# Dell EMC OpenManage Enterprise-Modular Edition für PowerEdge MX7000 Gehäuse

Benutzerhandbuch

Juli 2021
Rev. A02

## Hinweise, Vorsichtshinweise und Warnungen

**ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

**VORSICHT: Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.**

**WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.**

# Revisionsverlauf

| Date | Dokumentversionen | Beschreibung der Änderungen |
|---|---|---|
| April 2021 | A00 | V1.30.00: Updates für neue Funktionen und Erweiterungen |
| Mai 2021 | A01 | V1.30.00: Updates für die MX750c-Plattform |
| Juli 2021 | A02 | v1.30.10<br>Unterstützung für DC PSU<br>Updates für Lösungs-Baselines v1.20.00, v1.20.10, v1.30.00<br>Updates für OS10 Firmware-Update-Matrix |

# Inhaltsverzeichnis

# 1

# Übersicht

Die Anwendung Dell OpenManage EMC Enterprise Modular (OME-Modular) wird auf der PowerEdge M9002m Managementmodul (MM)-Firmware ausgeführt. OME-Modular vereinfacht die Konfiguration und Verwaltung von eigenständigen PowerEdge MX-Gehäusen oder einer Gruppe von MX-Gehäusen über eine einzige grafische Benutzeroberfläche (GUI). Sie können OME-Modular zum Bereitstellen von Servern und zum Aktualisieren von Firmware verwenden. Darüber hinaus können Sie den allgemeinen Funktionszustand des Gehäuses und der Gehäusekomponenten wie Rechnerschlitten, Netzwerkgeräte, Eingabe/Ausgabe-Module (EAMs) und Speichergeräte überwachen. OME – Modular vereinfacht außerdem die folgenden Aktivitäten auf der Hardware:

- Konnektivität des Verwaltungsnetzwerks
- Ermittlung und Bestandsaufnahme
- Überwachungs- und Stromregelungsvorgänge sowie thermische Funktionen

Sie können OME-Modular zur Verwaltung wichtiger Workloads auf MX7000-Plattformen verwenden.

- Große und unstrukturierte Datenmengen und Analytik
- Hyperkonvergente und herkömmliche Workloads
- Datenbank-Workloads
- Software Defined Storage
- HPC und Leistungsworkloads

Das Hauptgehäuse in einer Multi Chassis Management(MCM)-Gruppe ermöglicht Ihnen die Durchführung der folgenden Aufgaben:

- Verwalten von Servern über mehrere MX-Gehäuse.
- Bereitstellen oder Aktualisieren von Servern über das Hauptgehäuse ohne Starten der Web-Schnittstelle der Mitgliedsgehäuse.
- Verwalten von Fabric-Switch-Engines im Fabric-Modus mithilfe der Web-Schnittstelle von OME-Modular.
- Verwalten des Warnungsprotokolls und von Maßnahmen.
- Verwalten der virtuellen MAC-/WWN-Identitätspools.
- Problemloses Bereitstellen von Rechnerschlitten mithilfe von Serverprofilen und Vorlagen.

OME-Modular bietet einfache und statische Rollen wie z. B. Gehäuse-Administrator, Rechner-Manager, Fabric-Manager, Speicher-Manager und Viewer-Rollen, während OpenManage Enterprise statische und dynamische Gruppen mit rollenbasierter Zugriffskontrolle (RBAC) bietet.

**Themen:**



# Wichtige Funktionen

Die Hauptfunktionen von OME – Modular sind:

- End-to-End-Lifecycle-Verwaltung für Server, Speicher und Netzwerke.
- Hinzufügen eines neuen Gehäuses, um Server-, Speicher- und Netzwerkkapazität hinzuzufügen.
- Verwaltung mehrerer Gehäuse über eine einheitliche Benutzeroberfläche: Web- oder RESTful-Schnittstelle.
- Verwaltung von Netzwerk-EAMs und SmartFabric Services.
- Nutzung der Automatisierungs- und Sicherheitsfunktionen von iDRAC9.

# Was ist neu in dieser Version?

Diese Version von OME-Modular 1.30.10 unterstützt:

- Gleichstrom-Netzteil.
- Kompatibles BIOS 2.11.2 für MX740c und MX840c.
- Kompatibler iDRAC 4.40.29.00 für MX750c.
- Kompatible OS10 Version 10.5.0.9, 10.5.1.9 und 10.5.2.6.
- Überarbeitete OS10-Update-Einschränkungen im Abschnitt OS10-Firmware-Update-Matrix.

## 1.30.00

Diese Version von OME-Modular unterstützt:

- PowerEdge MX750c Plattform.
- Die Option „Gruppenkonfiguration“ auf der **Startseite** in einer Umgebung mit mehreren Gehäusen.
- Menü „Profile“ zum Erstellen, Zuweisen, Bearbeiten und erneuten Bereitstellen von Profilen mit Identitäten getrennt von Vorlagen.
- Vorlagen bearbeiten.
- Erweiterte Lizenz für:
  - Gehäuse-Telemetrie für Stromversorgung, Temperatur und Lüfter. Weitere Informationen finden Sie im *OpenManage Enterprise-Modular Edition RESTful API-Benutzerhandbuch*.
  - OpenID Connect-Anbieter für delegierte Authentifizierung.
- Redfish Warnungsweiterleitung. Weitere Informationen finden Sie im *OpenManage Enterprise-Modular Edition RESTful API-Benutzerhandbuch*.
- Assistent für den Austausch von Ethernet-EAM-Switches für den einfachen Austausch von defekten Fabric-Switches.
- L2-Multicast in SmartFabric Services.
- LCD-Erweiterung mit PIN-Eingabe zum Entsperren des Notzugriffs auf lokale Aktionen wie das Ausschalten des Gehäuses.
- Erinnerung zur Auswahl des Backup-Gehäuses.
- Dieselbe SSO-Anmeldesitzung wird auf Registerkarten freigegeben und wird bei der maximalen Anzahl der Sitzungen nicht gezählt.
- Fortschrittsbanner für die Fabric-Erstellung.
- OS10 DUP wird in den validierten Stapelkatalog eingetragen.
- Link zu Versionshinweisen über das Info-Symbol auf der Seite **Compliance-Bericht**.
- Anzeigen von Voraussetzungen und Abhängigkeiten für Komponenten im Compliance-Bericht.
- Automatische Wiederherstellung der Konfiguration „Rechtes Bedienfeld“ beim Austausch. Weitere Informationen finden Sie im Kundendiensthandbuch *Dell EMC PowerEdge MX7000 Enclosure*.

## 1.20.10

Diese Version von OME-Modular unterstützt:

- Zusätzlicher Support für Quad-Port-Ethernet-Adapter in bis zu 5 MX7000-Gehäusen in einem skalierbaren Fabric
- Erweiterte VLAN-Skalierung für SmartFabric-Services
- Zusätzliche Topologien für die Konnektivität des Fabric Expander Module
- Der Compliance-Status **Unbekannt** wurde im Compliance-Bericht hinzugefügt. Der Status **Unbekannt** markiert die Komponente oder Geräte-Firmware, die im Katalog fehlt, und muss für Compliance-Zwecke manuell verglichen werden.

## 1.20.00

Diese Version von OME-Modular unterstützt:

- Bereitstellen von Vorlagen in leeren Slots oder Slots, die von Rechnerschlitten belegt werden.
- MAC-Identitäten zurückfordern, nachdem Profile entfernt wurden, die Blade-Servern zugeordnet sind.
- Synchronisieren von VLAN-Definitionen von OME-Modular und OpenManage Enterprise.
- Warnmeldungen, wenn ein Gehäuse integriert ist.
- Konfigurieren von FEC (Forward Error Correction) für SmartFabric.
- Weitergabe von VLANs ohne Neustart des Servers.
- Bereitstellen des Betriebssystems mithilfe von „Boot to ISO“ nach dem Anwenden des Profils.

- Verbesserungen bei der Erkennung von Uplink-Fehlern.
- Aktivieren von `racadm connect` zu Brocade MXG610s.
- Hardware-Reset nur auf iDRAC anstelle des gesamten Schlittens durchführen.
- Feld „Name einstellen“ als Standardsortierreihenfolge in Geräteraster.
- Erweiterte Warnmeldung-Pop-ups werden in der oberen rechten Ecke der Nutzeroberfläche angezeigt.
- Neuer SmartFabric-Uplink-Typ: Ethernet – kein Spanning Tree.
- Reduzierung der Warnmeldungsvolumen API als Ersatz für die fehlgeschlagene automatische Erkennung einer skalierbaren Fabric-Erweiterung von einem oder zwei Gehäusen durch den Ethernetswitch.

## 1.10.20

Diese Version von OME-Modular unterstützt:

- Anpassung des Gehäuse-Sicherungsdateinamens.
- Anpassung des Hostbetriebssystem-Neustarts bei Fehlschlagen einer Vorlagenbereitstellung.
- Hardware-Reset der Steckplatz-basierten iDRAC-Schnittstelle über die Seite **Gehäusesteckplätze**.
- Update der MX7000-Komponenten

## 1.10.00

Diese Version von OME-Modular unterstützt:

- Gruppenverwaltung über LCD.
- Zuweisen eines Mitgliedsgehäuses in MCM als Backup-Gehäuse und Hochstufen des Backup-Gehäuses als Lead-Gehäuse.
- Konfigurieren des Hot-Spare für das Gehäuse.
- Zugriff auf das Gehäuse über USB.
- Anpassen von Zeichenfolgen, die auf dem Gehäuse-LCD angezeigt werden.
- Konfigurieren der Inaktivitätszeitüberschreitung für Netzwerksitzungen.
- Extrahieren von Protokollen auf ein lokales Laufwerk auf Ihrem System.
- Herunterladen der MIB-Datei (Management Information Base) auf ein lokales Laufwerk Ihres Systems.

## 1.00.10

Diese Version von OME-Modular unterstützt:

- 20 Gehäuse in einer MCM-Gruppe (Multichassis Management)
- Das Bearbeiten von VLANs, die bereits auf einem Server bereitgestellt wurden, mithilfe einer Vorlage.
- Aktivieren der Federal Information Processing Standards (FIPS) 140-2. Weitere Informationen finden Sie in Zertifikat Nr. 2861 unter csrc.nist.gov/projects/kryptographic-module-validation-program/Certificate/2861.

# Unterstützte Plattformen

OME - Modular unterstützt die folgenden Plattformen und Komponenten:

Plattformen:

- PowerEdge MX7000
- PowerEdge MX740c
- PowerEdge MX750c
- PowerEdge MX840c
- PowerEdge MX5016s
- PowerEdge MX5000s SAS-Switch
- PowerEdge MX 25 Gb Ethernet-Passthrough-Modul
- MX 10GBASE-T Ethernet-Passthrough-Modul
- Dell EMC MX9116n Fabric Switching Engine
- Dell EMC MX5108n Ethernetswitch
- Dell EMC MX7116n Fabric Expander Module

- Fibre-Channel-Switch-Modul Dell EMC MXG610s
- PowerEdge MX9002m Managementmodul

# Unterstützte Webbrowser

OME – Modular wird von den folgenden Webbrowsern unterstützt:

- Google Chrome Version 90
- Google Chrome Version 91
- Mozilla Firefox Version 88
- Mozilla Firefox Version 89
- Microsoft EDGE 90
- Microsoft EDGE 91
- Microsoft Internet Explorer 11
- Safari Version 13
- Safari Version 14

Damit die OME – Modular-Weboberfläche ordnungsgemäß in den Webbrowser geladen wird, stellen Sie sicher, dass die Active X oder Java-Script und die Schriftart-Download-Optionen aktiviert sind.

**ANMERKUNG:** OME – Modular unterstützt TLS 1.2 und höhere Versionen.

# Weitere nützliche Dokumente

Weitere Informationen zur Verwaltung des Systems finden Sie in den folgenden Dokumenten:

**Tabelle 1. Liste mit weiteren Dokumenten zu Referenzzwecken**

| Name des Dokuments | Kurze Einführung in das Dokument |
|---|---|
| *OpenManage Enterprise Modular RACADM-Befehlszeilenreferenzhandbuch* | Dieses Dokument enthält Informationen zu den RACADM-Unterbefehlen, den unterstützten Schnittstellen und Eigenschaften-Datenbankgruppen und Objektdefinitionen. |
| *OpenManage Enterprise Modular Versionshinweise* | Dieses Dokument gibt den letzten Stand der Änderungen am System oder der Dokumentation wieder oder enthält erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker. |
| OpenManage Enterprise und OpenManage Enterprise – Modulares RESTful API-Handbuch | Dieses Dokument enthält Informationen zur Integration Ihrer Anwendungen mit OpenManage Enterprise Modular unter Verwendung der Restful-API-Befehle. |
| *Benutzerhandbuch des integrierten Dell Remote Access Controller (iDRAC)* | Dieses Dokument enthält Informationen zur Installation, Konfiguration und Wartung des iDRAC auf verwalteten Systemen. |
| *OS10 Enterprise Edition Benutzerhandbuch* | Dieses Dokument enthält Informationen über die Funktionen der OS10-Switches und die Verwendung von Befehlen in der EAM-CLI zum Konfigurieren der Switches. |
| *PowerEdge MX SmartFabric-Konfigurations-und Fehlerbehebungshandbuch* | Dieses Dokument enthält Informationen zur Konfiguration und zum Troubleshooting von SmartFabric-Services, die auf PowerEdge MX-Systemen ausgeführt werden. |
| *Installations- und Service-Handbuch des Dell EMC PowerEdge MX7000-Gehäuses* | Dieses Dokument enthält Informationen zur Installation und zum Austausch von Komponenten im PowerEdge MX7000-Gehäuse. |
| *Installations- und Service-Handbuch des Dell EMC PowerEdge MX5016s und MX5000s* | Dieses Dokument enthält Informationen zur Installation und zum Austausch von Komponenten im PowerEdge MX5016s-Speicherschlitten und PowerEdge MX5000s SAS-EAM. |

# Zugriff auf Dokumente der Dell Support-Website

Sie können auf eine der folgenden Arten auf die folgenden Dokumente zugreifen:

- Verwendung der folgenden Links:
  - Für Dokumente zu OpenManage –**https://www.dell.com/openmanagemanuals**
  - Für Dokumente zu iDRAC und Lifecycle Controller –**https://www.dell.com/idracmanuals**
  - Für alle Enterprise-System-Verwaltungsdokumente – **https://www.dell.com/esmmanualsDell.com/SoftwareSecurityManuals**
  - Für Dokumente zu OpenManage Connections Enterprise Systems Management –**https://www.dell.com/esmmanuals**
  - Für Dokumente zu Serviceability Tools –**https://www.dell.com/serviceabilitytools**
  - Für Dokumente zu Client Command Suite Systems Management –**https://www.dell.com/omconnectionsclient**
  - Für Dokumente zu SmartFabric OS10 – **infohub.delltechnologies.com**
- Gehen Sie auf der Dell Support-Website folgendermaßen vor:
  1. Navigieren Sie zu **https://www.dell.com/support**.
  2. Klicken Sie auf **Alle Produkte durchsuchen**.
  3. Klicken Sie auf die gewünschte Produktkategorie, z. B. Server, Software, Speicher usw.
  4. Klicken Sie auf das gewünschte Produkt und anschließend auf die gewünschte Version, falls zutreffend.
     **ANMERKUNG:** Für einige Produkte müssen Sie eventuell durch die Unterkategorien navigieren.
  5. Klicken Sie auf **Handbücher und Dokumente**.

