      1) In diesem Fall zeigt die Webschnittstelle standardmäßig **Bereich 1** an.
      2) Wählen Sie die Laufwerke aus und klicken Sie auf **Member hinzufügen**, um die Laufwerke **Bereich 1** hinzuzufügen. Wenn **Bereich 1** nicht über genügend Laufwerke verfügt, deaktivieren Sie den Link **Bereich hinzufügen**.
      3) Klicken Sie auf **Bereich hinzufügen**, um **Bereich 2** hinzuzufügen. Wählen Sie die Laufwerke aus und klicken Sie auf **Member hinzufügen**, um die Laufwerke **Bereich 2** hinzuzufügen.
      4) Klicken Sie auf **Member hinzufügen**, um Laufwerke zum letzten Bereich hinzuzufügen. Wenn Sie Laufwerke erneut **Bereich 1** hinzufügen möchten, müssen Sie auf Bereich 1 klicken und die Laufwerke auswählen, um sie **Bereich 1** hinzuzufügen.
      5) Wenn die Anzahl der Bereiche die maximale Anzahl erreicht, deaktivieren Sie **Bereich hinzufügen**.

   b. Um virtuelle Platten in einer vorhandenen Platteneinheit zu erstellen, müssen Sie eine Platteneinheit auswählen, die freie Kapazität aufweist.
2. **Virtuelle Platte erstellen**
   a. Standardmäßig erstellen Sie eine virtuelle Platte, die die gesamte Speicherkapazität verwendet. Das Symbol **Hinzufügen** wird deaktiviert, wenn der gesamte Speicher aufgebraucht ist. Sie können auf das Stiftssymbol klicken, um die Kapazität oder andere Eigenschaften zu ändern.
   b. Wenn Sie die erste virtuelle Platte so bearbeiten, dass nur ein Teil der Speicherkapazität verwendet wird, wird das Symbol **Hinzufügen** aktiviert. Klicken Sie auf das Symbol, um das Fenster **Virtuelle Platte hinzufügen** zu öffnen.
   c. Wenn mehr als eine virtuelle Platte vorhanden ist, wird das Symbol **Entfernen** aktiviert. Dieses Symbol wird nicht angezeigt, wenn nur eine virtuelle Platte vorhanden ist. Wenn Sie auf das Symbol **Entfernen** klicken, wird die ausgewählte Zeile sofort gelöscht. Es wird kein Bestätigungsfenster angezeigt, da die virtuelle Platte noch nicht erstellt wurde.
   d. Klicken Sie auf **Erstellung einer virtuellen Platte starten**, um den Vorgang zu starten.

Anmerkung: Wenn der Controller nicht unterstützt wird, wird eine entsprechende Meldung angezeigt.

Speicherbestand anzeigen und konfigurieren

Mithilfe der Informationen in diesem Abschnitt können Sie den Speicherbestand anzeigen und konfigurieren.

Auf der Registerkarte **Speicherbestand** können Sie die Platteneinheiten, zugehörigen virtuellen Platten und Laufwerke für den RAID-Controller anzeigen und konfigurieren.

- **Für Speichereinheiten, die die RAID-Konfiguration unterstützen**:
  1. Wenn der Controller konfigurierte Platteneinheiten umfasst, werden die installierten Laufwerke basierend auf der Platteneinheit angezeigt. Im Folgenden werden die Elemente beschrieben, die im Fenster angezeigt werden.
     - **Tabellentitel**: Zeigt die ID der Platteneinheit, die RAID-Stufe und die Gesamtzahl der Laufwerke an.
     - **Tabelleninhalt**: Listet die grundlegenden Eigenschaften auf, z. B. Laufwerkname, RAID-Status, Typ, Seriennummer, Teilenummer, FRU-Nummer und Aktionen. Sie können auf die Seite **Bestand** wechseln, um alle Eigenschaften anzuzeigen, die der XClarity Controller erkennen kann.
     - **Aktionen**: Im Folgenden sind die Aktionselemente aufgeführt, die ausgeführt werden können. Einige Aktionen sind nicht verfügbar, wenn sich das Laufwerk in einem anderen Zustand befindet.
       - **Hot-Spare-Einheit zuordnen**: Gibt das Laufwerk als globale Hot-Spare- oder dedizierte Hot-Spare-Einheit an.
       - **Hot-Spare-Einheit entfernen**: Entfernt das Laufwerk aus dem Hot-Spare.
       - **Plattenlaufwerkstatus festlegen als offline**: Setzt das Laufwerk auf offline.
       - **Plattenlaufwerkstatus festlegen als online**: Setzt das Laufwerk auf online.
       - **Plattenlaufwerkstatus festlegen als wiederverwendbar**: Setzt das Laufwerk auf wiederverwendbar.
       - **Plattenlaufwerkstatus festlegen als fehlend**: Markiert das Laufwerk als fehlend.
       - **Laufwerk auf „gut für JBOD“ setzen**: Fügt das Laufwerk der JBOD-Plattenanordnung hinzu.
       - **Laufwerk auf „unkonfiguriert gut“ setzen**: Stellt das Laufwerk für die Konfiguration in einem Array oder zur Verwendung als Notfall-Hot-Spare zur Verfügung.
       - **Laufwerk auf „unkonfiguriert schlecht“ setzen**: Markiert das Laufwerk als fehlerhaft und verhindert, dass es in einem Array oder als Notfall-Hot-Spare verwendet wird.
       - **Plattenlaufwerkstatus festlegen als Vorbereiten für Entfernen**: Markiert das Laufwerk zum Entfernen.
  2. Wenn der Controller Laufwerke enthält, die noch nicht konfiguriert wurden, werden sie in der Tabelle **Non-RAID-Laufwerke** angezeigt. Durch Klicken auf **JBOD zu „Bereit zur Konfiguration“ konvertieren** wird ein Fenster geöffnet, das alle Laufwerke anzeigt, die dieses Aktionselement unterstützen. Sie können ein oder mehrere Laufwerke für die Konvertierung auswählen.

Für Speichereinheiten, die keine RAID-Konfiguration unterstützen: Der XClarity Controller ist möglicherweise nicht in der Lage, die Eigenschaften von einigen Laufwerken zu erkennen.

Kapitel 7. Server-Firmware aktualisieren

Mithilfe der Informationen in diesem Abschnitt können Sie die Server-Firmware aktualisieren.

Übersicht

Allgemeine Informationen zur Aktualisierung von Server-Firmware.

Die Option **Firmwareaktualisierung** im Navigationsbereich hat 4 Funktionen:

- **Systemfirmware:** Übersicht über Status und Version der Systemfirmware. Dient außerdem zur Aktualisierung der Systemfirmware.
- **Automatisierte Hochstufung von primärem XCC zu Sicherung**: Nach dem Aktivieren wird die ausstehende Sicherungsspeicherbank-Firmware von der Primärgruppe synchronisiert, nachdem die Primärgruppe die ISM-Messung (Image Stability Metric) bestanden hat.
- **Adapterfirmware:** Übersicht über installierte Adapterfirmware, ihren Status und die Version. Dient außerdem zur Aktualisierung der Adapterfirmware.

Der aktuelle Status und die aktuellen Versionen der BMC-, UEFI-, LXPM- und LXPM-Treiber und -Adapter werden angezeigt, einschließlich der primären BMC-Versionen und BMC-Sicherungsversionen. Der Status der Firmware wird in vier Kategorien angegeben:

- **Aktiv:** Die Firmware ist aktiv.
- **Inaktiv:** Die Firmware ist inaktiv.
- **Ausstehend:** Die Firmware befindet sich im Wartestatus vor der Aktivierung.
- **Nicht zutreffend:** Für diese Komponente wurde keine Firmware installiert.

Achtung:

- XCC und IMM müssen auf die neueste Version aktualisiert werden, bevor Sie UEFI aktualisieren. Wenn die Aktualisierung in einer anderen Reihenfolge erfolgt, kann dies zu einem falschen Verhalten führen.
- Die Installation der falschen Firmware könnte eine Serverstörung verursachen. Bevor Sie eine Firmware- oder Einheitentreiberaktualisierung installieren, lesen Sie alle Readme- und Änderungsprotokolldateien, die mit der heruntergeladenen Aktualisierung bereitgestellt werden. Diese Dateien enthalten wichtige Informationen zur Aktualisierung und zur Installationsprozedur der Aktualisierung, einschließlich Informationen zu besonderen Prozeduren bei der Aktualisierung von einer frühen Firmware- oder Einheitentreiberversion auf die neueste Version. Da der Webbrowser möglicherweise XCC-Cachedaten enthält, wird empfohlen, die Webseite nach der Aktualisierung der XCC-Firmware neu zu laden.
- Bei einigen Firmwareaktualisierungen ist ein Neustart des Systems erforderlich, durch den die Firmware aktiviert oder die interne Aktualisierung ausgeführt wird. Dieser Vorgang beim Systemstart wird als „Systemwartungsmodus“ bezeichnet und er lässt vorübergehend keine Stromversorgungsaktionen durch den Benutzer zu. Der Modus wird außerdem während der Firmwareaktualisierung aktiviert. Wenn das System in den Wartungsmodus wechselt, darf der Benutzer die Wechselstromversorgung nicht trennen.

System-, Adapter- und PSU-Firmwareaktualisierung

Schritte zum Update von Systemfirmware, Adapterfirmware und PSU-Firmware.

Gehen Sie wie folgt vor, um die **Systemfirmware**, **Adapterfirmware** und **PSU-Firmware** manuell zu aktualisieren:

1. Klicken Sie in den einzelnen Funktionen auf **Firmware aktualisieren**. Das Fenster „Server-Firmware aktualisieren“ wird geöffnet.
2. Klicken Sie auf **Durchsuchen**, um die Firmwareaktualisierungsdatei auszuwählen, die Sie verwenden möchten.
3. Navigieren Sie zu der Datei, die Sie auswählen möchten, und klicken Sie auf **Öffnen**. Sie kehren zum Fenster „Server-Firmware aktualisieren“ zurück. Die ausgewählte Datei wird angezeigt.
4. Klicken Sie auf **Weiter >**, um die ausgewählte Datei hochzuladen und zu prüfen. Eine Fortschrittsanzeige erscheint, während die Datei hochgeladen und überprüft wird. Sie können dieses Statusfenster anzeigen, um zu prüfen, ob Sie die richtige Datei zur Aktualisierung ausgewählt haben. Bei **Systemfirmware** enthält das Statusfenster Informationen zum Dateityp der Firmware, die aktualisiert wird, wie BMC, UEFI oder LXPM. Nachdem die Firmwaredatei erfolgreich hochgeladen und überprüft wurde, klicken Sie auf **Weiter**, um die Einheit auszuwählen, die Sie aktualisieren möchten.
5. Klicken Sie zum Starten der Firmwareaktualisierung auf **Aktualisieren**. Eine Statusanzeige zeigt den Fortschritt der Aktualisierung an. Wenn die Firmwareaktualisierung erfolgreich abgeschlossen wurde, klicken Sie auf **Fertigstellen**. Wenn die Aktualisierung einen Neustart von XClarity Controller erfordert, damit sie wirksam wird, wird eine Warnung angezeigt. Weitere Informationen zum Neustart vom XClarity Controller finden Sie unter „Stromversorgungsaktionen“ auf Seite 66.

Kapitel 8. Lizenzverwaltung

Über die Lenovo XClarity Controller-Lizenzverwaltung können Sie optionale Server und Systemmanagementfunktionen installieren und verwalten.

Für Ihren Server gibt es mehrere Versionen von XClarity Controller-Firmwarefunktionalitäten und -Funktionen. Die Version der auf Ihrem Server installierten Firmwarefunktionen variiert je nach Hardwaretyp.

Sie können die XClarity Controller-Funktionen aktualisieren, indem Sie einen Aktivierungsschlüssel erwerben und installieren.

Wenden Sie sich an den zuständigen Vertriebsmitarbeiter oder Vertragshändler, um einen Aktivierungsschlüssel anzufordern.

Verwenden Sie die XClarity Controller-Webschnittstelle oder die XClarity Controller-Befehlszeilenschnittstelle, um manuell einen Aktivierungsschlüssel zu installieren, mit dem Sie eine optionale Funktion verwenden können, die Sie erworben haben. Beachten Sie Folgendes, bevor Sie einen Schlüssel aktivieren:

- Der Aktivierungsschlüssel muss sich auf dem System befinden, das Sie verwenden, um sich am XClarity Controller anzumelden.
- Sie müssen den Lizenzschlüssel angefordert und seinen Berechtigungscode per Post oder E-Mail erhalten haben.

Informationen zur Verwaltung eines Aktivierungsschlüssels mithilfe der XClarity Controller-Webschnittstelle finden Sie unter „Aktivierungsschlüssel installieren“ auf Seite 95, „Aktivierungsschlüssel entfernen“ auf Seite 96 oder „Aktivierungsschlüssel exportieren“ auf Seite 96. Informationen zur Verwaltung eines Aktivierungsschlüssels mithilfe der XClarity Controller-Befehlszeilenschnittstelle finden Sie unter „Befehl „keycfg““ auf Seite 134.

Um eine ID für die Verwaltung Ihrer XClarity Controller-Lizenz zu registrieren, klicken Sie auf den folgenden Link: https://fod.lenovo.com/lkms/angular/app/pages/index.htm#/welcome

Weitere Informationen zur Lizenzverwaltung für Lenovo Server finden Sie auf der folgenden **Lenovo Press**-Website:

https://lenovopress.com/redp4895-using-lenovo-features-on-demand

Achtung: Sie können nicht direkt von Standard XClarity Controller auf die Enterprise Level-Funktionalität aktualisieren. Sie müssen zuerst ein Upgrade auf das Advanced Level durchführen, bevor die Enterprise Level-Funktionalität aktiviert werden kann.

Aktivierungsschlüssel installieren

Mithilfe der Informationen in diesem Abschnitt können Sie eine Zusatzfunktion zu Ihrem Server hinzufügen.

Gehen Sie wie folgt vor, um einen Aktivierungsschlüssel zu installieren:

Schritt 1. Klicken Sie auf unter **BMC-Konfiguration** auf **Lizenz**.

Schritt 2. Klicken Sie auf **Upgrade-Lizenz**.

Schritt 3. Klicken Sie im Fenster **Neue Lizenz hinzufügen** auf **Durchsuchen**, wählen Sie dann die hinzuzufügende Aktivierungsschlüsseldatei im Fenster zum Hochladen von Dateien aus und

klicken Sie auf **Öffnen**, um die Datei hinzuzufügen, oder klicken Sie auf **Abbrechen**, um die Installation abzubrechen. Um das Hinzufügen des Schlüssels fertigzustellen, klicken Sie im Fenster „Aktivierungsschlüssel hinzufügen“ auf **OK** oder klicken Sie auf **Abbrechen**, um die Installation zu stoppen.

Das Fenster „Erfolg“ gibt an, dass der Aktivierungsschlüssel installiert wurde.

Anmerkungen:

- Wenn der Aktivierungsschlüssel nicht gültig ist, wird ein Fehlernachrichtenfenster angezeigt.

Schritt 4. Klicken Sie auf **OK**, um das Fenster „Erfolg“ zu schließen.

Aktivierungsschlüssel entfernen

Mithilfe der Informationen in diesem Abschnitt können Sie eine Zusatzfunktion vom Server löschen.

Gehen Sie wie folgt vor, um einen Aktivierungsschlüssel zu entfernen:

Schritt 1. Klicken Sie auf unter **BMC-Konfiguration** auf **Lizenz**.

Schritt 2. Wählen Sie den zu entfernenden Aktivierungsschlüssel aus. Klicken Sie anschließend auf **Löschen**.

Schritt 3. Klicken Sie im Fenster „Löschen des Aktivierungsschlüssels bestätigen“ auf **OK**, um das Löschen des Aktivierungsschlüssels zu bestätigen, oder klicken Sie auf **Abbrechen**, um die Schlüsseldatei zu behalten.
Der ausgewählte Aktivierungsschlüssel wird vom Server entfernt und nicht mehr auf der Seite „Lizenzverwaltung“ angezeigt.

Aktivierungsschlüssel exportieren

Mithilfe der Informationen in diesem Abschnitt können Sie eine Zusatzfunktion vom Server exportieren.

Gehen Sie wie folgt vor, um einen Aktivierungsschlüssel zu exportieren:

Schritt 1. Klicken Sie auf unter **BMC-Konfiguration** auf **Lizenz**.

Schritt 2. Wählen Sie auf der Seite „Lizenzverwaltung“ den Aktivierungsschlüssel aus, den Sie exportieren möchten. Klicken Sie anschließend auf **Exportieren**.

Schritt 3. Klicken Sie im Fenster **Ausgewählte Lizenz exportieren** auf **Exportieren**, um das Exportieren des Aktivierungsschlüssels zu bestätigen, oder klicken Sie auf **Abbrechen**, um das Exportieren des Schlüssels abzubrechen.

Schritt 4. Wählen Sie das Speicherverzeichnis für die Datei aus.
Der ausgewählte Aktivierungsschlüssel wird vom Server exportiert.

Kapitel 9. Lenovo XClarity Controller Redfish REST-API

Der Lenovo XClarity Controller bietet eine Redfish-konforme Reihe von benutzerfreundlichen REST-APIs für den Zugriff auf Lenovo XClarity Controller-Daten und -Services mit Anwendungen, die außerhalb des Lenovo XClarity Controller-Frameworks ausgeführt werden.

Dies ermöglicht die einfache Integration von Lenovo XClarity Controller-Funktionen in anderer Software, unabhängig davon, ob die Software auf demselben System wie der Lenovo XClarity Controller-Server oder auf einem fernen System im gleichen Netzwerk ausgeführt wird. Diese APIs basieren auf der standardmäßigen Redfish REST-API der Branche und der Zugriff erfolgt über das HTTPS-Protokoll.

Das XClarity Controller Redfish REST-API Benutzerhandbuch finden Sie hier: https://pubs.lenovo.com/xcc-restapi/xcc_restapi_book.pdf.

Lenovo stellt Open-Source-Beispielscripts für Redfish zur Verfügung, die als Referenz für die Entwicklung von Software verwendet werden können, die mit der Lenovo Redfish REST-API kommuniziert. Diese Beispielscripts finden Sie hier:

- Python: https://github.com/lenovo/python-redfish-lenovo
- PowerShell: https://github.com/lenovo/powershell-redfish-lenovo

DMTF-Spezifikationen für die Redfish API finden Sie hier: https://redfish.dmtf.org/. Diese Website enthält allgemeine Spezifikationen und weiteres Referenzmaterial zur Redfish REST-API.

Kapitel 10. Befehlszeilenschnittstelle

Mithilfe der Informationen in diesem Abschnitt können Sie Befehle eingeben, mit denen der XClarity Controller verwaltet und überwacht wird, ohne dass die XClarity Controller-Webschnittstelle verwendet werden muss.

Verwenden Sie die XClarity Controller-Befehlszeilenschnittstelle (CLI), um auf den XClarity Controller zuzugreifen, ohne die Webschnittstelle verwenden zu müssen. Diese Schnittstelle stellt einen Teil der Verwaltungsfunktionen bereit, die von der Webschnittstelle bereitgestellt werden.

Sie können über eine SSH-Sitzung auf die Befehlszeilenschnittstelle zugreifen. Bevor Sie CLI-Befehle absetzen können, müssen Sie durch den XClarity Controller authentifiziert werden.

Auf die Befehlszeilenschnittstelle zugreifen

Mithilfe der Informationen in diesem Abschnitt können Sie auf die CLI zugreifen.

Um auf die Befehlszeilenschnittstelle zuzugreifen, starten Sie eine SSH-Sitzung mit der IP-Adresse des XClarity Controller (weitere Informationen siehe „Seriell-zu-SSH-Umleitung konfigurieren“ auf Seite 99).

An der Befehlszeilensitzung anmelden

Dieser Abschnitt enthält Informationen zur Anmeldung bei an der Befehlszeilensitzung.

Gehen Sie wie folgt vor, um sich an der Befehlszeile anzumelden:

Schritt 1. Stellen Sie eine Verbindung mit dem XClarity Controller her.

Schritt 2. Wenn Sie nach dem Benutzernamen gefragt werden, geben Sie die Benutzer-ID ein.

Schritt 3. Wenn Sie nach dem Kennwort gefragt werden, geben Sie das Kennwort ein, das Sie zur Anmeldung am XClarity Controller verwenden.

Sie werden an der Befehlszeile angemeldet. Die Befehlszeilenaufforderung lautet `system>`. Die Befehlszeilensitzung wird aufrechterhalten, bis Sie in der Befehlszeile `exit` eingeben. Dann werden Sie abgemeldet und die Sitzung wird beendet.

Seriell-zu-SSH-Umleitung konfigurieren

Dieser Abschnitt enthält Informationen zur Verwendung des XClarity Controller als seriellen Terminal-Server.

Die Seriell-zu-SSH-Umleitung ermöglicht es einem Systemadministrator, den XClarity Controller als seriellen Terminal-Server zu verwenden. Auf einen seriellen Serveranschluss kann ein Zugriff von eine SSH-Verbindung aus erfolgen, wenn die serielle Umleitung aktiviert ist.

Anmerkung: Mit dem Befehl **console 1** für die Befehlszeilenschnittstelle wird eine Sitzung für serielle Umleitung mit dem COM-Anschluss gestartet.

Beispielsitzung

```
$ ssh USERID@10.240.1.12
Password:

system>
```

Der gesamte Datenverkehr von der SSH-Sitzung wir zu COM2 umgeleitet.

```
ESC (
```

Geben Sie die Tastenkombination zum Beenden ein, um zur Befehlszeilenschnittstelle zurückzukehren. In diesem Beispiel drücken Sie die Taste „Esc“ und geben dann eine linke Klammer ein. Die Eingabeaufforderung der Befehlszeilenschnittstelle erscheint und gibt an, dass Sie zur Befehlszeilenschnittstelle des IMM zurückgekehrt sind.

```
system>
```

Befehlssyntax

Überprüfen Sie die Richtlinien in diesem Abschnitt, um zu erfahren, wie Sie Befehle in die Befehlszeilenschnittstelle eingeben können.

Lesen Sie die folgenden Richtlinien, bevor Sie die Befehle verwenden:

- Jeder Befehl weist das folgende Format auf:
  `command [`**`arguments`**`] [-`**`options`**`]`
- In der Befehlssyntax muss die Groß-/Kleinschreibung beachtet werden.
- Der Befehlsname wird in Kleinbuchstaben angegeben.
- Alle Argumente müssen direkt auf den Befehl folgen. Die Optionen wiederum folgen direkt auf die Argumente.
- Vor jeder Option steht ein Bindestrich (-). Eine Option kann als Kurzoption (ein einzelner Buchstabe) oder als Langoption (mehrere Buchstaben) angegeben werden.
- Wenn eine Option ein Argument aufweist, ist dieses Argument obligatorisch. Beispiel:
  `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`
  Dabei ist **ifconfig** der Befehl, „eth0“ ist ein Argument und „-i“, „-g“ und „-s“ sind Optionen. In diesem Beispiel weisen alle drei Optionen Argumente auf.
- Eckige Klammern geben an, dass ein Argument oder eine Option optional ist. Dabei sind die eckigen Klammern nicht Teil des Befehls, den Sie eingeben.

Merkmale und Einschränkungen

Dieser Abschnitt enthält Informationen zu CLI-Merkmalen und -Einschränkungen.

Die Befehlszeilenschnittstelle weist folgende Merkmale und Einschränkungen auf:

- Mehrere gleichzeitige CLI-Sitzungen sind über SSH zulässig.
- Es ist ein Befehl pro Zeile zulässig (maximal 1.024 Zeichen, einschließlich Leerzeichen).
- Für lange Befehle gibt es kein Fortsetzungszeichen. Die einzige Editierfunktion ist die Rückschritttaste, mit der Sie das zuvor eingegebene Zeichen löschen können.
- Sie können die Aufwärts- und die Abwärtspfeiltaste verwenden, um durch die letzten acht Befehle zu blättern. Mit dem Befehl **history** können Sie eine Liste der letzten acht Befehle anzeigen, die Sie anschließend als Direktaufruf zum Ausführen eines Befehls verwenden können, wie im folgenden Beispiel dargestellt:
  ```
  system > history
   0 ifconfig eth0
   1 readlog
   2 readlog
   3 readlog
   4 history
  ```

```
system > !O
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n XClarity ControllerA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system >
```

- In der Befehlszeilenschnittstelle liegt der Ausgabepuffergrenzwert bei 2 KB. Es gibt keine Pufferung. Die Ausgabe eines einzelnen Befehls darf 2.048 Zeichen nicht überschreiten. Dieser Grenzwert gilt nicht im Modus für serielle Umleitung (die Daten werden bei der seriellen Umleitung gepuffert).
- Der Befehlsausführungsstatus wird durch einfache Textnachrichten angegeben, wie im folgenden Beispiel dargestellt:
  ```
  system> power on
  ok
  system> power state
  Power: On
  State: System power off/State unknown
  system>
  ```
- In der Befehlssyntax muss die Groß-/Kleinschreibung beachtet werden.
- Zwischen einer Option und dem zugehörigen Argument muss mindestens ein Leerzeichen stehen. `ifconfig eth0 -i192.168.70.133` ist zum Beispiel eine falsche Syntax. Die korrekte Syntax lautet `ifconfig eth0 -i 192.168.70.133`.
- Alle Befehle verfügen über die Optionen `-h`, `-help` und `?`, mit denen Hilfe zur Syntax angezeigt werden kann. Alle der folgenden Beispiele haben dasselbe Ergebnis:
  ```
  system> power -h
  system> power -help
  system> power ?
  ```
- Einige der Befehle, die in den folgenden Abschnitten beschrieben werden, sind möglicherweise für Ihre Systemkonfiguration nicht verfügbar. Um eine Liste der von Ihrer Konfiguration unterstützten Befehle anzuzeigen, verwenden Sie die Option `help` oder `?`, wie in den folgenden Beispielen dargestellt:
  ```
  system> help
  system> ?
  ```
- In einem Flex System werden manche Einstellungen vom CMM verwaltet und können auf dem XClarity Controller nicht geändert werden.

Alphabetische Befehlsliste

Dieser Abschnitt enthält eine Liste der CLI-Befehle in alphabetischer Reihenfolge. Für jeden Befehl werden Links zu den Abschnitten bereitgestellt. Jeder Befehlsabschnitt enthält Informationen zum Befehl, seiner Funktion, Syntax und Nutzung.

Dies ist eine vollständige Liste aller CLI-Befehle von XClarity Controller in alphabetischer Reihenfolge:

- „Befehl „accseccfg““ auf Seite 118
- „Befehl „adapter““ auf Seite 185
- „Befehl „alertcfg““ auf Seite 119
- „Befehl „alertentries““ auf Seite 168
- „Befehl „asu““ auf Seite 120

Dienstprogrammbefehle

Dieser Abschnitt enthält eine Liste der CLI-Befehle in alphabetischer Reihenfolge.

Es gibt derzeit 3 Dienstprogrammbefehle:

Befehl „exit“

Mit diesem Befehl können Sie sich von der CLI-Sitzung abmelden.

Mit dem Befehl **exit** können Sie sich abmelden und die Sitzung der Befehlszeilenschnittstelle beenden.

Befehl „help“

Mit diesem Befehl wird eine Liste aller Befehle angezeigt.

Mit dem Befehl **help** können Sie eine Liste aller Befehle und eine Kurzbeschreibung zu den einzelnen Befehlen anzeigen. Sie können auch ? an der Eingabeaufforderung eingeben.

Befehl „history“

Dieser Befehl bietet eine Liste der zuvor ausgegebenen Befehle.

Mit dem Befehl **history** können Sie eine indexierte Protokollliste der letzten acht Befehle anzeigen, die ausgegeben wurden. Die Indizes können dann als Direktaufrufe (mit davor stehendem !) verwendet werden, um die Befehle aus dieser Protokollliste erneut auszugeben.

Beispiel:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Überwachungsbefehle

Dieser Abschnitt enthält eine Liste der CLI-Überwachungsbefehle in alphabetischer Reihenfolge.

Es gibt derzeit 11 Überwachungsbefehle:

Befehl „clearlog“

Mit diesem Befehl können Sie das IMM-Ereignisprotokoll löschen.

Mit dem Befehl **clearlog** können Sie das Ereignisprotokoll des IMM löschen. Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung zu Löschen von Ereignisprotokollen verfügen.

Anmerkung: Dieser Befehl sollte nur von Supportmitarbeitern verwendet werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 7. Befehl „clearlog“

Die folgende einzeilige und zweispaltige Tabelle enthält die Option mit entsprechenden Beschreibungen.

Option	Beschreibung
-t <all | platform | audit>	Ereignistyp; wählen Sie, welcher Ereignistyp gelöscht werden soll. Ohne diesen Parameter werden alle Ereignistypen ausgewählt.

Ereignistypbeschreibungen

- all: Alle Ereignistypen, einschließlich Plattformereignis und Prüfereignis.

- platform: Plattformereignistyp.
- audit: Prüfereignistyp.

Beispiel:
```
system> clearlog
All event log cleared successfully
system> clearlog -t all
All event log cleared successfully
system> clearlog -t platform
Platform event log cleared successfully
system> clearlog -t audit
Audit event log cleared successfully
```

Befehl „fans“

Mit diesem Befehl wird die Geschwindigkeit der Serverlüfter angezeigt.

Mit dem Befehl **fans** können Sie die Geschwindigkeit der einzelnen Serverlüfter anzeigen.