# OME Modular mit anderen Dell EMC Anwendungen positionieren

OME – Modular funktioniert mit den folgenden Anwendungen, um Vorgänge zu verwalten, zu vereinfachen und zu rationalisieren:

- OME – Modular ermittelt und inventarisiert MX7000-Gehäuse im Rechenzentrum über die OME – Modular RESTful-API-Befehle.
- Integrated Dell Remote Access Controller (iDRAC) – OME – Modular verwaltet virtuelle Konsolen über iDRAC.
- Repository Manager – OME – Modular verwendet Repository Manager zum Erstellen benutzerdefinierter Repositorys in freigegebenen Netzwerken für die Erstellung von Katalogen. Die Kataloge werden für Firmwareaktualisierungen verwendet.
- OME – Modular extrahiert die OpenManage SupportAssist-Protokolle von iDRAC, um Probleme zu lösen.

2

# Aktualisieren der Firmware für die PowerEdge MX-Lösung

Komponenten- und Geräte-Firmware für die MX-Lösung werden ausgiebig als validierter Lösungsstack oder Firmware-Baseline getestet. Detaillierte Informationen sind in der Tabelle Aktualisieren von MX7000-Komponenten mithilfe von OME-Modular mit aktuellen und vorherigen Baselines aufgeführt. Wenn die Dell Update Packages (DUPS) auf https://www.dell.com/support verfügbar sind, wird ein validierter Lösungsstack des Gehäuse-Firmware-Katalogs veröffentlicht, der darauf verweist. OME-M vergleicht die Update-Pakete mithilfe eines Compliance-Berichts mit den derzeit installierten Versionen. Weitere Informationen finden Sie im Kapitel Firmware verwalten.

Die Vorteile der Verwendung von OME-M zum Durchführen von Updates mithilfe des Katalogs:

- DUPs werden automatisch von der Support-Website heruntergeladen.
- Alle Komponenten werden gleichzeitig in der erforderlichen Reihenfolge aktualisiert.

Die Reihenfolge für die manuelle Aktualisierung von Komponenten und Geräten wird im Abschnitt Komponenten-Aktualisierungsreihenfolge beschrieben. Die erforderlichen Firmwareversionen für die Aktualisierung von OME-M finden Sie unter Firmwareupdate-Matrix.

Führen Sie in einer MCM-Umgebung das Firmwareupdate für alle Geräte vom Hauptgehäuse aus durch. Wählen Sie außerdem für ein erfolgreiches Firmwareupdate die EAMs und Speicherschlitten als einzelne Geräte und nicht als Gehäusekomponenten aus.

**Themen:**



## MX7000 Lösungs-Baselines

Sie können die folgenden Komponenten von MX7000 unter Verwendung der OME-Modular-Weboberfläche aktualisieren. In der folgenden Tabelle sind die neuen Versionen der MX7000-Komponenten aufgeführt:

**Tabelle 2. MX7000 – OME modulare 1.30.10 und vorherige Lösungs-Baselines**

| **Validierte MX-Stack-Katalogversion** | **-** | **20.07.00** | **20.10.00** | **21.04.00** | **21.07.00** | |
|---|---|---|---|---|---|---|
| **Komponente** | **v1.10.20** | **v1.20.00** | **v1.20.10** | **v1.30.00** | **v1.30.10** | **Ausnahmen im Katalog** |
| iDRAC mit Lifecycle Controller für PowerEdge MX740c und MX840c | 4.11.11.11 | 4.20.20.20 | 4.22.00.00 | 4.40.10.00 | 4.40.10.00 | |
| iDRAC mit Lifecycle Controller für PowerEdge MX750c | - | - | - | 4.40.20.00<br>4.40.29.00** | 4.40.20.00**<br>4.40.29.00 | |
| Dell EMC Server BIOS | 2.5.4 | 2.8.2 | 2.9.4**<br>2.11.2** | 2.10.2<br>2.11.2** | 2.10.2**<br>2.11.2 | |

**Tabelle 2. MX7000 – OME modulare 1.30.10 und vorherige Lösungs-Baselines (fortgesetzt)**

| **Validierte MX-Stack-Katalogversion** | **-** | **20.07.00** | **20.10.00** | **21.04.00** | **21.07.00** | |
|---|---|---|---|---|---|---|
| **Komponente** | **v1.10.20** | **v1.20.00** | **v1.20.10** | **v1.30.00** | **v1.30.10** | **Ausnahmen im Katalog** |
| PowerEdge MX740c | | | | | | |
| Dell EMC Server BIOS PowerEdge MX750c | - | - | - | 1.1.3 | 1.2.4 | |
| Dell EMC Server BIOS PowerEdge MX840c | 2.5.4 | 2.8.2 | 2.9.4**<br>2.11.2** | 2.10.2<br>2.11.2** | 2.10.2**<br>2.11.2 | |
| Fibre Channel-Adapter der QLogic 26XX-Serie | 15.05.12 | 15.05.14 | 15.15.06 | 15.20.14 | 15.20.14 | |
| Fibre Channel-Adapter der Serie QLogic 27XX | 15.05.12 | 15.05.13 | 15.15.06 | 15.20.14 | 15.20.14 | |
| Adapter der QLogic 41xxx-Serie | 15.05.14 | 15.05.18 | 15.15.11 | 15.20.16 | 15.20.16 | |
| Geräteadapter Broadcom 57504 Quad Port | - | - | 21.65.33.33 | 21.80.16.92, nur werkseitige Installation<br>21.80.16.95: Empfohlene Upgradeversion | 21.80.16.92, nur werkseitige Installation<br>21.80.16.95: Empfohlene Upgradeversion | |
| Mellanox ConnectX-4 Lx Ethernet-Adapter-Firmware | 14.25.80.00 | 14.26.60.00 | 14.27.61.22 | 14.28.45.12 | 14.28.45.12 | |
| Intel NIC-Produktreihe Version 19.5.x, Firmware für X710-, XXV710- und XL710-Adapter | 19.5.12 | 19.5.12 | 19.5.12 | 20.0.17 | 20.0.17 | |
| Emulex Fibre Channel-Adapter- | 03.02.18 | 03.02.18 | 03.03.37 | 03.04.24 | 3.04.24 | |

**Tabelle 2. MX7000 – OME modulare 1.30.10 und vorherige Lösungs-Baselines (fortgesetzt)**

| **Validierte MX-Stack-Katalogversion** | **-** | **20.07.00** | **20.10.00** | **21.04.00** | **21.07.00** | |
|---|---|---|---|---|---|---|
| **Komponente** | **v1.10.20** | **v1.20.00** | **v1.20.10** | **v1.30.00** | **v1.30.10** | **Ausnahmen im Katalog** |
| Firmware 32G | | | | | | |
| OpenManage Enterprise Modular | 1.10.20 | 1.20.00 | 1.20.10 | 1.30.00 | 1.30.10 | |
| MX9116n Fabric Switching Engine OS10 | 10.5.0.5* | 10.5.0.7***<br>10.5.0.9 | 10.5.1.6***<br>10.5.1.7***<br>10.5.1.9 | 10.5.2.3, nur werkseitige Installation***<br>10.5.2.4***<br>10.5.2.6 | 10.5.2.6 | |
| MX5108n Ethernetswitch OS10 | 10.5.0.5* | 10.5.0.7***<br>10.5.0.9 | 10.5.1.6***<br>10.5.1.7***<br>10.5.1.9 | 10.5.2.3, nur werkseitige Installation***<br>10.5.2.4***<br>10.5.2.6 | 10.5.2.6 | |
| MX5016s-Speicherschlitten | 2,40 | 2,40 | 2,40 | 2,40 | 2,40 | |
| MX5000s SAS-EAM | 1.0.9.6 | 1.0.9.8 | 1.0.9.8 | 1.0.9.8 | 1.0.9.8 | |
| MXG610s | 8.1.0_lnx3 | 8.1.0_lnx3 | 8.1.0_lnx3 | 9.0.1a | 9.0.1a | Kein Katalog-Update oder DUP |
| Netzwerk-EAM ONIE | - | - | - | 3.35.5.1-23 | 3.35.5.1-23 | |
| Delta AC PSU | 68.5F | 68.5F | 68.5F | 68.5F | 68.5F | Manuelles dup |
| Artesyn AC PSU | 36.6C | 36.6C | 36.6C | 36.6C | 36.6C | Manuelles dup |

*Update auf Betriebssystem 10.5.0.9 und anschließend 10.5.1.9 oder 10.5.2.6. Führen Sie das Skript für das X.509v3 Zertifikat-Upgrade aus, bevor Sie eine Betriebssystemversion aktualisieren. Weitere Informationen finden Sie unter OS10 Firmwareupdate-Matrix.

**Aktualisieren mit individuellem DUP oder aus dem Katalog Neueste Komponenten-Firmware-Versionen unter dell.com.

***Einschränkungen für Updates gelten. Weitere Informationen unter OS10 Firmwareupdate-Matrix.

Überprüfen Sie vor dem Update von MX7000 die PSU-Version. Wenn die PSU-Version 00.36.6B ist, aktualisieren Sie die PSU. Entsprechende Details finden Sie unter https://www.dell.com/support/home/en-us/drivers/driversdetails?driverid=5tc17&oscode=naa&productcode=poweredge-mx7000.

**ANMERKUNG:** Das Aktualisieren des MXG610s FC EAM wird von der OME-Modular-Nutzeroberfläche nicht unterstützt. Verwenden Sie die Brocade-Schnittstelle auf dem EAM.

**ANMERKUNG:** Das Update von MX9116n oder MX5108n mit der Katalogmethode wird für OME-M-Versionen 1.20.10 und niedriger nicht unterstützt. Diese Methode wird ab 1.30.00 unterstützt.

**ANMERKUNG:** Da diese Aktualisierungsanleitungen Aktualisierungen für verschiedene Komponenten der Lösung beinhalten, kann dies Auswirkungen auf den Datenverkehr für vorhandene Workloads haben. Es wird empfohlen, die Aktualisierungen nur während eines regulären Wartungszeitfensters durchzuführen.

**ANMERKUNG:** Bei Upgrades von Baselines vor 1.20.00 kann ein Powercycle (Kaltstart) des MX7000-Gehäuses nach der Aktualisierung aller anwendbaren Lösungskomponenten als letzter Schritt zum Troubleshooting erforderlich sein. Weitere Informationen finden Sie unter Stromversorgung des Gehäuses steuern.

# Komponenten-Aktualisierungsreihenfolge für die individuelle Paketauswahl-Methode

**WARNUNG: Lesen Sie die Anweisungen zum Update vor der Implementierung des Updateverfahrens. Sammeln Sie die aktuellen Versionen der MX7000-Komponenten in Ihrer Umgebung und notieren Sie die speziellen Anweisungen, die im Aktualisierungsverfahren genannt werden können.**

**ANMERKUNG:** Die Migration von Rechnerschlitten-Workloads in Batches zur Durchführung von Rechnerschlitten-Updates wird während des erforderlichen Wartungszeitfensters für den MX Solution-Aktualisierungsvorgang unterstützt.

Wenden Sie sich bei Bedarf an Dell Support, um die MX7000-Komponenten zu aktualisieren, da dies ein komplexer Vorgang ist. Es wird empfohlen, dass Sie alle Komponenten in einem geplanten einzelnen Wartungszeitfenster aktualisieren.

Bevor Sie mit dem Update fortfahren, überprüfen und beheben Sie alle wiederkehrenden Port-Warnmeldungen, die auf der OME-Modular-Seite **Warnmeldungen** gemeldet werden.

**ANMERKUNG:** Die Meldungs-ID für einen **betriebsfähigen** Port ist **NINT0001** und für einen **nicht betriebsfähigen** Port **NINT0002**.

**Aktualisieren Sie die Komponenten in der folgenden Reihenfolge:**

1. Betriebssystemtreiber
   - Aktualisieren Sie die Betriebssystemtreiber des Geräteadapters, gefolgt von der Firmware des Geräteadapters. Siehe MX7000-Komponenten mit OME-Modular 1.30.00 aktualisieren für Geräteadapter und die unterstützen Firmware-Versionen.
2. Rechnerschlitten

   **ANMERKUNG:** Updates von Rechnerschlitten haben keine Abhängigkeiten und können direkt auf ihre entsprechenden OME-Modular 1.30.00-Basisversionen aktualisiert werden, die in Tabelle 2 unter Update von MX7000-Komponenten mit OME-Modular 1.30.00 angegeben sind.
3. OME-Modular-Anwendung
4. Fabric Switching Engine MX9116n und/oder Ethernetswitch MX5108n

Informationen zum Aktualisieren des MXG610s-EAM finden Sie im Abschnitt „Softwareupgrade oder -downgrade“ in Kapitel 6 des Installationshandbuchs für das Fibre-Channel-Switch-Modul MXG610s unter https://dl.dell.com/manuals/all-products/esuprt_networking_int/esuprt_networking_switches_series.

**ANMERKUNG:** Wenn Sie MX5016s Speicherschlitten oder MX5000s SAS EAM installiert haben, aktualisieren Sie diese in der Reihenfolge der Rechnerschlitten bzw. EAM-Komponenten.

**ANMERKUNG:** Zum Aktualisieren des Intel Geräteadapters und der Boss-Firmware führen Sie zunächst ein Upgrade von OME-Modular auf 1.10.10 oder höher durch oder verwenden Sie die iDRAC-Weboberfläche.

# Firmware unter Verwendung der Katalog-basierten Compliance-Methode aktualisieren

**ANMERKUNG:** Die Migration von Rechnerschlitten-Workloads in Batches zur Durchführung von Rechnerschlitten-Aktualisierungen wird während des erforderlichen Wartungszeitfensters für den MX Solution-Aktualisierungsvorgang unterstützt.

Die Aktualisierung der Firmware mithilfe der Katalog-basierten Compliance ist eine bewährte Methode und ein empfohlener Aktualisierungsvorgang.

So aktualisieren Sie die Firmware über die Katalog-basierte Compliance-Methode:

1. Aktualisieren Sie die Betriebssystemtreiber des Geräteadapters, gefolgt von der Firmware des Geräteadapters.

   **ANMERKUNG:** Die Firmwareversionen der Geräteadapter finden Sie im jeweiligen Benutzerhandbuch und in den Versionshinweisen.
2. Navigieren Sie zur Seite **Konfigurationsfirmware**, um den Katalog und die Baseline mit Validierter Stapel zu erstellen.
3. Wählen Sie die Baseline aus und klicken Sie auf **Bericht anzeigen**. Die Seite **Compliance-Report** wird angezeigt.

4. Aktualisieren Sie die Geräte in der folgenden Reihenfolge:
   a. **Rechnerschlitten**
      i. Wählen Sie in **Erweiterte Filter Compute** unter **Typ** aus. Die Liste der Compute-Geräte wird angezeigt.
      ii. Aktivieren Sie das Kontrollkästchen **Alle auswählen** und klicken Sie auf **Kompatibel machen**.
      iii. Gehen Sie zur Seite **Überwachen > Jobs**, um den Jobstatus anzeigen.
      iv. Warten Sie, bis die Compute-Aktualisierungen abgeschlossen sind, und starten Sie dann das Gehäuse-Update.
   b. **Gehäuse**
      i. Wählen Sie unter **Erweiterte FilterGehäuse** unter **Typ** aus, und geben Sie **OpenManage Enterprise Modular** in das Feld **Komponente enthält** ein.
      ii. Aktivieren Sie das Kontrollkästchen **Alle auswählen** und klicken Sie auf **Kompatibel machen**.
      iii. Gehen Sie zur Seite **Überwachen > Jobs**, um den Jobstatus anzeigen.
      iv. Warten Sie, bis die Gehäuseaktualisierungen abgeschlossen sind und starten Sie das Netzwerk-EAM-Update.
   c. **Netzwerk-EAM**
      i. Wählen Sie unter **Erweiterte FilterNetzwerk-EAM** unter **Gerätetyp** aus. Die Liste der Netzwerk-EAM-Geräte wird angezeigt.
      ii. Wählen Sie die erforderliche Anzahl von EAMs und klicken Sie auf **Kompatibel machen**.
      **ANMERKUNG:** Siehe EAM-Firmwareupdatematrix und EAMs für Firmwareupdate gruppieren im Abschnitt Aktualisierung der Firmware, um die Kombination der EAMs anzuzeigen, die aktualisiert werden können.
      iii. Gehen Sie zur Seite **Überwachen > Jobs**, um den Jobstatus anzeigen.
      iv. Warten Sie, bis die Netzwerk-EAM-Aktualisierungen abgeschlossen sind und starten Sie die Aktualisierung der ONIE-Komponente.
   d. **ONIE-Komponente**
      i. Wählen Sie die Baseline aus und klicken Sie auf **Bericht anzeigen**. Die Seite **Compliance-Report** wird angezeigt. Nachdem Sie alle Aktualisierungen durchgeführt haben, können Sie nur die Liste der zu aktualisierenden ONIE-Komponenten anzeigen.
      **ANMERKUNG:** ONIE-Komponenten werden erst dann aufgelistet, wenn alle EAMs auf die Basisversion 1.30.00 aktualisiert sind.
      ii. Aktivieren Sie das Kontrollkästchen **Alle auswählen** und klicken Sie auf **Kompatibel machen**.
      iii. Gehen Sie zur Seite **Überwachen > Jobs**, um den Jobstatus anzeigen.

# OME-M-Firmwareupdate-Matrix

### Tabelle 3. OME-M-Firmwareupdate-Matrix

| | | | Um | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | **OME-M 1.00.01** | **OME-M 1.00.10** | **OME-M 1.10.00** | **OME-M 1.10.10** | **OME-M 1.10.20** | **OME-M 1.20.00** | **OME-M 1.20.10** | **OME-M 1.30.00** | **OME-M 1.30.10** |
| **Von** | **OME-M 1.00.01** | Ja | Ja | | | | | | | |
| | **OME-M 1.00.10** | | Ja | Ja | Ja | | | | | |
| | **OME-M 1.10.00** | | | Ja | Ja | Ja | Ja | Ja | Ja | Ja |
| | **OME-M 1.10.10** | | | | Ja | Ja | Ja | Ja | Ja | Ja |
| | **OME-M 1.10.20** | | | | | Ja | Ja | Ja | Ja | Ja |
| | **OME-M 1.20.00** | | | | | | Ja | Ja | Ja | Ja |
| | **OME-M 1.20.10** | | | | | | | Ja | Ja | Ja |
| | **OME-M 1.30.00** | | | | | | | | Ja | Ja |

**ANMERKUNG:** Die Installation einer früheren Version von OME-M setzt die Konfiguration effektiv auf die Werkseinstellungen zurück. Mit dieser Option können Sie einen bestimmten Firmware-Level beibehalten.

# iDRAC mit Lifecycle Controller unter Verwendung der individuellen Paketauswahl-Methode aktualisieren

1. Wenn OME-Modular eine Gehäusegruppe verwaltet, melden Sie sich bei der OME-Modular-Schnittstelle des Hauptgehäuses an.
2. Klicken Sie auf **Geräte** > **Rechner**. Es wird eine Liste der verfügbaren Rechner im Gehäuse oder in der Gehäusegruppe angezeigt.
3. Aktivieren Sie das Kontrollkästchen in der Kopfzeile der Liste, um alle Rechner auf der aktuellen Seite auszuwählen. Wenn die Liste mehrere Seiten umfasst, gehen Sie zu jeder Seite und aktivieren Sie das Kontrollkästchen.
4. Klicken Sie nach Auswahl aller Rechner auf **Aktualisieren**.
5. Wählen Sie im Assistent **Gerätaktualisierung** das einzelne Paket und klicken Sie auf **Durchsuchen**, um das **iDRAC mit Lifecycle Controller**-DUP zu wählen.
6. Nachdem das DUP hochgeladen wurde, klicken Sie auf **Weiter** und aktivieren Sie das Kontrollkästchen **Compliance**.
7. Klicken Sie auf **Fertig stellen**, um das Update auf allen Rechnern zu starten.
8. Warten Sie, bis der Vorgang abgeschlossen ist, bevor Sie mit dem Update der Komponenten Dell EMC Server-BIOS PowerEdge MX740c, MX750c und MX840c fortfahren.

**ANMERKUNG:** Die Aktualisierung von iDRAC auf 4.40.10.00 unter Verwendung einzelner DUPs von OME-M Version 1.10.20 oder niedriger zeigt keine Compliance-Details an und kann fehlschlagen. Verwenden Sie die empfohlene Methode zur Katalogaktualisierung.

**ANMERKUNG:** Als alternative Methode zum Aktualisieren von Rechner-Hosts und/oder Speicherschlitten können Sie katalogbasierte Aktualisierungen implementieren, sobald die Kataloge mit den Baseline-Versionen aktualisiert wurden. Weitere Informationen finden Sie unter Kataloge verwalten.

## Aktualisierung von MX740c, MX750c und MX840c Server BIOS

Wiederholen Sie die Schritte, die im Abschnitt *iDRAC mit Lifecycle Controller mithilfe von OME-Modular aktualisieren* beschrieben sind, um Dell EMC Server-BIOS PowerEdge MX740c, MX750c und MX840c nach Bedarf zu aktualisieren.

## Adapter aktualisieren

Laden Sie die Betriebssystemtreiber für Ihren Geräteadapter, die mit der Firmware des Geräteadapters veröffentlicht wurden, herunter und installieren Sie sie. Befolgen Sie die Installationsanleitungen des Geräteadaptertreibers für Ihr Betriebssystem.

Wiederholen Sie die im Abschnitt beschriebenen Schritte, um die folgende Adapter-Firmware zu aktualisieren:

| Folgen Sie diesem Abschnitt | Zur Aktualisierung |
|---|---|
| iDRAC mit Lifecycle Controller mithilfe von OME-Modular aktualisieren | Fibre Channel-Adapter der QLogic 26XX-Serie |
| | Fibre Channel-Adapter der Serie QLogic 27XX |
| | Adapter der QLogic 41xxx-Serie |
| | Geräteadapter Broadcom 57504 Quad Port |
| | Mellanox ConnectX-4 Lx Ethernet-Adapter-Firmware |
| | Intel NIC-Produktreihe Version 19.5.x, Firmware für X710-, XXV710- und XL710-Adapter |
| | Adapter Emulex Picard-16/Picard-32 |

Gehen Sie zu Dell.com, um die neuesten Gerätetreiber für das jeweilige Firmwareupdate herunterzuladen.

# Aktualisierung von OME-Modular auf 1.30.10

Sie können von verschiedenen Versionen auf OME-Modular 1.30.10 aktualisieren. Weitere Informationen finden Sie im Abschnitt OME-M-Firmwareupdate-Matrix.

**ANMERKUNG:** Wenn Sie alle Management-Module in einer MCM-Gruppe auswählen, aktualisiert die OME-M diese in der gewünschten Reihenfolge.

**ANMERKUNG:** Das Update auf 1.10.x oder höher kann zur Warnungsprotokollmeldung HWC7522 führen. Möglicherweise müssen Sie die Stromversorgung des MX7116n oder der PTM-EAMs (Pass-Through-Modul) neu einstellen.

**ANMERKUNG:** Wenn das Firmwareupdate eines Mitgliedsgehäuses länger als zwei Stunden nicht reagiert, brechen Sie den Job mithilfe der Option **Job beenden** auf der Seite **Jobdetails** ab. Überprüfen Sie den Status des Firmwareupdates auf dem Mitgliedsgehäuse direkt. Die Option **Job anhalten** würde das Firmwareupdate für ein bestimmtes Ziel stoppen, das nicht reagiert, und zum nächsten Zielupdate wechseln. Starten Sie bei allen Firmwareupdate-Fehlern auf Mitgliedsgehäusen das Firmwareupdate nur auf dem spezifischen Ziel vom **Hauptgehäuse** aus neu.

## Best Practices für das Update auf 1.30.10

Stellen Sie beim Aktualisieren des Managementmoduls von einer früheren Version auf 1.30.10 sicher, dass auf der Seite **Jobs** keine fehlgeschlagenen Vorlagenbereitstellungsaufträge vorhanden sind. Gibt es fehlgeschlagene Bereitstellungsaufträge, dann werden die virtuellen Identitäten, die für das Gerät für diese fehlgeschlagenen Bereitstellungen reserviert sind, nach dem Upgrade auf 1.30.10 wieder dem freien Pool hinzugefügt.

## Aktualisieren der Managementmodul-Firmware

**ANMERKUNG:** Stellen Sie sicher, dass Sie die OME-Modular-Firmware aktualisieren, bevor Sie ein Upgrade auf OS10 durchführen.

Die Managementmodul-Firmware kann anhand einer der folgenden Methoden aktualisiert werden:

1. Individuelle Paketauswahl-Methode – Über die OME – Modular-Webschnittstelle oder RESTful API.
2. Katalog-basierte Compliance-Methode

So aktualisieren Sie die Firmware über die individuelle Paketauswahl-Methode:

1. Laden Sie das DUP über die Website **www.dell.com/support/drivers** herunter.
2. Gehen Sie in der OME – Modular-Webschnittstelle zu **Geräte** > **Gehäuse** und wählen das Gehäuse aus, dessen Firmware Sie aktualisieren wollen.
3. Klicken Sie auf **Firmware aktualisieren**.
   Die Seite **Firmwarequelle auswählen** wird angezeigt.
4. Wählen Sie die Option **Einzelnes Paket** aus und klicken Sie auf **Durchsuchen**, um zum Speicherort des heruntergeladenen DUP zu gehen, und klicken Sie auf **Weiter**.
   Warten Sie auf den Vergleichsreport. Die unterstützten Komponenten werden angezeigt.
5. Wählen Sie die gewünschten Komponenten aus, zum Beispiel: OME – Modular, und klicken Sie auf **Aktualisieren**, um das Firmwareupdate zu starten:

   Sie können den Aktualisierungsvorgang für einen gewünschten Zeitpunkt planen.
6. Gehen Sie zur Seite **Überwachen** > **Jobs**, um den Jobstatus anzeigen.

**ANMERKUNG:** Die Konsole ist während des OME – Modular-Aktualisierungsvorgangs nicht zugänglich. Warten Sie nach dem OME – Modular-Update, bis die Konsole einen stabilen Zustand erreicht.

## Fehlgeschlagenen Managementmodul-Firmwareaktualisierungsprozess wiederherstellen

Wenn die Firmwareaktualisierung eines Managementmoduls (MM) fehlschlägt, führen Sie die folgenden Schritte aus:

1. Führen Sie ein Failover auf dem MM durch. Wenn das Failover fehlschlägt, fahren Sie mit Schritt 2 fort.
2. Setzen Sie das aktive MM manuell zurück.

3. Überprüfen Sie nach Abschluss des Failover oder Reset die Firmwareversion, um zu überprüfen, ob auf dem aktiven MM die gleiche oder eine neuere Version von OME-Modular wie auf dem Standby-MM ausgeführt wird. Falls dies nicht der Fall ist, führen Sie einen Reset des MM durch, um ein Failover zu erzwingen.
4. Versuchen Sie die Aktualisierung der Firmware erneut.

# Ethernetswitch über DUP aktualisieren

**WARNUNG: Für IOMs im Full-Swith-Modus wählen Sie nicht beide IOMs in einem redundantem Paar gleichzeitig. Diese Aktion kann zu Netzwerkausfällen führen.**

**ANMERKUNG:** Aktualisieren Sie die Switches MX9116n-und MX5108n erst, nachdem Sie die anderen MX7000-Komponenten auf die entsprechenden PowerEdge MX-Baseline-Versionen 1.30.00 aktualisiert haben.

**ANMERKUNG:** Das DUP-Update-Verfahren wird für das Upgrade von OS10, Firmware und ONIE, auf den Switches MX9116n und MX5108n empfohlen.