Beispiel:
```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

Befehl „ffdc“

Dieser Befehl wird verwendet, um eine neue Servicedatendatei zu generieren.

Verwenden Sie den Befehl **ffdc** (first failure data capture, Erfassung von Fehlerdaten beim ersten Auftreten), um Servicedaten zu generieren und an den Support zu übertragen.

Die folgende Liste enthält Befehle, die zusammen mit dem Befehl **ffdc** verwendet werden können:

- **generate** erstellt eine neue Servicedatendatei
- **status** überprüft den Status der Servicedatendatei
- **copy** kopiert die vorhandenen Servicedaten
- **delete** löscht die vorhandenen Servicedaten

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 8. Befehl „ffdc“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-t	Typennummer	1 (Prozessorspeicherauszug) und 4 (Servicedaten). Der Prozessorspeicherauszug enthält alle verfügbaren Protokolle und Dateien. Die Servicedaten enthalten nur eine Teilmenge der Protokolle und Dateien. Der Standardwert ist 1.
-f [1]	Name der fernen Datei oder des SFTP-Zielverzeichnisses	Verwenden Sie für SFTP den vollständigen Pfad oder einen abschließenden Schrägstrich (/) für den Verzeichnisnamen (~/ oder /tmp/). Der Standardwert ist der vom System generierte Name.

Tabelle 8. Befehl „ffdc“ (Forts.)

Option	Beschreibung	Werte
-ip [1]	Adresse des TFTP/SFTP-Servers	
-pn [1]	Portnummer des TFTP/SFTP-Servers	Der Standardwert ist 69/22.
-u [1]	Benutzername für den SFTP-Server	
-pw [1]	Kennwort für den SFTP-Server	

1. Zusätzliches Argument für die Befehle **generate** und **copy**

Syntax:
```
ffdc [options]
option:
  -t 1 or 4
  -f
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

Beispiel:
```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

Befehl „hreport“

Verwenden Sie diesen Befehl, um einen eingebetteten Statusbericht anzuzeigen.

In der folgenden Tabelle werden die hreport-Befehle aufgeführt.

Tabelle 9. hreport-Befehle

Die folgende mehrzeilige Tabelle mit zwei Spalten enthält die verschiedenen hreport-Befehle mit den entsprechenden Beschreibungen.

Option	Beschreibung
generate	Erstellen eines neuen Statusberichts
status	Prüfen des Status
copy	Kopieren eines vorhandenen Statusberichts
delete	Löschen eines vorhandenen Statusberichts

In der folgenden Tabelle sind die Argumente für die Optionen „generate“ und „copy“ aufgelistet.

Tabelle 10. Befehl „generate“ und „copy“

Die folgende mehrzeilige Tabelle mit zwei Spalten enthält die Befehlsoptionen „generate“ und „copy“ mit entsprechenden Beschreibungen.

Option	Beschreibung
-f	Name der fernen Datei oder des SFTP-Zielverzeichnisses (standardmäßig ein vom System generierter Name; verwenden Sie für SFTP den vollständigen Pfad oder einen abschließenden Schrägstrich (/) für den Verzeichnisnamen (~/ oder /tmp/))
-ip	Adresse des TFTP/SFTP-Servers
-pn	Portnummer des TFTP/SFTP-Servers (Standardwert 69/22)
-u	Benutzername für SFTP-Server
-pw	Kennwort für SFTP-Server

Befehl „mhlog“

Mit diesem Befehl können Aktivitätenprotokolleinträge zum Wartungsverlauf angezeigt werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 11. Befehl „mhlog“

Die folgende mehrzeilige Tabelle mit zwei Spalten enthält die Optionen mit entsprechenden Beschreibungen.

Option	Beschreibung
-c <count>	Zeigt die 'count'-Einträge (1-250)
-i <index>	Zeigt die Einträge, die am Index beginnen (1-250)
-f	Name der fernen Datei der Protokolldatei
-ip	Adresse des TFTP/SFTP-Servers
-pn	Portnummer des TFTP/SFTP-Servers (Standardwert 69/22)
-u	Benutzername für SFTP-Server
-pw	Kennwort für SFTP-Server

Beispiel

Die Anzeige sieht ungefähr so aus:

```
Type            Message                                                                  Time
-------------   ------------                                                             ----
Hardware        SAS Backplane1(SN: XXXX9CE009L) is added.                               05/08/2020,04:23:18
Hardware        CPU 1(SKU NO: 50844440) is added.                                        05/08/2020,04:23:22
Hardware        CPU 2(SKU NO: 50844440) is added.                                        05/08/2020,04:23:22
Hardware        M2 Card(SN: R1SH9AJ0037) is added.                                       05/08/2020,04:23:22
Firmware        Primary XCC firmware is updated to TGBT99T by XCC Web.                   05/08/2020,06:40:37
Firmware        Primary XCC firmware is activated to TGBT99T .                           05/08/2020,06:41:26
Hardware        PSU1(SN: D1DG94C0075) is added.                                          05/08/2020,06:43:28
```

Befehl „led“

Mit diesem Befehl können Sie den Zustand von Anzeigen anzeigen und festlegen.

Der Befehl **led** zeigt die Status der Serverbetriebsanzeigen an und legt sie fest.

- Wird der Befehl **led** ohne Optionen ausgeführt, so wird der Status der Anzeigen im Bedienfeld angezeigt.
- Die Befehlsoption **led -d** muss gemeinsam mit der Befehlsoption **led -identify on** angewendet werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 12. Befehl „led“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-l	Den Status aller Systemanzeigen und deren Unterkomponenten abrufen	
-chklog	Anzeige für Prüfprotokoll ausschalten	aus
-identify	Zustand der Gehäusebestimmungsanzeige ändern	off, on, blink
-d	Identifikationsanzeige für einen angegebenen Zeitraum einschalten	Zeitraum (Sekunden)

Syntax:

```
led [options]
option:
  -l
  -chklog off
  -identify state
  -d time
```

Beispiel:

```
system> led
Fault                Off
Identify             On            Blue
Chklog               Off
Power                Off

system> led -l
Label                Location                State         Color
Battery              Planar                  Off
```

```
BMC Heartbeat          Planar                 Blink          Green
BRD                    Lightpath Card         Off
Channel A              Planar                 Off
Channel B              Planar                 Off
Channel C              Planar                 Off
Channel D              Planar                 Off
Channel E              Planar                 Off
Chklog                 Front Panel            Off
CNFG                   Lightpath Card         Off
CPU                    Lightpath Card         Off
CPU 1                  Planar                 Off
CPU 2                  Planar                 Off
DASD                   Lightpath Card         Off
DIMM                   Lightpath Card         Off
DIMM 1                 Planar                 Off
DIMM 10                Planar                 Off
DIMM 11                Planar                 Off
DIMM 12                Planar                 Off
DIMM 13                Planar                 Off
DIMM 14                Planar                 Off
DIMM 15                Planar                 Off
DIMM 16                Planar                 Off
DIMM 2                 Planar                 Off
DIMM 3                 Planar                 Off
DIMM 4                 Planar                 Off
DIMM 5                 Planar                 Off
DIMM 6                 Planar                 Off
DIMM 7                 Planar                 Off
DIMM 8                 Planar                 Off
DIMM 9                 Planar                 Off
FAN                    Lightpath Card         Off
FAN 1                  Planar                 Off
FAN 2                  Planar                 Off
FAN 3                  Planar                 Off
Fault                  Front Panel (+)        Off
Identify               Front Panel (+)        On             Blue
LINK                   Lightpath Card         Off
LOG                    Lightpath Card         Off
NMI                    Lightpath Card         Off
OVER SPEC              Lightpath Card         Off
PCI 1                  FRU                    Off
PCI 2                  FRU                    Off
PCI 3                  FRU                    Off
PCI 4                  FRU                    Off
Planar                 Planar                 Off
Power                  Front Panel (+)        Off
PS                     Lightpath Card         Off
RAID                   Lightpath Card         Off
Riser 1                Planar                 Off
Riser 2                Planar                 Off
SAS ERR                FRU                    Off
SAS MISSING            Planar                 Off
SP                     Lightpath Card         Off
TEMP                   Lightpath Card         Off
VRM                    Lightpath Card         Off
system>
```

Befehl „readlog“

Dieser Befehl zeigt die IMM-Ereignisprotokolle an.

Mit dem Befehl **readlog** können Sie IMM-Ereignisprotokolleinträge anzeigen. Es werden fünf Ereignisprotokolle gleichzeitig angezeigt. Die Einträge werden in der Reihenfolge vom aktuellen bis zum ältesten Eintrag angezeigt.

readlog zeigt die ersten fünf Einträge im Ereignisprotokoll an, angefangen mit dem aktuellen Eintrag (bei seiner ersten Ausführung), und dann die nächsten fünf für jeden nachfolgenden Aufruf.

readlog -a zeigt alle Einträge im Ereignisprotokoll an, angefangen mit dem aktuellen Eintrag.

readlog -f setzt den Zähler zurück und zeigt die ersten fünf Einträge im Ereignisprotokoll an, angefangen mit dem aktuellen Eintrag.

readlog -date date zeigt Ereignisprotokolleinträge für das angegebene Datum im Format mm/tt/jj an. Es kann sich um eine Liste handeln, in der die einzelnen Datumsangaben durch ein Pipe-Zeichen (|) voneinander getrennt sind.

readlog -sev severity zeigt Ereignisprotokolleinträge des angegebenen Schweregrades an (E, W, I). Es kann sich um eine Liste handeln, in der die einzelnen Schweregrade durch ein Pipe-Zeichen (|) voneinander getrennt sind.

readlog -i ip_address legt die IPv4- oder die IPv6-IP-Adresse des TFTP- oder SFTP-Servers fest, auf dem das Ereignisprotokoll gespeichert wird. Die Befehlsoptionen **-i** und **-l** werden gemeinsam verwendet, um den Standort anzugeben.

readlog -l filename legt den Dateinamen der Ereignisprotokolldatei fest. Die Befehlsoptionen **-i** und **-l** werden gemeinsam verwendet, um den Standort anzugeben.

readlog -pn port_number zeigt die Portnummer des TFTP- oder SFTP-Servers an oder legt sie fest (Standard: 69/22).

readlog -u username gibt den Benutzernamen für den SFTP-Server an.

readlog -pw password gibt das Kennwort für den SFTP-Server an.

Syntax:

```
readlog [options]
option:
  -a
  -f
  -date date
  -sev severity
  -i ip_address
  -l filename
  -pn port_number
  -u username
  -pw password
```

Beispiel:

```
system> readlog -f
1 I 2017-06-17T09:31:59.217  Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685  Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581  Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5  I 2017-06-16T10:40:14.352  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

Befehl „syshealth“

Dieser Befehl bietet eine Zusammenfassung des Serverzustands oder der aktiven Ereignisse.

Mit dem Befehl **syshealth** können Sie eine Zusammenfassung des Serverzustands oder der aktiven Ereignisse auf dem Server anzeigen. Der Stromversorgungsstatus, der Systemstatus, der Hardwarestatus (einschließlich Lüfter, Netzteil, Speicher, Prozessor, Hauptspeicher), die Anzahl der Neustarts und der Status der IMM-Software werden angezeigt.

Syntax:

```
syshealth [argument]
argument:
  summary      -display the system health summary
  activeevents -display active events
  cooling - display cooling devices health status
  power - display power modules health status
  storage - display local storage health status
  processors - display processors health status
  memory - display memory health status
```

Beispiel:

```
system> syshealth summary
Power    On
State    OS booted
Restarts 29

system> syshealth activeevents
No Active Event Available!
```

Befehl „temps“

Dieser Befehl zeigt alle Temperaturwerte und Temperaturschwellenwerte an.

Mit dem Befehl **temps** können Sie alle Temperaturwerte und Temperaturschwellenwerte anzeigen. Dieselben Temperaturwerte werden auch in der Webschnittstelle angezeigt.

```
Example
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius

         WR       W       T       SS      HS
-----------------------------------------------
CPU1     N/A     N/A    80/27    N/A     N/A
CPU2     N/A     N/A    80/27    N/A     N/A
DASD1   66/19   73/23   82/28   88/31   92/33
Amb     59/15   70/21   83/28   90/32   95/35
system>
```

Anmerkungen:

1. Die Ausgabe weist die folgenden Spaltenüberschriften auf:

   WR: Warnungszurücksetzung (Wert für positive Schwellenwert-Hysterese)

   W: Warnung (Oberer unkritischer Schwellenwert)

   T: Temperatur (Aktueller Wert)

   SS: Normaler Systemabschluss (Oberer kritischer Schwellenwert)

HS: Erzwungener Systemabschluss (Oberer nicht wiederherstellbarer Schwellenwert)

2. Alle Temperaturwerte sind in Grad Fahrenheit/Grad Celsius angegeben.
3. „N/A“ bedeutet „Nicht anwendbar“.

Befehl „volts“

Mit diesem Befehl können Sie die Informationen zur Serverspannung anzeigen.

Mit dem Befehl **volts** können Sie alle Spannungswerte und Spannungsschwellenwerte anzeigen. Dieselben Spannungswerte werden auch in der Webschnittstelle angezeigt.

```
Example:
system> volts

     i HSL    SSL    WL     WRL    V      WRH    WH    SSH     HSH
-------------------------------------------------------------------
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75   6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70   3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40  12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40  -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80  -2.70
VRM1                          3.45
VRM2                          5.45
system>
```

Anmerkung: Die Ausgabe weist die folgenden Spaltenüberschriften auf:

HSL: Erzwungener Systemabschluss (Unterspannung) (Unterer nicht wiederherstellbarer Schwellenwert)

SSL: Normaler Systemabschluss (Unterspannung) (Unterer kritischer Schwellenwert)

WL: Warnung (Unterspannung) (Unterer unkritischer Schwellenwert)

WRL: Warnungszurücksetzung (Unterspannung) (Wert für negative Schwellenwert-Hysterese)

V: Spannung (aktueller Wert)

WRH: Warnungszurücksetzung (Überspannung) (Wert für positive Schwellenwert-Hysterese)

WH: Warnung (Überspannung) (Oberer unkritischer Schwellenwert)

SSH: Normaler Systemabschluss (Überspannung) (Oberer kritischer Schwellenwert)

HSH: Erzwungener Systemabschluss (Überspannung) (Oberer nicht wiederherstellbarer Schwellenwert)

Befehl „vpd“

Dieser Befehl zeigt die Konfiguration und Informationsdaten (elementare Produktdaten) im Zusammenhang mit der Hardware und der Software des Servers an.

Mit dem Befehl **vpd** können Sie elementare Produktdaten für das System (sys), den IMM (bmc), das Server-BIOS (uefi), Lenovo XClarity Provisioning Manager (lxpm), die Server-Firmware (fw), die Serverkomponenten (comp) und PCIe-Einheiten (pcie) anzeigen. Dieselben Informationen werden auch in der Webschnittstelle angezeigt.

Syntax:

```
vpd sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw   - displays Vital Product Data for the system firmware
```

```
vpd comp - displays Vital Product Data for the system components
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

Beispiel:

```
system> vpd bmc
Type            Status       Version      Build      ReleaseDate
----            -------       -----       ------
BMC (Primary)   Active       0.00        DVI399T    2017/06/06
BMC (Backup)    Inactive     1.00        TEI305J    2017/04/13

system>
```

Steuerbefehle für Serverstromversorgung und -neustart

Dieser Abschnitt enthält eine Liste der CLI-Befehle zur Stromversorgung und zum Neustart in alphabetischer Reihenfolge.

Es gibt derzeit 4 Befehle für Serverstromversorgung und -neustart:

Befehl „power“

In diesem Befehl wird beschrieben, wie die Serverstromversorgung gesteuert wird.

Mit dem Befehl **power** können Sie die Stromversorgung des Servers steuern. Um Befehle vom Typ **power** ausgeben zu können, benötigen Sie die Berechtigungsstufe zum Starten und zum Neustarten des fernen Servers.

Die folgende Tabelle enthält eine Untermenge von Befehlen, die zusammen mit dem Befehl **power** verwendet werden können.

Tabelle 13. Befehl „power“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die „power“-Befehle, Beschreibungen der Befehle und zugeordnete Werte für die Befehle enthalten.

Befehl	Beschreibung	Wert
power on	Verwenden Sie diesen Befehl, um die Serverstromversorgung anzuschalten.	on, off
power off	Verwenden Sie diesen Befehl, um die Serverstromversorgung auszuschalten. **Anmerkung:** Mit der Option **-s** wird das Betriebssystem heruntergefahren, bevor der Server ausgeschaltet wird.	on, off
power cycle	Verwenden Sie diesen Befehl, um die Serverstromversorgung aus- und wieder einzuschalten. **Anmerkung:** Mit der Option **-s** wird das Betriebssystem heruntergefahren, bevor der Server ausgeschaltet wird.	
power enterS3	Verwenden Sie diesen Befehl, um das Betriebssystem in den S3-Modus (Ruhemodus) zu versetzen. **Anmerkung:** Dieser Befehl wird nur verwendet, wenn das Betriebssystem eingeschaltet ist. Der S3-Modus wird nicht auf allen Servern unterstützt.	
power rp	Verwenden Sie diese Option, um die Richtlinie für die Wiederherstellung der Stromversorgung des Hosts anzugeben.	alwayson|alwaysoff|restore

Tabelle 13. Befehl „power“ (Forts.)

Befehl	Beschreibung	Wert
power S3resume	Verwenden Sie diesen Befehl, um das Betriebssystem aus dem S3-Modus (Ruhemodus) zu aktivieren. **Anmerkung:** Dieser Befehl wird nur verwendet, wenn das Betriebssystem eingeschaltet ist. Der S3-Modus wird nicht auf allen Servern unterstützt.	
power state	Verwenden Sie diesen Befehl, um den Stromversorgungsstatus und den aktuellen Zustand des Servers anzuzeigen.	on, off

Die folgende Tabelle enthält die Optionen für die Befehle **power on**, **power off** und **power cycle**.

Tabelle 14. Befehl „power“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-s	Verwenden Sie diese Option, um das Betriebssystem herunterzufahren, bevor der Server ausgeschaltet wird. **Anmerkung:** Die Option **-s** ist bei der Verwendung der Option **-every** für die Befehle **power off** und **power cycle** inbegriffen.	
-every	Verwenden Sie diese Option zusammen mit den Befehlen **power on**, **power off** und **power cycle**, um die Serverstromversorgung zu steuern. Sie können die Daten und Zeiten sowie die Häufigkeit (täglich oder wöchentlich) für das Einschalten, das Ausschalten und das Aus- und wieder Einschalten Ihres Servers konfigurieren.	**Anmerkung:** Die Werte für diese Option werden aufgrund von Zeilenbeschränkungen in separaten Zeilen angezeigt. Sun|Mon|Tue|Wed|Thu| Fri|Sat|Day|clear
-t	Verwenden Sie diese Option, um die Zeit für das Einschalten des Servers, das Herunterfahren des Betriebssystems und das Ausschalten oder Neustarten des Servers in Stunden und Minuten anzugeben.	Verwenden Sie das folgende Format: hh:mm
-d	Verwenden Sie diese Option, um das Datum für das Einschalten des Servers anzugeben. Dies ist eine zusätzliche Option für den Befehl **power on**. **Anmerkung:** Die Optionen **-d** und **-every** können nicht zusammen im gleichen Befehl verwendet werden.	Verwenden Sie das folgende Format: mm/tt/jjjj
-clear	Verwenden Sie diese Option, um den geplanten Wert für das Datum zum Einschalten zu löschen. Dies ist eine zusätzliche Option für den Befehl **power on**.	

Syntax:

```
power on
power off [-s]
power state
power cycle [-s]
```

Bei den folgenden Informationen handelt es sich um Beispiele für den Befehl **power**.

Um jeden Sonntag um 01:30 Uhr das Betriebssystem herunterzufahren und den Server auszuschalten, geben Sie den folgenden Befehl ein:

```
system> power off
-every Sun -t 01:30
```

Um jeden Tag um 01:30 Uhr das Betriebssystem herunterzufahren und den Server neu zu starten, geben Sie den folgenden Befehl ein:

```
system> power cycle
-every Day -t 01:30
```

Um den Server jeden Montag um 01:30 Uhr einzuschalten, geben Sie den folgenden Befehl ein:

```
system> power on
-every Mon -t 13:00
```

Um den Server am 31. Dezember 2013 um 23:30 Uhr einzuschalten, geben Sie den folgenden Befehl ein:

```
system> power on
-d 12/31/2013 -t 23:30
```

Um ein wöchentliches Aus- und Wiedereinschalten aufzuheben, geben Sie den folgenden Befehl ein:

```
system> power cycle
-every clear
```

Befehl „reset“

In diesem Befehl wird beschrieben, wie der Server zurückgesetzt wird.

Mit dem Befehl **reset** können Sie den Server neu starten. Um diesen Befehl ausgeben zu können, müssen Sie über eine Zugriffsberechtigung für Stromversorgung und Neustarts verfügen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 15. Befehl „reset“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-s	Betriebssystem herunterfahren, bevor der Server zurückgesetzt wird	
-d	Zurücksetzen um die angegebene Anzahl an Sekunden verzögern	0 - 120
-nmi	Einen nicht maskierbaren Interrupt (NMI) auf dem Server generieren	

Syntax:

```
reset [option]
option:
-s
-d
-nmi
```

Befehl „fuelg“

Mit diesem Befehl können Sie Informationen zur Stromversorgung des Servers anzeigen.

Mit dem Befehl **fuelg** können Sie Informationen zum Stromverbrauch des Servers anzeigen und die Stromverbrauchssteuerung des Servers konfigurieren. Mit diesem Befehl werden auch Richtlinien für den Verlust von Stromversorgungsredundanz konfiguriert. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 16. Befehl „fuelg“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-pme	Stromverbrauchssteuerung und Energieverbrauchsbegrenzung für den Server aktivieren oder deaktivieren	on, off
-pcapmode	Energieverbrauchsbegrenzungsmodus für den Server festlegen	input, output
-pcap	Ein numerischer Wert innerhalb des Bereichs der Energieverbrauchsbegrenzungswerte, die bei Ausführung des fuelg-Befehls ohne Optionen für das Ziel angezeigt werden	numerischer Leistungswert (Watt)
-history	Stromverbrauchs- oder Leistungsverlauf anzeigen	pc, perf
-period	Ein numerischer Wert zur Verlaufsanzeige (1, 6, 12, 24 Stunden)	numerischer Wert in Stunden
-pm	Richtlinienmodus für den Verlust der redundanten Stromversorgung festlegen	• **bt**- allgemein mit Regulierung • **rt**- redundant mit Regulierung (Standard) • **ort**- N_1 redundant mit Regulierung
-zm	Nullausgabemodus aktivieren oder deaktivieren. Diese Einstellung kann nur festgelegt werden, wenn der Richtlinienmodus auf „redundant mit Regulierung“ festgelegt ist.	on, off
-perf	Aktuelle Rechenauslastung anzeigen, einschließlich System, Mikroprozessor und E/A	Prozentsatz
-pc	Aktuellen Stromverbrauch anzeigen	• **output**- aktuellen Gleichstromverbrauch anzeigen. Bei Rack- und Tower-Servern umfasst dies den Stromverbrauch von System, CPU, Speicher und anderen Komponenten, bei ITE-Bladeservern umfasst dies nur den Stromverbrauch des Systems. • **input**- Aktuelle Eingangsversorgung anzeigen, einschließlich Stromverbrauch des Systems.

Syntax:

```
fuelg [options]
option:
  -pme on|off
  -pcapmode input|output
  -pcap
  -history
```

```
  -period
  -pm bt|r|rt
  -zm on|off
  -perf
  -pc input|output
```

Beispiel:

```
system> fuelg
-pme: on
system>
```

Befehl „pxeboot“

Dieser Befehl zeigt die Bedingung für die Ausführungsumgebung vor dem Starten (Preboot eXecution Environment - PXE) an und stellt sie ein.

Wird **pxeboot** ohne Optionen ausgeführt, so wird auf die aktuelle PXE-Einstellung zurückgegriffen. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 17. Befehl „pxeboot“

Die folgende Tabelle ist eine einzeilige Tabelle mit drei Spalten, die die Option, eine Beschreibung der Option und zugeordnete Werte für die Option enthält.

Option	Beschreibung	Werte
-en	Legt die PXE-Bedingung für den nächsten Systemwiederanlauf fest.	enabled, disabled

Syntax:

```
pxeboot [options]
option:
  -en state
```

Beispiel:

```
system> pxeboot
-en disabled
system>
```

Befehl zur seriellen Umleitung

Dieser Abschnitt enthält den Befehl zur seriellen Umleitung.

Es gibt nur einen Befehl zur seriellen Umleitung: „Befehl „console““ auf Seite 117.

Befehl „console“

Mit diesem Befehl können Sie eine Konsolensitzung mit serieller Umleitung starten.

Mit dem Befehl **console** können Sie eine Konsolensitzung mit serieller Umleitung zum designierten seriellen Anschluss des IMM starten.

Syntax:

```
console 1
```

Konfigurationsbefehle

Dieser Abschnitt enthält eine Liste der CLI-Konfigurationsbefehle in alphabetischer Reihenfolge.

Es gibt derzeit 41 Konfigurationsbefehle:

Befehl „accseccfg“

Mit diesem Befehl können Sie Accountsicherheitseinstellungen anzeigen und konfigurieren.

Wird der Befehl **accseccfg** ohne Optionen ausgeführt, so werden alle Informationen zur Kontensicherheit angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 18. Befehl „accseccfg“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-am	Legt Benutzerauthentifizierungsverfahren fest.	local, ldap, localldap, ldaplocal
-lp	Sperrzeitraum nach maximaler Anzahl von fehlgeschlagenen Anmeldeversuchen (in Minuten).	0 bis 2880, 0 = Sperrzeit läuft nicht ab
-pe	Zeitraum bis Verfallsdatum des Kennworts (Tage).	Zwischen 0 und 365, 0 = läuft nie ab
-pew	Warnzeitraum vor Ablauf des Kennworts **Anmerkung:** Der Warnzeitraum vor Ablauf des Kennworts muss kleiner als der Zeitraum bis Verfallsdatum des Kennworts sein.	Zwischen 0 und 30, 0 = warnt nie
-pc	Regeln zur Kennwortkomplexität sind aktiviert.	on, off
-pl	Kennwortlänge.	Wenn die Regeln zur Kennwortkomplexität aktiviert sind, liegt die Länge des Kennworts zwischen 8 und 32. Andernfalls liegt sie zwischen 0 und 32.
-ci	Mindestintervall für Kennwortänderung (in Stunden).	Zwischen 0 und 240, 0 = sofort ändern
-lf	Maximaler Anzahl fehlgeschlagener Anmeldeversuche.	Zwischen 0 und 10, 0 = nie gesperrt
-chgdft	Standardkennwort nach erster Anmeldung ändern.	on, off
-chgnew	Neues Benutzerkennwort nach erster Anmeldung ändern.	on, off
-rc	Zyklus für erneute Kennwortverwendung.	Zwischen 0 und 10, 0 = sofort wiederverwenden
-wt	Sitzungszeitlimit bei Web- und Secure-Shell-Inaktivität (Minuten).	Zwischen 0 und 1440

Syntax:

```
accseccfg [options]
option:
   -legacy
   -high
   -custom
   -am authentication method
   -lp lockout_period
   -pe time_period
   -pr state
   -pc state
   -pd number_characters
   -pl number_characters
   -ci minimum_interval
   -lf number_failures
   -chgdft state
   -chgnew state
   -rc reuse_cycle
   -wt timeout
```

Beispiel:

```
system> accseccfg
-legacy
-am local
-lp 2
-pe 0
-pr off
-pd 1
-pl 4
-ci 0
-lf 0
-chgdft off
-chgnew off
-rc 0
-wt user
system>
```

Befehl „alertcfg“

Mit diesem Befehl können Sie die Parameter für allgemeine ferne Alerts von IMM anzeigen und konfigurieren.

Wird der Befehl **alertcfg** ohne Optionen ausgeführt, so werden alle Parameter für allgemeine ferne Alerts angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 19. Befehl „alertcfg“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Tabelle 19. Befehl „alertcfg“ (Forts.)

Option	Beschreibung	Werte
-dr	Legt fest, wie viel Zeit zwischen Wiederholungsversuchen liegen soll, bevor der IMM erneut einen Alert sendet.	Minutenangaben von „0“ bis „4,0“ (für 4,0 Minuten), in Inkrementen von einer halben Minute
-da	Legt fest, wie viel Zeit vergehen soll, bevor der IMM einen Alert an den nächsten Empfänger auf der Liste sendet.	Minutenangaben von „0“ bis „4,0“ (für 4,0 Minuten), in Inkrementen von einer halben Minute
-rl	Legt fest, wie oft der IMM zusätzlich versucht, einen Alert zu senden, wenn vorherige Versuche nicht erfolgreich waren.	0 bis 8

Syntax:
```
alertcfg [options]
  options:
   -rl retry_limit
   -dr retry_delay
   -da agent_delay
```

Beispiel:
```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
system>
```

Befehl „asu“

Dieser Befehl wird verwendet, um UEFI-Einstellungen zu konfigurieren.

Befehle des Dienstprogramms für erweiterte Einstellungen werden verwendet, um UEFI-Einstellungen zu konfigurieren. Das Hostsystem muss erneut gestartet werden, damit Änderungen an UEFI-Einstellungen wirksam werden.

Die folgende Tabelle enthält einige Befehle, die zusammen mit dem Befehl **asu** verwendet werden können.

Tabelle 20. Befehl „asu“

Die folgende mehrzeilige Tabelle mit drei Spalten enthält einige Befehle, die in Verbindung mit dem Befehl **asu** verwendet werden können. Die Befehle werden hier beschrieben und es werden die zugehörigen Werte aufgeführt.

Befehl	Beschreibung	Wert
delete	Verwenden Sie diesen Befehl, um eine Instanz oder einen Datensatz einer Einstellung zu löschen. Bei der Einstellung muss es sich um eine Instanz handeln, für die das Löschen zulässig ist, z. B. „iSCSI.AttemptName.1“.	**setting_instance**
Hilfe	Verwenden Sie diesen Befehl, um Hilfetext zu einer oder mehreren Einstellungen anzuzeigen.	**Einstellung**

Tabelle 20. Befehl „asu“ (Forts.)

Befehl	Beschreibung	Wert
set	Verwenden Sie diesen Befehl, um den Wert einer Einstellung zu ändern. Legen Sie als UEFI-Einstellung den Eingabewert fest. **Anmerkungen:** • Legen Sie ein oder mehrere Paare aus Einstellung und Wert fest. • Die Einstellung kann Platzhalterzeichen enthalten, wenn sie für eine einzelne Einstellung gilt. • Der Wert muss in Anführungszeichen gesetzt werden, wenn er Leerzeichen enthält. • Sortierlistenwerte werden durch das Gleichheitszeichen (=) getrennt. Beispiel: set B*.Bootorder „CD/DVD Rom=Hard Disk 0=PXE Network“.	**Einstellungswert**
showgroups	Verwenden Sie diesen Befehl, um die verfügbaren Einstellungsgruppen anzuzeigen. Dieser Befehl zeigt die Namen der bekannten Gruppen an. Gruppennamen können je nach den installierten Einheiten variieren.	**Einstellung**
show	Verwenden Sie diesen Befehl, um den aktuellen Wert einer oder mehrerer Einstellungen anzuzeigen.	**Einstellung**
showvalues	Verwenden Sie diesen Befehl, um alle möglichen Werte für eine oder mehrere Einstellungen anzuzeigen. **Anmerkungen:** • Dieser Befehl zeigt Informationen zu den zulässigen Werten für die Einstellung an. • Die minimale und maximale Anzahl der für diese Einstellung zulässigen Instanzen werden angezeigt. • Der Standardwert wird angezeigt, falls er verfügbar ist. • Der Standardwert steht zwischen einer öffnenden und einer schließenden spitzen Klammer (< und >). • Die Textwerte zeigen die minimale und die maximale Länge sowie den regulären Ausdruck.	**Einstellung**
Anmerkungen: • In der Befehlssyntax ist **Einstellung** der Name einer Einstellung, die Sie anzeigen oder ändern möchten, und **Wert** ist der Wert, den Sie für die Einstellung festlegen. • Für **Einstellung** können mehrere Werte angegeben werden, außer bei Verwendung des Befehls **set**. • Der Wert für **Einstellung** kann Platzhalterzeichen enthalten, z. B. einen Stern (*) oder ein Fragezeichen (?). • Bei **Einstellung** kann es sich um eine Gruppe, einen Einstellungsnamen oder den Wert **all** (alles) handeln.		

In der folgenden Liste werden Beispiele für die Syntax des Befehls **asu** aufgeführt:

- Um alle Befehlsoptionen für den Befehl „asu“ anzuzeigen, geben Sie `asu --help` ein.
- Um die ausführliche Hilfe für alle Befehle anzuzeigen, geben Sie `asu -v --help` ein.
- Um die ausführliche Hilfe für einen Befehl anzuzeigen, geben Sie `asu -v set --help` ein.
- Um einen Wert zu ändern, geben Sie `asu set` **setting value** ein.
- Um den aktuellen Wert anzuzeigen, geben Sie `asu show` **setting** ein.
- Um Einstellungen im Langformat anzuzeigen, geben Sie `asu show -l -b all` ein.

- Um alle möglichen Werte für eine Einstellung anzuzeigen, geben Sie `asu showvalues` **setting** ein. Beispiel für den Befehl **show values**:
```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 21. „asu“-Optionen

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-b	Im Batchformat anzeigen	
--help[1]	Befehlssyntax und -optionen anzeigen. Die Option „--help“ wird vor den Befehl gesetzt, z. B. **asu --help show**.	
--help[1]	Hilfe zum Befehl anzeigen. Die Option „--help“ wird hinter den Befehl gesetzt, z. B. **asu show --help**.	
-l	Name der Einstellung im Langformat (Konfigurationsgruppe einschließen)	
-m	Name der Einstellung im Mischformat (Konfigurations-ID verwenden)	
-v[2]	Ausführliche Ausgabe	

1. Die Option „--help“ kann zusammen mit jedem Befehl verwendet werden.
2. Die Option „-v“ wird nur zwischen **asu** und dem Befehl verwendet.