**ANMERKUNG:** Aktualisieren Sie die MX9116n- und MX5108n-Switches auf 10.5.1.9 oder 10.5.2.6, und zwar nur dann, wenn auf den Switches die Version 10.5.0.9 oder das Zertifikat 10.5.0.7 installiert ist.

Die Upgrade-Zeit für einen Switch kann zwischen 30 und 120 Minuten dauern. Manchmal kann die Upgrade-Zeit auch bis zu 4,5 Stunden betragen.

Um den Upgrade-Status zu überprüfen, können Sie die OME-M-Job-Seite einsehen oder sich am Switch anmelden und`smart-fabric upgrade-status` ausführen.

## Networking OS10 über DUP aktualisieren

Gehen Sie folgendermaßen vor, um OS10 mit DUP zu aktualisieren:

1. Laden Sie die neueste DUP-Datei für den Switch von https://www.dell.com/support herunter.
2. Gehen Sie in der OME-Modular-Weboberfläche zu **Geräte** > **E/A-Module**.
3. Wählen Sie das EAM-Modul aus, auf dem Sie das OS10-Upgrade durchführen möchten.
4. Klicken Sie auf **Firmware aktualisieren**.
5. Wählen Sie die Option „Einzelnes Paket“ aus und klicken Sie auf **Durchsuchen**, um zum Speicherort des heruntergeladenen OS10 DUP zu navigieren. Warten Sie, bis der Compliance-Bericht abgeschlossen ist, anschließend werden die unterstützten Komponenten angezeigt.
6. Wählen Sie die gewünschten Komponenten aus und klicken Sie auf **Update**, um das Update zu starten.

   Informationen zum Upgrade unterschiedlicher Versionen vor 10.5.0.7 finden Sie unter Netzwerkswitch über unterschiedliche DUP-Versionen aktualisieren.
7. Gehen Sie zur Seite **Monitoring-** > **Jobs**, um den Jobstatus anzeigen.

## Firmware und ONIE über DUP aktualisieren

**ANMERKUNG:** Update von ONIE unter Verwendung von DUP wird nur unterstützt, wenn alle EAMs in der Gruppe Version 10.5.2.4 und höher sind.

Gehen Sie folgendermaßen vor, um ONIE über DUP zu aktualisieren:

1. Laden Sie die neueste ONIE DUP-Datei für den Switch von https://www.dell.com/support herunter.
2. Gehen Sie in der OME-Modular-Weboberfläche zu **Geräte** > **E/A-Module**.
3. Wählen Sie das EAM-Modul aus, auf dem Sie das ONIE-Upgrade durchführen möchten.
4. Klicken Sie auf **Firmware aktualisieren**.
5. Wählen Sie die Option „Einzelnes Paket“ aus und klicken Sie auf **Durchsuchen**, um zum Speicherort des heruntergeladenen ONIE DUP zu navigieren. Warten Sie, bis der Compliance-Bericht abgeschlossen ist, anschließend werden die unterstützten Komponenten angezeigt.
6. Wählen Sie die gewünschten Komponenten aus und klicken Sie auf **Update**, um das Update zu starten.
7. Gehen Sie zur Seite **Monitoring-** > **Jobs**, um den Jobstatus anzeigen.

# OS10-Firmwareupdate-Matrix

### Tabelle 4. OS10-Firmwareupdate-Matrix

| | | Um | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **OS10-Version** | **10.4.0E(R3SP2)** | **10.4.0E(R4SP2)** | **10.5.0.1** | **10.5.0.3P1** | **10.5.0.5** | **10.5.0.9** | **10.5.1.9** | **10.5.2.4** | **10.5.2.6** |
| **Von** | **10.4.0E(R3SP2)** | — | — | — | — | — | Ja* | — | — | — |
| | **10.4.0E(R4SP2)** | — | — | — | — | — | Ja* | — | — | — |
| | **10.5.0.1** | — | — | — | — | — | Ja | — | — | — |
| | **10.5.0.3P1** | — | — | — | — | — | Ja | — | — | — |
| | **10.5.0.5** | — | — | — | — | — | Ja | — | — | — |
| | **10.5.0.7** | — | — | — | — | — | — | Ja | — | Ja |
| | **10.5.0.9** | — | — | — | — | — | — | Ja | — | Ja |
| | **10.5.1.6/ 10.5.1.7/ 10.5.1.9/** | — | — | — | — | — | — | — | Ja | Ja |
| | **10.5.2.4** | — | — | — | — | — | — | — | — | Ja |

* – Das Aktualisieren der EAM VLT-Peers von Version 10.4.X auf 10.5.X hat Auswirkungen auf den Datenverkehr. Das reguläre Wartungszeitfenster wird für diese Aktivität empfohlen.

**ANMERKUNG:** Führen Sie das X.509v3-Zertifikat-Upgrade-Skript aus, bevor Sie ein Upgrade von 10.5.0.1/10.5.0.3P1/10.5.0.5/10.5.0.7 OS10-Versionen durchführen. Siehe PSQN, bevor Sie von diesen OS10-Versionen aktualisieren. Das Upgrade-Skript ist verfügbar unter https://www.dell.com/support/kbdoc/000184027/dell-emc-networking-os10-certificate-expiration-and-solution.

**ANMERKUNG:** Das Upgrade von IOMs im SmartFabric-Modus auf OS10.5.1.6 mit VLAN 1 als getaggt, unterbricht den Datenverkehr. Ist VLAN 1 markiert, aktualisieren Sie auf OS10.5.1.7. In den Versionshinweisen finden Sie eine vollständige Liste der Korrekturen in OS10.5.1.7.

Die Anzahl der EAMs, die aktualisiert werden können, variiert je nach EAM-Versionen. In der folgenden Tabelle wird die Anzahl der EAMs angezeigt, die gleichzeitig aktualisiert werden können.

### Tabelle 5. EAM-Firmwareupdatematrix

| IOM Version | OME-M Version | Anzahl der EAMs |
|---|---|---|
| 10.5.0.5 | 1.10.20 oder höher | 4 |
| 10.5.0.7/10.5.0.9 | 1.20.00 oder höher | 6 |
| 10.5.1.X | 1.20.10 oder höher | 6 |
| 10.5.2.4 or later | 1.30.00 oder höher | Keine Beschränkungen |

Sie müssen die EAMs für das Firmwareupdate je nach Typ des EAM gruppieren. Die folgende Tabelle zeigt ein Beispiel für die Gruppierung von 12 EAMs für ein Firmwareupdate.

### Tabelle 6. EAMs für Firmwareupdate gruppieren

| Beispiel für 12 E/A-Module | Kombination | Gruppe 1 | Gruppe 2 | Gruppe 3 |
|---|---|---|---|---|
| **10.5.0.5** | 6 Fabrics | Fabric 1 und 2 | Fabric 3 und 4 | Fabric 5 und 6 |
| | 12 Full-Switches | EAM 1 bis 4 | EAM 5 bis 8 | EAM 9 bis 12 |

**Tabelle 6. EAMs für Firmwareupdate gruppieren (fortgesetzt)**

| Beispiel für 12 E/A-Module | Kombination | Gruppe 1 | Gruppe 2 | Gruppe 3 |
|---|---|---|---|---|
| | 4 Fabrics und 4 Full-Switch | Fabric 1 und 2 | Fabric 3 und 4 | 4 Full-Switch-EAM |
| **10.5.0.7/10.5.0.9 or 10.5.1.X** | 6 Fabrics | Fabric 1 bis 3 | Fabric 4 bis 6 | Nicht anwendbar |
| | 12 Full-Switches | EAM 1 bis 6 | EAM 6 bis 12 | Nicht anwendbar |
| | 4 Fabrics und 4 Full-Switch | Fabric 1 bis 3 | Fabric 4 und 4 Full-Switch-EAM | Nicht anwendbar |

Wenn alle EAMs auf den Stack 10.5.2.4/10.5.2.6 aktualisiert sind, zeigen die Netzwerk-EAMs zwei Softwarekomponenten zum Update an. Folgende Optionen stehen zur Verfügung:

- Dell EMC Networking SmartFabric OS10
- Dell EMC Networking ONIE Firmware

Einschränkungen für ONIE-Firmwareupdates:

- Die Updateoption für die ONIE-Firmware ist nur verfügbar, wenn die OS10-Version 10.5.2.4 oder höher ist.
- Wenn Sie für das ONIE-Update ein Netzwerk-EAM auswählen, das Teil einer Fabric ist, werden andere Nodes in der Fabric automatisch aktualisiert.
- Wenn Sie eine alte Version von EAM einfügen, kann die ONIE-Firmware nicht aktualisiert werden, bis OS10 auf 10.5.2.4 aktualisiert wurde.

**ANMERKUNG:** Die Firmware der ONIE-Komponente wird nicht aktualisiert, da das System nicht in ONIE booten kann, wenn das GRUB-Menü mit seriellen Steuerzeichen angezeigt wird. Dieses Problem wird in der ONIE-Firmwareversion 3.35.1.1-15 behoben. Wenn das ONIE-Update fehlschlägt oder ein ONIE-Boot-Problem auftritt, wiederholen Sie das Update der ONIE-Komponenten-Firmware.

## Problemumgehung bei fehlgeschlagener EAM-Aktualisierung

- Wenn EAMs von 10.5.0.7 oder 10.5.0.9 auf 10.5.2.4 oder 10.5.2.6 aktualisiert werden, zeigt die Seite **Jobs** auf OME-Modular den Job als Fehler an, aber die Software-Aktualisierung ist erfolgreich.
- Wenn ein Job fehlschlägt, führen Sie den Befehl `show smartfabric nodes` in der EAM-CLI aus und prüfen, ob die fehlgeschlagene EAM im Status OFFLINE ist.
- Ist OFFLINE-EAM in: 10.5.2.4 oder 10.5.2.6
  - Full-Switch-Modus: Es ist keine sofortige Aktion erforderlich, es wird automatisch wiederhergestellt, wenn der Fabric-Manager auf die neueste Version aktualisiert wird.
  - Fabric-Modus: Neustart der EAM, die OFFLNE ist.
- Wenn einer der Nodes des Fabric aufgrund des obigen Fehlers nicht aktualisiert wird, starten Sie den Upgrade-Job erneut.

# Voraussetzungen für ein Upgrade von 10.5.0.7 oder 10.5.0.9

- Stellen Sie bei dem Update sicher, dass die EAMs in Gruppen mit nicht mehr als sechs pro Upgrade-Job aktualisiert werden.
- Wenn sich in einem VLT mit Full-Switch-Modus zwei Switches befinden, sollte jeder Switch aus Redundanzgründen Teil eines anderen Upgrade-Batches sein.
- Wenn zwei Switches in einer SmartFabric vorhanden sind, wählen Sie nur einen Switch aus. Der andere Switch wird automatisch aktualisiert. Dies wird in dieser Upgrade-Gruppe als „2“ gezählt.

# 3

# OME-Modular-Lizenzen

OME-Modular-Funktionen sind auf Basis von Lizenzen verfügbar, die im XML-Format vorliegen. Nachfolgend sind die unterstützten Lizenztypen aufgeführt:

- Unbefristet – die Gültigkeit ist unbegrenzt und gilt, bis die Lizenz entfernt oder gelöscht wird. Die unbefristete Lizenz ist an die Service-Tag-Nummer des Gehäuses gebunden.
- Evaluierung – Kurze Gültigkeit, der Timer startet nach dem Import oder der Installation der Lizenz. Der Timer ist eine monotone Uhr, die die Betriebsdauer des Systems erfasst. Die Zeit wird in einer Prüfpunktdatei akkumuliert, um sicherzustellen, dass die Lizenzbeschränkungen nicht umgangen werden. Der Timer stoppt während eines Firmware-Shutdowns oder -Reboots und wird fortgesetzt, nachdem die Firmware bereit ist. Es wird eine Warnung angezeigt, wenn die Lizenz bald abläuft.

Die Lizenzen können über den Dell Digital Locker heruntergeladen werden.

Sie können die Lizenzdetails auf der Seite **Installierte Lizenzen** importieren und anzeigen. Der Lizenztyp wird auch auf der Seite **Gehäuseübersicht** angezeigt.

**Themen:**



## Import von Lizenzen

Sie können Lizenzdateien im XML-Format importieren.

So importieren Sie eine Lizenz:

1. Klicken Sie auf **Anwendungseinstellungen** > **Lizenzen**.
   Das Fenster **Installierte Lizenzen** wird angezeigt.
2. Klicken Sie auf **Importieren**.
   Der Bildschirm **Lizenzdatei importieren** wird angezeigt.
3. Klicken Sie auf **Datei auswählen** und gehen Sie zum Speicherort der Lizenz.
4. Wählen Sie die Datei aus und klicken Sie auf **Öffnen**, um die Datei zu importieren.
   Der Bildschirm **Lizenzdatei importieren** wird angezeigt.
5. Klicken Sie auf **Fertigstellen** , um die Datei zu importieren.
   Die importierte Lizenzdatei wird auf der Seite **Installierte Lizenzen** angezeigt.

## Anzeigen der Lizenzdetails

So zeigen Sie die Lizenzdetails an:

Wählen Sie auf der Seite **Installierte Lizenzen** die Lizenzen aus, deren Details Sie anzeigen möchten.
Die Lizenzdetails werden auf der rechten Seite der Liste der installierten Lizenzen angezeigt.

Die Details sind: Beschreibung, Berechtigungs-ID, Lizenztyp und Ablaufzeitstempel.

# 4

# Bei OME – Modular anmelden

Sie können sich bei OME – Modular als lokaler, Active Directory- oder allgemeiner LDAP-Nutzer (Lightweight Directory Access Protocol) anmelden. OME – Modular unterstützt maximal je zwei Active Directory- oder LDAP-Serverkonfigurationen.

**Themen:**



## Bei OME – Modular als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer anmelden

OME – Modular ermöglicht die Authentifizierung von 64 lokalen Nutzerkonten. So melden Sie sich bei OME – Modular als Active Directory (AD)- oder LDAP-Benutzer an:

1. Verzeichnisdienst hinzufügen
2. Verzeichnisgruppe importieren
3. Mit Verzeichnisbenutzer-Anmeldeinformationen anmelden

Für Active Directory- und generische LDAP-Nutzerkonten unterstützt OME – Modular mindestens ein Nutzerkonto in einer einfachen Umgebung und maximal zwei Konten in einer komplexen Umgebung.

LDAP-Benutzer können mit OME – Modular die folgenden Aufgaben durchführen:

- Aktivieren Sie den LDAP-Zugang.
- Ein Verzeichnisdienst-Zertifizierungsstellenzertifikat hochladen und anzeigen.
- Während der Konfiguration von LDAP Attribute zuzuweisen Die Attribute sind: LDAP-Serveradresse, LDAP-Serverschnittstelle, Bindungs-DN, Bindungskennwort, Nutzeranmeldeattribut, Gruppenmitgliedschaftsattribut und Suchfilter.
- Verknüpfen Sie eine LDAP-Gruppe mit einer vorhandenen oder neuen Managementmodulrollengruppe.

So melden Sie sich als lokaler, Active Directory- oder LDAP-Benutzer an.

1. Geben Sie den **Nutzernamen** ein.
2. Geben Sie das **Kennwort** ein.
3. Klicken Sie auf **Anmelden**.

Nachdem Sie sich erfolgreich angemeldet haben, können Sie Folgendes tun:

- Konfigurieren Sie Ihr Konto.
- Ändern Sie das Kennwort.
- Stellen Sie das Stammkennwort wieder her.

# Integrieren von Verzeichnisdiensten in OME-Modular

Sie können Verzeichnisdienste zum Importieren von Verzeichnisgruppen aus AD oder LDAP zur Verwendung in der Web-Schnittstelle verwenden. OME-Modular unterstützt die Integration der folgenden Verzeichnisdienste:

1. Windows Active Directory
2. Windows AD-LDS
3. OpenLDAP
4. PHP LDAP

## Unterstützte Attribute und Voraussetzungen für die LDAP-Integration

**Tabelle 7. Voraussetzungen/unterstützte Attribute von OME-Modular für LDAP-Integration**

| | Attribut der Nutzeranmeldung | Attribut der Gruppenmitgliedschaft | Zertifikatanforderung |
|---|---|---|---|
| Windows AD-LDS | Cn, sAMAccountName | Mitglied | • Abhängig von der Verfügbarkeit von FQDN im Domain-Controller-Zertifikat. Das SAN-Feld kann sowohl IPv4 und IPv6 als auch IPv4 oder IPv6 oder einen FQDN haben.<br>• Nur das Base64-Zertifikatformat wird unterstützt. |
| OpenLDAP | UID, SN | Uniquemember | Nur das PEM-Zertifikatformat wird unterstützt. |
| PHP LDAP | UID | MemberUid | |

## Nutzer-Voraussetzungen für die Verzeichnisdienst-Integration

Stellen Sie sicher, dass die folgenden Nutzer-Voraussetzungen erfüllt sind, bevor Sie mit der Integration von Verzeichnisdiensten beginnen:

1. Der BindDN-Nutzer und der für die Testverbindung verwendete Nutzer müssen identisch sein.
2. Wenn das Attribut der Nutzeranmeldung bereitgestellt wird, ist nur der entsprechende Nutzername, der dem Attribut zugewiesen ist, für die Gerät-Anmeldung zulässig.
3. Der für die Testverbindung verwendete Nutzer muss Teil einer nicht standardmäßigen Gruppe in LDAP sein.
4. Das Attribut der Gruppenmitgliedschaft muss den „Nutzer-DN“ oder den (für die Anmeldung verwendeten) Kurznamen des Nutzers haben.
5. Wenn MemberUid als „Attribut der Gruppenmitgliedschaft“ verwendet wird, wird beim Nutzernamen, der in der Gerät-Anmeldung verwendet wird, in einigen LDAP-Konfigurationen zwischen Groß- und Kleinschreibung unterschieden.
6. Wenn der Suchfilter in der LDAP-Konfiguration verwendet wird, ist die Nutzeranmeldung für diejenigen Nutzer, die nicht Teil der angegebenen Suchkriterien sind, nicht erlaubt.
7. Die Gruppensuche funktioniert nur, wenn den Gruppen Nutzer unter dem angegebenen Attribut der Gruppenmitgliedschaft zugewiesen sind.

**ANMERKUNG:** Wenn OME-Modular in einem IPv6-Netzwerk gehostet wird, schlägt die SSL-Authentifizierung gegenüber Domänencontrollern mit FQDN fehl, wenn IPv4 als bevorzugte Adresse im DNS festgelegt ist. Führen Sie einen der folgenden Schritte aus, um diesen Fehler zu vermeiden:

- Das DNS sollte so eingestellt sein, dass bei einer Abfrage mit FQDN "IPv6" als bevorzugte Adresse zurückgegeben wird.
- Das DC-Zertifikat muss IPv6 im Feld „SAN“ haben.

# Hinzufügen eines Active Directory-Service

So fügen Sie den Active Directory-Service hinzu:

1. Klicken Sie in der OME – Modular-Webschnittstelle auf **Anwendungseinstellungen** > **Benutzer** > **Verzeichnisdienste** > **Hinzufügen** > **Verzeichnistyp**.
   Die Seite **Verbindung zum Verzeichnisdienst** wird angezeigt.
2. Wählen Sie unter **Verzeichnistyp** die Option **AD** oder **LDAP** aus. Die Standardoption ist **AD**.
3. Geben Sie den **Verzeichnisnamen** ein.
4. Wählen Sie die **Domain-Controller-Suche** aus:

   Wenn der **Domänen-Controller-Suchtyp** DNS und der Verzeichnistyp **AD** ist, geben Sie den Domänennamen und die Gruppendomäne ein.

   Wenn der **Domänen-Controller-Suchtyp** beim Verzeichnistyp **AD DNS** ist, geben Sie den Domänennamen und die Gruppendomäne ein. Wenn der **Domänencontroller-Suchtyp Manuell** ist, geben Sie den FQDN oder die IP-Adresse des Domänen-Controllers ein. Wenn Sie mehrere Server haben, werden maximal drei Server unterstützt, verwenden Sie eine durch Kommas getrennte Liste.

   In der Gruppendomäne können Sie nach Verzeichnisgruppen suchen. Sie können die Verzeichnisgruppen als Anwendungsbenutzer einschließen. Sie können auch die Gruppendomäne für die Authentifizierung von Benutzern während der Anmeldung verwenden. Das Format der Gruppendomäne kann `<Domain>.<Sub-Domain>` oder `ou=org, dc=example, dc=com` sein.

   Verwenden Sie den Domain Controller-Suchtyp **DNS**, wenn Sie die Details der Domain-Controller nicht kennen, von denen Sie die Gruppe oder Gruppen importieren möchten. Stellen Sie sicher, dass Sie die folgenden Schritte auf der Seite **Netzwerkeinstellungen** ausgeführt haben, um den DNS Domain Controller zu verwenden:

   - Aktivieren Sie das Kontrollkästchen **Mit DNS registrieren**.
   - Die primäre und die alternative DNS Server-Adressen werden zugewiesen.

   Nachdem Sie den Domänennamen eingegeben haben, durchsucht OME-Modular die SRV-Datensätze auf den DNS-Servern, um die Details der Domänen-Controller in dieser Domäne abzurufen.

   Wenn Sie die IP-Adresse oder FQDN der Domain-Controller kennen, können Sie einen **manuelle** Domain-Controller-Suchtyp verwenden.

5. Geben Sie unter **Erweiterte Optionen** den **Server-Port**ein. Wenn der **Verzeichnistyp AD** ist, fahren Sie mit Schritt 6 fort.

   Unter **Server-Port** ist standardmäßig Portnummer 3269 der Adresse des globalen Katalogs ausgefüllt. Geben Sie für den **Domain-Controller**-Zugriff 636 für die Portnummer ein.
6. Wählen Sie die **Netzwerkzeitüberschreitung** und die **Suchzeitüberschreitung** aus.
7. Aktivieren Sie das Kontrollkästchen **Zertifikatsvalidierung**, wenn Sie das Zertifikat für den Verzeichnisdienst validieren möchten, und wählen Sie das zu validierende Zertifikat aus.

   Das Zertifikat muss ein Stamm-CA-Zertifikat sein, das im Base64-Format kodiert ist.

   Die Option **Verbindung testen** wird aktiviert.
8. Klicken Sie auf **Verbindung testen**, um die AD-Verbindung zu überprüfen, und geben Sie den Benutzernamen und das Kennwort der Domäne ein, mit der Sie eine Verbindung herstellen möchten.

   **ANMERKUNG:** Der Benutzername muss entweder im UPN- (Benutzername@Domäne) oder im NetBIOS-Format (Domäne\Benutzername) eingegeben werden.

9. Klicken Sie auf **Verbindung testen**.
   Das Fenster **Verzeichnisdienstinformationen**, das auf eine erfolgreiche Verbindung hinweist, wird angezeigt.
10. Klicken Sie auf **OK** und anschließend auf **Fertigstellen**.
    Es wird ein Job erstellt und ausgeführt, um das angeforderte Verzeichnis auf der Seite **Verzeichnisdienste** hinzuzufügen.

# Hinzufügen eines LDAP-Service

So fügen Sie den LDAP-Service hinzu:

1. Klicken Sie in der OME – Modular-Webschnittstelle auf **Anwendungseinstellungen** > **Benutzer** > **Verzeichnisdienste** > **Hinzufügen** > **Verzeichnistyp**.
   Die Seite **Verbindung zum Verzeichnisdienst** wird angezeigt.
2. Wählen Sie im **Verzeichnistyp** die Option **LDAP** aus. Die Standardoption ist **AD**.
3. Geben Sie den **Verzeichnisnamen** ein.
4. Wählen Sie die **Domain-Controller-Suche** aus:

Wenn der **Domänen-Controller-Suchtyp DNS** ist, geben Sie den Domänennamen ein.

Wenn der **Domänencontroller-Suchtyp Manuell** ist, geben Sie den FQDN oder die IP-Adresse des Domänen-Controllers ein. Wenn Sie mehrere Server haben, werden maximal drei Server unterstützt, verwenden Sie eine durch Kommas getrennte Liste.

Verwenden Sie den Domain Controller-Suchtyp **DNS**, wenn Sie die Details der Domain-Controller nicht kennen, von denen Sie die Gruppe oder Gruppen importieren möchten. Stellen Sie sicher, dass Sie die folgenden Aufgaben auf der Seite **Netzwerkeinstellungen** durchgeführt haben, um den DNS Domain Controller zu verwenden:

- Aktivieren Sie das Kontrollkästchen **Mit DNS registrieren**.
- Die primäre und die alternative DNS Server-Adressen werden zugewiesen.

Nachdem Sie den Domänennamen eingegeben haben, durchsucht OME-Modular die SRV-Datensätze auf den DNS-Servern, um die Details der Domänen-Controller in dieser Domäne abzurufen.

Wenn Sie die IP-Adresse oder FQDN der Domain-Controller kennen, können Sie einen **manuelle** Domain-Controller-Suchtyp verwenden.

5. Geben Sie den **Bind-DN** und das **Bind-Kennwort** ein.

   **ANMERKUNG:** Anonyme Bindung wird für AD LDS nicht unterstützt.

6. Geben Sie unter **Erweiterte Optionen Server-Port**, **Abgegrenzter Basis-Name zur Suche**, **Attribut der Benutzeranmeldung**, **Attribut der Gruppenmitgliedschaft** und **Suchfilter** ein.

   Die LDAP-Portnummer wird standardmäßig mit 636 befüllt. Geben Sie eine Portnummer ein, um diese zu ändern.

   Geben Sie die im LDAP-System bereits konfigurierten Benutzerattribute ein. Es wird empfohlen, dass die Attribute innerhalb des ausgewählten Basis-DN eindeutig sind. Andernfalls konfigurieren Sie einen Suchfilter, um sicherzustellen, dass die Attribute eindeutig sind. Wenn die Kombination aus Attribut- und Suchfilter den Benutzer-DN nicht eindeutig identifizieren kann, schlägt die Anmeldung fehl.

   Das **Attribut der Gruppenmitgliedschaft** speichert Informationen über Gruppen und Mitglieder im Verzeichnis.

   **ANMERKUNG:** Konfigurieren Sie die Benutzerattribute im für die Abfrage verwendeten LDAP-System vor der Integration in die Verzeichnisdienste.

   **ANMERKUNG:** Geben Sie die Benutzerattribute als `cn` oder `sAMAccountName` für die AD-LDS-Konfiguration und als `UID` für die LDAP-Konfiguration ein.

7. Wählen Sie die **Netzwerkzeitüberschreitung** und die **Suchzeitüberschreitung** aus.

   Das maximal unterstützte Zeitlimit beträgt 300 Sekunden.

8. Aktivieren Sie das Kontrollkästchen **Zertifikatsvalidierung**, wenn Sie das Zertifikat für den Verzeichnisdienst validieren möchten, und wählen Sie das zu validierende Zertifikat aus.

   Das Zertifikat muss ein Stamm-CA-Zertifikat sein, das im Base64-Format kodiert ist.

   Die Option **Verbindung testen** wird aktiviert.

9. Klicken Sie auf **Netzwerkverbindung testen** zur Überprüfung der LDAP-Verbindung.
10. Geben Sie die Bind-Benutzeranmeldeinformationen der Domäne ein, mit der Sie eine Verbindung herstellen möchten.

    **ANMERKUNG:** Stellen Sie beim Testen der Verbindung sicher, dass **Test-Benutzername** den Wert für **Attribut der Benutzeranmeldung** enthält, der zuvor eingegeben wurde.

11. Klicken Sie auf **Verbindung testen**.
    Das Fenster **Verzeichnisdienstinformationen**, das auf eine erfolgreiche Verbindung hinweist, wird angezeigt.
12. Klicken Sie auf **OK** und anschließend auf **Fertigstellen**.
    Es wird ein Job erstellt und ausgeführt, um das angeforderte Verzeichnis auf der Seite **Verzeichnisdienste** hinzuzufügen.

# Bei OME – Modular mithilfe der Verzeichnisbenutzer-Anmeldeinformationen anmelden

So melden Sie sich bei OME – Modular mithilfe der Verzeichnisbenutzer-Anmeldeinformationen an:

Melden Sie sich von der OME – Modular-Anmeldeseite aus mithilfe der AD-Benutzer-Anmeldeinformationen an. Geben Sie gegebenenfalls den Domänennamen ein.

# Importieren von Active Directory- und LDAP-Benutzergruppen

Sie können Active Directory (AD)- und LDAP-Gruppen importieren und sie den vorhandenen OME – Modular-Gruppen zuordnen.

**ANMERKUNG:** Benutzer ohne Administratorrechte können die Active Directory (AD)- und LDAP-Benutzer nicht aktivieren oder deaktivieren.