Syntax:
```
asu [options] command [cmdopts]
options:
   -v verbose output
   --help display main help
cmdopts:
   --help help for the command
```

Anmerkung: Weitere Befehlsoptionen finden Sie bei den einzelnen Befehlen.

Verwenden Sie die asu-Transaktionsbefehle, um mehrere UEFI-Einstellungen festzulegen und Batchmodusbefehle zu erstellen und auszuführen. Verwenden Sie die Befehle **tropen** und **trset**, um eine Transaktionsdatei zu erstellen, die mehrere Einstellungen enthält. Eine Transaktion mit einer angegebenen ID wird mit dem Befehl **tropen** geöffnet. Einstellungen werden mithilfe des Befehls **trset** zur Gruppe hinzugefügt. Die abgeschlossene Transaktion wird mithilfe des Befehls **trcommit** festgeschrieben. Wenn Sie mit der Transaktion fertig sind, kann diese mithilfe des Befehls **trrm** gelöscht werden.

Anmerkung: Die Operation zum Wiederherstellen der UEFI-Einstellungen erstellt eine Transaktion mit einer ID unter Verwendung einer willkürlichen dreistelligen Zahl.

Die folgende Tabelle enthält Transaktionsbefehle, die zusammen mit dem Befehl **asu** verwendet werden können.

Tabelle 22. „asu“-Transaktionsbefehle

Die folgende mehrzeilige Tabelle mit drei Spalten enthält die Transaktionsbefehle sowie Beschreibungen der Befehle und zugehörige Werte.

Befehl	Beschreibung	Wert
tropen **ID**	Dieser Befehl erstellt eine neue Transaktionsdatei mit mehreren festzulegenden Einstellungen.	**ID** ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trset **ID**	Dieser Befehl fügt eine oder mehrere Einstellungen oder Wertepaare zu einer Transaktion hinzu.	**ID** ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trlist **ID**	Dieser Befehl zeigt zuerst die Inhalte der Transaktionsdatei an. Dies kann hilfreich sein, wenn die Transaktionsdatei in der CLI-Shell erstellt wird.	**ID** ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trcommit **ID**	Dieser Befehl schreibt die Inhalte der Transaktionsdatei fest und führt sie aus. Die Ergebnisse der Ausführung sowie eventuelle Fehler werden angezeigt.	**ID** ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.
trrm **ID**	Dieser Befehl entfernt die Transaktionsdatei, nachdem sie festgeschrieben wurde.	**ID** ist die ID-Zeichenfolge aus 1-3 alphanumerischen Zeichen.

Beispiel für das Erstellen mehrerer UEFI-Einstellungen:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

Befehl „backup“

Mit diesem Befehl können Sie eine Sicherungsdatei mit den aktuellen Systemsicherheitseinstellungen erstellen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 23. Befehl „backup“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-f	Name der Sicherungsdatei	Gültiger Dateiname
-pp	Kennwort oder Verschlüsselungstext, mithilfe dessen Kennwörter innerhalb der Sicherungsdatei verschlüsselt sind	Gültiges Kennwort oder durch Anführungszeichen begrenzter Verschlüsselungstext
-ip	IP-Adresse des TFTP-/SFTP-Servers	Gültige IP-Adresse

Tabelle 23. Befehl „backup“ (Forts.)

Option	Beschreibung	Werte
-pn	Portnummer des TFTP/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP-Server	Gültiges Kennwort
-fd	Dateiname für die XML-Beschreibung von CLI-Sicherungsbefehlen	Gültiger Dateiname

Syntax:

```
backup [options]
  option:
   -f    filename
   -pp   password
   -ip   ip address
   -pn   port number
   -u    username
   -pw   password
   -fd   filename
```

Beispiel:

```
system> backup f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

Befehl „dhcpinfo“

Mit diesem Befehl können Sie die dem DHCP-Server zugeordnete IP-Konfiguration für eth0 anzeigen.

Mit dem Befehl **dhcpinfo** können Sie die durch den DHCP-Server zugeordnete IP-Konfiguration für eth0 anzeigen, wenn die Schnittstelle automatisch durch einen DHCP-Server konfiguriert wird. Mit dem Befehl **ifconfig** können Sie DHCP aktivieren oder inaktivieren.

Syntax:

```
dhcpinfo eth0
```

Example:

```
system> dhcpinfo eth0
   -server :  10.240.0.10
   -n      :  XCC-7X19-123456789A
   -i      :  10.243.4.66
   -i6     :  ::
   -g      :  10.243.0.1
   -s      :  255.255.240.0
   -d      :  labs.lenovo.com
   -d6     :
   -dns1   :  10.240.0.10
   -dns2   :  10.240.0.11
   -dns3   :  0.0.0.0
   -dns61  :  ::
   -dns62  :  ::
   -dns63  :  ::
```

In der folgenden Tabelle wird die Ausgabe dieses Beispiels beschrieben.

Tabelle 24. Befehl „dhcpinfo“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit zwei Spalten, in der die im vorherigen Beispiel verwendeten Optionen beschrieben werden.

Option	Beschreibung
-server	DHCP-Server, der die Konfiguration zugeordnet hat
-n	Zugeordneter Hostname
-i	Zugeordnete IPv4-Adresse
-g	Zugeordnete Gateway-Adresse
-s	Zugeordnete Teilnetzmaske
-d	Zugeordneter Domänenname
-dns1	Primäre IP-Adresse des IPv4-DNS-Servers
-dns2	Sekundäre IPv4-DNS-IP-Adresse
-dns3	Tertiäre IP-Adresse des IPv4-DNS-Servers
-i6	IPv6-Adresse
-d6	IPv6-Domänenname
-dns61	Primäre IP-Adresse des IPv6-DNS-Servers
-dns62	Sekundäre IPv6-DNS-IP-Adresse
-dns63	Tertiäre IP-Adresse des IPv6-DNS-Servers

Befehl „dns“

Mit diesem Befehl können Sie die DNS-Konfiguration des IMM anzeigen und einstellen.

Anmerkung: In einem Flex System können DNS-Einstellungen nicht auf dem IMM geändert werden. DNS-Einstellungen werden vom CMM verwaltet.

Wird der Befehl **dns** ohne Optionen ausgeführt, so werden alle Informationen zur DNS-Konfiguration angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 25. Befehl „dns“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-state	DNS-Zustand	on, off
-ddns	DDNS-Zustand	enabled, disabled
-i1	Primäre IP-Adresse des IPv4-DNS-Servers	IP-Adresse im IP-Adressformat mit Trennzeichen.
-i2	Sekundäre IPv4-DNS-IP-Adresse	IP-Adresse im IP-Adressformat mit Trennzeichen.
-i3	Tertiäre IP-Adresse des IPv4-DNS-Servers	IP-Adresse im IP-Adressformat mit Trennzeichen.
-i61	Primäre IP-Adresse des IPv6-DNS-Servers	IP-Adresse im IPv6-Format.

Tabelle 25. Befehl „dns“ (Forts.)

Option	Beschreibung	Werte
-i62	Sekundäre IPv6-DNS-IP-Adresse	IP-Adresse im IPv6-Format.
-i63	Tertiäre IP-Adresse des IPv6-DNS-Servers	IP-Adresse im IPv6-Format.
-p	IPv4-/IPv6-Priorität	ipv4, ipv6

Syntax:
```
dns [options]
option:
  -state state
  -ddns state
  -i1 first_ipv4_ip_address
  -i2 second_ipv4_ip_address
  -i3 third_ipv4_ip_address
  -i61 first_ipv6_ip_address
  -i62 second_ipv6_ip_address
  -i63 third_ipv6_ip_address
  -p priority
```

Anmerkung: Im folgenden Beispiel ist eine IMM-Konfiguration mit deaktiviertem DNS dargestellt.

Beispiel:
```
system> dns
   -state   :  disabled
   -i1      :  0.0.0.0
   -i2      :  0.0.0.0
   -i3      :  0.0.0.0
   -i61     :  ::
   -i62     :  ::
   -i63     :  ::
   -ddns    :  enabled
   -dnsrc   :  DHCP
   -ddn     :
   -ddncur  :  labs.lenovo.com
   -p       :  ipv6
   -dscvry  :  enabled

system>
```
In der folgenden Tabelle werden die im vorherigen Beispiel verwendeten Optionen beschrieben.

Tabelle 26. DNS-Befehlsausgabe

Die folgende Tabelle ist eine mehrzeilige Tabelle mit zwei Spalten, in der die im vorherigen Beispiel verwendeten Optionen beschrieben werden.

Option	Beschreibung
-state	Zustand des DNS (`on` oder `off`)
-i1	Primäre IP-Adresse des IPv4-DNS-Servers
-i2	Sekundäre IPv4-DNS-IP-Adresse
-i3	Tertiäre IP-Adresse des IPv4-DNS-Servers
-i61	Primäre IP-Adresse des IPv6-DNS-Servers
-i62	Sekundäre IPv6-DNS-IP-Adresse

Tabelle 26. DNS-Befehlsausgabe (Forts.)

Option	Beschreibung
-i63	Tertiäre IP-Adresse des IPv6-DNS-Servers
-ddns	Zustand des DDNS (`enabled` oder `disabled`)
-dnsrc	Bevorzugter DDNS-Domänenname (`dhcp` oder `manual`)
-ddn	Manuell angegebenes DDN
-ddncur	Aktuelles DDN (Lesezugriff)
-p	Bevorzugter DNS-Server (`ipv4` oder `ipv6`)

Befehl „encaps“

Verwenden Sie diesen Befehl, damit BMC den Kapselungsmodus beendet.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 27. Befehl „encaps“

Die folgende einzeilige Tabelle mit zwei Spalten enthält die Optionen mit entsprechenden Beschreibungen.

Option	Beschreibung
lite off	Der BMC beendet den Kapselungsmodus und öffnet den globalen Zugriff für alle Benutzer.

Befehl „ethtousb“

Mit dem Befehl **ethtousb** können Sie die Portzuordnung für Ethernet zu Ethernet-über-USB anzeigen und konfigurieren.

Mit diesem Befehl können Sie für Ethernet-über-USB eine externe Ethernet-Portnummer einer anderen Portnummer zuordnen.

Wird der Befehl **ethtousb** ohne Optionen ausgeführt, so werden Informationen zu Ethernet-über-USB angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 28. Befehl „ethtousb“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Tabelle 28. Befehl „ethtousb“ (Forts.)

Option	Beschreibung	Werte
-en	Zustand von Ethernet-über-USB	enabled, disabled
-m**x**	Portzuordnung für Index **x** konfigurieren	Durch einen Doppelpunkt (:) getrenntes Portpaar in der Form **port1:port2** Dabei gilt Folgendes: • Die Portindexnummer **x** wird in der Befehlsoption als Ganzzahl zwischen 1 und 10 angegeben. • Bei **port1** des Portpaares handelt es sich um die externe Ethernet-Portnummer. • Bei **port2** des Portpaares handelt es sich um die Ethernet-über-USB-Portnummer.
-rm	Portzuordnung für angegebenen Index entfernen	1 bis 10 Über den Befehl **ethtousb** ohne Optionen werden Portzuordnungsindizes angezeigt.

Syntax:
```
ethtousb [options]
option:
  -en state
  -mxport_pair
  -rm map_index
```

Beispiel:
```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
system>
```

Befehl „firewall“

Mit diesem Befehl können Sie die Firewall so konfigurieren, dass der Zugriff von bestimmten Adressen und optional auch der Zeitraum für den Zugriff eingeschränkt wird. Wenn keine Option angegeben wird, werden die aktuellen Einstellungen angezeigt.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 29. Befehl „firewall“

Die folgende mehrzeilige Tabelle mit drei Spalten enthält die Optionen mit entsprechenden Beschreibungen.

Option	Beschreibung	Werte
-bips	Blockieren von 1-3 IP-Adressen (getrennt durch Kommas, CIDR oder Bereich)	Gültige IP-Adressen **Anmerkung:** IPv4- und IPv6-Adressen können das CIDR-Format verwenden, um einen Adressbereich zu blockieren.
-bmacs	Blockieren von 1-3 MAC-Adressen (getrennt durch Kommas)	Gültige MAC-Adressen **Anmerkung:** Die MAC-Adressfilterung funktioniert nur mit bestimmten Adressen.

Tabelle 29. Befehl „firewall“ (Forts.)

Option	Beschreibung	Werte
-bbd	Beginndatum der Blockierung	Datum mit Format <JJJJ-MM-TT>
-bed	Enddatum der Blockierung	Datum mit Format <JJJJ-MM-TT>
-bbt	Beginnzeit der Blockierung	Uhrzeit mit Format <hh:mm>
-bet	Endzeit der Blockierung	Uhrzeit mit Format <hh:mm>
-bti	Blockieren von 1-3 Zeitintervallen (getrennt durch Kommas) **firewall - bti 01:00–02:00,05:05–10:30** blockiert beispielsweise den Zugriff jeden Tag von 01:00 bis 02:00 und 05:05 bis 10:30	Zeitraum mit Format <hh:mm-hh:mm>
-clr	Firewall-Regel für einen bestimmten Typ löschen	ip, mac, datetime, interval, all
Die folgenden Optionen stehen für die IP-Adressblockierung zur Verfügung		
-iplp	Sperrzeit für IP-Adresse in Minuten	Numerischer Wert zwischen 0 und 2880, 0 = läuft nie ab
-iplf	Maximale Anzahl fehlgeschlagener Anmeldeversuche, bevor die IP-Adresse gesperrt wird. **Anmerkung:** Wenn dieser Wert nicht 0 ist, muss er größer oder gleich <Maximale Anzahl fehlgeschlagener Anmeldeversuche> sein, die von **<accseccfg -lf>** festgelegt wird	Numerischer Wert zwischen 0 und 32, 0 = sperrt nie
-ipbl	Liste der gesperrten IP-Adressen anzeigen/ konfigurieren.	del, clrall, show • **-del**: eine IPv4- oder IPv6-Adresse aus der Sperrliste löschen • **-clrall**: alle gesperrten IPs löschen • **-show**: alle gesperrten IPs anzeigen

Beispiel:

```
· “firewall”: Show all options’ value and IP addresses blocking list.
· “firewall -bips  192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5”: Block the access from multi IPs
· “firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00”: Block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day.
· “firewall –clr all”: Clear all rules of “Block List and Time Restriction”.
· “firewall -iplp 60”:Set IP address lockout period to 60 minutes.
· “firewall -iplf 5”:Set maximum number of login failures to 5 timesi.
· “firewall -ipbl -del 192.168.100.1”:Delete 192.168.100.1 from IP address blocking list.
· “firewall –ipbl -del 3fcc:1234::2”:Delete 3fcc:1234::2 from IP address blocking list.
· “firewall –ipbl –clrall”:  Delete all blocking IP addresses.
· “firewall –ipbl –show”:    Show all blocking IP addresses.
```

Befehl „gprofile“

Mit diesem Befehl können Sie Gruppenprofile für den IMM anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 30. Befehl „gprofile“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-clear	Eine Gruppe löschen	enabled, disabled
-n	Der Name der Gruppe	Zeichenfolge mit bis zu 63 Zeichen für **group_name**. Der **group_name** muss eindeutig sein.
-a	Rollenbasierte Berechtigungsstufe	supervisor, operator, rbs <role list>: nsc|am|rca|rcvma|pr|bc|cel|ac Die Rollenlistenwerte werden in einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, angegeben.
-h	Befehlssyntax und -optionen anzeigen	

Syntax:
```
gprofile [1 - 16 group_profile_slot_number] [options]
options:
-clear state
-n  group_name
-a  authority level:
    -nsc network and security
    -am user account management
    -rca remote console access
    -rcvma remote console and remote disk access
    -pr remote server power/restart access
    -bc basic adapter configuration
    -cel ability to clear event logs
    -ac advanced adapter configuration
-h help
```

Befehl „hashpw“

Verwenden Sie diesen Befehl mit der Option „-sw“, um die Drittanbieterkennwortfunktion zu aktivieren/deaktivieren oder mit der Option „-re“, um das Abrufen des Drittanbieterkennworts zu aktivieren/deaktivieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 31. Befehl „hashpw“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-sw	Schaltstatus des Drittanbieterkennworts	enabled, disabled
-re	Abrufstatus des Drittanbieterkennworts **Anmerkung:** Abrufen kann festgelegt werden, wenn der Schalter aktiviert ist.	enabled, disabled

Beispiel:

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f -a super
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account      Login ID      Advanced Attribute               Role             Password Expires
 -------      --------      ------------------              ------            ----------------
    1           USERID                   Native                 Administrator      Password doesn't expire
5           guest5    Third-party Password              Administrator                    90 day(s)
```

Befehl „ifconfig“

Mit diesem Befehl können Sie die Ethernet-Schnittstelle konfigurieren.

Geben Sie `ifconfig eth0` ein, um die aktuelle Ethernet-Schnittstellenkonfiguration anzuzeigen. Um die Konfiguration der Ethernet-Schnittstelle zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Schnittstellenkonfiguration ändern zu können, müssen Sie mindestens über die Berechtigung „Konfiguration von Adapternetzbetrieb und -sicherheit“ verfügen.

Anmerkung: In einem Flex System werden die VLAN-Einstellungen von einem Flex System-CMM verwaltet und können auf dem IMM nicht geändert werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 32. Befehl „ifconfig“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-b	Herstellerkennung der MAC-Adresse (schreibgeschützt und nicht konfigurierbar)	
-state	Schnittstellenstatus	disabled, enabled
-c	Konfigurationsmethode	dhcp, static, dthens („dthens“ entspricht der Option **Try dhcp server, if it fails use static config** (Nach DHCP-Server suchen. Falls das fehlschlägt, statische Konfiguration verwenden) in der Webschnittstelle)
-i	Statische IP-Adresse	Adresse im gültigen Format.
-g	Gateway-Adresse	Adresse im gültigen Format.
-s	Subnetzmaske	Adresse im gültigen Format.
-n	Hostname	Zeichenfolge von bis zu 63 Zeichen. Die Zeichenfolge kann Buchstaben, Ziffern, Punkte, Unterstriche und Bindestriche enthalten.
-r	Übertragungsgeschwindigkeit	10, 100, auto
-d	Duplexmodus	full, half, auto
-m	MTU	Numerisch zwischen 60 und 1500.
-l	LAA	MAC-Adressenformat. Multicastadressen sind nicht zulässig (das erste Byte muss gerade sein).
-dn	Domänenname	Domänenname im gültigen Format.

Tabelle 32. Befehl „ifconfig“ (Forts.)

Option	Beschreibung	Werte
-auto	Einstellung für automatische Vereinbarung, die bestimmt, ob die Netzeinstellungen für die Übertragungsgeschwindigkeit und den Duplexmodus konfigurierbar sind.	true, false
-ghn	Hostnamen von DHCP abrufen	disabled, enabled
-nic	NIC-Modus umschalten[1]	shared, dedicated, shared:nixX[2]
-failover[2]	Funktionsübernahmemodus	none, shared, shared:nicX
-nssync[3]	Netzeinstellungssynchronisation	enabled, disabled
-address_table	Tabelle der automatisch generierten IPv6-Adressen und ihre Präfixlängen **Anmerkung:** Diese Option wird nur dann angezeigt, wenn IPv6 und die statusunabhängige automatische Konfiguration aktiviert sind.	Dieser Wert ist schreibgeschützt und nicht konfigurierbar.
-ipv6	IPv6-Status	disabled, enabled
-lla	Lokale Verbindungsadresse **Anmerkung:** Die lokale Verbindungsadresse wird nur angezeigt, wenn IPv6 aktiviert ist.	Die Link-Local-Adresse wird vom IMM bestimmt. Dieser Wert ist schreibgeschützt und nicht konfigurierbar.
-ipv6static	Statischer IPv6-Status	disabled, enabled
-i6	Statische IP-Adresse	Statische IP-Adresse für Ethernet-Kanal 0 im IPv6-Format.
-p6	Länge des Adresspräfix	Numerischer Wert zwischen 1 und 128.
-g6	Gateway oder Standardroute	IP-Adresse für das Gateway oder die Standardroute für Ethernet-Kanal 0 im IPv6-Format.
-dhcp6	DHCPv6-Status	enabled, disabled
-sa6	Statusunabhängiger IPv6-Status mit automatischer Konfiguration	enabled, disabled
-vlan	VLAN-Tagging aktivieren oder inaktivieren	enabled, disabled

Tabelle 32. Befehl „ifconfig“ (Forts.)

Option	Beschreibung	Werte
-vlanid	Identifikationsmarkierung des Netzwerkpakets für den IMM	Numerischer Wert zwischen 1 und 4094.

Anmerkungen:

1. -nic zeigt auch den nic-Status an. [aktiv] gibt an, welche nic XCC derzeit verwendet.

   Beispiel:
   ```
   -nic: shared:nic3
   nic1: dedicate
   nic2: ext card slot #3
   nic3: ext card slot 5 [active]
   ```
   Gibt an, dass sich nic3 im gemeinsam genutzten Modus befindet und auf Steckplatz 5 ist, nic2 auf Steckplatz 3 ist, nic1 ein XCC-dedizierter Port ist und XCC nic3 verwendet.
2. Der Wert „shared:nicX“ ist auf Servern verfügbar, in denen eine Mezzanine-Netzkarte als Zusatzeinrichtung installiert ist. Diese Mezzanine-Netzwerkkarte kann vom IMM verwendet werden.
3. Wenn der IMM für die Verwendung des dedizierten Management-Netzanschlusses konfiguriert ist, weist die Option „-failover“ den IMM an, zum gemeinsam genutzten Netzwerkanschluss zu wechseln, wenn der dedizierte Anschluss nicht verbunden ist.
4. Wenn der Failover-Modus aktiviert ist, weist die Option „-nssync“ den IMM an, dieselben Netzwerkeinstellungen für den gemeinsam genutzten Netzwerkanschluss wie für den dedizierten Management-Netzwerkanschluss zu verwenden.

Syntax:
```
ifconfig eth0 [options]
options:

  -state interface_state
  -c config_method
  -i static_ipv4_ip_address
  -g ipv4_gateway_address
  -s subnet_mask
  -n hostname
  -r data_rate
  -d duplex_mode
  -m max_transmission_unit
  -l locally_administered_MAC
  -b burned_in_MAC_address
  -dn domain_name
  -auto state
  -nic state
  -failover mode
  -nssync state
  -address_table
  -lla ipv6_link_local_addr
  -dhcp6 state
  -ipv6 state
  -ipv6static state
  -sa6 state
  -i6 static_ipv6_ip_address
  -g6 ipv6_gateway_address
  -p6 length
  -vlan state
  -vlanid VLAN ID
```

Beispiel:
```
system> ifconfig eth0
-state    :   enabled
```

```
-c         :   dthens
-ghn       :   disabled
-i         :   192.168.70.125
-g         :   0.0.0.0
-s         :   255.255.255.0
-n         :   IMM00096B9E003A
-auto      :   true
-r         :   auto
-d         :   auto
-vlan      :   disabled
-vlanid  :   1
-m         :   1500
-b         :   00:09:6B:9E:00:3A
-l         :   00:00:00:00:00:00
-dn        :
-ipv6      :  enabled
-ipv6static :  disabled
-i6        :  ::
-p6        :  64
-g6        :  ::
-dhcp6    :  enabled
-sa6       :  enabled
-lla       :  fe80::6eae:8bff:fe23:91ae
-nic :  shared:nic3
       nic1: dedicate
       nic2: ext card slot #3
       nic3: ext card slot #5  [active]
-address_table    :

system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
```

Befehl „keycfg“

Mit diesem Befehl können Sie Aktivierungsschlüssel anzeigen, hinzufügen oder löschen.

Über diese Aktivierungsschlüssel wird der Zugriff auf optionale IMM-Funktionen gesteuert.

Anmerkungen:

- Wird der Befehl **keycfg** ohne Optionen ausgeführt, so wird die Liste installierter Aktivierungsschlüssel angezeigt. Die angezeigten Schlüsselinformationen umfassen eine Indexzahl für jeden Aktivierungsschlüssel, den Aktivierungsschlüsseltyp, das Datum, bis zu dem der Schlüssel gültig ist, die Anzahl verbleibender Verwendungen, den Schlüsselstatus und eine Beschreibung des Schlüssels.
- Durch Dateiübertragung neue Aktivierungsschlüssel hinzufügen.
- Löschen Sie alte Schlüssel, indem Sie die Zahl des Schlüssels oder den Schlüsseltyp angeben. Beim Löschen von Schlüsseln nach Typ wird nur der erste Schlüssel eines bestimmten Typs gelöscht.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 33. Befehl „keycfg“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Tabelle 33. Befehl „keycfg“ (Forts.)

Option	Beschreibung	Werte
-add	Aktivierungsschlüssel hinzufügen	Werte für die Befehlsoptionen -ip, -pn, -u, -pw und -f
-ip	IP-Adresse des TFTP-Servers mit hinzuzufügendem Aktivierungsschlüssel	Gültige IP-Adresse für TFTP-Server
-pn	Portnummer für TFTP-/SFTP-Server mit hinzuzufügendem Aktivierungsschlüssel	Gültige Portnummer für TFTP-/SFTP-Server (Standard 69/22)
-u	Benutzername für SFTP-Server mit hinzuzufügendem Aktivierungsschlüssel	Gültiger Benutzername für SFTP-Server
-pw	Kennwort für SFTP-Server mit hinzuzufügendem Aktivierungsschlüssel	Gültiges Kennwort für SFTP-Server
-f	Dateiname für hinzuzufügenden Aktivierungsschlüssel	Gültiger Dateiname für Aktivierungsschlüsseldatei
-del	Aktivierungsschlüssel nach Indexzahl löschen	Gültige Indexzahl für Aktivierungsschlüssel aus **keycfg**-Liste
-deltype	Aktivierungsschlüssel nach Schlüsseltyp löschen	Gültiger Wert für Schlüsseltyp

Syntax:
```
keycfg [options]
option:
  -add
     -ip tftp/sftp server ip address
     -pn pn port number of tftp/sftp server (default 69/22)
     -u  username for sftp server
     -pw password for sftp server
     -f  filename
     -del   n ( where n is a valid ID number from listing)
     -deltype x ( where x is a Type value)
```

Beispiel:
```
system> keycfg
ID  Type  Valid           Uses           Status    Description
1   4     10/10/2010      5              "valid"   "IMM remote presence"
2   3     10/20/2010      2              "valid"   "IMM feature
3   32796 NO CONSTRAINTS  NO CONSTRAINTS "valid"   "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

Anmerkung: Das Feld **Beschreibung** für ID-Nummer 3 wird aufgrund von Platzeinschränkungen in separaten Zeilen angezeigt.

Befehl „ldap“

Mit diesem Befehl können Sie die Konfigurationsparameter des LDAP-Protokolls anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 34. Befehl „ldap“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-a	Benutzerauthentifizierungs-verfahren	„local only“, „LDAP only“, „local first then LDAP“, „LDAP first then local“
-aom	Modus nur für Authentifizierung	enabled, disabled
-b	Bindungsmethode	„anonymous“, „bind with ClientDN and password“, „bind with Login Credential“
-c	Definierter Name des Clients	Zeichenfolge mit bis zu 127 Zeichen für **client_dn**
-d	Suchdomäne	Zeichenfolge mit bis zu 63 Zeichen für **search_domain**
-f	Gruppenfilter	Zeichenfolge mit bis zu 127 Zeichen für **group_filter**
-fn	Gesamtstrukturname	Für aktive Verzeichnisumgebungen. Zeichenfolge mit bis zu 127 Zeichen.
-g	Gruppensuchattribut	Zeichenfolge mit bis zu 63 Zeichen für **group_search_attr**
-l	Anmeldeberechtigungsattri-but	Zeichenfolge mit bis zu 63 Zeichen für **string**
-p	Clientkennwort	Zeichenfolge mit bis zu 15 Zeichen für **client_pw**
-pc	Clientkennwort bestätigen	Zeichenfolge mit bis zu 15 Zeichen für **confirm_pw** Befehlssyntax: ldap -p **client_pw** -pc **confirm_pw** Diese Option ist erforderlich, wenn Sie das Clientkennwort ändern. Sie vergleicht das Argument **confirm_pw** mit dem Argument **client_pw**. Der Befehl schlägt fehl, wenn die beiden Argumente nicht miteinander übereinstimmen.
-ep	Verschlüsseltes Kennwort	Kennwort sichern/wiederherstellen (nur interne Verwendung)
-r	Definierter Name des Stammeintrags (DN)	Zeichenfolge mit bis zu 127 Zeichen für **root_dn**
-rbs	Erweiterte rollenbasierte Sicherheit für Active Directory-Benutzer	enabled, disabled
-s1ip	Hostname/IP-Adresse von Server 1	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für **host name/ip_addr**
-s2ip	Hostname/IP-Adresse von Server 2	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für **host name/ip_addr**
-s3ip	Hostname/IP-Adresse von Server 3	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für **host name/ip_addr**
-s4ip	Hostname/IP-Adresse von Server 4	Zeichenfolge mit bis zu 127 Zeichen oder eine IP-Adresse für **host name/ip_addr**
-s1pn	Portnummer von Server 1	Eine numerische Portnummer mit bis zu 5 Ziffern für **port_number**
-s2pn	Portnummer von Server 2	Eine numerische Portnummer mit bis zu 5 Ziffern für **port_number**

Tabelle 34. Befehl „ldap“ (Forts.)

Option	Beschreibung	Werte
-s3pn	Portnummer von Server 3	Eine numerische Portnummer mit bis zu 5 Ziffern für **port_number**
-s4pn	Portnummer von Server 4	Eine numerische Portnummer mit bis zu 5 Ziffern für **port_number**
-t	Zielname des Servers	Wenn die Option „rbs“ aktiviert ist, gibt dieses Feld einen Zielnamen an, der mithilfe des Snap-ins für die rollenabhängige Sicherheit auf dem Active Directory-Server einem oder mehreren Rollen zugeordnet werden kann.
-u	UID-Suchattribut	Zeichenfolge mit bis zu 63 Zeichen für **search_attrib**
-v	LDAP-Serveradresse über DNS abrufen	off, on
-h	Zeigt die Befehlssyntax und die Optionen an.	

Syntax:

```
ldap [options]
options:
   -a loc|ldap|locld|ldloc
   -aom enable/disabled
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -fn forest_name
   -g group_search_attr
   -l string
   -p client_pw
   -pc confirm_pw
   -ep encrypted_pw
   -r root_dn
   -rbs enable|disabled
   -s1ip host name/ip_addr
   -s2ip host name/ip_addr
   -s3ip host name/ip_addr
   -s4ip host name/ip_addr
   -s1pn port_number
   -s2pn port_number
   -s3pn port_number
   -s4pn port_number
   -t name
   -u search_attrib
   -v off|on
   -h
```

Befehl „ntp“

Mit diesem Befehl können Sie das Network Time Protocol (NTP) anzeigen und konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 35. Befehl „ntp“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Tabelle 35. Befehl „ntp“ (Forts.)

Option	Beschreibung	Werte
-en	Aktiviert oder deaktiviert das Network Time Protocol.	enabled, disabled
-i[1]	Name oder IP-Adresse des Network Time Protocol-Servers. Hierbei handelt es sich um die Indexnummer des Network Time Protocol-Servers.	Der Name des NTP-Servers, der für die Taktgebersynchronisation verwendet werden soll. Die Reichweite der Indexnummer des NTP-Servers reicht von -i1 bis -i4.
-f	Die Häufigkeit (in Minuten), mit der die IMM-Uhr mit dem Network Time Protocol-Server synchronisiert wird.	3 - 1.440 Minuten
-synch	Fordert eine sofortige Synchronisation mit dem Network Time Protocol-Server an.	Mit diesem Parameter werden keine Werte verwendet.

1. -i entspricht i1.

Syntax:
```
ntp [options]
options:
-en state
-i  hostname/ip_addr
-f  frequency
-synch
```

Beispiel:
```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

Befehl „portcfg“

Mit diesem Befehl können Sie den IMM für die Funktion zur seriellen Umleitung konfigurieren.