So importieren Sie die Gruppen:

1. Klicken Sie auf der Listenseite **Benutzer** auf **Verzeichnisgruppe importieren**.
   Das Fenster **Verzeichnis importieren** wird angezeigt.
2. Wählen Sie aus dem Drop-Down-Menü **Verzeichnisquelle** die Quelle aus, von der Sie das AD oder LDAP importieren möchten.
3. Unter **Verfügbare Gruppen** können Sie nach Directory-Gruppen suchen.

   Geben Sie im Textfeld **Gruppe suchen** die ersten Buchstaben des Gruppennamens ein, der im getesteten Verzeichnis verfügbar ist. Eine Liste aller Gruppennamen, die mit dem von Ihnen eingegebenen Text beginnen, wird unten in der Spalte **GRUPPENNAME** angezeigt.
4. Wählen Sie eine Gruppe aus, und klicken Sie auf **>>**.
   Die ausgewählte Gruppe wird unter **Zu importierende Gruppen** angezeigt.

   Um Gruppen zu entfernen, aktivieren Sie das entsprechende Kontrollkästchen für die Gruppe, die Sie entfernen möchten, und klicken Sie auf **<<**.
5. Klicken Sie auf das der Gruppe entsprechende Kontrollkästchen, wählen Sie im Drop-down-Menü **Gruppenrolle zuweisen** die Rolle aus, die Sie der Gruppe zuweisen möchten, und klicken Sie auf **Zuweisen**.
   Den Benutzern in der Gruppe unter dem ausgewählten Verzeichnisdienst werden die ausgewählten Benutzerrollen zugewiesen.
6. Wiederholen Sie die Schritte 3, 4 und 5, falls erforderlich.
7. Klicken Sie auf **Importieren**.
   Die Verzeichnisgruppen werden importiert und in der Liste **Benutzer** angezeigt. Allerdings verwenden alle Benutzer in diesen Gruppen Ihre Domänen-Benutzernamen und -Anmeldeinformationen für die Anmeldung bei OME-Modular.

# Anmelden bei OME-Modular mit OpenID Connect

Die OpenID Connect-Multifaktor-Authentifizierungsfunktion ermöglicht den Nutzern, die beim OpenID Connect-Anbieter (OIDC) registriert sind, den Zugriff auf die OME-Modular-Weboberfläche. Für die Registrierung wird zunächst das OIDC-Konfigurationsdokument über einen RESTful-API-URI abgefragt. Die Informationen aus der Abfrage werden für die Anmeldung bei OME-Modular verwendet.

**ANMERKUNG:** Wenn Sie sich mit den Anmeldeinformationen für den OpenID Connect-Anbieter anmelden, wird der Nutzername im Format **Name@ProviderName@Sub** angezeigt, was möglicherweise zu zusätzlichen Zeichen im Nutzernamen führt.

**ANMERKUNG:** Dell Technologies empfiehlt, bei der Konfiguration des OIDC-Servers den DNS-Namen und den DNS-Namen in der Discovery-URI zu verwenden, anstatt der IP-Adresse. Die Verwendung von DNS-Namen hilft, Einschränkungen bei einigen OIDC-Servern zu vermeiden, bei denen die dynamische Client-Registrierung fehlschlägt, wenn eine Kombination aus IPv6 und initialem Zugriffstoken verwendet wird.

## Wichtige Hinweise

- Sie müssen über die Berechtigung SECURITY_SETUP verfügen, um OIDC-Provider hinzufügen, ändern und löschen zu können. Sie können maximal vier OIDC-Anbieter auf OME-Modular hinzufügen. Die Option **Hinzufügen** ist deaktiviert, wenn bereits vier OIDC-Anbieter hinzugefügt wurden.
- Wenn Sie einen Vorgang zum Hinzufügen oder Beitreten zu einer Gehäusegruppe mit OIDC-Anbietern durchführen, die in Haupt- oder Mitgliedsgehäusen konfiguriert sind, stellen Sie sicher, dass der OIDC-Server über das Gehäuse erreichbar ist.
- Wenn der OIDC-Server nicht erreichbar ist, wird der Registrierungsstatus auch dann als fehlgeschlagen angezeigt, wenn die OIDC-Anbieter erfolgreich vom Hauptgehäuse zu Mitglied übertragen wurden, wenn die Option zur Nutzerauthentifizierung aktiviert ist. Für alle Vorgänge in Verbindung mit OIDC-Anbietern im Haupt- oder Mitgliedsgehäuse muss die Kommunikation zwischen dem OIDC-Server und dem Gehäuse erfolgreich sein.
- Während des Firmware-Upgrade-Prozesses kann die OIDC-Registrierung fehlschlagen, wodurch das Token ablaufen kann. Registrieren Sie in diesem Fall den OIDC-Provider nach dem Firmware-Upgrade-Vorgang neu.
- OIDC-Nutzer, die bei PingFederate registriert sind, müssen sich möglicherweise erneut beim OIDC-Anbieter registrieren, da die folgenden Aktionen die Open ID-Client-Richtlinie, die mit dem Client verbunden ist, auf **Standard** zurücksetzen können.
  - Firmware-Upgrade
  - Änderung der Netzwerkkonfiguration

- Ändern des SSL-Zertifikats

- Die erneute Registrierung beim OIDC-Provider wird möglicherweise auf die Standardrichtlinie zurückgesetzt, die in der PingFederate konfiguriert ist. Um Sicherheitsbedenken nach der Neuregistrierung zu vermeiden, muss der Administrator alle OpenManage Enterprise Client-IDs auf der PingFederate-Site neu konfigurieren. Außerdem wird dringend empfohlen, dass Client-IDs nur für Administrator-Nutzer mit Ping federate erstellt werden, bis dieses Problem behoben ist.

**ANMERKUNG:** Wenn Sie die Firmware des Management-Moduls von 1.30.10 auf 1.30.00 herabstufen, bleiben die verifizierten OpenID Connect-Nutzerdetails nicht erhalten.

Im Folgenden sind die vordefinierten Rollen aufgeführt, die im OIDC-Anbieter konfiguriert werden müssen, damit sich OIDC-Nutzer bei OME-Modular anmelden können:

**Tabelle 8. Vordefinierte Rollen**

| Rollen in OME-Modular | Rollen im OIDC-Anbieter | Beschreibung |
|---|---|---|
| CHASSIS_ADMINISTRATOR | CA | Kann alle Aufgaben im Gehäuse durchführen. |
| COMPUTE_MANAGER | CM | Kann Dienste aus einer Vorlage für Rechnerschlitten bereitstellen und Aufgaben für den Dienst ausführen. |
| STORAGE_MANAGER | SM | Kann Aufgaben auf Speicherschlitten im Gehäuse durchführen. |
| FABRIC_MANAGER | FM | Kann Aufgaben durchführen, die mit Fabrics in Verbindung stehen. |
| VIEWER | VE | Hat schreibgeschützten Zugriff. |

So melden Sie sich mit OpenID Connect bei OME-Modular an:

1. Klicken Sie auf der Seite **Anmelden** auf **Mit OpenID anmelden**.
2. Geben Sie Ihren Nutzernamen und Ihr Kennwort ein, um sich anzumelden. Sobald Ihre Anmeldedaten authentifiziert wurden, werden Sie auf die Seite **OME-Modular-Anmeldung** umgeleitet.

# Hinzufügen von OpenID Connect-Anbieter

So fügen Sie einen OIDC-Anbieter hinzu:

1. Klicken Sie auf der Seite **Anwendungseinstellungen** > **Benutzer** > **OpenID Connect-Anbieter** auf **Hinzufügen**.
   Das Fenster **Neuen OpenID Connect-Anbieter hinzufügen** wird angezeigt.
2. Geben Sie einen **Namen** und eine **Ermittlungs-URI** für den OIDC-Anbieter ein.
3. Wählen Sie den **Authentifizierungstyp** aus.
   Folgende Optionen stehen zur Verfügung:
   - Erstes Zugriffstoken
   - Nutzername

   Ist der **Authentifizierungstyp Erstes Zugriffstoken**, fahren Sie mit Schritt 4 fort. Andernfalls fahren Sie mit Schritt 5 fort.
4. Geben Sie das **Erste Zugriffstoken** ein.
5. Ist der **Authentifizierungstyp Benutzername**, geben Sie den **Benutzernamen** und das **Kennwort** für den OIDC-Anbieter ein.
6. Markieren Sie das Kontrollkästchen **Zertifikatsvalidierung**.
   Die Option **Zertifikate** wird angezeigt.
7. Klicken Sie auf **Durchsuchen**, um zu dem Speicherort zu wechseln, an dem das Zertifikat gespeichert ist, oder ziehen Sie das Zertifikat per Drag und Drop in den markierten Bereich, um es hochzuladen
8. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob die URI- und SSL-Verbindung funktioniert.
9. Wählen Sie das Kontrollkästchen **Aktiviert** , um den OIDC-Anbieter für die Anmeldung bei OME-Modular zu verwenden. Standardmäßig ist das Kontrollkästchen **Aktiviert** ausgewählt.

## Bearbeiten der OpenID Connect-Anbieter

Registrierte Nutzer können die Details bearbeiten oder ändern, einschließlich Name, Ermittlungs-URI, Authentifizierungstyp und andere Informationen. Ein neuer Job führt die Änderungen durch und der Endnutzer kann den Jobstatus abfragen.

So bearbeiten Sie einen OpenID Connect-Anbieter:

1. Wählen Sie auf der Seite **OpenID Connect-Anbieter** die OIDC-Details, die Sie bearbeiten möchten und klicken Sie auf **Bearbeiten**. Das Fenster **OpenID Connect-Anbieter bearbeiten** wird angezeigt.
2. Nehmen Sie die erforderlichen Änderungen vor, und klicken Sie auf **Speichern**.

## Aktivieren eines OpenID Connect-Anbieters

So aktivieren Sie einen OpenID Connect-Anbieter:

1. Wählen Sie auf der Seite **OpenID Connect-Anbieter** den OIDC-Anbieter aus, den Sie aktivieren möchten, und klicken Sie auf **Aktivieren**.
   Sie werden aufgefordert, die Aktivierung des OIDC-Anbieters zu bestätigen.
2. Klicken Sie auf **OK**, um fortzufahren.

## Deaktivieren eines OpenID Connect-Anbieters

So deaktivieren Sie einen OpenID Connect-Anbieter:

1. Wählen Sie auf der Seite **OpenID Connect-Anbieter** den OIDC-Anbieter aus, den Sie löschen möchten, und klicken Sie auf **Deaktivieren**.
   Sie werden aufgefordert, die Deaktivierung des OIDC-Anbieters zu bestätigen.
2. Klicken Sie auf **OK**, um fortzufahren.

## Löschen eines OpenID Connect-Anbieters

Sie können einen oder mehrere OIDC-Anbieter gleichzeitig löschen.

So löschen Sie einen OIDC-Anbieter:

1. Wählen Sie auf der Seite **OpenID Connect-Anbieter** den OIDC-Anbieter aus, den Sie löschen möchten, und klicken Sie auf **Löschen**. Sie werden aufgefordert, das Löschen des OIDC-Anbieters zu bestätigen.
2. Klicken Sie auf **OK**, um fortzufahren.

   Wenn Sie in der MCM-Umgebung OIDC-Anbieter im Hauptgehäuse löschen, werden die Details des Löschauftrags auch im Mitgliedsgehäuse angezeigt.

   Wenn ein Auftrag zum Löschen des OIDC-Anbieters im Mitgliedsgehäuse fehlschlägt, müssen Sie sich beim Mitgliedsgehäuse anmelden, um den OIDC-Anbieter zu löschen.

Wenn Sie einen OIDC-Anbieter löschen, wird die Option zur Anmeldung bei OME-Modular mit OIDC-Anbietern nicht angezeigt.

# OME – Modular-Startseite

Wenn Sie sich bei OME – Modular anmelden, wird die Startseite angezeigt. Die Menüleiste am oberen Rand der OME-Modular-Nutzeroberfläche zeigt Folgendes an:

- den Namen der Anwendung in der oberen linken Ecke.
- Das Textfeld „Suche“
- Anzahl der Jobs
- Anzahl der Warnungen
- Den Namen des angemeldeten Nutzers
- Hilfesymbol
- Informationssymbol

Die Startseite zeigt ein Dashboard mit Informationen auf höchster Ebene über das System und die Unterkomponenten an.

Sie können auch die Jobaktivität und Ereignisse anzeigen. Zum Anzeigen der Jobaktivität klicken Sie auf  , und zum Anzeigen von Ereignissen klicken Sie auf  .

Um wieder zur OME – Modular-Startseite zurückzukehren, klicken Sie auf das OME – Modular-Logo oder auf **Startseite**.

- Grafische Ansicht des Gehäuses – Links auf der Seite wird eine grafische Darstellung der Vorder- und Rückseite des Gehäuses angezeigt. Darin werden alle Module (Schlitten, Lüfter, Netzteile, EAMs und MMS), die im Gehäuse vorhanden sind, gezeigt. Bewegen Sie den Mauszeiger über jedes Modul, um eine kurze Beschreibung und den Funktionszustand des Moduls anzuzeigen. Klicken Sie auf **Geräte anzeigen**, um mehr Details über die Module im Gehäuse zu sehen. Klicken Sie auf **Steckplatzinformationen anzeigen**, um die Anzeige des Widgets auf die Steckplatzinformationen-Liste umzuschalten.
- Steckplatzinformationen anzeigen – In der linken oberen Ecke der Seite wird eine Liste der im Gehäuse vorhandenen Module mit Steckplatzinformationen, Funktionsstatus und einem Link für weitere Details angezeigt. Module in dieser Liste umfassen Rechnerschlitten, Speicherschlitten und EAMs. Klicken Sie auf **Bestandsaufnahme anzeigen**, um mehr Details über die Module im Gehäuse zu sehen. Klicken Sie auf **Gehäuseabbildung anzeigen**, um die Anzeige des Widgets auf die grafische Ansicht des Gehäuses umzuschalten.
- **Gehäuseinformationen**: In der linken Mitte der Seite können Sie eine Zusammenfassung der Gehäuseinformationen anzeigen, z. B. FIPS-Status, Name, Modell, Service-Tag-Nummer, Bestands-Tag, Express-Servicecode, Firmware-Version, Stromzustand, Maximalenergie, Obergrenze, Stromredundanz, Standort und Lizenzen.
- **Gruppeninformationen**: In der unteren linken Ecke der Seite können Sie die Zusammenfassung der Gehäusegruppe anzeigen. Zu den Gruppeninformationen gehören: Gruppenname, Name des Hauptgehäuses, Service-Tag-Nummer des Hauptgehäuses, Hauptgehäuse-IP, Redundanz, Name des Backup-Gehäuses, Service-Tag-Nummer des Backup-Gehäuses, Backup-Gehäuse-IP und Backup-Synchronisationsstatus.
- **Gehäuse-Subsysteme**: In der oberen rechten Ecke der Seite können Sie den Zustand der Komponenten des Gehäuse-Subsystems anzeigen - Batterie, Lüfter, EAM-Steckplatz, MM, Sonstiges, Netzteil, Temperatur, Rechnerschlitten und Speicherschlitten. . Wenn das Subsystem funktionsuntüchtig ist, können Sie in das Feld **Grund** klicken, um eine Liste der Fehlermeldungen anzuzeigen.
- **Warnungen** – In der oberen Mitte der Seite sehen Sie die neuesten Warnungen für Ereignisse im Gehäuse. Klicken Sie auf **Alle anzeigen**, um alle Benachrichtigungen auf der Seite **Warnungen** zu sehen.
- **Kürzlich durchgeführte Aktivitäten**: Unterhalb des Widget **Letzten Warnungen** sehen Sie die letzten Aktivitäten im Gehäuse. Klicken Sie auf **Alle anzeigen**, um alle Aktivitäten auf der Seite **Jobs** zu sehen.
- **Umgebung**: In der unteren rechten Ecke der Seite können Sie die Leistungs- und Temperaturdetails des Gehäuses anzeigen. Klicken Sie auf **Stromverbrauch anzeigen**, um die Details der Stromnutzung des Gehäuses auf der Seite **Hardware** anzuzeigen. Klicken Sie auf **Stromstatistik anzeigen**, um Informationen wie den aktuellen Redundanzzustand, Spitzen-Toleranzbereich, Spitzenstrom, Zeitstempel und Minimalstrom sowie Systemstromverbrauch-Zeitstempel anzuzeigen. Klicken Sie auf **Temperaturstatistik anzeigen**, um die Temperaturinformationen Dauer, Höchsttemperatur Zeitstempel und Mindesttemperatur-Zeitstempel anzuzeigen.

**ANMERKUNG:** Wenn Sie die Bestandsaufnahme aktualisieren und das Gehäuse einschalten, nachdem Sie einen vollständigen AC/DC-Stromkreislauf durchgeführt haben, wird die Bestandsliste des Rechnerschlittens und des EAM nach 3-5 Minuten angezeigt.

**ANMERKUNG:** Wenn Sie die Bestandsaufnahme aktualisieren und das Gehäuse einschalten, nachdem Sie einen vollständigen AC/DC-Stromkreislauf durchgeführt haben, wird die Bestandsliste des Rechnerschlittens und des EAM nach 3-5 Minuten angezeigt.

**ANMERKUNG:** Die maximale Anzahl der Browserverbindungen ist auf drei Verbindungen pro Domäne beschränkt. Das mehrmalige Starten der Konsole innerhalb desselben Browsers führt zu einem Fehler. Schließen Sie alle nicht verwendeten Sitzungen und aktualisieren Sie die Seite.

# Suchfunktion in OME-Modular

Die Suchfunktion ermöglicht Ihnen, nach Informationen zu Jobs, Geräten, Warnmeldungen, Links, Warnmeldungsrichtlinien, Benutzern und Auditprotokollen zu suchen. Die Funktion ist nur in Englisch verfügbar und unterscheidet zwischen Groß- und Kleinschreibung. Sie können bei der Eingabe nach Datensätzen suchen. Beispiel: Wenn Sie nach Warnmeldungen suchen und mit der Eingabe des Wortes beginnen möchten, schlägt OME-Modular die passenden Begriffe vor.

Die Suchfunktion unterstützt:

- maximal 255 Zeichen, einschließlich Sonderzeichen.
  - Folgende Sonderzeichen werden unterstützt: #, @,%, -,:, =, &, $, +, |, /,., _, ( und ).
  - Folgende Sonderzeichen werden nicht unterstützt: *, <, >, {,}, ^, ~, [,], ',,?, ", \ und ‘

  **ANMERKUNG:** Die Suchfunktion unterstützt keine Rechtschreibfehler.

  Sie können die Sonderzeichen als Präfix und Suffix für den Suchtext verwenden. Wenn Sie z. B. über die ID nach einem Gerät suchen, aber nur einen Teil der Geräte-ID kennen, können Sie mit einem Platzhalterzeichen am Anfang und am Ende der ID nach dem Gerät suchen, z. B.: *911*. Die Ergebnisse der Suche werden unter dem Such-Textfeld angezeigt.

- Inkrementelle Suche: Die Ergebnisse werden während der Eingabe des Suchtexts angezeigt. Wenn Sie z B. „con..“ eingeben, um nach Konfigurationsdatensätzen zu suchen, werden die entsprechenden Einträge in Form einer Liste angezeigt.
- Mehrere z. B. durch eine Oder-Bedingung verknüpfte Wörter: Suchwörter werden durch Leerzeichen getrennt. Beispiele:
  - Verwenden Sie die Begriffe, die Service-Tag-Nummer oder die IDs, um Geräte nach Service-Tag-Nummern oder IDs zu suchen.
  - Verwenden Sie die Begriffe „Firmware“ oder „Warnmeldungen“, um nach Aufgaben zu suchen, die im Zusammenhang mit Firmwareupdates stehen.
- Platzhaltersuche: OME-Modular unterstützt die Suffix- und Präfix-Platzhalter-Suche nach Datensätzen. Wenn Sie nach einem bestimmten Modell eines Geräts suchen, aber nur ein Teil des Modells kennen, z. B. 5108, können Sie die Teilinformationen eingeben. Eine Suche wird unter Verwendung der Platzhalterzeichen als – Präfix und Suffix – *5108* ausgeführt.

  **ANMERKUNG:** Bei einer Gruppe von Eingabe-Suchzeichen, die durch Leerzeichen getrennt sind, ist die Platzhaltersuche nur auf die letzte Zeichenfolge anwendbar. Beispiel: str1 str2 str3 str4 wird als str1 str2 str3 *str4* behandelt.

Die relevantesten Ergebnisse werden in einer Liste angezeigt. Klicken **Weitere anzeigen**, um alle Datensätze anzuzeigen. Aktivieren oder deaktivieren Sie die Kontrollkästchen der Komponenten, die Sie in die Suchergebnisse aufnehmen oder aus diesen ausschließen möchten. Standardmäßig sind alle Optionen aktiviert. Klicken Sie auf einen Suchergebnisdatensatz, um zur Seite **Warnungsprotokoll** zu gelangen.

Sie können die Suchfunktion wie in den folgenden Beispielen beschrieben verwenden:

- Suche nach Jobs mithilfe der Job-IDs.
- Suche nach Geräten mit der MAC-Adresse des Geräts als Suchtext.
- Suche nach Warnmeldungen unter Verwendung von Teilen der Warnmeldung wie z. B. Benachrichtigung-IDs.
- Suche nach IP-Adressen.
- Durchsuchen des Auditprotokolls auf Informationen aus Protokollen.

Sie können Felder, die auf den Seiten des OME-Moduls angezeigt werden, verwenden, um mithilfe der Suchfunktion nach Informationen zu suchen. Die Felder sind in der folgenden Tabelle aufgeführt.

| Seitenname | Felder |
|---|---|
| **Jobs** | • Name<br>• Beschreibung<br>• Mögliche Einstellungen: Aktiviert, Deaktiviert<br>• Letzter Ausführungsstatus<br>• Erstellt von/Aktualisiert von |
| **Warnungsprotokoll** | • Meldung<br>• Kategorie<br>• Definition<br>• Schweregrad<br>• Status<br>• Gerät<br>  ○ Modell<br>  ○ Kennung<br>  ○ Typ<br>  ○ Gerätemanagement: MAC-Adresse, Netzwerkadresse, Gerätename und Erkennungsprofil |
| **Auditprotokoll** | • Kategorie<br>• IP-Adresse<br>• Meldung<br>• Meldungsschnittstelle<br>• Schweregrad<br>• Nutzername |
| **Hilfe** | • Titel<br>• Inhalt |
| **Warnungsrichtlinie** | • Name<br>• Beschreibung<br>• Mögliche Einstellungen: Aktiviert, Deaktiviert |
| **Nutzer** | • Typ<br>• Verzeichnisserver-Typ |

| Seitenname | Felder |
|---|---|
| | • Name<br>• Beschreibung<br>• E-Mail<br>• Mögliche Einstellungen: Aktiviert, Deaktiviert |
| **Alle Geräte** | • Globaler Status<br>• Modell<br>• Kennung<br>• Typ<br>• Stromzustand<br>• IP-Adresse<br>• Bestands-Tag<br>• Service-Tag-Nummer des zugehörigen Gehäuses<br>• Bestandsaufnahme<br>• Standort: Beschreibung, Name, Details<br>• Software: Beschreibung, Instanz-ID, PCI-Geräte-ID, Softwaretyp, Status, Untergeräte-ID, Unterlieferanten-ID, Hersteller-ID, Version<br>• Lizenz: Zugewiesenes Gerät, Berechtigungs-ID, Beschreibung, Lizenztyp |
| **Gerätemanagementinformationen** | • MAC-Adresse<br>• Netzwerkadresse<br>• Gerätename<br>• Erkennungsprofil |

# Anzeigen von Warnungen

Im Abschnitt **Warnungen** werden die bestimmtem Typen von Warnungen angezeigt, z. B. Kritisch, Warnung und Unbekannt. Sie können auch Warnungen für bestimmte Gerätetypen anzeigen, wie z. B. Gehäuse, Rechner-, Netzwerk- und Speicherschlitten.

# Jobs und Aktivitäten anzeigen

Im Abschnitt **Kürzlich durchgeführte Aktivitäten** wird eine Liste der letzten Jobs und Aktivitäten und ihr Status angezeigt. Klicken Sie auf **Alle Aktivitäten**, um zur Seite **Jobs** zu wechseln und detaillierte Informationen zu den Jobs anzuzeigen.

# Verwaltungs-Dashboard für mehrere Gehäuse

Mehrere Gehäuse sind gruppiert, um Domänen zu bilden, die MCM (Multi-Chassis Management)-Gruppen genannt werden. Eine MCM-Gruppe kann aus 20 Gehäusen bestehen, wobei eines davon das Hauptgehäuse ist und die übrigen 19 Mitglieder sind. OME – Modular unterstützt drahtgebundene MCM-Gruppen, in der die Gehäuse über einen redundanten Port am Verwaltungscontroller linear verkabelt.

In einer Multi-Chassis Management (MCM)-Gruppe werden die Anzahl der Ereignisse und Jobs für die gesamte Gruppe angezeigt. Die Abschnitte **Gerätezustand**, **Warnungen** und **Kürzlich durchgeführte Aktivitäten** zeigen die konsolidierten Details aller Geräte in der Gruppe.

**ANMERKUNG:** Halten Sie zwischen dem Entfernen und Einsetzen jedes Geräts ein Mindestintervall von zwei Minuten ein.

## MCM-Startseite anzeigen

Sie können die folgenden Informationen über die MCM-Gruppe anzeigen:

- MCM-Gruppe: Sie können Folgendes anzeigen:
  - Name der Gruppe
  - Die Topologie der Gruppe über **Topologie anzeigen**
  - Name, IP-Adresse und Service-Tag-Nummer des Hauptgehäuses

- Name, IP-Adresse und Service-Tag-Nummer der Mitgliedsgehäuse

- **Gerätezustand** – Zeigt den Funktionszustand der Gehäuse-Untersysteme an: Gehäuse, Rechnerschlitten, Netzwerk und Speicher. Sie können auf den Funktionszustand der einzelnen Geräte oder auf **Alle Geräte** klicken, um eine Zusammenfassung der auf der Seite **Alle Geräte** angezeigten Geräte zu erhalten.
- **Warnungen** – Zeigt die letzten Warnungen für Ereignisse im Hauptgehäuse und in den Untersystemen an. Klicken Sie auf **Alle Warnungen**, um die Seite **Warnungen** für die Haupt- und Mitgliedsgehäuse anzuzeigen.
- **Kürzlich durchgeführte Aktivitäten** – Zeigt die letzten Aktivitäten an, die im Hauptgehäuse und den Untersystemen aufgetreten sind. Klicken Sie auf **Alle Aktivitäten**, um die Seite **Jobs** für das Haupt- und Mitgliedsgehäuse aufzurufen.

**ANMERKUNG:** Wenn ein Mitgliedsgehäuse basierend auf einer „Gruppe beitreten"-Anforderung vom Mitgliedsgehäuse zu einer Gehäusegruppe hinzugefügt wird, wird der Status des Mitgliedsgehäuses auf dem MCM-Dashboard eine Zeit lang als „Unbekannt" angezeigt.

### Listen von Gehäusen in einer MCM-Gruppe anzeigen

Auf der OME – Modular-Startseite wird die Liste der Gehäuse, die Teil der Gruppe sind, auf der linken Seite angezeigt. Die Liste zeigt das Modell, die IP-Adresse und die Service-Tag-Nummer des Gehäuses an. Das Hauptgehäuse ist gekennzeichnet, um eine leichtere Identifizierung zu ermöglichen. Klicken Sie auf den Namen des Gehäuses, um auf die spezifischen Details des Gehäuses zuzugreifen. Sie können auch über die aufgeführte IP-Adresse direkt auf die OME – Modular-Webschnittstelle des Gehäuses zugreifen.

## Systemzustand anzeigen

Die Seite **Geräte** > **Alle Geräte** zeigt eine Zusammenfassung des Zustands des Gehäuses, der Rechner- und Speicherschlitten und der Netzwerkkomponenten an.

Am unteren Rand der Seite **Alle Geräte** finden Sie eine Liste aller Geräte. Sie können ein Gerät auswählen, um rechts von der Liste eine Zusammenfassung anzuzeigen. Sie können diese Liste mithilfe der Optionen **Erweiterte Filter** filtern:

Auf der Seite **Alle Geräte** können Sie auch Folgendes ausführen:

- Betriebsschalter
- Aktualisieren Sie die Firmware.
- Blink LED
- Bestandsaufnahme aktualisieren

**ANMERKUNG:** Wenn Sie eine Anfrage zum Verlassen einer Gehäusegruppe initiieren, während das Update der Bestandsaufnahme durchgeführt wird, wird auf der Seite „Alle Geräte" eine Fehlermeldung angezeigt, selbst wenn die Task **Gehäusegruppe verlassen** erfolgreich ist.