Der IMM muss so konfiguriert sein, dass er mit den Servereinstellungen für interne serielle Anschlüsse übereinstimmt. Um die Konfiguration des seriellen Anschlusses zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Konfiguration des seriellen Anschlusses ändern zu können, müssen Sie mindestens über die Berechtigung „Konfiguration von Adapternetzbetrieb und -sicherheit“ verfügen.

Anmerkung: Der externe serielle Anschluss des Servers kann vom IMM nur für die IPMI-Funktion verwendet werden. Die Befehlszeilenschnittstelle wird durch den seriellen Anschluss nicht unterstützt. Die Optionen **serred** und **cliauth**, die in der Befehlszeilenschnittstelle von Remote Supervisor Adapter II vorhanden waren, werden nicht unterstützt.

Wird der Befehl **portcfg** ohne Optionen ausgeführt, so wird die Konfiguration des seriellen Anschlusses angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Anmerkung: Die Anzahl an Datenbits (8) ist in der Hardware festgelegt und kann nicht geändert werden.

Tabelle 36. Befehl „portcfg“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-b	Baudrate	9600, 19200, 38400, 57600, 115200
-p	Parität	none, odd, even
-s	Bits stoppen	1, 2
-climode	CLI-Modus	0, 1, 2 Dabei gilt Folgendes: • 0 = none: Die Befehlszeilenschnittstelle wird inaktiviert • 1 = cliems: Die Befehlszeilenschnittstelle wird mit EMS-kompatiblen Tastenfolgen aktiviert • 2 = cliuser: Die Befehlszeilenschnittstelle wird mit benutzerdefinierten Tastenfolgen aktiviert

Syntax:
```
portcfg [options]
 options:
   -b baud_rate
   -p parity
   -s stopbits
   -climode mode
```

Beispiel:
```
system> portcfg
-b: 57600
-climode: 2 (CLI with user defined keystroke sequence)
-p: even
-s: 1
system> portcfg -b 38400
ok
system>
```

Befehl „portcontrol“

Verwenden Sie diesen Befehl, um einen Netzwerkserviceport zu aktivieren oder zu deaktivieren.

Derzeit unterstützt dieser Befehl lediglich die Steuerung des Ports für das IPMI-Protokoll. Geben Sie **portcontrol** ein, um den Status des IPMI-Ports anzuzeigen. Geben Sie zum Aktivieren oder Deaktivieren des IPMI-Netzwerkports die Option **-ipmi** gefolgt vom Wert **on** oder **off** ein.

Tabelle 37. Befehl „portcontrol“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-all	Alle Schnittstellen und Erkennungsprotokolle aktivieren oder deaktivieren	on, off
-cim	CIM-Erkennung aktivieren oder deaktivieren	on, off

Tabelle 37. Befehl „portcontrol“ (Forts.)

Option	Beschreibung	Werte
-ipmi	IPMI-Zugriff über LAN aktivieren oder deaktivieren	on, off
-ipmi-kcs	IPMI-Zugriff vom Server aktivieren oder deaktivieren	on, off
-rest	REST-Erkennung aktivieren oder deaktivieren	on, off
-slp	SLP-Erkennung aktivieren oder deaktivieren	on, off
-snmp	SNMP-Erkennung aktivieren oder deaktivieren	on, off
-ssdp	SSDP-Erkennung aktivieren oder deaktivieren	on, off
-cli	CLI-Erkennung aktivieren oder deaktivieren	on, off
-web	WEB-Erkennung aktivieren oder deaktivieren	on, off

Syntax:
```
portcontrol [options]
 options:
   -ipmi on/off
```

Beispiel:
```
system> portcontrol
cim : on
ipmi : on
ipmi-kcs : on
rest : on
slp : on
snmp : off
ssdp : on
cli : on
web : on
```

Befehl „ports“

Mit diesem Befehl können Sie IMM-Ports anzeigen und konfigurieren.

Wird der Befehl **ports** ohne Optionen ausgeführt, so werden Informationen für alle IMM-Ports angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 38. Befehl „ports“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-open	Offene Ports anzeigen	
-reset	Ports auf Standardeinstellungen zurücksetzen	

Tabelle 38. Befehl „ports“ (Forts.)

Option	Beschreibung	Werte
-httpp	HTTP-Portnummer	Standardportnummer: 80
-httpsp	HTTPS-Portnummer	Standardportnummer: 443
-sshp	Traditionelle SSH-CLI-Portnummer	Standardportnummer: 22
-snmpap	SNMP-Agenten-Portnummer	Standardportnummer: 161
-snmptp	SNMP-Traps-Portnummer	Standardportnummer: 162
-rpp	Remote-Presence-Portnummer	Standardportnummer: 3900
-cimhp	CIM-over-HTTP-Portnummer	Standardportnummer: 5988
-cimhsp	CIM-over-HTTPS-Portnummer	Standardportnummer: 5989

Syntax:
```
ports [options]
option:
  -open
  -reset
  -httpp port_number
  -httpsp port_number
  -sshp port_number
  -snmpap port_number
  -snmptp port_number
  -rpp port_number
  -cimhp port_number
  -cimhsp port_number
```

Beispiel:
```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-cimhp 5988
-cimhsp 5989
system>
```

Befehl „rdmount“

Verwenden Sie diesen Befehl, um ferne Datenträger-Images oder Netzwerkfreigaben anzuhängen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 39. Befehl „rdmount“

Die folgende mehrzeilige Tabelle mit zwei Spalten enthält die Optionen mit entsprechenden Beschreibungen.

Anmerkungen:

- Es können bis zu zwei Dateien in den XClarity Controller-Speicher hochgeladen und als virtuelle Datenträger mithilfe der RDOC-Funktion von XClarity Controller angehängt werden. Die Gesamtgröße beider Dateien darf 50 MB nicht überschreiten. Die hochgeladenen Images sind schreibgeschützt, es sei denn, die Option „–rw“ wird verwendet.

Tabelle 39. Befehl „rdmount“ (Forts.)

- Werden die Images unter Verwendung der HTTP-, SFTP- oder FTP-Protokolle angehängt oder zugeordnet, darf die Gesamtgröße aller Images nicht mehr als 50 MB betragen. Bei Verwendung der NFS- oder SAMBA-Protokolle gibt es keine Größenbegrenzung.

Option	Beschreibung
-r	rdoc-Vorgang (muss die erste Option sein, sofern verwendet) -r -map: Anhängen der RDOC-Images -r -unmap<filename>: Abhängen der angehängten RDOC-Images -r -maplist: Zeigt die angehängten RDOC-Images über den XClarity Controller-Webbrowser und die Befehlszeilenschnittstelle an
-map	-t <samba|nfs|http|sftp|ftp> Typ des Dateisystems -ro Lesezugriff -rw Lesen/Schreiben -u Benutzer -p Kennwort -l Speicherort der Datei (URL-Format) -o Option (zusätzliche Optionszeichenfolge für Samba- und NFS-Mounts) -d Domäne (Domäne für Samba-Mount)
-maplist	Zeigt die zugeordneten Images an
-unmap <id|fname>	ID für Netzwerkimages, Dateiname für RDOC verwenden
-mount	Anhängen der zugeordneten Images
-unmount	Abhängen der angehängten Images

Befehl „restore“

Mit diesem Befehl können Sie Systemeinstellungen aus einer Sicherungsdatei wiederherstellen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 40. Befehl „restore“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-f	Name der Sicherungsdatei	Gültiger Dateiname
-pp	Kennwort oder Verschlüsselungstext, mithilfe dessen Kennwörter innerhalb der Sicherungsdatei verschlüsselt sind	Gültiges Kennwort oder durch Anführungszeichen begrenzter Verschlüsselungstext
-ip	IP-Adresse des TFTP-/SFTP-Servers	Gültige IP-Adresse

Tabelle 40. Befehl „restore“ (Forts.)

Option	Beschreibung	Werte
-pn	Portnummer des TFTP/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP-Server	Gültiges Kennwort

Syntax:
```
restore [options]
option:
  -f filename
  -pp password
  -ip ip_address
  -pn port_number
username
  -pw password
```

Beispiel:
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

Befehl „restoredefaults“

Mit diesem Befehl können Sie alle IMM-Einstellungen auf die werkseitigen Voreinstellungen zurücksetzen.

- Für den Befehl **restoredefaults** gibt es keine Optionen.
- Sie werden aufgefordert, den Befehl zu bestätigen, bevor dieser verarbeitet wird.

Syntax:
```
restoredefaults
```

Beispiel:
```
system> restoredefaults

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults
```

Befehl „roles“

Mit diesem Befehl können Sie Rollen anzeigen oder konfigurieren.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 41. Befehl „roles“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Tabelle 41. Befehl „roles“ (Forts.)

Option	Beschreibung	Werte
-n	Zu konfigurierende Rollen	Auf 32 Zeichen begrenzt
-p	Berechtigungen festlegen	custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us • **am**: Benutzerkontenverwaltungszugriff • **rca**: Zugriff auf ferne Konsole • **rcvma**: Zugriff auf ferne Konsole und fernen (virtuellen) Datenträger • **pr**: Berechtigung für Einschalten/Neustart eines fernen Servers • **cel**: Berechtigung zum Löschen von Ereignisprotokollen • **bc**: Adapterkonfiguration (Allgemein) • **nsc**: Adapterkonfiguration (Netzwerk und Sicherheit) • **ac**: Adapterkonfiguration (Erweitert) • **us**: UEFI-Sicherheit **Anmerkung:** die oben genannten benutzerdefinierten Berechtigungskennzeichen können in beliebiger Kombination verwendet werden
d	Zeile löschen	

Syntax

```
   roles [-options] - display/configure roles
   - role_account -role number[3-31]
options:
   -n       - role name (limited to 32 characters)
   -p       - privilege (custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us)
      am    - User account management access
      rca   - Remote console access
      rcvma - Remote console and remote disk (virtual media) access
      pr    - Remote server power/restart access
      cel   - Ability to clear event logs
      bc    - Adapter Configuration (basic)
      nsc   - Adapter Configuration (network and security)
      ac    - Adapter Configuration (advanced)
      us    - UEFI Security
      Note: the above custom permission flags can be used in any combination
   -d       - delete a row
```

Beispiel

```
system> roles -3 -n test1 -p custom:am|rca|rcvma
ok


system> roles
Account             Role                            Privilege                   Assigned To
------- ----------------------------------   -------------------------     -------------------------------
    0                   Administrator                   all                         USERID
    1                        ReadOnly                     none
```

```
2                          Operator          custom:pr|cel|bc|nsc
3                             test1           custom:am|rca|rcvma
```

Befehl „seccfg“

Verwenden Sie diesen Befehl, um ein Firmware-Rollback auszuführen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 42. Befehl „seccfg“

Die folgende mehrzeilige Tabelle mit zwei Spalten enthält die Optionen mit entsprechenden Beschreibungen.

Option	Beschreibung	Wert
-fwrb	Ermöglicht ein Firmware-Rollback auf frühere Versionen	yes, no
-rppen	Physische Präsenz aus der Ferne aktivieren (schreibgeschützt)	/
-rppto	Zeitlimit für physische Präsenz aus der Ferne (schreibgeschützt)	/
-rpp	Physische Präsenz (falls von BIOS aktiviert)	yes, no
-aubp	Aktivieren oder Deaktivieren der Funktion der automatischen Sicherung zur primären Hochstufung	enabled, disabled

Befehl „set“

Mit diesem Befehl können Sie einige IMM-Einstellungen ändern.

- Manche IMM-Einstellungen können einfach durch den Befehl **set** geändert werden.
- Manche dieser Einstellungen, etwa Umgebungsvariablen, werden vom CLI verwendet.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 43. Befehl „set“

Die folgende Tabelle ist eine einzeilige Tabelle mit drei Spalten, die die Befehlsbeschreibung und zugehörige Informationen enthält.

Option	Beschreibung	Werte
Wert	Wert für angegebenen Pfad oder angegebene Einstellung festlegen	Entsprechender Wert für angegebenen Pfad oder angegebene Einstellung.

Syntax:

```
set [options]
option:
  value
```

Befehl „smtp“

Mit diesem Befehl können Sie Einstellungen für die SMTP-Schnittstelle anzeigen und konfigurieren.

Wird der Befehl **smtp** ohne Optionen ausgeführt, so werden alle Informationen zur SMTP-Schnittstelle angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 44. Befehl „smtp“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-auth	Authentifizierungssupport für SMTP	enabled, disabled
-authepw	Verschlüsseltes Kennwort für die SMTP-Authentifizierung	Gültige Kennwort-Zeichenkette
-authmd	SMTP-Authentifizierungsverfahren	CRAM-MD5, LOGIN
-authn	Benutzername zur SMTP-Authentifizierung	Zeichenkette (auf 256 Zeichen begrenzt).
-authpw	SMTP-Authentifizierungskennwort	Zeichenkette (auf 256 Zeichen begrenzt).
-pn	SMTP-Portnummer	Gültige Portnummer
-s	IP-Adresse oder Hostname des SMTP-Servers	Gültige IP-Adresse oder gültiger Hostname (max. 63 Zeichen)

Syntax:
```
smtp [options]
option:
  -auth enabled|disabled
  -authepw password
  -authmd CRAM-MD5|LOGIN
  -authn username
  -authpw password
  -s ip_address_or_hostname
  -pn port_number
```

Beispiel:
```
system> smtp
-s test.com
-pn 25
system>
```

Befehl „snmp“

Mit diesem Befehl können Sie die SNMP-Schnittstelleninformationen anzeigen und konfigurieren.

Wird der Befehl **snmp** ohne Optionen ausgeführt, so werden alle Informationen zur SNMP-Schnittstelle angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 45. Befehl „snmp“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Tabelle 45. Befehl „snmp“ (Forts.)

Option	Beschreibung	Werte
-a3	SNMPv3-Agent	on, off **Anmerkungen:** Folgende Kriterien müssen zum Aktivieren des SNMPv3-Agenten erfüllt sein: • Über die Befehlsoption „-cn“ angegebener Ansprechpartner für den IMM. • Über die Befehlsoption „-l“ angegebener Standort des IMM.
-t1	SNMPv1-Traps	on, off
-t2	SNMPv2-Traps	on, off
-t	SNMPv3-Traps	on, off
-l	IMM-Standort	Zeichenkette (auf 47 Zeichen begrenzt). **Anmerkungen:** • Argumente mit Leerzeichen müssen in Anführungszeichen eingeschlossen werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig. • Löschen Sie beim IMM-Standort den Inhalt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument angeben, etwa „“.
-cn	IMM-Ansprechpartner	Zeichenkette (auf 47 Zeichen begrenzt). **Anmerkungen:** • Argumente mit Leerzeichen müssen in Anführungszeichen eingeschlossen werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig. • Löschen Sie beim IMM-Ansprechpartner den Inhalt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument angeben, etwa „“.
-c	SNMP-Community-Name	Zeichenkette (auf 15 Zeichen begrenzt). **Anmerkungen:** • Argumente mit Leerzeichen müssen in Anführungszeichen eingeschlossen werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig. • Löschen Sie bei einem SNMP-Community-Namen den Inhalt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument angeben, etwa „“.
-ct	Community-Name von SNMPv2-Trap	Zeichenkette (auf 15 Zeichen begrenzt). **Anmerkungen:** • Argumente mit Leerzeichen müssen in Anführungszeichen eingeschlossen werden. Führende oder nachgestellte Leerzeichen sind in Argumenten nicht zulässig. • Löschen Sie beim IMM-Ansprechpartner den Inhalt, indem Sie kein Argument angeben oder indem Sie eine leere Zeichenkette als Argument angeben, etwa „“.

Tabelle 45. Befehl „snmp“ (Forts.)

Option	Beschreibung	Werte
-ci	IP-Adresse von SNMP-Community/Hostname	Gültige IP-Adresse oder gültiger Hostname (auf 63 Zeichen begrenzt). **Anmerkungen:** • Eine IP-Adresse oder ein Hostname darf nur Punkte, Unterstriche, Minuszeichen, Buchstaben und Ziffern enthalten. Eingebettete Leerzeichen oder aufeinanderfolgende Punkte sind nicht zulässig. • Löschen Sie den Inhalt bei der IP-Adresse oder beim Hostnamen einer SNMP-Community, indem Sie kein Argument angeben.
-cti	IP-Adresse/Hostname von SNMPv2-Trap-Community	Gültige IP-Adresse oder gültiger Hostname (auf 63 Zeichen begrenzt). **Anmerkungen:** • Eine IP-Adresse oder ein Hostname darf nur Punkte, Unterstriche, Minuszeichen, Buchstaben und Ziffern enthalten. Eingebettete Leerzeichen oder aufeinanderfolgende Punkte sind nicht zulässig. • Löschen Sie den Inhalt bei der IP-Adresse oder beim Hostnamen einer SNMP-Community, indem Sie kein Argument angeben.
-eid	SNMP-Engine-ID	Zeichenkette (auf 1 bis 27 Zeichen begrenzt)

Syntax:
```
snmp [options]
option:
 -a3 state
  -t state
  -l location
  -cn contact_name
  -t1 state
  -c community name
  -ci community IP address/hostname
  -t2 state
  -ct community name
  -cti community IP address/hostname
  -eid engine id
```

Beispiel:
```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
-c community1
-ci host1
-t2 enabled
-ct community2
-cti host2
-eid XCC-7Z70-DSYM09X
system>
```

Befehl „snmpalerts“

Mit diesem Befehl können Sie über das SNMP gesendete Alerts verwalten.

Wird **snmpalerts** ohne Optionen ausgeführt, so werden alle SNMP-Alerteinstellungen angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 46. Befehl „snmpalerts“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-status	SNMP-Alertstatus	on, off
-crt	Legt kritische Ereignisse fest, die Alerts senden	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Benutzerdefinierte Einstellungen für kritische Alerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **snmpalerts -crt custom:te|vo** angegeben; benutzerdefinierte Werte sind: • te: kritischer Temperaturschwellenwert überschritten • vo: kritischer Spannungsschwellenwert überschritten • po: kritischer Netzausfall • di: Fehler beim Festplattenlaufwerk • fa: Lüfterfehler • cp: Mikroprozessorfehler • me: Speicherfehler • in: Hardwareinkompatibilität • re: Stromversorgungsredundanzfehler • ot: alle anderen kritischen Ereignisse
-crten	Alerts bei kritischen Ereignissen senden	enabled, disabled
-wrn	Legt Warnungsereignisse fest, die Alerts senden	all, none, custom:rp|te|vo|po|fa|cp|me|ot Benutzerdefinierte Einstellungen für Warnungsalerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **snmpalerts -wrn custom:rp|te** angegeben; benutzerdefinierte Werte sind: • rp: Warnung bei Stromversorgungsredundanz • te: Warnungstemperaturschwellenwert überschritten • vo: Warnungsspannungsschwellenwert überschritten • po: Warnungsnetzschwellenwert überschritten • fa: unkritischer Lüfterfehler • cp: Mikroprozessor in beeinträchtigtem Zustand • me: Speicherwarnung • ot: alle anderen Warnungsereignisse
-wrnen	Alerts bei Warnungsereignissen senden	enabled, disabled

Tabelle 46. Befehl „snmpalerts“ (Forts.)

Option	Beschreibung	Werte
-sys	Legt Routineereignisse fest, die Alerts senden	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Benutzerdefinierte Einstellungen für Routinealerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **snmpalerts -sys custom:lo|tio** angegeben; benutzerdefinierte Werte sind: • lo: erfolgreiche Fernanmeldung • tio: Zeitlimit des Betriebssystems • ot: alle anderen Informations- und Systemereignisse • po: Stromversorgung des Systems ein/aus • bf: Bootfehler des Betriebssystems • til: Watchdog-Zeitlimitüberschreitung des Betriebssystemladeprogramms • pf: vorhergesagter Fehler (PFA - Predictive Failure Analysis) • el: Ereignisprotokoll zu 75 % voll • ne: Netzänderung
-sysen	Alerts bei Routineereignissen senden	enabled, disabled

Syntax:
```
snmpalerts [options]
   options:
     -status status
     -crt event_type
     -crten state
     -wrn event_type
     -wrnen state
     -sys event_type
     -sysen state
```

Befehl „srcfg“

Mit diesem Befehl können Sie die Tastenkombination für den Zugang zur Befehlszeilenschnittstelle vom Modus für serielle Umleitung angeben.

Um die Konfiguration der seriellen Umleitung zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein. Um die Konfiguration der seriellen Umleitung ändern zu können, müssen Sie mindestens über die Berechtigung „Konfiguration von Adapternetzbetrieb und -sicherheit“ verfügen.

Anmerkung: Die IMM-Hardware sieht keine Pass-Through-Fähigkeit zwischen seriellen Anschlüssen vor. Daher werden die Optionen `-passthru` und `entercliseq`, die in der Befehlszeilenschnittstelle des Remote Supervisor Adapter II vorhanden sind, nicht unterstützt.

Wird der Befehl **srcfg** ohne Optionen ausgeführt, so wird die aktuelle Tastenfolge für die serielle Umleitung angezeigt. In der folgenden Tabelle sind die Argumente für die Befehlsoption `srcfg -entercliseq` aufgelistet.

Tabelle 47. Befehl „srcfg“

Die folgende Tabelle ist eine einzeilige Tabelle mit drei Spalten, die die Option, eine Beschreibung der Option und Werteinformationen für die Option enthält.

Tabelle 47. Befehl „srcfg“ (Forts.)

Option	Beschreibung	Werte
-entercliseq	Tastenfolge für Befehlszeilenschnitt-stelle eingeben	Benutzerdefinierte Tastenfolge für den Zugang zur Befehlszeilenschnittstelle. **Anmerkung:** Diese Sequenz muss mindestens ein Zeichen und darf höchstens 15 Zeichen enthalten. Das Winkelzeichen (^) hat in dieser Sequenz eine spezielle Bedeutung. Es steht bei Tastatureingaben, die 'Strg'-Sequenzen zugeordnet sind (beispielsweise ^[für die Abbruchtaste und ^M für einen Zeilenumbruch), für 'Strg'. Jedes Auftreten von '^' wird als Teil einer 'Strg'-Sequenz interpretiert. Eine vollständige Liste mit 'Strg'-Sequenzen finden Sie in der ASCII-Konvertierungstabelle. Der Standardwert für dieses Feld ist ^[(, d. h. die Abbruchtaste gefolgt von einer (.

Syntax:
```
srcfg [options]
options:
-entercliseq entercli_keyseq
```

Beispiel:
```
system> srcfg
-entercliseq ^[Q
system>
```

Befehl „sshcfg“

Mit diesem Befehl können Sie SSH-Parameter anzeigen und konfigurieren.

Wird der Befehl **sshcfg** ohne Optionen ausgeführt, so werden alle SSH-Parameter angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 48. Befehl „sshcfg“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-cstatus	Zustand von SSH-CLI	enabled, disabled
-hk gen	Privaten Schlüssel für SSH-Server generieren	
-hk rsa	Öffentlichen Schlüssel von Server-RSA anzeigen	

Syntax:
```
sshcfg [options]
option:
  -cstatus state
  -hk gen
  -hk rsa
```

Beispiel:
```
system> sshcfg
-cstatus enabled
CLI SSH port 22
```

```
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

Befehl „ssl“

Mit diesem Befehl können Sie die SSL-Parameter anzeigen und konfigurieren.

Um einen SSL-Client aktivieren zu können, muss ein Clientzertifikat installiert werden. Wird der Befehl **ssl** ohne Optionen ausgeführt, so werden SSL-Parameter angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 49. Befehl „ssl“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-ce	Aktiviert oder deaktiviert einen SSL-Client	on, off
-se	Aktiviert oder deaktiviert einen SSL-Server	on, off
-cime	Aktiviert oder deaktiviert CIM over HTTPS auf dem SSL-Server	on, off

Syntax:

```
portcfg [options]
 options:
  -ce state
  -se state
  -cime state
```

Parameter: Die folgenden Parameter erscheinen in der Optionsstatusanzeige für den Befehl **ssl** und werden nur über die Befehlszeilenschnittstelle ausgegeben:

Server secure transport enable
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden.

Status Server-Web/CMD-Schlüssel
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Privater Schlüssel gespeichert, Zertifikatssignieranforderung zum Download verfügbar

Status CSR-Schlüssel für SSL-Server
Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Privater Schlüssel gespeichert, Zertifikatssignieranforderung zum Download verfügbar

Status LDAP-Schlüssel für SSL-Client

Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Privater Schlüssel gespeichert, Zertifikatssignieranforderung zum Download verfügbar

Status CSR-Schlüssel für SSL-Client

Diese Statusanzeige ist schreibgeschützt und kann nicht direkt festgelegt werden. Folgende Befehlszeilenausgabewerte sind möglich:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Privater Schlüssel gespeichert, Zertifikatssignieranforderung zum Download verfügbar

Befehl „sslcfg“

Mit diesem Befehl können Sie SSL für den IMM anzeigen und konfigurieren und Zertifikate verwalten.

Wird der Befehl **sslcfg** ohne Optionen ausgeführt, so werden alle Informationen zur SSL-Konfiguration angezeigt. Der Befehl **sslcfg** wird verwendet, um einen neuen Chiffrierschlüssel und ein selbst signiertes Zertifikat oder eine Zertifikatssignieranforderung (CSR) zu generieren. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 50. Befehl „sslcfg“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-server	SSL-Serverstatus	enabled, disabled **Anmerkung:** Der SSL-Server kann nur bei Vorliegen eines gültigen Zertifikats aktiviert werden.
-client	SSL-Clientstatus	enabled, disabled **Anmerkung:** Der SSL-Client kann nur bei Vorliegen eines gültigen Server- oder Clientzertifikats aktiviert werden.
-cim	CIM-over-HTTPS-Status	enabled, disabled **Anmerkung:** CIM over HTTPS kann nur bei Vorliegen eines gültigen Server- oder Clientzertifikats aktiviert werden.
-cert	Selbst signiertes Zertifikat generieren	server, client, sysdir, storekey **Anmerkungen:** • Werte für die Befehlsoptionen **-c**, **-sp**, **-cl**, **-on** und **-hn** sind bei der Erstellung eines selbst signierten Zertifikats erforderlich. • Werte für die Befehlsoptionen **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in** und **-dq** sind bei der Erstellung eines selbst signierten Zertifikats optional.

Tabelle 50. Befehl „sslcfg“ (Forts.)

Option	Beschreibung	Werte
-csr	Eine Zertifikatssignieranforderung generieren	server, client, sysdir, storekey **Anmerkungen:** • Werte für die Befehlsoptionen **-c**, **-sp**, **-cl**, **-on** und **-hn** sind bei der Erstellung einer Zertifikatssignieranforderung erforderlich. • Werte für die Befehlsoptionen **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd** und **-un** sind bei der Erstellung einer Zertifikatssignieranforderung optional.
-i	IP-Adresse für TFTP-/SFTP-Server	Gültige IP-Adresse **Anmerkung:** Beim Hochladen eines Zertifikats und beim Herunterladen eines Zertifikats oder einer Zertifikatssignieranforderung muss eine IP-Adresse für den TFTP- oder SFTP-Server angegeben werden.
-pn	Portnummer des TFTP/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP-Server	Gültiges Kennwort
-l	Dateiname des Zertifikats	Gültiger Dateiname **Anmerkung:** Beim Herunterladen oder Hochladen eines Zertifikats oder einer Zertifikatssignieranforderung ist ein Dateiname erforderlich. Wenn beim Herunterladen kein Dateiname angegeben wird, wird der Standardname für die Datei verwendet und angezeigt.
-dnld	Zertifikatsdatei herunterladen	Bei dieser Option sind keine Argumente erforderlich; es müssen jedoch Werte für die Befehlsoptionen **-cert** oder **-csr** angegeben werden (abhängig davon, welcher Zertifikatstyp heruntergeladen wird). Bei dieser Option sind keine Argumente erforderlich; es müssen jedoch Werte für die Befehlsoption **-i** und die (optionale) Befehlsoption **-l** angegeben werden.
-upld	Importiert Zertifikatsdatei	Bei dieser Option sind keine Argumente erforderlich, es müssen jedoch Werte für die Befehlsoptionen **-cert**, **-i** und **-l** angegeben werden.
-tc**x**	Vertrauenswürdiges Zertifikat **x** für SSL-Client	import, download, remove **Anmerkung:** Die vertrauenswürdige Zertifikatsnummer **x** wird in der Befehlsoption als Ganzzahl zwischen 1 und 3 angegeben.
-c	Land	Landescode (2 Buchstaben) **Anmerkung:** Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-sp	Land oder Bundesland	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cl	Ort oder Standort	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 50 Zeichen) **Anmerkung:** Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-on	Name des Unternehmens	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.

Tabelle 50. Befehl „sslcfg“ (Forts.)

Option	Beschreibung	Werte
-hn	IMM-Hostname	Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Erforderlich bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cp	Ansprechpartner	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-ea	E-Mail-Adresse des Ansprechpartners	Gültige E-Mail-Adresse (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-ou	Organisationseinheit	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-s	Nachname	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-gn	Vorname	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-in	Initialen	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 20 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-dq	Qualifikationsmerkmal des Domänennamens	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung eines selbst signierten Zertifikats oder einer Zertifikatssignieranforderung.
-cpwd	Kennwort abfragen	Zeichenkette (mindestens 6 Zeichen, höchstens 30 Zeichen) **Anmerkung:** Optional bei der Erstellung einer Zertifikatssignieranforderung.
-un	Unstrukturierter Name	Durch Anführungszeichen begrenzte Zeichenkette (höchstens 60 Zeichen) **Anmerkung:** Optional bei der Erstellung einer Zertifikatssignieranforderung.

Syntax:

```
sslcfg [options]
option:
  -server state
  -client state
  -cim state
  -cert certificate_type
  -csr certificate_type
  -i ip_address
port number
username
  -pw password
```

```
-l filename
-dnld
-upld
-tc xaction
-c country_code
-sp state_or_province
-cl city_or_locality
-on organization_name
-hn bmc_hostname
-cp contact_person
-ea email_address
-ou organizational_unit
-s surname
-gn given_name
-in initials
-dq dn_qualifier
-cpwd challenge_password
-un unstructured_name
```

Beispiele:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

Beispiele für ein Client-Zertifikat:

- Geben Sie den folgenden Befehl ein, um eine CSR für einen Speicherschlüssel zu generieren.

  ```
  system> sslcfg
  -csr storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou""
  ok
  ```

Das Beispiel oben wird je nach Platzeinschränkungen in mehreren Zeilen angezeigt.

- Um ein Zertifikat aus dem IMM in einen anderen Server herunterzuladen, geben Sie den folgenden Befehl ein:

  ```
  system> sslcfg
  -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
  ok
  ```

- Geben Sie den folgenden Befehl ein, um das von der Zertifizierungsstelle verarbeitete Zertifikat hochzuladen:

  ```
  system> sslcfg
  -cert storekey -upld -i 192.168.70.230 -l tklm.der
  ```

- Geben Sie den folgenden Befehl ein, um ein selbst signiertes Zertifikat zu generieren:

  ```
  system> sslcfg
  -cert storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  ```

```
-cp Contact -ea "" -ou "
ok
```

Das Beispiel oben wird je nach Platzeinschränkungen in mehreren Zeilen angezeigt.

Beispiel für ein SKLM-Serverzertifikat:

- Geben Sie den folgenden Befehl ein, um ein SKLM-Serverzertifikat zu importieren:
```
system> storekeycfg
-add -ip 192.168.70.200 -f tklm-server.der
ok
```

Befehl „storekeycfg“

Verwenden Sie diesen Befehl, um den Hostnamen oder die IP-Adresse und den Netzwerkanschluss für einen SKLM-Server zu konfigurieren.

Sie können bis zu vier SKLM-Serverziele konfigurieren. Der Befehl **storekeycfg** wird auch verwendet, um die Zertifikate zu installieren und zu entfernen, die vom IMM für die Authentifizierung zum SKLM-Server verwendet werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 51. Befehl „storekeycfg“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-add	Aktivierungsschlüssel hinzufügen	Werte sind die Befehlsoptionen -ip, -pn, -u, -pw und -f.
-ip	Hostname oder IP-Adresse für den TFTP/SFTP-Server	Gültiger Hostname oder IP-Adresse für den TFTP/SFTP-Server
-pn	Portnummer des TFTP/SFTP-Servers	Gültige Portnummer für den TFTP-/SFTP-Server (Standardwert: 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername für SFTP-Server
-pw	Kennwort für SFTP-Server	Gültiges Kennwort für SFTP-Server
-f	Dateiname für Aktivierungsschlüssel	Gültiger Dateiname für die Aktivierungsschlüsseldatei
-del	Verwenden Sie diesen Befehl, um den Aktivierungsschlüssel nach Indexnummer zu löschen.	Gültige Indexnummer für Aktivierungsschlüssel aus keycfg-Liste
-dgrp	Einheitengruppe hinzufügen	Name der Einheitengruppe
-sxip	Hostname oder IP-Adresse für den SKLM-Server hinzufügen	Gültiger Hostname oder gültige IP-Adresse für den SKLM-Server Numerischer Wert: 1, 2, 3 oder 4
-sxpn	Portnummer des SKLM-Servers hinzufügen	Gültige Portnummer für den SKLM-Server Numerischer Wert: 1, 2, 3 oder 4

Tabelle 51. Befehl „storekeycfg“ (Forts.)

Option	Beschreibung	Werte
-testx	Konfiguration und Verbindung zum SKLM-Server testen	Numerischer Wert: 1, 2, 3 oder 4
-h	Befehlssyntax und -optionen anzeigen	

Syntax:
```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -f filename
  -del key_index
  -dgrp device_group_name
  -sxip ip_address
  -sxpn port_number
  -testx numeric value of SKLM server
  -h
```

Beispiele:

Geben Sie den folgenden Befehl ein, um ein SKLM-Serverzertifikat zu importieren:
```
system> storekeycfg
add -ip 192.168.70.200 -f tklm-server.der
system> ok
```

Um die SKLM-Serveradresse und die Portnummer zu konfigurieren, geben Sie den folgenden Befehl ein:
```
system> storekeycfg
-s1ip 192.168.70.249
system> ok
```

Um den Namen der Einheitengruppe festzulegen, geben Sie den folgenden Befehl ein:
```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
system> ok
```

Befehl „syncrep“

Mit diesem Befehl können Sie die Firmwaresynchronisierung aus dem fernen Repository starten.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 52. Befehl „syncrep“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-t	Protokoll zum Verbinden des Repository	samba, nfs
-l	Position des fernen Repository	Im URL-Format

Tabelle 52. Befehl „syncrep“ (Forts.)

Option	Beschreibung	Werte
-u	Benutzer	
-p	Kennwort	
-o	Option	Zusätzliche Optionszeichenfolge für Samba- und NFS-Mounts
-d	Domain	Domäne für Samba-Mount
-q	Aktuellen Aktualisierungsstatus abfragen	
-c	Synchronisierungsprozess abbrechen	

Syntax

```
syncrep [options]  Launch firmware sync from remote repository
options:
     -t <samba|nfs> protocol to connect repository
     -l location of remote repository (URL format)
     -u User
     -p Password
     -o option (extra option string for samba and nfs mounts)
     -d domain (domain for samba mount)
     -q query current update status
     -c cancel the sync process
```

Beispiel

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password
(2) query current update status
system> syncrep -q
(3)cancel the sync process
system> syncrep -c
```

Befehl „thermal“

Mit diesem Befehl können Sie die Richtlinie für den Temperaturmodus des Hostsystems anzeigen und konfigurieren.

Wird der Befehl **thermal** ohne Optionen ausgeführt, so wird die Richtlinie für den Temperaturmodus angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 53. Befehl „thermal“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-mode	Auswahl des Temperaturmodus	Normal, Leistung, Minimal, Wirkungsgrad, Angepasst
-table	Hersteller, Geräte-ID und alternative Wärmetabelle	

Syntax:

```
thermal [options]
option:
```

```
  -mode thermal_mode
  -table vendorID_devicetable_number
```

Beispiel:

```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

Befehl „timeouts“

Mit diesem Befehl können Sie die Zeitlimitwerte anzeigen oder ändern.

- Geben Sie `timeouts` ein, um die Zeitlimitwerte anzuzeigen.
- Um die Zeitlimitwerte zu ändern, geben Sie die entsprechenden Optionen gefolgt von den Werten ein.
- Um Zeitlimitwerte ändern zu können, müssen Sie mindestens über die Berechtigung „Adapter Configuration“ (Adapterkonfiguration) verfügen.

In der folgenden Tabelle sind die Argumente für die Zeitlimitwerte aufgelistet. Diese Werte entsprechen den abgestuften Pulldownoptionsskalen für Serverzeitlimits in der Webschnittstelle.

Tabelle 54. Befehl „timeouts“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit vier Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Zeitlimit	Einheiten	Werte
-f	Ausschaltverzögerung	Minuten	disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-l	Zeitlimit für das Ladeprogramm	Minuten	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
-o	Zeitlimit für das Betriebssystem	Minuten	disabled, 2.5, 3, 3.5, 4
-s	Betriebssystem-Fehleranzeige mit HW-Fehler	/	disabled, enabled

Syntax:

```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
-s OS failure screen capture with HW error
```

Beispiel:

```
system> timeouts
-o disabled
-l 3.5
-f disabled
-s disabled
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
```

```
-f disabled
-s disabled
```

Befehl „tls“

Verwenden Sie diesen Befehl, um die TLS-Mindeststufen festzulegen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 55. Befehl „tls“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-min	TLS-Mindeststufe auswählen	1.0, 1.1, 1.2[1], 1.3
-h	Verwendung und Optionen auflisten	

Anmerkungen:

1. Wenn als Verschlüsselungsmodus der NIST-800-131A-Kompatibilitätsmodus festgelegt ist, muss als TLS-Version 1.2 festgelegt werden.

Nutzung:

```
tls [-options] - configures the minimum TLS level
   -min <1.0 | 1.1 | 1.2 | 1.3> - Selects the minimum TLS level
   -h - Lists usage and options
```

Beispiele:

Um die Verwendung für den Befehl „tls“ abzurufen, geben Sie den folgenden Befehl aus:

```
system> tls
-h
system>
```

Um die aktuelle TLS-Version abzurufen, geben Sie den folgenden Befehl aus:

```
system> tls
-min 1.2
system>
```

Um die aktuelle TLS-Version in 1.2 zu ändern, geben Sie den folgenden Befehl aus:

```
system> tls
-min 1.2
ok
system>
```

Befehl „trespass“

Mit diesem Befehl können Sie die Überschreitungsnachrichten konfigurieren und anzeigen.

Der Befehl **trespass** dient zum Konfigurieren und Anzeigen von Überschreitungsnachrichten. Die Überschreitungsnachrichten werden jedem Benutzer angezeigt, der sich über die Web- oder Befehlszeilenschnittstelle anmeldet.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 56. Befehl „trespass“

Die folgende mehrzeilige Tabelle mit zwei Spalten enthält die Optionen mit entsprechenden Beschreibungen.

Option	Beschreibung
-s	Überschreitungsnachrichten konfigurieren
-h	Listet die Befehlssyntax und die Optionen auf

Syntax:

```
usage:
   trespass display the trespass message
   -s <trespass message> configure trespass message
   -h - Lists usage and options
```

Beispiel:

Anmerkung: Die Überschreitungsnachricht enthält kein Leerzeichen.

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage

The trespass message contains spaces:
system> trespass -s "testing message"
ok
system> trespass
testing message
```

Befehl „trespass“

Mit diesem Befehl können Sie UEFI-Administratorkennwörter konfigurieren. Das Kennwort ist lesegeschützt.

Der Befehl **uefipw** kann mit der Option „-p“ zur Konfiguration des UEFI-Administratorkennworts für XCC oder mit der Option „-ep“ für LXCA zur Konfiguration des UEFI-Administratorkennworts über die Befehlszeilenschnittstelle verwendet werden. Das Kennwort ist lesegeschützt.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 57. Befehl „trespass“

Die folgende mehrzeilige Tabelle mit zwei Spalten enthält die Optionen mit entsprechenden Beschreibungen.

Option	Beschreibung
-cp	Aktuelles Kennwort (auf 20 Zeichen begrenzt)
-p	Neues Kennwort (auf 20 Zeichen begrenzt)
-cep	Aktuelles Kennwort, verschlüsselt
-ep	Neues Kennwort, verschlüsselt

Syntax:

```
usage:
   uefipw [-options] - Configure the UEFI admin password
options:
   -cp      - current password (limited to 20 characters)
```

```
-p       - new password (limited to 20 characters)
-cep     - current password encrypted
-ep      - new password encrypted
```

Befehl „usbeth“

Mit diesem Befehl können Sie die Inbandschnittstelle „LAN over USB“ aktivieren oder deaktivieren.

Syntax:
```
usbeth [options]
options:
-en <enabled|disabled>
```

Beispiel:
```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

Befehl „usbfp“

Verwenden Sie diesen Befehl, um die Verwendung des vorderseitigen USB-Anschlusses durch BMC zu steuern.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 58. Befehl „usbfp“

Die folgende mehrzeilige Tabelle mit zwei Spalten enthält die Optionen mit entsprechenden Beschreibungen.

Option	Beschreibung
-mode <bmc | server | shared>	Festlegung des Nutzungsmodus auf BMC, Server oder gemeinsam genutzt
-it <minutes>	Inaktivitätszeitlimit in Minuten (Modus der gemeinsamen Nutzung)
-btn <on | off>	Aktivierung mithilfe der ID-Taste zum Umschalten des Eigentümers (Modus der gemeinsamen Nutzung)
-own <bmc | server >	Festlegung des Eigentümers auf BMC oder Server (Modus der gemeinsamen Nutzung)

Befehl „users“

Mit diesem Befehl können Sie auf alle Benutzerkonten und auf die zugehörigen Berechtigungsstufen zugreifen.

Mit dem Befehl **users** können Sie außerdem neue Benutzerkonten erstellen und bereits vorhandene Konten ändern. Wenn Sie den Befehl **users** ohne Optionen ausführen, werden eine Liste der Benutzer und bestimmte grundlegende Benutzerinformationen angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 59. Befehl „users“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Tabelle 59. Befehl „users“ (Forts.)

Option	Beschreibung	Werte
-**user_index**	Indexnummer des Benutzeraccounts	1 bis 12 einschließlich oder `all` für alle Benutzer.
-n	Name des Benutzeraccounts	Eindeutige Zeichenfolge, die nur Zahlen, Buchstaben, Punkte und Unterstriche enthält. Mindestens vier Zeichen; höchstens 16 Zeichen.
-p	Kennwort des Benutzeraccounts	Zeichenfolge, die mindestens ein alphabetisches und ein nicht alphabetisches Zeichen enthält. Mindestens sechs Zeichen; höchstens 20 Zeichen. Mit null Zeichen wird ein Account ohne Kennwort erstellt. Der Benutzer muss das Kennwort bei der ersten Anmeldung festlegen.
-a	Berechtigungsstufe	Als Berechtigungsstufe kann eine der folgenden Stufen angegeben werden: • `super` (Supervisor) • `ro` (schreibgeschützt) • Eine beliebige Kombination aus den folgenden Werten, getrennt durch |: – `am` (Benutzerkontenverwaltungszugriff) – `rca` (Zugriff auf ferne Konsole) – `rcvma` (Zugriff auf ferne Konsole und virtuelle Datenträger) – `pr` (Zugriff auf Einschalten/Neustart eines fernen Servers) – `cel` (Berechtigung zum Löschen von Ereignisprotokollen) – `bc` (Adapterkonfiguration [allgemein]) – `nsc` (Adapterkonfiguration [Netz und Sicherheit]) – `ac` (Adapterkonfiguration [erweitert])
-ep	Verschlüsselungskennwort (für Sicherung/ Wiederherstellung)	Gültiges Kennwort
-clear	Angegebenen Benutzeraccount entfernen Wenn Sie dazu berechtigt sind, können Sie Ihren eigenen Account oder den Account anderer Benutzer entfernen, auch wenn sie derzeit angemeldet sind, es sei denn, dies ist der einzige verbleibende Account mit Berechtigungen zur Verwaltung von Benutzeraccounts. Sitzungen, die beim Löschen von Benutzeraccounts bereits aktiv sind, werden nicht automatisch beendet.	Die Indexnummer des zu entfernenden Benutzeraccounts muss im folgenden Format angegeben werden: `users -clear -`**user_index**
-curr	Aktuell angemeldete Benutzer anzeigen	
-sauth	SNMPv3-Authentifizierungsprotokoll	HMAC-SHA, keine

Tabelle 59. Befehl „users“ (Forts.)

Option	Beschreibung	Werte
-spriv	SNMPv3-Datenschutzprotokoll	CBC-DES, AES, none
-spw	SNMPv3-Datenschutzkennwort	Gültiges Kennwort
-sepw	SNMPv3-Datenschutzkennwort (verschlüsselt)	Gültiges Kennwort
-sacc	SNMPv3-Zugriffstyp	get, set
-strap	SNMPv3-Trap-Hostname	Gültiger Hostname
-pk	Öffentlichen SSH-Schlüssel für Benutzer anzeigen	Indexnummer des Benutzeraccounts. **Anmerkungen:** • Es werden jeder dem Benutzer zugeordnete SSH-Schlüssel und die jeweilige Schlüsselindexnummer angezeigt. • Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option **-userindex**) im folgenden Format verwendet werden: `users -2 -pk`. • Alle Schlüssel weisen das OpenSSH-Format auf. • Bei Flex Knoten sind die Befehle „users“ auf lokale IPMI- und SNMP-Konten beschränkt. Die Option `-pk` wird nicht für Flex Systeme unterstützt.
-e	Vollständigen SSH-Schlüssel im OpenSSH-Format anzeigen **(Option für öffentliche SSH-Schlüssel)**	Diese Option kann nur ohne Argumente verwendet werden. Sie muss ohne die anderen Optionen vom Typ `users -pk` verwendet werden. **Anmerkung:** Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option **-userindex**) im folgenden Format verwendet werden: `users -2 -pk -e`.
-remove	Öffentlichen SSH-Schlüssel für Benutzer entfernen **(Option für öffentliche SSH-Schlüssel)**	Die Indexnummer des öffentlichen Schlüssels, der entfernt werden soll, muss für einen bestimmten Schlüssel mit **-key_index** oder für alle dem Benutzer zugeordneten Schlüssel mit `-all` angegeben werden. **Anmerkungen:** • Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option **-userindex**) im folgenden Format verwendet werden: `users -2 -pk -remove -1`. • Bei Flex Knoten sind die Befehle „users“ auf lokale IPMI- und SNMP-Konten beschränkt. Die Option `-remove` wird nicht für Flex Systeme unterstützt.

Tabelle 59. Befehl „users“ (Forts.)

Option	Beschreibung	Werte
-add	Öffentlichen SSH-Schlüssel für Benutzer hinzufügen **(Option für öffentliche SSH-Schlüssel)**	Durch Anführungszeichen begrenzter Schlüssel im OpenSSH-Format **Anmerkungen:** • Die Option `-add` darf nicht zusammen mit anderen `users -pk`-Befehlsoptionen verwendet werden. • Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option **-userindex**) im folgenden Format verwendet werden: `users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc +o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E +mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="` • Bei Flex Knoten sind die Befehle „users“ auf lokale IPMI- und SNMP-Konten beschränkt. Die Option `-add` wird nicht für Flex Systeme unterstützt.
-upld	Öffentlichen SSH-Schlüssel hochladen **(Option für öffentliche SSH-Schlüssel)**	Die Optionen `-i` und `-l` sind für die Angabe der Schlüsselposition erforderlich. **Anmerkungen:** • Die Option `-upld` muss ohne die anderen Befehlsoptionen vom Typ `users -pk` (außer `-i` und `-l`) verwendet werden. • Um einen Schlüssel durch einen neuen Schlüssel zu ersetzen, müssen Sie einen **-key_index**. angeben. Wenn Sie einen Schlüssel zum Ende der Liste der aktuellen Schlüssel hinzufügen möchten, geben Sie keinen Schlüsselindex an. • Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option **-userindex**) im folgenden Format verwendet werden: `users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key`. • Bei Flex Knoten sind die Befehle „users“ auf lokale IPMI- und SNMP-Konten beschränkt. Die Option `-upld` wird nicht für Flex Systeme unterstützt.
-dnld	Angegebenen öffentlichen SSH-Schlüssel herunterladen **(Option für öffentliche SSH-Schlüssel)**	Der **-key_index** zum Herunterladen des betreffenden Schlüssels und die Optionen `-i` und `-l` zum Angeben der Speicherposition für den Download (auf einem anderen Computer als auf dem, auf dem ein TFTP-Server ausgeführt wird) sind erforderlich. **Anmerkungen:** • Die Option `-dnld` muss ohne die anderen Befehlsoptionen vom Typ `users -pk` (außer `-i`, `-l` und **-key_index**) verwendet werden. • Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option **-userindex**) im folgenden Format verwendet werden: `users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key`.
-i	IP-Adresse des TFTP/SFTP-Server zum Hoch- oder Herunterladen einer Schlüsseldatei **(Option für öffentliche SSH-Schlüssel)**	Gültige IP-Adresse **Anmerkung:** Die Option `-i` wird von den Befehlsoptionen `users -pk -upld` und `users -pk -dnld` benötigt.

Tabelle 59. Befehl „users“ (Forts.)

Option	Beschreibung	Werte
-pn	Portnummer des TFTP/SFTP-Servers **(Option für öffentliche SSH-Schlüssel)**	Gültige Portnummer (Standard 69/22) **Anmerkung:** Ein optionaler Parameter für die Befehlsoptionen `users -pk -upld` und `users -pk -dnld`.
-u	Benutzername für SFTP-Server **(Option für öffentliche SSH-Schlüssel)**	Gültiger Benutzername **Anmerkung:** Ein optionaler Parameter für die Befehlsoptionen `users -pk -upld` und `users -pk -dnld`.
-pw	Kennwort für SFTP-Server **(Option für öffentliche SSH-Schlüssel)**	Gültiges Kennwort **Anmerkung:** Ein optionaler Parameter für die Befehlsoptionen `users -pk -upld` und `users -pk -dnld`.
-l	Dateiname zum Hoch- oder Herunterladen einer Schlüsseldatei über TFTP oder SFTP **(Option für öffentliche SSH-Schlüssel)**	Gültiger Dateiname **Anmerkung:** Die Option `-l` wird von den Befehlsoptionen `users -pk -upld` und `users -pk -dnld` benötigt.
-af	Verbindungen vom Host akzeptieren **(Option für öffentliche SSH-Schlüssel)**	Eine durch Kommas getrennte Liste von Hostnamen und IP-Adressen, begrenzt auf 511 Zeichen. Gültige Zeichen: alphanumerisch, Komma, Stern, Fragezeichen, Ausrufezeichen, Punkt, Bindestrich, Doppelpunkt und Prozentzeichen.
-cm	Kommentar **(Option für öffentliche SSH-Schlüssel)**	Eine durch Anführungszeichen begrenzte Zeichenfolge von bis zu 255 Zeichen. **Anmerkung:** Wenn Sie die Optionen für öffentliche SSH-Schlüssel verwenden, muss die Option `-pk` nach dem Benutzerindex (Option **-userindex**) im folgenden Format verwendet werden: `users -2 -pk -cm "This is my comment."`.

Syntax:

```
users [-options] - display/configure user accounts
options:
   -[1-12]  - user account number
   -l       - display password expiration days
   -n       - username (limited to 16 characters)
   -p       - password (limited to 32 characters)
   -shp     - set hashpassword (total 64 characters)
   -ssalt   - set salt (limited to 64 characters)
   -ghp     - get hashpassword
   -gsalt   - get salt
   -ep      - encrypted password (used with backup/restore )

   -a       - authority level (super, ro, custom:am|rca|rcvma|pr|cel|bc|nsc|ac)
       -am    - User account management access
       -rca   - Remote console access
       -rcvma - Remote console and remote disk (virtual media) access
       -pr    - Remote server power/restart access
       -cel   - Ability to clear event logs
       -bc    - Adapter Configuration (basic)
       -nsc   - Adapter Configuration (network and security)
       -ac    - Adapter Configuration (advanced)

   -clear   - clear user account
   -curr    - display current users
```

```
   -sauth   (none|HMAC-SHA)           - snmpv3 authentication protocol
   -spriv   (none|CBC-DES|AES)        - snmpv3 privacy protocol
   -spw     password                    - snmpv3 privacy password
   -sepw    encryptedpassword          - snmpv3 privacy password (encrypted)
   -sacc    (Get)                   - snmpv3 Access type
   -strap   hostname                    - snmpv3 trap hostname

   -pk      - SSH public keys options:
       -e       - Displays the entire key in OpenSSH format
       -remove  - Removes the specified key for the specified user
       -add     - Adds a public key for the specified user
       -upld    - Used to upload a public key in OpenSSH/RFC4716 format
       -dnld    - Used to download the specified public key to a TFTP/SFTP server
       -i       - IP address of the TFTP/SFTP
       -pn      - port number of tftp/sftp server (default 69/22)
       -u       - username for sftp server
       -pw      - password for sftp server
       -l       - Filename of the key file when uploading or downloading via TFTP/SFTP
       -af      - accept connections from host, in the format: from="<list>", where
                  <list> is a comma-separated list of hostnames and IP addresses
                  (limited to 511 characters)
       -cm      - comment (limited to 255 characters, must be quote-delimited)
```

Anmerkung: – benutzerdefinierte Berechtigungskennzeichen können in beliebiger Kombination verwendet werden.

Beispiel:

```
system> users
 Account      Login ID      Advanced Attribute              Role             Password Expires
 -------      --------      ------------------              ------             ----------------
    1           USERID                  Native                 Administrator                    89 day(s)
system> users -2 -n sptest -p PasswOrd12 -a super
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Account      Login ID      Advanced Attribute            Role               Password Expires
 -------      --------      ------------------            ------             ----------------
    1           USERID                  Native           Administrator                  90 day(s)
2           sptest                  Native                 Administrator            Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -a super
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system> users -2 -n sptest -p PasswOrd12 -a custom:am|rca
The user is required to change the password when the user logs in to the management server for the first time
ok
```

IMM-Steuerbefehle

Dieser Abschnitt enthält eine Liste der CLI-Steuerbefehle von IMM in alphabetischer Reihenfolge.

Es gibt derzeit 7 IMM-Steuerbefehle:

Befehl „alertentries“

Mit diesem Befehl können Sie Alertempfänger verwalten.

- Wird **alertentries** ohne Optionen ausgeführt, so werden alle Alerteintragseinstellungen angezeigt.
- Beim Befehl **alertentries -number -test** wird ein Testalert an die angegebene Empfängerindexnummer generiert.
- Beim Befehl **alertentries -number** (wobei für „number“ eine Zahl zwischen 0–12 steht) werden Alerteintragseinstellungen für die angegebene Empfängerindexnummer angezeigt oder es wird Ihnen ermöglicht, die Alerteinstellungen für diesen Empfänger zu ändern.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 60. Befehl „alertentries“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-number	Indexnummer des Alertempfängers, der angezeigt, hinzugefügt, geändert oder gelöscht werden soll	1 bis 12
-status	Alertempfängerstatus	on, off
-type	Alerttyp	email, syslog
-log	Ereignisprotokoll in Alert-E-Mail einschließen	on, off
-n	Alertempfängername	Zeichenkette
-e	E-Mail-Adresse des Alertempfängers	Gültige E-Mail-Adresse
-ip	Syslog-IP-Adresse oder -Hostname	Gültige IP-Adresse oder gültiger Hostname
-pn	Syslog-Portnummer	Gültige Portnummer
-del	Angegebene Empfängerindexnummer löschen	
-test	Generiert einen Testalert an die angegebene Empfängerindexnummer	

Tabelle 60. Befehl „alertentries“ (Forts.)

Option	Beschreibung	Werte
-crt	Legt kritische Ereignisse fest, die Alerts senden	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Benutzerdefinierte Einstellungen für kritische Alerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **alertentries -crt custom:te|vo** angegeben; benutzerdefinierte Werte sind: • te: kritischer Temperaturschwellenwert überschritten • vo: kritischer Spannungsschwellenwert überschritten • po: kritischer Netzausfall • di: Fehler beim Festplattenlaufwerk • fa: Lüfterfehler • cp: Mikroprozessorfehler • me: Speicherfehler • in: Hardwareinkompatibilität • re: Stromversorgungsredundanzfehler • ot: alle anderen kritischen Ereignisse
-crten	Alerts bei kritischen Ereignissen senden	enabled, disabled
-wrn	Legt Warnungsereignisse fest, die Alerts senden	all, none, custom:rp|te|vo|po|fa|cp|me|ot Benutzerdefinierte Einstellungen für Warnungsalerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **alertentries -wrn custom:rp|te** angegeben; benutzerdefinierte Werte sind: • rp: Warnung bei Stromversorgungsredundanz • te: Warnungstemperaturschwellenwert überschritten • vo: Warnungsspannungsschwellenwert überschritten • po: Warnungsnetzschwellenwert überschritten • fa: unkritischer Lüfterfehler • cp: Mikroprozessor in beeinträchtigtem Zustand • me: Speicherwarnung • ot: alle anderen Warnungsereignisse
-wrnen	Alerts bei Warnungsereignissen senden	enabled, disabled

Tabelle 60. Befehl „alertentries“ (Forts.)

Option	Beschreibung	Werte
-sys	Legt Routineereignisse fest, die Alerts senden	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Benutzerdefinierte Einstellungen für Routinealerts werden mithilfe einer Liste, in der die einzelnen Werte durch Pipe-Zeichen voneinander getrennt sind, mit Werten in der Form **alertentries -sys custom:lo|tio** angegeben; benutzerdefinierte Werte sind: • lo: erfolgreiche Fernanmeldung • tio: Zeitlimit des Betriebssystems • ot: alle anderen Informations- und Systemereignisse • po: Stromversorgung des Systems ein/aus • bf: Bootfehler des Betriebssystems • til: Watchdog-Zeitlimitüberschreitung des Betriebssystemladeprogramms • pf: vorhergesagter Fehler (PFA - Predictive Failure Analysis) • el: Ereignisprotokoll zu 75 % voll • ne: Netzänderung
-sysen	Alerts bei Routineereignissen senden	enabled, disabled

Syntax:

```
alertentries [options]
   options:
   -number recipient_number
      -status status
      -type alert_type
      -log include_log_state
      -n recipient_name
      -e email_address
      -ip ip_addr_or_hostname
      -pn port_number
      -del
      -test
      -crt event_type
      -crten state
      -wrn event_type
      -wrnen state
      -sys event_type
      -sysen state
```

Beispiel:

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
```

```
system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

Befehl „batch“

Mit diesem Befehl können Sie einen oder mehrere in einer Datei enthaltene CLI-Befehle ausführen.

- Kommentarzeilen in der Batchdatei beginnen mit einem #.
- Beim Ausführen einer Batchdatei werden fehlgeschlagene Befehle zusammen mit einem Fehlerrückgabecode zurückgeleitet.
- Batchdateibefehle, die nicht erkannte Befehlsoptionen enthalten, generieren möglicherweise Warnungen.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 61. Befehl „batch“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-f	Name der Batchdatei	Gültiger Dateiname
-ip	IP-Adresse des TFTP-/SFTP-Servers	Gültige IP-Adresse
-pn	Portnummer des TFTP/SFTP-Servers	Gültige Portnummer (Standard 69/22)
-u	Benutzername für SFTP-Server	Gültiger Benutzername
-pw	Kennwort für SFTP-Server	Gültiges Kennwort

Syntax:

```
batch [options]
option:
  -f filename
  -ip ip_address
  -pn port_number
 username
  -pw password
```

Beispiel:

```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

Befehl „clearcfg“

Mit diesem Befehl können Sie die IMM-Konfiguration auf die werkseitigen Voreinstellungen zurücksetzen.

Sie müssen mindestens über die Berechtigung „Advanced Adapter Configuration“ (Erweiterte Adapterkonfiguration) verfügen, um diesen Befehl ausgeben zu können. Nachdem die Konfiguration des IMM gelöscht wurde, wird der IMM erneut gestartet.

Befehl „clock“

Mit diesem Befehl können Sie das aktuelle Datum und die aktuelle Uhrzeit anzeigen. Sie können die UTC-Abweichung und die Sommerzeiteinstellungen festlegen.

Der BMC empfängt die Uhrzeit vom Host-Server oder NTP-Server.

Die Zeit, die vom Host abgerufen wird, kann in Ortszeit oder UTC-Zeit vorliegen. Die Hostoption sollte auf UTC festgelegt sein, wenn kein NTP verwendet wird und der Host das UTC-Format verwendet. Die UTC-Abweichung kann im Format +0200, +2:00, +2 oder 2 (für positive Abweichungen) und im Format -0500, -5:00 oder -5 (für negative Abweichungen) angegeben werden. Die Zeiten für UTC-Abweichung und Sommerzeit werden mit NTP verwendet oder wenn der Hostmodus UTC lautet.

Für eine UTC-Abweichung von +2, -7, -6, -5, -4 und -3 sind besondere Einstellungen für die Sommerzeit erforderlich.

- Für +2 gibt es folgende Optionen für die Sommerzeit: off, ee (Eastern Europe), tky (Turkey), bei (Beirut), amm (Amman), jem (Jerusalem).
- Für -7 gibt es folgende Sommerzeiteinstellungen: off, mtn (Mountain), maz (Mazatlan).
- Für -6 gibt es folgende Sommerzeiteinstellungen: off, mex (Mexico), cna (Central North America).
- Für -5 gibt es folgende Sommerzeiteinstellungen: off, cub (Cuba), ena (Eastern North America).
- Für -4 gibt es folgende Sommerzeiteinstellungen: off, asu (Asuncion), cui (Cuiaba), san (Santiago), cat (Canada - Atlantic).
- Für -3 gibt es folgende Sommerzeiteinstellungen: off, gtb (Godthab), bre (Brazil - East).

Syntax:
```
clock [options]
options:
-u UTC offset
-dst on/off/special case
-host - local | utc , format of time obtained from host (default: utc)
Windows systems use local, Linux uses utc
```

Beispiel:
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

Befehl „identify“

Mit diesem Befehl können Sie die Gehäusekennzeichnungsanzeige einschalten, ausschalten oder blinken lassen.

Die Option **-d** kann zusammen mit **-s on** verwendet werden, um die Anzeige nur für eine bestimmte Anzahl an Sekunden einzuschalten, die mit der Option **-d** angegeben werden. Nachdem die Anzahl an Sekunden verstrichen ist, wird die Anzeige ausgeschaltet.

Syntax:
```
identify [options]
options:
-s on/off/blink
-d seconds
```

Beispiel:

```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

Befehl „info“

Mit diesem Befehl können Sie die Informationen zum IMM anzeigen und konfigurieren.

Wird der Befehl **info** ohne Optionen ausgeführt, so werden alle Standort- und Kontaktinformationen zum IMM angezeigt. In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 62. Befehl „info“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-name	IMM-Name	Zeichenkette
-contact	Name des Ansprechpartners für den IMM	Zeichenkette
-location	IMM-Standort	Zeichenkette
-room[1]	Raum-ID des IMM	Zeichenkette
-rack[1]	Rack-ID des IMM	Zeichenkette
-rup[1]	Position des IMM im Rack	Zeichenkette
-ruh	Höhe der Gehäuserahmeneinheit	Nur Lesen
-bbay	Standort der Bladeposition	Nur Lesen

1. Der Wert lautet „read only“ und kann nicht zurückgesetzt werden, wenn sich der IMM in einem Flex System befindet.

Syntax:

```
info [options]
option:
  -name xcc_name
  -contact contact_name
  -location xcc_location
  -room room_id
  -rack rack_id
  -rup rack_unit_position
  -ruh rack_unit_height
  -bbay blade_bay
```

Befehl „spreset“

Mit diesem Befehl können Sie den IMM neu starten.

Sie müssen mindestens über die Berechtigung „Advanced Adapter Configuration“ (Erweiterte Adapterkonfiguration) verfügen, um diesen Befehl ausgeben zu können.

Agentenlose Befehle

Dieser Abschnitt enthält eine Liste der agentenlosen Befehle in alphabetischer Reihenfolge.

Es gibt derzeit 3 agentenlose Befehle:

Befehl „storage“

Verwenden Sie diesen Befehl, um Informationen zu den Speichereinheiten des Servers anzuzeigen und zu konfigurieren (sofern von der Plattform unterstützt), die vom IMM verwaltet werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 63. Befehl „storage“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-list	Speicherziele auflisten, die durch den IMM verwaltet werden	**controllers|pools|volumes|drives** Dabei steht **Ziel** für: • **controllers**: Unterstützte RAID-Controller auflisten[1] • **pools**: Dem RAID-Controller zugehörige Speicherpools auflisten[1] • **volumes**: Dem RAID-Controller zugehörige Speicherdatenträger auflisten[1] • **drives**: Dem RAID-Controller zugehörige Speicherlaufwerke auflisten[1]
-list -target **target_id**	**Speicherziele**, die vom IMM verwaltet werden, entsprechend ihrer **target_id** auflisten	**pools|volumes|drives ctrl[x]|pool[x]** Dabei stehen **target** und **target_id** für: • **pools ctrl[x]**: Dem RAID-Controller zugehörige Speicherpools auflisten, gemäß ihrer Ziel-ID[1] • **volumes ctrl[x]|pool[x]**: Dem RAID-Controller zugehörige Speicherdatenträger auflisten, gemäß ihrer Ziel-ID[1] • **drives ctrl[x]|pool[x]**: Dem RAID-Controller zugehörige Speicherlaufwerke auflisten, gemäß ihrer Ziel-ID[1]
-list flashdimms	Flash-DIMMs auflisten, die durch den IMM verwaltet werden	
-list devices	Status aller Platten und Flash-DIMMS anzeigen, die durch den IMM verwaltet werden	
-show **target_id**	Informationen zum ausgewählten Ziel anzeigen, das vom IMM verwaltet wird	Dabei steht **target_id** für: **ctrl[x]|vol[x]|disk[x]|pool[x]** **|flashdimm[x]** 3

Tabelle 63. Befehl „storage“ (Forts.)

Option	Beschreibung	Werte
-show **target_id** info	Detaillierte Informationen zum ausgewählten Ziel anzeigen, das vom IMM verwaltet wird	Dabei steht **target_id** für: **ctrl[x]|vol[x]|disk[x]|pool[x]** **|flashdimm[x]** [3]
-show **target_id firmware**[3]	Firmwareinformationen zum ausgewählten Ziel anzeigen, das vom IMM verwaltet wird	Dabei steht **target_id** für: **ctrl[x]|disk[x]|flashdimm[x]**[2]
-showlog **target_id<m:n|all>**[3]	Ereignisprotokolle zum ausgewählten Ziel anzeigen, das vom IMM verwaltet wird	Dabei steht **target_id** für: **ctrl[x]**[4] **m:n|all** Hierbei steht **m:n** für eine maximalen Anzahl von Ereignisprotokollen. Und **alle** steht für alle Ereignisprotokolle.
-config ctrl -scanforgn -target **target_id**[3]	Fremde RAID-Konfiguration erkennen	Dabei steht **target_id** für: **ctrl[x]**[5]
-config ctrl -imptforgn -target **target_id**[3]	Fremde RAID-Konfiguration importieren	Dabei steht **target_id** für: **ctrl[x]**[5]
-config ctrl -clrforgn -target **target_id**[3]	Fremde RAID-Konfiguration löschen	Dabei steht **target_id** für: **ctrl[x]**[5]
-config ctrl -clrcfg -target **target_id**[3]	RAID-Konfiguration löschen	Dabei steht **target_id** für: **ctrl[x]**[5]
-config drv -mkoffline -target **target_id**[3]	Laufwerkstatus von online in offline ändern	Dabei steht **target_id** für: **disk[x]**[5]
-config drv -mkonline -target **target_id**[3]	Laufwerkstatus von offline in online ändern	Dabei steht **target_id** für: **disk[x]**[5]
-config drv -mkmissing -target **target_id**[3]	Offline-Laufwerk als unkonfiguriertes funktionierendes Laufwerk kennzeichnen	Dabei steht **target_id** für: **disk[x]**[5]
-config drv -prprm -target **target_id**[3]	Unkonfiguriertes funktionierendes Laufwerk zum Entfernen vorbereiten	Dabei steht **target_id** für: **disk[x]**[5]
-config drv -undoprprm -target **target_id**[3]	Vorbereitung eines unkonfigurierten funktionierenden Laufwerks zum Entfernen abbrechen	Dabei steht **target_id** für: **disk[x]**[5]
-config drv -mkbad -target **target_id**[3]	Unkonfiguriertes funktionierendes Laufwerk in ein unkonfigurierten nicht funktionierendes Laufwerk ändern	Dabei steht **target_id** für: **disk[x]**[5]

Tabelle 63. Befehl „storage“ (Forts.)

Option	Beschreibung	Werte
-config drv -mkgood -target **target_id**[3]	Unkonfiguriertes nicht funktionierendes Laufwerk in ein unkonfiguriertes funktionierendes Laufwerk ändern oder JBOD-Laufwerk in ein unkonfiguriertes funktionierendes Laufwerk umwandeln	Dabei steht **target_id** für: **disk[x]**[5]
-config drv -addhsp -**[dedicated pools]** -target **target_id**[3]	Das ausgewählte Laufwerk als Ersatz (Hot Spare) einem Controller oder vorhandenen Speicherpools zuweisen	Dabei steht **target_id** für: **disk[x]**[5]
-config drv -rmhsp -target **target_id**[3]	Hot-Spare-Einheit entfernen	Dabei steht **target_id** für: **disk[x]**[5]
-config vol -remove -target **target_id**[3]	Einen Datenträger entfernen	Die **target_id** ist: **vol[x]**[5]

Tabelle 63. Befehl „storage“ (Forts.)

Option	Beschreibung	Werte
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target **target_id**[3]	Eigenschaften eines Datenträgers ändern	• [-N **volume_name**] ist der Name des Datenträgers. • [-w **<0|1|2>**] ist die Cache-Write-Richtlinie: – Geben Sie **0** für die Write-Through-Richtlinie ein. – Geben Sie **1** für die Write-Back-Richtlinie ein. – Geben Sie **2** für die Richtlinie „Write With Battery Backup Unit (BBU)“ ein. • [-r **<0|1|2>**] ist die Cache-Read-Richtlinie: – Geben Sie **0** für die Richtlinie „No Read Ahead“ ein. – Geben Sie **1** für die Richtlinie „Read Ahead“ ein. – Geben Sie **2** für die Richtlinie „Adaptive Read Ahead“ ein. • [-i **<0|1>**] ist die Cache-I/O-Richtlinie: – Geben Sie **0** für die Direct-I/O-Richtlinie ein. – Geben Sie **1** für die Cached-I/O-Richtlinie ein. • [-a **<0|2|3>**] ist die Zugriffsrichtlinie: – Geben Sie **0** für die Read-Write-Richtlinie ein. – Geben Sie **2** für die Read-Only-Richtlinie ein. – Geben Sie **3** für die Blocked-Richtlinie ein. • [-d **<0|1|2>**] ist die Disk-Cache-Richtlinie: – Geben Sie **0** ein, wenn die Richtlinie unverändert ist. – Geben Sie **1** ein, um die Richtlinie zu aktivieren[6] – Geben Sie **2** ein, um die Richtlinie zu deaktivieren • [-b **<0|1>**] ist die Hintergrundinitialisierung: – Geben Sie **0** ein, um die Initialisierung zu aktivieren. – Geben Sie **1** ein, um die Initialisierung zu deaktivieren. • Die **-target_id** ist: **vol[x]**[5]
-config vol -add<[-R] [-D disk] [-H disk] [-1 hole]> [-N] [-w] [-r][3],[7]	Erstellen Sie einen Datenträger für einen neuen Speicherpool, wenn das Ziel ein Controller ist. oder Erstellen Sie einen Datenträger mit einem vorhandenen Speicherpool, wenn das Ziel ein Speicherpool ist.	• [-R **<0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0>**] Diese Option definiert die RAID-Stufe und wird nur mit einem neuen Speicherpool verwendet. • [-D disk **[id11]:disk[id12]:..disk[id21]:disk [id22]:..**] Diese Option definiert die Laufwerksgruppe (einschl. Reichweite) und wird nur mit einem neuen Speicherpool verwendet. • [-H disk **[id1]:disk[id2]:..**]Diese Option definiert die Hot-Spare-Gruppe und wird nur mit einem neuen Speicherpool verwendet.

Tabelle 63. Befehl „storage“ (Forts.)

Option	Beschreibung	Werte
		• [-1 hole] Diese Option definiert die Indexnummer des freien Lückenraums für einen vorhandenen Speicherpool. • [-N **volume_name**] ist der Name des Datenträgers. • [-w **<0|1|2>**] ist die Cache-Write-Richtlinie: – Geben Sie **0** für die Write-Through-Richtlinie ein. – Geben Sie **1** für die Write-Back-Richtlinie ein. – Geben Sie **2** für die Richtlinie „Write With Battery Backup Unit (BBU)“ ein. • [-r **<0|1|2>**] ist die Cache-Read-Richtlinie: – Geben Sie **0** für die Richtlinie „No Read Ahead“ ein. – Geben Sie **1** für die Richtlinie „Read Ahead“ ein. – Geben Sie **2** für die Richtlinie „Adaptive Read Ahead“ ein.
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target **target_id**[3]	Erstellen Sie einen Datenträger für einen neuen Speicherpool, wenn das Ziel ein Controller ist. oder Erstellen Sie einen Datenträger mit einem vorhandenen Speicherpool, wenn das Ziel ein Speicherpool ist.	• [-i **<0|1>**] ist die Cache-I/O-Richtlinie: – Geben Sie **0** für die Direct-I/O-Richtlinie ein. – Geben Sie **1** für die Cached-I/O-Richtlinie ein. • [-a **<0|2|3>**] ist die Zugriffsrichtlinie: – Geben Sie **0** für die Read-Write-Richtlinie ein. – Geben Sie **2** für die Read-Only-Richtlinie ein. – Geben Sie **3** für die Blocked-Richtlinie ein. • [-d **<0|1|2>**] ist die Disk-Cache-Richtlinie: – Geben Sie **0** ein, wenn die Richtlinie unverändert bleibt. – Geben Sie **1** ein, um die Richtlinie zu aktivieren[6] – Geben Sie **2** ein, um die Richtlinie zu deaktivieren • [-f **<0/1/2>**] gibt die Art der Initialisierung an: – Geben Sie **0** für keine Initialisierung ein. – Geben Sie **1** für eine schnelle Initialisierung ein. – Geben Sie **2** für eine vollständige Initialisierung ein. • [-S **volume_size**] ist die Größe des neuen Datenträgers in MB. • [-P **strip_size**] ist die Stripgröße des Datenträgers, z. B. 128.000 oder 1 Mio. • -target **target_id** ist: – **ctrl[x]** (neuer Speicherpool)[5] – **pool[x]** (vorhandener Speicherpool)[5]

Tabelle 63. Befehl „storage“ (Forts.)

Option	Beschreibung	Werte
-config vol -getfreecap [-R] [-D disk] [-H disk] -target **target_id**[3]	Freie Kapazität der Laufwerksgruppe anfordern	• [-R **<0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0>**] Diese Option definiert die RAID-Stufe und wird nur mit einem neuen Speicherpool verwendet. • [-D disk **[id11]:[id12]:..[id21]:[id22]:..**] Diese Option definiert die Laufwerksgruppe (einschl. Reichweite) und wird nur mit einem neuen Speicherpool verwendet. • [-H disk **[id1]:[id2]:..**] Diese Option definiert die Hot-Spare-Gruppe und wird nur mit einem neuen Speicherpool verwendet. • -target **target_id** ist: – **ctrl[x]**[5]
-help	Befehlssyntax und -optionen anzeigen	

Anmerkungen:
1. Dieser Befehl wird nur auf Servern unterstützt, auf denen der IMM auf den RAID-Controller zugreifen kann.
2. Es werden nur Firmwareinformationen für die zugehörigen Controller, Platten und Flash-DIMMs angezeigt. Firmwareinformationen für zugehörige Pools und Datenträger werden nicht angezeigt.
3. Die Informationen werden je nach Platzbeschränkungen in mehreren Zeilen angezeigt.
4. Dieser Befehl wird nur auf Servern unterstützt, die RAID-Protokolle unterstützen.
5. Dieser Befehl wird nur auf Servern unterstützt, die RAID-Konfigurationen unterstützen.
6. Der Wert **Aktivieren** unterstützt keine Konfigurationen für RAID-Stufe 1.
7. Eine teilweise Liste der verfügbaren Optionen ist hier aufgeführt. Die restlichen Optionen für den Befehl **storage -config vol -add** sind in der folgenden Zeile aufgeführt.

Syntax:
```
storage [options]
option:
  -config ctrl|drv|vol -option [-options] -target target_id
  -list controllers|pools|volumes|drives
  -list pools -target ctrl[x]
  -list volumes -target ctrl[x]|pool[x]
  -list drives -target ctrl[x]|pool[x]
  -list devices
  -list flashdimms
  -show target_id
  -show {ctrl[x]|pool[x]|disk[x]|vol[x]|flashdimm[x]} info
  -show {ctrl[x]|disk[x]|flashdimm[x]}firmware
  -showlog ctrl[x]m:n|all
  -h help
```

Beispiele:
```
system> storage
-config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage
-config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage
-config ctrl -imptforgn -target ctrl[0]
ok
```

```
system>
system> storage
-config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage
-config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage
-config drv -addhsp -target disk[0-0]
ok
system>
system> storage
-config drv -mkbad -target disk[0-0]
ok
system>
system> storage
-config drv -mkgood -target disk[0-0]
ok
system>
system> storage
-config drv -mkmissing -target disk[0-0]
ok
system>
system> storage
-config drv -mkoffline -target disk[0-0]
ok
system>
system> storage
-config drv -mkonline -target disk[0-0]
ok
system>
system> storage
-config drv -prprm -target disk[0-0]
ok
system>
system> storage
-config drv -rmhsp -target disk[0-0]
ok
system>
system> storage
-config drv -undoprprm -target disk[0-0]
ok
system>
system> storage
-config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage
-config vol -add -R 1 -D disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage
-config vol -getfreecap -R 1 -D disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage
-config vol -remove -target vol[0-1]
ok
```

```
system>
system> storage
-config vol -set -N LD_volume -w 0 -target vol[0-0]
ok
system>
system> storage
-list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
system> storage
-list drives
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list flashdimms
flashdimm[1]    Flash DIMM 1
flashdimm[4]    Flash DIMM 4
flashdimm[9]    Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage
-list volumes
system>storage -list volumes
vol[0-0]    Volume 0
vol[0-1]    Volume 1
Vol[0-2]    Volume 2
system>
system> storage
-list drives -target ctrl[0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list drives -target pool[0-0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
system>
system> storage
-list pools -target ctrl[0]
pool[0-0]    Storage Pool 0
system>
system> storage
-list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show ctrl[0] firmware
```

```
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage
-show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 12345678901
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
storage[0-0]    Pool 0
storage[0-1]    Pool 1
Drives: 3
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
system> storage
-show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
```

```
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
system>
system> storage
-show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]    LD_volume
system>
system> storage
-show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage
-show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
```

```
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

Befehl „adapter“

Mit diesem Befehl können Sie Bestandsinformationen zu PCIe-Adaptern anzeigen.

Wenn der Befehl **adapter** nicht unterstützt wird, reagiert der Server bei Ausgabe des Befehls mit der folgenden Nachricht:
`Your platform does not support this command.`
Wenn Sie Adapter entfernen, austauschen oder konfigurieren, müssen Sie den Server (mindestens einmal) neu starten, um die aktualisierten Adapterinformationen anzeigen zu können.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 64. Befehl „adapter“

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Option	Beschreibung	Werte
-list	Alle PCIe-Adapter im Server auflisten	
-show **target_id**	Detaillierte Informationen zum PCIe-Zieladapter anzeigen	**target_id [info|firmware|ports|chips]** Dabei gilt Folgendes: • **info**: Hardwareinformationen zum Adapter anzeigen • **firmware**: Alle Firmwareinformationen zum Adapter anzeigen • **ports**: Alle Informationen zu den Ethernet-Anschlüssen des Adapters anzeigen • **chips**: Alle Informationen zum GPU-Chip des Adapters anzeigen
-h	Befehlssyntax und -optionen anzeigen	

Syntax:
```
adapter [options]
option:
  -list
  -show target_id [info|firmware|ports|chips]
  -h help
```

Beispiele:
```
system> adapter
list
ob-1     Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2     GPU Card 1
slot-1   Raid Controller 1
```

```
slot-2   Adapter 01:02:03
system> adapter
show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2

Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x

Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
```

```
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
```

Befehl „m2raid“

Mit diesem Befehl können Sie M.2-bezogene Bestandsinformationen abrufen und die virtuellen Datenträger verwalten.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 65. Befehl „m2raid“

Die folgende mehrzeilige Tabelle mit zwei Spalten enthält die Optionen mit entsprechenden Beschreibungen.

Option	Beschreibung
-h/?	Hilfeinformationen für diesen Befehl drucken
-version	Informationen zur Controller-Firmware anzeigen
-disks	Informationen zu den Datenträgern anzeigen
-volumes	Informationen zu den virtuellen Datenträgern anzeigen
-create	Einen virtuellen Datenträger erstellen; VD_Name, RAIDLevel und StripeSize können angegeben werden
-delete	Virtuellen Datenträger löschen
-import	Einen fremden virtuellen Datenträger importieren. Nachdem Sie den virtuellen Datenträger importiert haben, wird er automatisch durch einen Systemneustart wiederhergestellt.

Nutzung

```
m2raid [-options] - raid configuration for M.2 adapter with Mirroring Enablem
options:
   -version                    - displays controller firmware version.
   -disks                      - displays information of media disks.
   -volumes                    - displays information of virtual volumes
   -create -VD_Name <nameStr> -RaidLevel <0|1> -StripeSize <32|64>  - create virt
   -delete -VD_ID <0|1>       - delete the virtual volume
   -import -VD_ID <0|1>       - import a foreign virtual volume
```

Beispiel

```
system> m2raid -version
    ThinkSystem M.2 with Mirroring Enablement Kit
 Firmware Version = 2.3.10.1193

system> m2raid -disks
    M.2 Bay0          32GB M.2 SATA SSD     LEN     100%
M.2 Bay1          32GB M.2 SATA SSD     LEN      100%

system> m2raid -volumes
    VD_ID    VD_Name    RaidLevel    StripSize    VD Capacity    Status
     0       M2RAID       1             64k          29 GB           Optimal

system> m2raid -delete -VD_ID 0
VD_ID 0 is deleted

system> m2raid -create -VD_Name M2RAID -RaidLevel 1 -StripeSize 64
New volume is created
```

```
system> m2raid -import -VD_ID 0
VD_ID 0 is imported
```

Support-Befehle

Dieser Abschnitt enthält eine Liste der Support-Befehle in alphabetischer Reihenfolge.

Es gibt nur einen Support-Befehl: „Befehl „dbgshimm““ auf Seite 188.

Befehl „dbgshimm“

Verwenden Sie diesen Befehl, um den Netzwerkzugriff auf die sichere Debug-Shell zu entsperren.

Anmerkung: Dieser Befehl sollte nur von Supportmitarbeitern verwendet werden.

In der folgenden Tabelle sind die Argumente für die Optionen aufgelistet.

Tabelle 66. Befehl „dbgshimm“

Die folgende mehrzeilige Tabelle mit zwei Spalten enthält die Optionen mit entsprechenden Beschreibungen.

Option	Beschreibung
Status	Status anzeigen
Aktivieren	Debugzugriff aktivieren (Standardeinstellung, falls keine Option angegeben)
Deaktivieren	Debugzugriff deaktivieren

Kapitel 11. IPMI-Schnittstelle

In diesem Kapitel wird die IPMI-Schnittstelle beschrieben, die vom XClarity Controller unterstützt wird.

Informationen zu den Standard-IPMI-Befehlen finden Sie im Dokument zur IPMI-Spezifikation (Intelligent Platform Management Interface) (Version 2.0 oder höher). Dieses Dokument enthält Beschreibungen zu den OEM-Parametern, die mit den Standard-IPMI- und OEM-IPMI-Befehlen verwendet werden, die von der XClarity Controller-Firmware unterstützt werden.

XClarity Controller mit IPMI verwalten

Mithilfe der Informationen in diesem Abschnitt können Sie den XClarity Controller über die Intelligent Platform Management Interface (IPMI) verwalten.

Anfangs ist beim XClarity Controller die Benutzer-ID auf den Benutzernamen „USERID“ und das Kennwort „PASSW0RD“ (mit einer Null anstelle des Buchstabens „O“) eingestellt. Dieser Benutzer hat Administratorzugriff.

Wichtig: Ändern Sie für größere Sicherheit diesen Benutzernamen und das zugehörige Kennwort bei der Erstkonfiguration.

In einem Flex System kann ein Benutzer ein Flex System-CMM konfigurieren, um die XClarity Controller-IPMI- Benutzeraccounts zentral zu verwalten. In diesem Fall können Sie möglicherweise nicht mithilfe von XClarity Controller auf das IPMI zugreifen, bis das CMM die IPMI-Benutzer-IDs konfiguriert hat.

Anmerkung: Die vom CMM konfigurierten Benutzer-ID-Anmeldeinformationen können sich von der oben genannten Kombination „USERID/PASSW0RD“ unterscheiden. Wenn keine IPMI-Benutzer-IDs vom CMM konfiguriert wurden, wird der Netzwerkanschluss, der dem IPMI-Protokoll zugeordnet ist, geschlossen.

Der XClarity Controller bietet außerdem die folgenden IPMI-Fernverwaltungsfunktionen für den Server:

IPMI-Befehlszeilenschnittstellen
Über die IPMI-Befehlszeilenschnittstelle erhalten Sie über das Protokoll IPMI 2.0 direkten Zugriff auf die Serververwaltungsfunktionen. Sie können IPMItool verwenden, um Befehle zum Steuern der Stromversorgung am Server, zum Anzeigen von Serverinformationen und zum Identifizieren des Servers auszugeben. Weitere Informationen zu IPMItool finden Sie unter „IPMItool verwenden“ auf Seite 189.

Serial over LAN
Verwenden Sie zum Verwalten von Servern von einem fernen Standort aus IPMItool, um eine SOL-Verbindung (Serial over LAN) herzustellen. Weitere Informationen zu IPMItool finden Sie unter „IPMItool verwenden“ auf Seite 189.

IPMItool verwenden

Mithilfe der Informationen in diesem Abschnitt können Sie auf die Informationen zum IPMItool zugreifen.

IPMItool bietet diverse Tools, die Sie zum Verwalten und Konfigurieren eines IPMI-Systems verwenden können. Sie können IPMItool in der Inneband- oder Außerband-Methode verwenden, um den XClarity Controller zu verwalten und zu konfigurieren.

Gehen Sie für weitere Informationen zu IPMItool oder zum Herunterladen von IPMItool auf https://github.com/ipmitool/ipmitool.

IPMI-Befehle mit OEM-Parametern

LAN-Konfigurationsparameter abrufen/festlegen

Um die vom XCC für einige Netzwerkeinstellungen bereitgestellten Funktionen widerzuspiegeln, werden die Werte für einige der Parameterdaten wie unten dargestellt definiert.

DHCP

Zusätzlich zu den üblichen Methoden zum Abrufen einer IP-Adresse bietet XCC einen Modus, in dem versucht wird, eine IP-Adresse für einen bestimmten Zeitraum von einem DHCP-Server abzurufen. Ist dies nicht erfolgreich, wird ein Failover auf die Verwendung einer statischen IP-Adresse durchgeführt.

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Parameter	#	Parameterdaten
IP-Adress-quelle	4	Daten 1 [7:4] – reserviert [3:0] – Adressquelle 0h = nicht spezifiziert 1h = statische Adresse (manuell konfiguriert) 2h = Adresse, die von XCC mit DHCP abgerufen wird 3h = Adresse, die durch BIOS oder Systemsoftware abgerufen wird 4h = Adresse, die von XCC mit einem anderen Adresszuordnungsprotokoll abgerufen wird XCC verwendet den Wert 4h, um den Adressmodus von DHCP mit Failover auf statisch anzugeben.

Ethernet-Schnittstellenauswahl

Die XCC-Hardware enthält zwei 10/100-Ethernet-MACs mit RMII-Schnittstellen. Die XCC-Hardware enthält außerdem zwei 1-Gbit/s-Ethernet-MACs mit RGMII-Schnittstellen. Einer der MACs ist normalerweise mit dem gemeinsam genutzten Server-NIC verbunden und der andere MAC wird als dedizierter Systemmanagementanschluss verwendet. Es ist jeweils nur ein Ethernet-Anschluss an einem Server aktiv. Es können nicht beide Anschlüsse gleichzeitig aktiviert sein.

Bei einigen Servern steht es Systemdesignern frei, nur eine der beiden Ethernet-Schnittstellen an die Systemplatine anzuschließen. Bei diesen Systemen wird nur die Ethernet-Schnittstelle von XCC unterstützt, die mit der Platine verbunden ist. Eine Anforderung zum Verwenden des nicht verbundenen Anschlüsse gibt den Code „CCh completion“ zurück.

Die Paket-IDs für alle optionalen Netzwerkkarten sind wie folgt nummeriert:

- optionale Karte Nr. 1, Paket-ID = 03h (eth2)
- optionale Karte Nr. 2, Paket-ID = 04h (eth3)

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Parameter	#	Parameterdaten
OEM-Parameter Diese Parameternummer wird von XCC verwendet, um anzugeben, welcher der möglichen Ethernet-Anschlüsse (logische Pakete) verwendet werden soll. Dieser Parameter im Befehl „LAN-Konfigurationsparameter abrufen/festlegen“ verwendet keinen Set Selector und erfordert keinen Block Selector, daher sollten diese Felder auf 00h festgelegt werden. Die Antwortdaten geben 3 Bytes oder optional 4 Bytes zurück, wenn sich die Einheit in einem NCSI-Paket befindet. Byte 1 = Rückgabecode Byte 2 = Revision Byte 3 = 00h für eth0 oder 01h für eth1 etc. Byte 4 = (optional) Kanalnummer, wenn die Einheit ein NCSI-Paket ist	C0h	Daten 1 00h = eth0 01h = eth1 02h = eth2 etc. FFh = deaktiviert alle externen Netzwerkanschlüsse XCC unterstützt ein zweites optionales Daten-Byte, um anzugeben, welcher Kanal in einem Paket verwendet wird. Daten 2 00h = Kanal 0 01h = Kanal 1 etc. Wenn „Daten 2“ nicht in der Anforderung angegeben wird, wird Kanal 0 angenommen.

Das Daten-1-Byte wird verwendet, um das logische Paket anzugeben. Möglicherweise handelt es sich um einen dedizierten Systemmanagement-NIC oder eine NCSI-Schnittstelle in den mit dem Server gemeinsam genutzten NIC.

Das Daten-2-Byte wird verwendet, um den Kanal für das logische Paket anzugeben, wenn es sich bei dem Paket um eine NCSI-Einheit handelt. Wenn „Daten 2“ nicht in der Anforderung angegeben ist und das logische Paket eine NCSI-Einheit ist, wird der Kanal 0 angenommen. Wenn „Daten 2“ in der Anforderung angegeben ist, aber das logische Paket keine NCSI-Einheit ist, wird die Kanalinformation ignoriert.

Beispiele:

Anhang A: Wenn Kanal 2 des gemeinsam genutzten NIC auf der Platine (Paket-ID = 0, eth0) als Verwaltungsanschluss verwendet werden soll, lautet die Eingabe: 0xC0 0x00 0x02

Anhang B: Wenn der erste Kanal der ersten Netzwerk-Mezzanine-Karte verwendet werden soll, lautet die Eingabe: 0xC0 0x02 0x0

Ethernet-over-USB aktivieren/deaktivieren

Der folgende Parameter wird verwendet, um die XCC-Inband-Schnittstelle zu aktivieren oder zu deaktivieren.

Die folgende Tabelle ist eine mehrzeilige Tabelle mit drei Spalten, die die Optionen, Beschreibungen der Optionen und zugeordnete Werte für die Optionen enthalten.

Parameter	#	Parameterdaten
OEM-Parameter (Diese Parameternummer wird von XCC verwendet, um die Ethernet-over-USB-Schnittstelle zu aktivieren oder zu deaktivieren.) Dieser Parameter im Befehl „LAN-Konfigurationsparameter abrufen“ verwendet keinen Set Selector und erfordert keinen Block Selector, daher sollten diese Felder auf 00h festgelegt werden. Die Antwortdaten geben 3 Bytes zurück: Byte 1 = Rückgabecode Byte 2 = Revision Byte 3 = 00h (deaktiviert) oder 01h (aktiviert)	C1h	Daten 1 0x00 = deaktiviert 0x01 = aktiviert

Das Daten-1-Byte wird verwendet, um das logische Paket anzugeben. Möglicherweise handelt es sich um einen dedizierten Systemmanagement-NIC oder eine NCSI-Schnittstelle in den mit dem Server gemeinsam genutzten NIC.

Das Daten-2-Byte wird verwendet, um den Kanal für das logische Paket anzugeben, wenn es sich bei dem Paket um eine NCSI-Einheit handelt. Wenn „Daten 2“ nicht in der Anforderung angegeben ist und das logische Paket eine NCSI-Einheit ist, wird der Kanal 0 angenommen. Wenn „Daten 2“ in der Anforderung angegeben ist, aber das logische Paket keine NCSI-Einheit ist, wird die Kanalinformation ignoriert.

Beispiele:

Anhang A: Wenn Kanal 2 des gemeinsam genutzten NIC auf der Platine (Paket-ID = 0, eth0) als Verwaltungsanschluss verwendet werden soll, lautet die Eingabe: 0xC0 0x00 0x02

Anhang B: Wenn der erste Kanal der ersten Netzwerk-Mezzanine-Karte verwendet werden soll, lautet die Eingabe: 0xC0 0x02 0x0

IPMI-Option zum Abrufen der DUID-LLT

Ein zusätzlicher schreibgeschützter Wert, der über IPMI verfügbar gemacht werden muss, ist der DUID. Gemäß RFC3315 basiert dieses Format von DUID auf der Link-Layer-Adresse plus Zeit.

Parameter	#	Parameterdaten
OEM-Parameter (Diese Parameternummer wird von XCC verwendet, um die Ethernet-over-USB-Schnittstelle zu aktivieren oder zu deaktivieren.) Dieser Parameter im Befehl „LAN-Konfigurationsparameter abrufen“ verwendet keinen Set Selector und erfordert keinen Block Selector, daher sollten diese Felder auf 00h festgelegt werden. Die Antwortdaten geben 3 Bytes zurück: Byte 1 = Rückgabecode Byte 2 = Parameterrevision (wie in IPMI-Spezifikation) Byte 3 = Länge der folgenden Datenbytes (derzeit 16 Bytes) Bytes 4-n = DUID_LLT	C2h	

Ethernet-Konfigurationsparameter

Die folgenden Parameter können zur Konfiguration bestimmter Ethernet-Einstellungen verwendet werden.

Parameter	#	Parameterdaten
OEM-Parameter (Diese Parameternummer wird von XCC verwendet, um die Einstellung für die automatische Verbindungsherstellung für die Ethernet-Schnittstelle zu aktivieren oder zu deaktivieren.) Die Antwortdaten geben 3 Bytes zurück: Byte 1 = Rückgabecode Byte 2 = Revision Byte 3 = 00h (deaktiviert) oder 01h (aktiviert)	C3h	Daten 1 0x00 = deaktiviert 0x01 = aktiviert Hinweis: auf Flex und ThinkSystem D2 Enclosure (ThinkSystem SD530 Compute Node) Systemen kann die Einstellung für die automatische Verbindungsherstellung nicht geändert werden, da sie den Netzwerkkommunikationspfad über das CMM und das SMM unterbrechen kann.
OEM-Parameter (Diese Parameternummer wird von XCC verwendet, um die Übertragungsgeschwindigkeit der Ethernet-Schnittstelle abzurufen oder festzulegen.) Die Antwortdaten geben 3 Bytes zurück: Byte 1 = Rückgabecode Byte 2 = Revision Byte 3 = 00h (10 Mbit/s) oder 01h (100 Mbit/s)	C4h	Daten 1 0x00 = 10 Mbit/s 0x01 = 100 Mbit/s
OEM-Parameter (Diese Parameternummer wird von XCC verwendet, um die Duplex-Einstellung der Ethernet-Schnittstelle abzurufen oder festzulegen.) Die Antwortdaten geben 3 Bytes zurück: Byte 1 = Rückgabecode Byte 2 = Revision Byte 3 = 00h (Halbduplex) oder 01h (Vollduplex)	C5h	Daten 1 0x00 = Halbduplex 0x01 = Vollduplex

Parameter	#	Parameterdaten
OEM-Parameter (Diese Parameternummer wird von XCC verwendet, um die größte zu übertragende Einheit (MTU) der Ethernet-Schnittstelle abzurufen oder festzulegen.) Die Antwortdaten geben 3 Bytes zurück: Byte 1 = Rückgabecode Byte 2 = Revision Byte 3-4 = MTU-Größe	C6h	Daten 1 MTU-Größe
OEM-Parameter (Diese Parameternummer wird von XCC verwendet, um die lokal verwaltete MAC-Adresse abzurufen oder festzulegen.) Die Antwortdaten geben 3 Bytes zurück: Byte 1 = Rückgabecode Byte 2 = Revision Bytes 3-8 = MAC-Adresse	C7h	Daten 1-6 MAC-Adresse

IPMI-Option zum Abrufen der Link-Local-Adresse

Hierbei handelt es sich um einen schreibgeschützten Parameter zum Abrufen der IPv6-Link-Local-Adresse.

Parameter	#	Parameterdaten
OEM-Parameter Dieser Parameter wird verwendet, um die Link-Local-Adresse von XCC zu erhalten: Die Antwortdaten geben Folgendes zurück: Byte 1 = Rückgabecode Byte 2 = Parameterrevision (wie in IPMI-Spezifikation) Byte 3 = Präfixlänge der IPv6-Adresse Bytes 4-19 = Local-Link-Adresse im Binärformat	C8h	

IPMI-Option zum Aktivieren/Deaktivieren von IPv6

Hierbei handelt es sich um einen Schreib/Lese-Parameter zum Aktivieren/Deaktivieren von IPv6 im XCC.

Parameter	#	Parameterdaten
OEM-Parameter Dieser Parameter wird verwendet, um IPv6 im XCC zu aktivieren oder zu deaktivieren. Die Antwortdaten geben Folgendes zurück: Byte 1 = Rückgabecode Byte 2 = Parameterrevision (wie in IPMI-Spezifikation) Byte 3 = 00h (deaktiviert) oder 01h (aktiviert)	C9h	Daten 1 0x00 = deaktiviert 0x01 = aktiviert

Pass-Through mit Ethernet-over-USB zu externem Netzwerk

Der folgende stehende Parameter wird verwendet, um Ethernet-over-USB für den externen Ethernet-Pass-Through zu konfigurieren.

Parameter	#	Parameterdaten
OEM-Parameter Dieser Parameter im Befehl „LAN-Konfigurationsparameter abrufen/festlegen“ verwendet keinen Set Selector und erfordert keinen Block Selector, daher sollten diese Felder auf 00h festgelegt werden. Die Abruf-Antwortdaten geben Folgendes zurück: Byte 1 = Rückgabecode Byte 2 = Revision Byte 3 = reserviert (00h) Bytes 4:5 = Ethernet-over-USB-Anschlussnummer (zuerst LS-Byte) Bytes 6:7 = Externe Ethernet-Anschlussnummer (zuerst LS-Byte) Die Anzahl der zu befolgenden Bytes kann je nach Adressierungsmodus variieren (1, 4 oder 16 Byte): • Byte 8 = vordefinierte Modi: 00h = Pass-Through ist deaktiviert 01h = IP-Adresse von CMM wird verwendet Bytes 8:11 = IPv4-IP-Adresse für externes Netzwerk im Binärformat Bytes 8:23 = IPv6-IP-Adresse für externes Netzwerk im Binärformat Rückgabecodes: 00h – Erfolg 80h – Parameter wird nicht unterstützt C1h – Befehl wird nicht unterstützt C7h – Länge der Anforderungsdaten ist ungültig	CAh	LAN-Konfigurationsparameter festlegen: Daten 1 00h = reserviert Daten 2:3 Ethernet-over-USB-Anschlussnummer, zuerst LS-Byte Daten 4:5 Externe Ethernet-Anschlussnummer, zuerst LS-Byte Die Anzahl der zu befolgenden Bytes kann je nach Adressierungsmodus variieren (1, 4 oder 16 Byte): Daten 6 00h = Pass-Through ist deaktiviert 01h = IP-Adresse von CMM wird verwendet Daten 6:9 IPv4-IP-Adresse für externes Netzwerk im Binärformat Daten 6:21 IPv6-IP-Adresse für externes Netzwerk im Binärformat
OEM-Parameter Dieser Parameter wird verwendet, um die IP-Adresse von LAN-over-USB und die Netzmaske von XCC festzulegen und abzurufen: Die Antwortdaten geben Folgendes zurück: Byte 1 = Rückgabecode	CBh	Daten 1:4 IP-Adresse von XCC-Seite, LAN-over-USB-Schnittstelle Daten 5:8 Netzmaske von XCC-Seite, LAN-over-USB-Schnittstelle

Parameter	#	Parameterdaten
Byte 2 = Parameterrevision (wie in IPMI-Spezifikation) Bytes 3:10 = IP-Adresse und Netzmaskenwert (zuerst MS-Byte)		
OEM-Parameter Dieser Parameter wird verwendet, um die IP-Adresse von LAN-over-USB des Host-BS festzulegen und abzurufen: Die Antwortdaten geben Folgendes zurück: Byte 1 = Rückgabecode Byte 2 = Parameterrevision (wie in IPMI-Spezifikation) Byte 3:6 = IP-Adresse (zuerst MS-Byte)	CCh	Daten 1:4 IP-Adresse von Host-Seite, LAN-over-USB-Schnittstelle

Logischen Paketbestand abfragen

Der folgende Parameter wird für die Abfrage des NCSI-Paketbestands verwendet.

Parameter	#	Parameterdaten
OEM-Parameter Dieser Parameter im Befehl „LAN-Konfigurationsparameter abrufen/festlegen“ verwendet keinen Set Selector und erfordert keinen Block Selector, daher sollten diese Felder auf 00h festgelegt werden. Vorgang „Paketbestand abfragen“ Der Vorgang „Paketbestand abfragen“ wird ausgeführt, indem die Anforderung mit zwei 0x00-Datenbytes neben der D3h-Parameternummer ausgegeben wird. Paketbestand abfragen: --> 0x0C 0x02 0x00 0xD3 0x00 0x00 Die XCC-Antwort enthält ein Byte mit Informationen zu jedem vorhandenen Paket: Bits 7:4 = Anzahl der NCSI-Kanäle im Paket Bits 3:0 = logische Paketnummer Antwort --> 0x00 0x00 0x40 0x01 0x32 Gibt an, dass 3 logische Pakete vorhanden sind: Paket 0 hat 4 NCSI-Kanäle Paket 1 ist kein NCSI-NIC und unterstützt daher keine NCSI-Kanäle Paket 2 hat 3 NCSI-Kanäle	D3h	LAN-Konfigurationsparameter abrufen/festlegen:

Logische Paketdaten abrufen/festlegen

Der folgende Parameter wird verwendet, um die jedem Paket zugeordnete Priorität abzurufen und festzulegen.

Parameter	#	Parameterdaten
OEM-Parameter Dieser Parameter im Befehl „LAN-Konfigurationsparameter abrufen/festlegen“ verwendet keinen Set Selector und erfordert keinen Block Selector, daher sollten diese Felder auf 00h festgelegt werden. Der Befehl unterstützt 2 Vorgänge: • Paketpriorität abrufen • Paketpriorität festlegen Vorgang „Paketpriorität abrufen“ Der Vorgang „Paketpriorität abrufen“ wird ausgeführt, indem die Anforderung mit zwei 0x00-Datenbytes neben der D4h-Parameternummer ausgegeben wird. Paketpriorität abrufen: --> 0x0C 0x02 0x01 0xD4 0x00 0x00 Antwort --> 0x00 0x00 0x00 0x12 0x23 Logisches Paket 0 = Priorität 0 Logisches Paket 2 = Priorität 1 Logisches Paket 3 = Priorität 2 Vorgang „Paketpriorität festlegen“ Der Vorgang „Paketpriorität festlegen“ wird ausgeführt, indem die Anforderung mit mindestens einem Parameter zusätzlich zur D4h-Parameternummer ausgegeben wird. Paketpriorität festlegen: --> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23 Logisches Paket 0 festlegen = Priorität 0 Logisches Paket 2 festlegen = Priorität 1	D4	LAN-Konfigurationsparameter abrufen/festlegen: Bit [7-4] = Priorität des logischen Pakets (1 = höchste, 15 = niedrigste) Bit [3-0] = logische Paketnummer

Parameter	#	Parameterdaten
Logisches Paket 3 festlegen = Priorität 2 Antwort: Nur Rückgabecode, keine zusätzlichen Daten		

XCC-Netzwerk-Synchronisierungsstatus abrufen/festlegen

Parameter	#	Parameterdaten
OEM-Parameter Das Byte wird zur Konfiguration für die Synchronisation der Netzwerkeinstellung zwischen dediziertem und NIC-Modus für gemeinsame Nutzung verwendet. Dieser Parameter im Befehl „LAN-Konfigurationsparameter abrufen“ verwendet keinen Set Selector und erfordert keinen Block Selector, daher sollten diese Felder auf 00h festgelegt werden. Die Antwortdaten geben 3 Bytes zurück: Byte 1 = Rückgabecode Byte 2 = Revision Byte 3 = 00h (aktiviert) oder 01h (deaktiviert)	D5h	Daten 1 0x00 = Synchronisation 0x01 = Unabhängigkeit

Das Byte wird zur Konfiguration für die Synchronisation der Netzwerkeinstellung zwischen dediziertem und NIC-Modus für gemeinsame Nutzung verwendet. Der Standardwert ist hier 0h, was bedeutet, dass XCC automatisch die Netzwerkeinstellung zwischen den Modusänderungen aktualisiert und den gemeinsam genutzten NIC (integriert) als Hauptreferenz verwendet. Wenn 1h festgelegt ist, ist jede Netzwerkeinstellung unabhängig, was bedeutet, dass unterschiedliche Netzwerkeinstellungen zwischen Modi konfiguriert werden können, z. B. VLAN-Aktivierung bei „Dediziert“ und VLAN-Deaktivierung im gemeinsam genutzten NIC-Modus.

XCC-Netzwerkmodus abrufen/festlegen

Parameter	#	Parameterdaten
OEM-Parameter Dieser Parameter wird verwendet, um den Netzwerkmodus des XCC-Verwaltungs-NIC abzurufen/ festzulegen. Die Antwortdaten geben 4 Bytes zurück: Byte 1 = Rückgabecode Byte 2 = Revision Byte 3 = angewendeter/ angegebener Netzmodus Byte 4 = Paket-ID des angewendeten Netzmodus Byte 5 = Kanal-ID des angewendeten Netzmodus	D6h	LAN-Konfigurationsparameter festlegen: Daten 1 Festzulegender Netzmodus LAN-Konfigurationsparameter abrufen: Daten 1 Abzurufender Netzmodus. Dies sind optionale Daten, standardmäßig wird der aktuelle Netzmodus abgefragt

OEM-IPMI-Befehle

Der XCC unterstützt die folgenden IPMI-OEM-Befehle. Jeder Befehl erfordert eine andere Berechtigungsstufe (siehe unten).

Code	Netfn 0x2E-Befehle	Berechtigung
0xCC	XCC auf Standard zurücksetzen	PRIV_USR

Code	Netfn 0x3A-Befehle	Berechtigung
0x00	Firmwareversion abfragen	PRIV_USR
0x0D	Platineninformationen	PRIV_USR
0x1E	Verzögerungsoptionen für Wiederherstellung der Gehäusestromversorgung	PRIV_USR
0x38	NMI und Zurücksetzen	PRIV_USR
0x49	Datenerfassung einleiten	PRIV_USR
0x4A	Datei weiterleiten	PRIV_USR
0x4D	Status der Datenerfassung	PRIV_USR
0x50	Build-Informationen abrufen	PRIV_USR
0x55	Hostnamen abrufen/ festlegen	PRIV_USR

Code	Netfn 0x3A-Befehle	Berechtigung
0x6B	FPGA-Firmware-Revisionsstufe abfragen	PRIV_USR
0x6C	Platinenhardware-Revisionsstufe abfragen	PRIV_USR
0x6D	PSoC-Firmware-Revisionsstufe abfragen	PRIV_USR
0x98	Steuerung BF-USB-Anschluss	PRIV_USR
0xC7	Nativer NM-IPMI-Switch	PRIV_ADM

Befehl „XCC auf Standard zurücksetzen“

Mit diesem Befehl wird die XCC-Konfigurationseinstellung auf die Standardwerte zurückgesetzt.

Nettofunktion = 0x2E			
Code	**Befehl**	**Anforderungsdaten, Antwortdaten**	**Beschreibung**
0xCC	XCC auf Standard zurücksetzen	**Anforderung:** Byte 1 – 0x5E Byte 2 – 0x2B Byte 3 – 0x00 Byte 4 – 0x0A Byte 5 – 0x01 Byte 6 – 0xFF Byte 7 – 0x00 Byte 8 – 0x00 Byte 9 – 0x00 **Antwort:** Byte 1 – Rückgabecode Byte 2 – 0x5E Byte 3 – 0x2B Byte 4 – 0x00 Byte 5 – 0x0A Byte 6 – 0x01 Byte 7 – Antwortdaten 0 = Erfolg ungleich Null = Fehler	Mit diesem Befehl werden die XCC-Konfigurationseinstellungen auf die Standardwerte zurückgesetzt.

Befehle „Platinen-/Firmwareinformationen“

In diesem Abschnitt werden die Befehle für die Abfrage der Platinen- und Firmwareinformationen aufgeführt.

Nettofunktion = 0x3A			
Code	**Befehl**	**Anforderungsdaten, Antwortdaten**	**Beschreibung**
0x00	Firmwareversion abfragen	**Anforderung**: Keine Daten bei Anforderung **Antwort**: Byte 1 – Rückgabecode Byte 2 – Hauptversion Byte 3 – Unterversion	Dieser Befehl gibt die Haupt- und Unterversionsnummern der Firmware zurück. Wenn der Befehl mit dem optionalen 1 Byte an Anforderungsdaten erfolgt, gibt die XCC-Antwort auch das dritte Feld (Revision) der Version zurück. (Haupt.Unter.Revision)
0x0D	Platineninformationen abfragen	**Anforderung**: Nicht zutreffend **Antwort**: Byte 1 – System-ID Byte 2 – Platinenrevision	Dieser Befehl gibt die Platinen-ID und -Revision zurück.
0x50	Build-Informationen abfragen	**Anforderung**: Nicht zutreffend **Antwort**: Byte 1 – Rückgabecode Bytes 2:10 – ASCIIZ-Build-Name Bytes 11:23 – ASCIIZ-Build-Datum Bytes 24:31 – ASCII-Build-Zeit	Dieser Befehl gibt Build-Name, -Datum und -Zeit zurück. Die Zeichenfolge für Build-Name und -Datum weisen eine Nullterminierung auf. Das Format des Build-Datums ist JJJJ-MM-TT. Bsp.: „ZUBT99A“ “2005-03-07” “23:59:59”

Nettofunktion = 0x3A			
Code	**Befehl**	**Anforderungsdaten, Antwortdaten**	**Beschreibung**
0x6B	FPGA-Firmware-Revisionsstufe abfragen	**Anforderung**: Byte 1 – FPGA-Einheitentyp* FPGA-Einheitentyp 0 = Lokal (aktive Stufe) 1 = CPU-Karte 1 (aktive Stufe) 2 = CPU-Karte 2 (aktive Stufe) 3 = CPU-Karte 3 (aktive Stufe) 4 = CPU-Karte 4 (aktive Stufe) 5 = Lokaler primärer ROM 6 = Lokaler Wiederherstellungs-ROM **Antwort**: Byte 1 – Rückgabecode Byte 2 – Hauptrevisionsstufe Byte 3 – Unterrevisionsstufe Byte 4 – Sub-Unterrevisionsstufe (Test-Byte auf XCC-Plattformen)	Dieser Befehl gibt die Revisionsstufe der FPGA-Firmware zurück. Wenn Byte 1 ausgelassen wird, wird „Lokal (aktive Stufe)“ ausgewählt.
0x6C	Platinen-hardware-Revisionsstufe abfragen	**Anforderung**: Keine Daten **Antwort**: Byte 1 – Rückgabecode Byte 2 – Revisionsstufe	Dieser Befehl gibt die Revisionsstufe der Platinenhardware zurück, auf der sich das FPGA befindet.
0x6D	PSoC-Firmware-Revisionsstufe abfragen	**Anforderung**: Keine Angabe **Antwort**: Byte 1 – Rückgabecode Byte 2 – bin# Byte 3 – APID Byte 4 – Rev	Dieser Befehl gibt die Revisionsstufe aller erkannten PSoC-Einheiten zurück. Hinweis: bin# stellt eine physische Position dar. Weitere Informationen finden Sie in der Systemspezifikation.

Nettofunktion = 0x3A			
Code	**Befehl**	**Anforderungsdaten, Antwortdaten**	**Beschreibung**
		Byte 5-6 – FRU-ID Bytes 6:n – Wiederholung von Bytes 2-6 für jeden erkannten PSoC	

Systemsteuerbefehle

Die IPMI-Spezifikation bietet eine grundlegende Stromversorgungs- und Wiederherstellungssteuerung. Lenovo fügt zusätzliche Steuerfunktionen hinzu.

<table>
<tr><th colspan="4">Nettofunktion = 0x3A</th></tr>
<tr><th>Code</th><th>Befehl</th><th>Anforderungsdaten, Antwortdaten</th><th>Beschreibung</th></tr>
<tr><td>0x1E</td><td>Verzögerungsoptionen für Wiederherstellung der Gehäusestromversorgung</td><td>Anforderung:<table><tr><td>Byte 1</td><td>Anforderungstyp:

0x00 = Verzögerungsoptionen festlegen

0x01 = Verzögerungsoptionen abfragen</td></tr><tr><td>Byte 2</td><td>(falls Byte 1 = 0x00)

0x00 = Deaktiviert (Standard)

0x01 = Zufällig

0x02 - 0xFF reserviert</td></tr></table>Antwort:

Byte 1 – Rückgabecode

Byte 2 – Verzögerungsoptionen (nur für Abfrageanforderung)</td><td>Diese Einstellung wird verwendet, wenn die Richtlinie zum Wiederherstellen der Gehäusestromversorgung so konfiguriert ist, dass die Stromversorgung nach der (erneuten) Aktivierung der Wechselstromversorgung immer eingeschaltet oder wieder eingeschaltet wird (falls zuvor eingeschaltet). Es gibt 2 Optionen: „Deaktiviert“ (die Standardeinstellung, keine Verzögerung beim Einschalten) und „Zufällig“. Die zufällige Verzögerungseinstellung bietet eine zufällige Verzögerung zwischen 1 und 15 Sekunden ab dem Moment, in dem der Wechselstrom (wieder) eingeschaltet wird und wenn der Server automatisch eingeschaltet wird.

Der Befehl wird von XCC nur auf Rack-Servern unterstützt.</td></tr>
<tr><td>0x38</td><td>NMI und Zurücksetzen</td><td>Anforderung:

Byte 1 – Anzahl der Sekunden
0 = nur NMI

Byte 2 – Rücksetzungstyp
0 = Warmstart
1 = Aus- und Wiedereinschaltung

Antwort:

Byte 1 – Rückgabecode</td><td>Dieser Befehl wird verwendet, um einen System-NMI durchzuführen. Optional kann das System warmgestartet (neu gestartet) oder nach dem NMI aus- und wieder eingeschaltet werden.

Wenn das Feld „Anzahl der Sekunden“ nicht 0 ist, wird das System nach der angegebenen Anzahl von Sekunden warmgestartet oder aus- und wieder eingeschaltet.

Byte 2 der Anforderung ist optional. Wenn Byte 2 nicht angegeben wird oder den Wert 0x00 hat, wird ein Warmstart ausgeführt. Wenn Byte 2 den Wert 0x01 hat, wird das System aus- und wieder eingeschaltet.</td></tr>
</table>

Verschiedene Befehle

In diesem Abschnitt befinden sich Befehle, die nicht in andere Abschnitte passen.

<table>
<tr><th colspan="4">Nettofunktion = 0x3A</th></tr>
<tr><th>Code</th><th>Befehl</th><th>Anforderungsdaten, Antwortdaten</th><th>Beschreibung</th></tr>
<tr><td>0x55</td><td>Hostnamen abrufen/ festlegen</td><td>Anforderungslänge = 0:

Leere Anforderungsdaten

Antwort:

<table><tr><td>Byte 1</td><td>Rückgabecode</td></tr><tr><td>Bytes 2-65</td><td>Aktueller Hostname

ASCIIZ, nullterminierte Zeichenfolge</td></tr></table>
Anforderungslänge 1-64:

<table><tr><td>Bytes 1-64</td><td>DHCP-Hostname

ASCIIZ, terminiert mit 00h</td></tr></table></td><td>Verwenden Sie diesen Befehl, um den Hostnamen abzurufen/ festzulegen.

Bei der Einstellung des Hostnamens muss der gewünschte Wert mit 00h terminiert werden. Der Hostname ist auf 63 Zeichen plus die Null beschränkt.</td></tr>
<tr><td>0x98</td><td>Steuerung BF-USB-Anschluss</td><td>Anforderung:

Byte 1

<table><tr><td>01h:</td><td>Aktuellen Eigentümer des USB-Anschlusses am Bedienfeld abrufen</td></tr></table>
Antwort:

Byte 1 – Rückgabecode

Byte 2

<table><tr><td>00h:</td><td>Eigentum von Host</td></tr><tr><td>01h:</td><td>Eigentum von BMC</td></tr></table>
Anforderung:

Byte 1

<table><tr><td>02h:</td><td>Konfiguration des USB-Anschlusses</td></tr></table></td><td>Dieser Befehl wird für die Abfrage von Status/Konfiguration des BF-USB-Anschlusses, Konfiguration von Modus/Zeitlimit des BF-USB-Anschlusses und Eigentümerwechsel des USB-Anschlusses zwischen Host und BMC verwendet.

Bei Konfiguration kann der BF-USB 3 Modi haben: dediziert für Host, nur Eigentum von BMC oder Modus für gemeinsame Nutzung, mit dem ein Eigentümerwechsel zwischen Host und BMC durchgeführt werden kann.

Wenn der Modus für gemeinsame Nutzung aktiviert ist, ist der USB-Anschluss bei ausgeschaltetem Server mit dem BMC verbunden und bei eingeschaltetem Server mit dem Server verbunden.

Wenn der Modus für gemeinsame Nutzung aktiviert und die Serverstromversorgung eingeschaltet ist, gibt der BMC den USB-Anschluss zurück zum Server, nachdem das in der</td></tr>
</table>

<table>
<tr><th colspan="4">Nettofunktion = 0x3A</th></tr>
<tr><th>Code</th><th>Befehl</th><th>Anforderungsdaten, Antwortdaten</th><th>Beschreibung</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>am Bedienfeld abrufen</td></tr>
</table>
Antwort:

Byte 1 – Rückgabecode

Byte 2

<table>
<tr><td>00h:</td><td>Dediziert für Host</td></tr>
<tr><td>01h:</td><td>Dediziert für BMC</td></tr>
<tr><td>02h:</td><td>Modus für gemeinsame Nutzung</td></tr>
</table>
Byte 3:4 – Inaktivitätszeitlimit in Minuten (zuerst MS-Byte)

Byte 5 – ID-Taste aktivieren

<table>
<tr><td>00h:</td><td>Deaktiviert</td></tr>
<tr><td>01h:</td><td>Aktiviert</td></tr>
</table>
Byte 6 – Hysterese (optional) in Sekunden

Anforderung:

Byte 1

03h: Konfiguration des USB-Anschlusses am Bedienfeld festlegen

Byte 2

<table>
<tr><td>00h:</td><td>Dediziert für Host</td></tr>
<tr><td>01h:</td><td>Dediziert für BMC</td></tr>
<tr><td>02h:</td><td>Modus für gemeinsame Nutzung</td></tr>
</table>
Byte 3:4 – Inaktivitätszeitlimit in Minuten (zuerst MS-Byte)

Byte 5 – ID-Taste aktivieren</td><td>Konfiguration festgelegte Inaktivitätszeitlimit abgelaufen ist.

Wenn der Server über eine ID-Taste verfügt, können Benutzer die ID-Taste aktivieren/deaktivieren, um den Eigentümer des BF-USB-Anschlusses zu wechseln, indem Sie die ID-Taste länger als 3 Sekunden gedrückt halten.

Bei automatischer Umschaltung des Anschlusses bei einer Aus- und Wiedereinschaltung wird die Hysterese in Sekunden festgelegt. Dies ist ein optionaler Parameter.

SD530 Server

Auf der SD530 Plattform ist der Anschluss optional und, falls vorhanden, direkt und ausschließlich mit dem XCC verbunden. Wechsel des Anschlusses zum Host in nicht verfügbar.

Wenn der Befehl mit Byte 1 = 1 ausgegeben wird, antwortet der XCC immer, dass der Anschluss das Eigentum des BMC ist.
Wenn der Befehl mit Byte 1 = 2 ausgegeben wird, antwortet der XCC immer, dass der Anschluss dediziert für den BMC ist.
Wenn der Befehl mit Byte 1 = 3 oder Byte 1 = 4 ausgegeben wird, antwortet der XCC mit dem Rückgabecode D6h.

Andere Server

Auf allen Plattformen außer SD530 kann die XCC-Verwendung des USB-Anschlusses am Bedienfeld deaktiviert werden, indem Sie auf den Modus „Nur Host“ umschalten.

Wenn der Befehl mit Byte 1 = 5 oder Byte 1 = 6 ausgegeben wird, antwortet der XCC mit dem Rückgabecode D6h.</td></tr>
</table>

<table>
<tr><th colspan="4">Nettofunktion = 0x3A</th></tr>
<tr><th>Code</th><th>Befehl</th><th>Anforderungsdaten, Antwortdaten</th><th>Beschreibung</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>00h:</td><td>Deaktiviert</td></tr>
<tr><td>01h:</td><td>Aktiviert</td></tr>
</table>
Byte 6 – Hysterese (optional) in Sekunden

Antwort:

Byte 1 – Rückgabecode Byte 2
<table>
<tr><td>00h:</td><td>Zu Host wechseln</td></tr>
<tr><td>01h:</td><td>Switch zu BMC</td></tr>
</table>
Antwort:

Byte 1 – Rückgabecode

Byte 1
<table>
<tr><td>05h:</td><td>USB-Anschluss am Bedienfeld aktivieren/ deaktivieren</td></tr>
</table>
Byte 2
<table>
<tr><td>00h:</td><td>Deaktivieren</td></tr>
<tr><td>01h:</td><td>Aktivieren</td></tr>
</table>
Antwort:

Byte 1 – Rückgabecode

Anforderung:

Byte 1
<table>
<tr><td>06h:</td><td>Aktiviert/ Deaktiviert-Status des USB-Anschlusses am Bedienfeld abrufen</td></tr>
</table>
Antwort:
</td><td></td></tr>
</table>

<table>
<tr><th colspan="4">Nettofunktion = 0x3A</th></tr>
<tr><th>Code</th><th>Befehl</th><th>Anforderungsdaten,
Antwortdaten</th><th>Beschreibung</th></tr>
<tr><td></td><td></td><td>Byte 1 – Rückgabecode

Byte 2</td><td></td></tr>
<tr><td>0xC7</td><td>Nativer NM-IPMI-Switch</td><td>Anforderungslänge = 0:

Leere Anforderungsdaten

Antwort:

<table><tr><td>Byte 1</td><td>Rückgabec-ode</td></tr><tr><td>Byte 2</td><td>Aktueller Aktiviert/ Deaktiviert-Status</td></tr></table>
Anforderungslänge = 1:

<table><tr><td>Byte 1</td><td>Aktivieren/ Deaktivieren-Attribut für native NM-IPMI-Schnittstelle

00h – Deaktivieren

01h – Aktivieren</td></tr></table>
Antwort:

<table><tr><td>Byte 1</td><td>Rückgabec-ode</td></tr></table></td><td>Dieser Befehl wird verwendet, um die Überbrückungsfunktion von XCC für native Intel IPMI-Befehle zu aktivieren oder zu deaktivieren.</td></tr>
</table>

Kapitel 12. Edge-Server

In diesem Abschnitt werden bestimmte Funktionen für Edge-Server beschrieben.

Anmerkungen:

1. Das System fordert Sie bei der ersten Anmeldung dazu auf, das XCC-Kennwort zu ändern.
2. IPMI-über-LAN ist standardmäßig deaktiviert.
3. IPMI-über-KCS ist standardmäßig deaktiviert.

Systemsperrmodus

Wenn der **Systemsperrmodus** den Status „Aktiv“ hat, bedeutet dies, dass das System im Sperrmodus ist. Sie müssen das System aktivieren und entsperren, da das Hostsystem andernfalls nicht booten kann.

Anmerkung: Der Systemsperrmodus ist nur für SE350 mit Sicherheitspaket verfügbar, aber nicht standardmäßig bei SE350 enthalten. Die Version kann auf der Registerkarte **Start** unter **Systeminformationen und Einstellungen** überprüft werden.

Klicken Sie unter **BMC-Konfiguration** auf **Sicherheit** und blättern Sie zu **Systemsperrmodus**.

Systemsperrmodus

Gehen Sie wie folgt vor, um das System zu aktivieren und den **Systemsperrmodus** zu beenden:

1. Klicken Sie auf die Schaltfläche **Inaktiv**. Ein Fenster **Key Vault-Aktivierung** wird geöffnet und zeigt den **Challenge-Text** an.
2. Wenden Sie sich an Ihren IT-Administrator und teilen Sie ihm den **Challenge-Text** mit.
3. Sie erhalten die **Challenge-Antwort** von Ihrem IT-Administrator. Geben Sie sie im Fenster **Key Vault-Aktivierung** ein.
4. Klicken Sie auf die Schaltfläche **OK** und dann auf **Übernehmen**.
5. Wenn alle Einstellungen ordnungsgemäß funktionieren, wird der Status des **Systemsperrmodus** zu **Inaktiv** geändert.

Anmerkung: Wenn der Systemsperrmodus den Status „Aktiv“ hat, wird der Zugriff auf Systemgeheimnisse, z. B. SED-Schlüssel, **verweigert**.

Gehen Sie wie folgt vor, um das System zum Aktivieren des Systemsperrmodus zu zwingen:

1. Klicken Sie auf die Schaltfläche **Aktiv**.
2. Klicken Sie auf die Schaltfläche **OK** und dann auf **Übernehmen**.

Bewegungserkennung

Sie können diese Funktion aktivieren, um physische Bewegungen des Servers zu erkennen und Ihren Server auf diese Weise zu schützen.
Wenn die Bewegungserkennung aktiviert ist, können Sie je nach Vorliebe und Konfiguration die folgenden Optionen festlegen:

- **Empfindlichkeitsstufe**: Wählen Sie abhängig von Ihren Vorlieben die Empfindlichkeitsstufe **Niedrig**, **Mittel** oder **Hoch** aus.
- **Ausrichtung**: Wählen Sie Ihre Konfiguration aus den Optionen **Stand-Desktop**, **Wandhalterung (horizontal)**, **Wandhalterung (vertikal)**, **Bücherregal** oder **Deckenhalterung** aus.

Anmerkung: Die Bewegungserkennung wird automatisch deaktiviert, wenn das System in den Sperrmodus wechselt.

Erkennung von unbefugtem Gehäusezugriff
Sie können diese Funktion aktivieren, um physische Bewegungen an der oberen Abdeckung zu erkennen und Ihren Server auf diese Weise zu schützen.

Zusätzliche Konfigurationen
Wenn das wireless-fähige LOM-Paket installiert ist, können Sie aus drei Einstellungen für ein erkanntes Manipulationsereignis wählen.
Unter einigen ungewöhnlichen Umständen kann der **Challenge-Text** möglicherweise nicht vom ThinkShield Key Vault Portal verifiziert werden. In diesen Fällen muss möglicherweise der interne Zähler der Einheit zurückgesetzt werden, bevor die Einheit auf Anforderung Ihres IT-Administrators aktiviert werden kann.

Verwaltung des SED-Authentifizierungsschlüssels

Für das mit SED (selbstverschlüsselndes Laufwerk) installierte System kontrolliert diese Funktion das BMC bei der Implementierung des SED-Schlüssels. Sie können den SED-Schlüssel verwenden, um Boot- und Datenlaufwerke zu verschlüsseln und das System ohne manuellen Eingriff zu booten.

Anmerkung: Dieser Vorgang ist nicht zulässig, wenn das System nicht aktiviert ist (Systemsperrmodus ist bestätigt) oder der aktuelle Benutzer nicht über die Berechtigung zur Verwaltung des SED-Schlüssels verfügt.

Anmerkung: Der Systemsperrmodus ist nur für SE350 mit Sicherheitspaket verfügbar, aber nicht standardmäßig bei SE350 enthalten. Die Version kann auf der Registerkarte **Start** unter **Systeminformationen und Einstellungen** überprüft werden.

Anmerkung: Der SE350 unterstützt auch eine Funktion zur automatischen Sicherung, solange entweder der ThinkSystem M.2-Einrichtungssatz oder der ThinkSystem M.2 Spiegelungs-Einrichtungssatz fehlerfrei ist. Wenn Hardware beschädigt ist, aber sowohl SED als auch der M.2-Satz fehlerfrei sind, können sie in einem anderen SE350 installiert werden und der SED AK kann anschließend wiederhergestellt werden. Damit Sie jedoch auf einen vollständigen Hardwareabsturz vorbereitet sind, empfiehlt Lenovo, eine Sicherung des SED AK zu erstellen.

Klicken Sie unter **BMC-Konfiguration** auf **Sicherheit** und blättern Sie zu **Verwaltung des SED-Authentifizierungsschlüssels**.

SED AK ändern
SED AK aus Passphrase generieren: Legen Sie das Kennwort fest und geben Sie es zur Bestätigung erneut ein. Klicken Sie auf **Erneut generieren**, um den neuen SED AK zu erhalten.
Zufälligen SED AK generieren: Klicken Sie auf **Erneut generieren**, um einen zufällig generierten SED AK zu erhalten.
SED AK sichern: Legen Sie das Kennwort fest und geben Sie es zur Bestätigung erneut ein. Klicken Sie auf **Sicherung starten**, um den SED AK zu sichern. Laden Sie dann die SED AK-Datei herunter und speichern Sie sie an einem sicheren Ort für die zukünftige Verwendung.

Anmerkung: Wenn Sie die SED AK-Sicherungsdatei zum Wiederherstellen einer Konfiguration verwenden, fragt das System nach dem Kennwort, das Sie hier festgelegt haben.

SED AK wiederherstellen: Sie können diesen Vorgang nur ausführen, während das SED nicht ordnungsgemäß funktioniert. Es gibt zwei Möglichkeiten für die Wiederherstellung des SED AK:

- **SED AK mit Passphrase wiederherstellen**: Verwenden Sie das Kennwort, das im Modus **SED AK aus Passphrase generieren** festgelegt wurde, um den SED AK wiederherzustellen.

- **SED AK aus Sicherungsdatei wiederherstellen**: Laden Sie die im Modus **SED AK sichern** generierte Sicherungsdatei hoch und geben Sie das Kennwort für die Sicherungsdatei ein, um den SED AK wiederherzustellen.

Edge-Netzwerkbetrieb

Diese Funktionsseite wird nur unterstützt, wenn das wireless-fähige LOM-Paket installiert ist.

Weitere Informationen zu den vordefinierten Netzwerktopologie-Tabellen finden Sie unter https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html.

Wi-Fi-Konnektivität
Klicken Sie auf **Aktiviert**, um die Einstellungen gemäß ihrer Wi-Fi-Konfiguration zu konfigurieren.

LTE-Konnektivität
Auf diese Weise können Sie die LTE-Konnektivität für die Edge-Netzwerkplatine steuern.

Adresse der Edge-Netzwerkplatine

IPv4 oder IPv6-Status	**DHCP-Server**-Status	**Methode**
Deaktiviert	**Deaktiviert**	**IP-Adresse von DHCP abrufen**
Aktiviert	**Aktiviert**	**Statische IP-Adresse verwenden**
Aktiviert	**Deaktiviert**	**IP-Adresse von DHCP abrufen** oder **Statische IP-Adresse verwenden**, abhängig von ihrer Verwendung

BMC-Netzwerkbrücke
Sie können über **Downlink-Ports**, **Wi-Fi-Ports** oder **Uplink-Ports** auf den BMC zugreifen oder **Keine** auswählen.

Anmerkung: Wählen Sie **Keine** aus, um diese Funktion zu deaktivieren.

Fehlerbehebung für Edge-Netzwerkplatine
Sofort neu starten: Mit dieser Schaltfläche können Sie die Netzwerkplatine neu starten.
Auf werkseitige Voreinstellungen zurücksetzen: Mit dieser Schaltfläche können Sie die Netzwerkplatine auf die Standardeinstellung zurücksetzen.

Anhang A. Hilfe und technische Unterstützung anfordern

Wenn Sie Hilfe, Serviceleistungen oder technische Unterstützung benötigen oder einfach nur weitere Informationen zu Lenovo Produkten erhalten möchten, finden Sie bei Lenovo eine Vielzahl von hilfreichen Quellen.

Aktuelle Informationen zu Lenovo Systemen, Zusatzeinrichtungen, Services und Unterstützung erhalten Sie im World Wide Web unter:

http://datacentersupport.lenovo.com

Anmerkung: Dieser Abschnitt enthält Referenzen zu IBM Websites und Informationen zur Inanspruchnahme von Service. IBM ist der bevorzugte Service-Provider von Lenovo für ThinkSystem.

Bevor Sie sich an den Kundendienst wenden

Bevor Sie Hilfe und technische Unterstützung anfordern, können Sie die folgenden Schritte durchführen und versuchen, den Fehler selbst zu beheben. Wenn Sie sich dazu entschließen, Unterstützung anzufordern, stellen Sie alle Informationen zusammen, mit deren Hilfe der Kundendiensttechniker Ihr Problem schneller beheben kann.

Problem selbst beheben

Viele Probleme können Sie ohne Hilfe von außen lösen, wenn Sie die Schritte zur Fehlerbehebung durchführen, die Lenovo in der Onlinehilfefunktion oder der Lenovo Produktdokumentation bereitstellt. Die Lenovo Produktdokumentation enthält auch Beschreibungen der Diagnosetests, die Sie ausführen können. Die Dokumentation für die meisten Systeme, Betriebssysteme und Programme enthält Fehlerbehebungsprozeduren sowie Erklärungen zu Fehlernachrichten und Fehlercodes. Wenn Sie einen Softwarefehler vermuten, können Sie die Dokumentation zum Betriebssystem oder zum Programm zu Rate ziehen.

Die Produktdokumentation für Ihre ThinkSystem Produkte finden Sie hier:

https://pubs.lenovo.com/

Sie können die folgenden Schritte durchführen und versuchen, den Fehler selbst zu beheben:

- Überprüfen Sie alle Kabel und stellen Sie sicher, dass sie angeschlossen sind.
- Überprüfen Sie die Netzschalter, um sich zu vergewissern, dass das System und alle optionalen Einheiten eingeschaltet sind.
- Überprüfen Sie, ob aktualisierte Software, Firmware und Betriebssystem-Einheitentreiber für Ihr Lenovo Produkt vorhanden sind. Laut den Bedingungen des Lenovo Herstellerservice sind Sie als Eigentümer des Lenovo Produkts für die Wartung und Aktualisierung der gesamten Software und Firmware für das Produkt verantwortlich (sofern für das Produkt kein zusätzlicher Wartungsvertrag abgeschlossen wurde). Der Kundendiensttechniker wird Sie dazu auffordern, ein Upgrade der Software und Firmware durchzuführen, wenn für das Problem eine dokumentierte Lösung in einem Software-Upgrade vorhanden ist.
- Wenn Sie neue Hardware oder Software in Ihrer Umgebung installiert haben, überprüfen Sie auf http://www.lenovo.com/serverproven/, ob die Hardware und Software von Ihrem Produkt unterstützt werden.
- Überprüfen Sie http://datacentersupport.lenovo.com auf Informationen, die zur Lösung des Problems beitragen könnten.

– Besuchen Sie die Lenovo Foren unter https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg, um herauszufinden, ob jemand anders ein ähnliches Problem hat.

Viele Probleme können Sie ohne Hilfe von außen lösen, wenn Sie die Schritte zur Fehlerbehebung durchführen, die Lenovo in der Onlinehilfefunktion oder der Lenovo Produktdokumentation bereitstellt. Die Lenovo Produktdokumentation enthält auch Beschreibungen der Diagnosetests, die Sie ausführen können. Die Dokumentation für die meisten Systeme, Betriebssysteme und Programme enthält Fehlerbehebungsprozeduren sowie Erklärungen zu Fehlernachrichten und Fehlercodes. Wenn Sie einen Softwarefehler vermuten, können Sie die Dokumentation zum Betriebssystem oder zum Programm zu Rate ziehen.

Für den Kundendiensttechniker wichtige Informationen sammeln

Falls Sie den Garantieservice für Ihr Lenovo Produkt in Anspruch nehmen möchten, sollten Sie sich entsprechend vorbereiten, bevor Sie sich an Lenovo wenden, damit Ihnen die Kundendiensttechniker effizienter helfen können. Unter http://datacentersupport.lenovo.com/warrantylookup finden Sie weitere Informationen zu Ihrer Produktgarantie.

Stellen Sie die folgenden Informationen für den Kundendiensttechniker zusammen. Mithilfe dieser Daten findet der Kundendiensttechniker schnell eine Lösung für das Problem und kann sicherstellen, dass Sie genau die Servicestufe erhalten, die Sie vertraglich vereinbart haben.

- Nummern von Hardware- und Softwarewartungsverträgen, falls zutreffend
- Maschinentypennummer (vierstellige Lenovo Maschinen-ID)
- Modellnummer
- Seriennummer
- Aktuelle UEFI- und Firmwareversionen des Systems
- Weitere relevante Informationen wie Fehlernachrichten und Protokolle

Alternativ zum Anruf bei der Lenovo Unterstützung können Sie auch unter https://www-947.ibm.com/support/servicerequest/Home.action eine elektronische Serviceanforderung senden. Durch Senden einer ESR beginnt der Lösungsfindungsprozess für Ihr Problem, da den Kundendiensttechnikern die relevanten Informationen zur Verfügung gestellt werden. Die Lenovo Kundendiensttechniker können mit der Arbeit an einer Lösung für Ihr Problem beginnen, sobald Sie die ESR (Electronic Service Request) ausgefüllt und gesendet haben.

Servicedaten erfassen

Um die Ursache eines Serverproblems eindeutig zu bestimmen oder auf Anfrage der Lenovo Unterstützung müssen Sie möglicherweise Servicedaten sammeln, die für eine weitere Analyse verwendet werden können. Servicedaten enthalten Informationen wie Ereignisprotokolle und Hardwarebestand.

Servicedaten können über die folgenden Tools erfasst werden:

- **Lenovo XClarity Controller**

  Sie können die Lenovo XClarity Controller Webschnittstelle oder die CLI verwenden, um Servicedaten für den Server zu sammeln. Die Datei kann gespeichert und an die Lenovo Unterstützung gesendet werden.

  – Weitere Informationen über die Verwendung der Webschnittstelle zum Sammeln von Servicedaten finden Sie unter https://pubs.lenovo.com/xcc/NN1ia_c_servicesandsupport.html.

  – Weitere Informationen zur Verwendung der CLI zum Sammeln von Servicedaten erhalten Sie unter https://pubs.lenovo.com/xcc/nn1ia_r_ffdccommand.html.

- **Lenovo XClarity Administrator**

Lenovo XClarity Administrator kann so eingerichtet werden, dass Diagnosedateien automatisch gesammelt und an die Lenovo Unterstützung gesendet werden, wenn bestimmte wartungsfähige Ereignisse in Lenovo XClarity Administrator und den verwalteten Endpunkten auftreten. Sie können auswählen, ob die Diagnosedateien an die Lenovo Unterstützung über die Call HomeFunktion oder mit SFTP an einen anderen Service Provider gesendet werden. Sie können Diagnosedateien auch manuell sammeln, einen Problemdatensatz öffnen und Diagnosedateien an das Lenovo Unterstützungszentrum senden.

Weitere Informationen zum Einrichten der automatischen Problembenachrichtigung finden Sie in Lenovo XClarity Administrator unter https://pubs.lenovo.com/lxca/admin_setupcallhome.html.

- **Lenovo XClarity Provisioning Manager**

  Verwenden Sie die Funktion „Servicedaten sammeln“ von Lenovo XClarity Provisioning Manager, um Systemservicedaten zu sammeln. Sie können vorhandene Systemprotokolldaten sammeln oder eine neue Diagnose ausführen, um neue Daten zu sammeln.

- **Lenovo XClarity Essentials**

  Lenovo XClarity Essentials kann innerhalb des Betriebssystems ausgeführt werden. Zusätzlich zu den Hardwareservicedaten kann Lenovo XClarity Essentials Informationen zum Betriebssystem, wie das Ereignisprotokoll des Betriebssystems, sammeln.

  Um Servicedaten abzurufen, können Sie den Befehl `getinfor` ausführen. Weitere Informationen zum Ausführen von `getinfor` finden Sie unter https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command.html.

Support kontaktieren

Sie können sich an die Unterstützung wenden, um Hilfe für Ihre Probleme zu erhalten.

Sie können Hardwareservice über einen autorisierten Lenovo Service Provider erhalten. Um nach einem Service Provider zu suchen, der von Lenovo zur Erbringung von Garantieleistungen autorisiert wurde, rufen Sie die Adresse https://datacentersupport.lenovo.com/us/en/serviceprovider auf und suchen Sie mithilfe des Filters nach dem gewünschten Land. Informationen zu den Rufnummern der Lenovo Unterstützung für Ihre Region finden Sie unter https://datacentersupport.lenovo.com/us/en/supportphonelist.

Anhang B. Hinweise

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

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

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es Lenovo Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Dokuments sind kein Angebot und keine Lizenz unter Patenten oder Patentanmeldungen verbunden. Anfragen sind schriftlich an die nachstehende Adresse zu richten:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO STELLT DIESE VERÖFFENTLICHUNG IN DER VORLIEGENDEN FORM (AUF „AS-IS“-BASIS) ZUR VERFÜGUNG UND ÜBERNIMMT KEINE GARANTIE FÜR DIE HANDELSÜBLICHKEIT, DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK UND DIE FREIHEIT DER RECHTE DRITTER. Einige Rechtsordnungen erlauben keine Garantieausschlüsse bei bestimmten Transaktionen, sodass dieser Hinweis möglicherweise nicht zutreffend ist.

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

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

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

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

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten überprüfen, welche Daten für ihre jeweilige Umgebung maßgeblich sind.

Marken

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

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

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

Linux ist eine eingetragene Marke von Linus Torvalds.

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

Wichtige Anmerkungen

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

Die Geschwindigkeit von CD- oder DVD-Laufwerken wird als die variable Lesegeschwindigkeit angegeben. Die tatsächlichen Geschwindigkeiten können davon abweichen und liegen oft unter diesem Höchstwert.

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

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

Bei der Angabe zur maximalen Kapazität von internen Festplattenlaufwerken wird vom Austausch aller Standardfestplattenlaufwerke und der Belegung aller Festplattenlaufwerkpositionen mit den größten derzeit unterstützten Laufwerken, die Lenovo anbietet, ausgegangen.

Zum Erreichen der maximalen Speicherkapazität muss der Standardspeicher möglicherweise durch ein optionales Speichermodul ersetzt werden.

Jede Solid-State-Speicherzelle verfügt über eine interne, endliche Zahl an Schreibzyklen, die bei der Zelle anfallen können. Daher verfügt eine Solid-State-Einheit über eine maximale Anzahl an Schreibzyklen, die auf dieser Einheit ausgeführt werden kann. Dies wird als `total bytes written` (TBW) angegeben. Eine Einheit, die dieses Limit überschreitet, kann möglicherweise nicht auf vom System generierte Befehle antworten oder es ist kein Schreiben auf diese Einheit möglich. Lenovo ist für den Austausch einer Einheit, die diese garantierte maximale Anzahl an Programm-/Löschzyklen (wie in den offiziell veröffentlichten Spezifikationen angegeben) überschritten hat, nicht verantwortlich.

Lenovo übernimmt keine Verantwortung oder Gewährleistungen bezüglich der Produkte anderer Hersteller. Eine eventuelle Unterstützung für Produkte anderer Hersteller erfolgt durch Drittanbieter, nicht durch Lenovo.

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

Verunreinigung durch Staubpartikel

Achtung: Staubpartikel in der Luft (beispielsweise Metallsplitter oder andere Teilchen) und reaktionsfreudige Gase, die alleine oder in Kombination mit anderen Umgebungsfaktoren, wie Luftfeuchtigkeit oder Temperatur, auftreten, können für den in diesem Dokument beschriebenen Server ein Risiko darstellen.

Zu den Risiken, die aufgrund einer vermehrten Staubbelastung oder einer erhöhten Konzentration gefährlicher Gase bestehen, zählen Beschädigungen, die zu einer Störung oder sogar zum Totalausfall der Einheit führen können. Durch die in dieser Spezifikation festgelegten Grenzwerte für Staubpartikel und Gase sollen solche Beschädigungen vermieden werden. Diese Grenzwerte sind nicht als unveränderliche Grenzwerte zu betrachten oder zu verwenden, da viele andere Faktoren, wie z. B. die Temperatur oder der Feuchtigkeitsgehalt der Luft, die Auswirkungen von Staubpartikeln oder korrosionsfördernden Stoffen in der Umgebung sowie die Verbreitung gasförmiger Verunreinigungen beeinflussen können. Sollte ein bestimmter Grenzwert in diesem Dokument fehlen, müssen Sie versuchen, die Verunreinigung durch Staubpartikel und Gase so gering zu halten, dass die Gesundheit und die Sicherheit der beteiligten Personen dadurch nicht gefährdet sind. Wenn Lenovo feststellt, dass die Einheit aufgrund einer erhöhten Konzentration von Staubpartikeln oder Gasen in Ihrer Umgebung beschädigt wurde, kann Lenovo die Reparatur oder den Austausch von Einheiten oder Teilen unter der Bedingung durchführen, dass geeignete Maßnahmen zur Minimierung solcher Verunreinigungen in der Umgebung des Servers ergriffen werden. Die Durchführung dieser Maßnahmen obliegen dem Kunden.

Tabelle 67. Grenzwerte für Staubpartikel und Gase

Verunreinigung	Grenzwerte
Staubpartikel	• Die Raumluft muss kontinuierlich mit einem Wirkungsgrad von 40 % gegenüber atmosphärischem Staub (MERV 9) nach ASHRAE-Norm 52,2[1] gefiltert werden. • Die Luft in einem Rechenzentrum muss mit einem Wirkungsgrad von mindestens 99,97 % mit HEPA-Filtern (HEPA - High-Efficiency Particulate Air) gefiltert werden, die gemäß MIL-STD-282 getestet wurden. • Die relative hygroskopische Feuchtigkeit muss bei Verunreinigung durch Staubpartikel mehr als 60 % betragen[2]. • Im Raum dürfen keine elektrisch leitenden Verunreinigungen wie Zink-Whisker vorhanden sein.
Gase	• Kupfer: Klasse G1 gemäß ANSI/ISA 71.04-1985[3] • Silber: Korrosionsrate von weniger als 300 Å in 30 Tagen

[1] ASHRAE 52.2-2008 – **Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size**. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] Die relative hygroskopische Feuchtigkeit der Verunreinigung durch Staubpartikel ist die relative Feuchtigkeit, bei der der Staub genug Wasser absorbiert, um nass zu werden und Ionen leiten zu können.

[3] ANSI/ISA-71.04-1985. **Umgebungsbedingungen für Prozessmessung und Kontrollsysteme: luftübertragene Verunreinigungen**. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Hinweis zu Bestimmungen zur Telekommunikation

Möglicherweise ist dieses Produkt in Ihrem Land nicht für den Anschluss an Schnittstellen von öffentlichen Telekommunikationsnetzen zertifiziert. Vor der Herstellung einer solchen Verbindung ist eine entsprechende Zertifizierung ggf. gesetzlich vorgeschrieben. Wenden Sie sich an einen Lenovo Ansprechpartner oder Reseller, wenn Sie Fragen haben.

Hinweise zur elektromagnetischen Verträglichkeit

Beim Anschließen eines Bildschirms an das Gerät müssen Sie das hierfür vorgesehene Bildschirmkabel und alle mit dem Bildschirm gelieferten Störschutzeinheiten verwenden.

Weitere Hinweise zur elektromagnetischen Verträglichkeit finden Sie hier:

https://pubs.lenovo.com/

Taiwanesische BSMI RoHS-Erklärung

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “○”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝-〞係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

Kontaktinformationen für Import und Export in Taiwan

Kontaktinformationen für Import und Export in Taiwan.

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

Index

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Lenovo

Teilenummer: SP47A30085

Printed in China

(1P) P/N: SP47A30085