**ANMERKUNG:** Wenn ein Rechnerschlitten in ein Gehäuse eingesetzt wird, wird mitunter die Meldung "Kein Geräteimage gefunden" angezeigt. Um dieses Problem zu beheben, aktualisieren Sie die Bestandsaufnahme des Rechnerschlittens manuell.

**ANMERKUNG:** Wenn Sie die Bestandsaufnahme aktualisieren und das Gehäuse einschalten, nachdem Sie einen vollständigen AC/DC-Stromkreislauf durchgeführt haben, wird die Bestandsliste des Rechnerschlittens und des EAM nach 3-5 Minuten angezeigt.

## Gehäuse einrichten

Wenn Sie sich zum ersten Mal an der OME – Modular-Webschnittstelle anmelden, wird der Konfigurationsassistent angezeigt. Wenn Sie den Assistenten schließen, können Sie durch Klicken auf **Konfigurieren** > **Erstkonfiguration** erneut darauf zugreifen. Diese Option wird nur angezeigt, wenn das Gehäuse noch nicht konfiguriert ist.

So konfigurieren Sie das Gehäuse:

1. Melden Sie sich bei OME – Modular an.
   Die **Startseite** wird angezeigt.
2. Klicken Sie auf **Konfigurieren** > **Erstkonfiguration**.
   Der **Gehäuse-Bereitstellungsassistent** wird angezeigt.

   Weitere Schritte finden Sie unter Erstkonfiguration.

# Erstkonfiguration

Dell EMC empfiehlt den folgenden Konfigurationsschwellenwert, um die Leistung des Gehäuses zu verbessern. Wenn die Konfiguration den Schwellenwert überschreitet, funktionieren einige Merkmale wie Firmwareupdate, Sicherung und Wiederherstellung möglicherweise nicht wie erwartet. Dies kann auch die Systemleistung beeinträchtigen.

| Komponente | Anzahl |
|---|---|
| **Vorlagen** | 320 |
| **Warnungsrichtlinie** | 50 |
| **Identitäts-Pools** | 501 |
| **Netzwerk (VLAN)** | 214 |
| **Katalog** | 50 |
| **Baseline** | 50 |

So konfigurieren Sie ein Gehäuse:

1. Klicken Sie auf **Geräte** > **Gehäuse** > **Details anzeigen** > **Konfigurieren** > **Erstkonfiguration**.
   Der **Gehäuse-Bereitstellungsassistent** wird angezeigt.
   **ANMERKUNG:** Sie können das Gehäuse unter Verwendung eines vorhandenen Gehäuse-Profils konfigurieren.
2. Klicken Sie auf der Registerkarte **Profil importieren** auf **Importieren** und öffnen das Fenster **Profil importieren**.
   Geben Sie die Einzelheiten der Netzwerkfreigabe an, auf der sich das Gehäuseprofil befindet, und klicken Sie auf **Importieren**.
3. Auf der Registerkarte **Zeitkonfiguration** wählen Sie die Option **Zeiteinstellungen konfigurieren** aus, um die Zeitzone und den Zeitstempel der Konfiguration festzulegen.
4. Markieren Sie das Kontrollkästchen **NTP verwenden**, um die primäre, sekundäre oder tertiäre NTP-Serveradresse zu konfigurieren, und klicken Sie auf **Weiter**.
   **ANMERKUNG:** Es wird empfohlen, zur Gewährleistung einer zuverlässigen Synchronisierung mindestens drei gültige NTP-Server zu verwenden, die mit einer einzigen Zeitquelle synchronisiert werden.

   Wenn Sie mehrere NTP-Server auswählen, wählt OME – Modular den NTP-Server nach einem algorithmischen Verfahren.

   Die Registerkarte **Aktivität und Warnungen** wird angezeigt.
5. Konfigurieren Sie die E-Mail-, SNMP- und Systemprotokoll-Einstellungen und klicken Sie auf **Weiter**.
   Die Registerkarte **iDRAC** wird angezeigt.
6. Aktivieren Sie das Kontrollkästchen **Konfiguration von iDRAC Quick Deploy Settings**, um das Kennwort zum Zugriff auf die iDRAC-Webschnittstelle und die Management-IP zu konfigurieren, und klicken Sie auf **Weiter**.
   Sie können die Steckplätze auswählen, auf die die iDRAC Quick Deploy-Einstellungen angewendet werden müssen.

   Die Registerkarte **Netzwerk-EAM** wird angezeigt.
7. Aktivieren Sie das Kontrollkästchen **Quick Deploy-Einstellungen des E/A-Moduls konfigurieren**, um das Kennwort zum Zugriff auf die EAM-Konsole und die Management-IPs zu konfigurieren, und klicken Sie auf **Weiter**.
   Die Registerkarte **Firmware** wird angezeigt.
8. Markieren Sie das Kontrollkästchen **Alle Geräte für die Verwendung des folgenden Katalogs konfigurieren**, um die Netzwerkfreigabe auszuwählen, und klicken Sie auf **Katalog**, um das Fenster **Firmwarekatalog hinzufügen** zu öffnen.
9. Geben Sie einen Namen für den Katalog ein, wählen Sie die Katalogquelle aus, und klicken Sie auf **Fertig stellen**, um die Änderungen zu speichern und zum **Gehäuse-Bereitstellungsassistenten** zurückzukehren.
10. Klicken Sie auf **Weiter** zum Anzeigen der Registerkarte **Proxy**, und konfigurieren Sie die Proxy-Einstellungen.
    OME – Modular verwendet die Proxy-Einstellungen für den Zugriff auf die Dell EMC Website für die neuesten Kataloge. Sie können auch die HTTPS-Proxy-Einstellungen und Proxy-Authentifizierung aktivieren.
11. Klicken Sie auf **Weiter**, um die Registerkarte **Gruppendefinition** anzuzeigen.
12. Wählen Sie **Gruppe erstellen**, um die Gehäuse-Gruppeneinstellungen zu konfigurieren.
13. Klicken Sie auf **Weiter**, um die Registerkarte **Zusammenfassung** anzuzeigen.
    **ANMERKUNG:** Warten Sie nach dem Einrichten der Uhrzeit im Hauptgehäuse, bis die Uhrzeit des Hauptgehäuses und des Mitgliedsgehäuses synchronisiert wurden, bevor Sie weitere Vorgänge ausführen. Die Konfiguration der Uhrzeit kann störend sein.

# Gehäuseeinstellungen konfigurieren

Sie können die folgenden Einstellungen eines Gehäuses konfigurieren:

- Stromverbrauch
- Netzwerk
- Netzwerkdienste
- Remotezugriffskonfiguration
- Speicherort
- Quick Deploy

## Stromversorgung des Gehäuses konfigurieren

So konfigurieren Sie die Energieeinstellungen des Gehäuses:

1. Klicken Sie auf **Geräte** > **Gehäuse** > **Details anzeigen** > **Einstellungen** > **Strom**.
   Der Abschnitt **Stromkonfiguration** wird erweitert.
2. Wählen Sie **Stromobergrenze aktivieren**, um die maximale Stromverbrauchskapazität für das Gehäuse festzulegen. Die **Stromobergrenze** legt den Stromverbrauch des Gehäuses fest. Wird die Stromobergrenze erreicht, werden die Schlitten basierend auf der Stromriorität gedrosselt. Sie können die Kapazität in Watt, BTU/h oder einem Prozentsatz angeben. Diese **Stromobergrenze** wird nur angezeigt, wenn das Kontrollkästchen **Stromobergrenze aktivieren** aktiviert ist. Die empfohlene Stromobergrenze beträgt 0 bis 32767 Watt bzw. 0 bis 100 %. Wenn Sie die Stromobergrenze in BTU/h ändern, ändert sich auch die Stromobergrenze in W.

   Das MX7000-Gehäuse unterstützt sowohl AC- (High Line-220V und Low Line-110V) als auch DC-Stromversorgungseingangstypen.
3. Im Abschnitt **Redundanzkonfiguration** wählen Sie die erforderliche Redundanzregel aus.

   Richtlinien zur Stromredundanz erleichtern die Verwaltung des Stromverbrauchs und die Überbrückung von Stromausfällen im Gehäuse. Folgende Optionen stehen zur Verfügung:
   - **Keine Redundanz:** Bei dieser Richtlinie wird die Strombelastung des Gehäuses auf alle Netzteile verteilt. Bei **Keine Redundanz** gibt es keine speziellen Anforderungen für die PSU-Bestückung. Der Zweck der Richtlinie **Keine Redundanz** ist die höchstmögliche Grenze für die Stromversorgung von Geräten, die zum Gehäuse hinzugefügt werden. Bei Ausfall eines oder mehrerer Netzteile schränkt das Gehäuse die Leistung ein, um den Betrieb innerhalb der Stromversorgungskapazitäten der verbleibenden Netzteile aufrechtzuerhalten.
   - **Netzredundanz:** Bei dieser Richtlinie wird die Strombelastung des Gehäuses auf alle Netzteile verteilt. Die sechs Netzteile sind in zwei Gruppen unterteilt: Netz A besteht aus den Netzteilen 1, 2, 3 und Netz B besteht aus den Netzteilen 4, 5 und 6. Es wird empfohlen, die Netzteile in der folgenden Reihenfolge zu bestücken: 1, 4, 2, 5, 3, 6, wobei die gleiche Anzahl an Netzteilen in jedem Netz für Netzredundanz optimiert ist. Das Netz mit der größten Netzteilkapazität bestimmt die Grenze für die Stromversorgung von Geräten, die zum Gehäuse hinzugefügt werden. Beim Ausfall eines Netzes oder Netzteils wird die Strombelastung des Gehäuses zwischen den verbleibenden Netzteilen aufgeteilt mit der Absicht, dass ein einziges funktionsfähiges Netz das System weiterhin ohne Leistungsbeeinträchtigung versorgt.
   - **Netzteilredundanz:** Bei dieser Richtlinie wird die Strombelastung des Gehäuses auf alle Netzteile verteilt. Es gibt keine speziellen Anforderungen für die PSU-Bestückung für redundante Netzteile. Netzteilredundanz wird für eine Bestückung von sechs Netzteilen optimiert und das Gehäuse beschränkt die Stromversorgung von Geräten so, dass sie in fünf Netzteile passt. Wenn ein einziges Netzteil ausfällt, wird die Strombelastung des Gehäuses ohne Leistungsbeeinträchtigung auf die verbleibenden Netzteile verteilt. Wenn weniger als sechs Netzteile vorhanden sind, schränkt das Gehäuse die Stromversorgung von Geräten so ein, dass sie in alle bestückten Netzteile passt. Bei Ausfall eines einzelnen Netzteils schränkt das Gehäuse die Leistung ein, um den Betrieb innerhalb der Stromversorgungskapazitäten der verbleibenden Netzteile aufrechtzuerhalten.
4. Wählen Sie im Abschnitt **Hot Spare-Konfiguration Hot Spare aktivieren**, um das Primärnetz des Hot Spare zu konfigurieren.

   Die Hot Spare-Funktion erleichtert die Spannungsregelung, wenn die Stromauslastung der Stromversorgungseinheit (PSU) unter Berücksichtigung der Gesamtausgabekapazität der PSU niedrig ist. Standardmäßig ist die Hot Spare-Funktion aktiviert. Wenn die Hot Spare-Funktion aktiviert ist, wird eine redundante PSU in den Ruhezustand versetzt, wenn die Stromauslastung niedrig ist. Die Hot Spare-Funktion ist nicht aktiviert, wenn:
   - die PSU-Redundanz inaktiv ist,
   - das Strombudget der Systemkonfiguration die PSU-Ausgabekapazität überschreitet,
   - die Netzredundanzrichtlinie nicht ausgewählt ist.

   Die MX7000-Netzteile unterstützen die Hot Spare-Funktion mit drei PSU-Paaren. Mit dieser Funktion kann ein PSU-Paar ein aktives Netzteil und ein Netzteil im Energiesparmodus umfassen, während der Stromverbrauch des Gehäuses niedrig ist und die drei PSU-Paare alle Anforderungen an die Stromversorgung des Gehäuses erfüllen. Dies ermöglicht eine effiziente Energienutzung, wenn der

gesamte Strombedarf des Gehäuses niedrig ist. Die Partner-PSU weckt die gekoppelte PSU aus dem Energiesparmodus, indem sie ein Aktivierungssignal sendet, wenn der Strombedarf des Gehäuses ansteigt. Die PSU-Paare für MX7000 sind: 1 & 4, 2 & 5 und 3 & 6.

5. Wählen Sie unter der Option **Primärnetz** die PSU, auf der Sie die Hot Spare-Funktion aktivieren wollen, aus der Drop-Down-Liste aus.
6. Klicken Sie auf **Anwenden**, um die Stromeinstellungen des Gehäuses zu speichern.

# Gehäusemanagementnetzwerk konfigurieren

Sie können die Netzwerkeinstellungen für die Verwaltungsmodule konfigurieren, die in ein MX7000-Gehäuse eingesetzt werden.

- LAN/NIC-Schnittstelle
- IPv4
- IPv6
- DNS-Informationen
- Verwaltungs-VLAN

So konfigurieren Sie das Gehäusenetzwerk:

1. Klicken Sie auf **Geräte** > **Gehäuse** > **Details anzeigen** > **Einstellungen** > **Netzwerk**.
   Der Abschnitt **Netzwerkkonfiguration** wird erweitert.
2. Im Abschnitt **Allgemeine Einstellungen** können Sie die NIC, **Mit DNS registrieren** und **Automatische Verhandlung** aktivieren oder deaktivieren. Standardmäßig ist das Kontrollkästchen **NIC aktivieren** aktiviert.

   Wenn Sie die Option **Registrierung bei DNS** aktivieren, geben Sie den **DNS-Namen** des Gehäuses ein, das Sie bei einem DNS-Server registrieren möchten. Sie können auf OME-Modular mit dem vorhandenen FQDN zugreifen, auch wenn die Option **Mit DNS registrieren** in der Anwendung deaktiviert ist. Dies liegt daran, dass die frühere Option je nach konfigurierter TTL (Time To Live) im Netzwerk-Cache oder im DNS-Server-Cache verbleibt.

   **ANMERKUNG:** Der Zugriff auf den FQDN ist nur temporär möglich.

   **ANMERKUNG:** Löschen Sie den Cache im DNS, nachdem **Registrieren mit DNS** deaktiviert wurde, um die Protokollierung mit der FQDN-Adresse zu verhindern.

   **ANMERKUNG:** Wenn die Option **Registrieren mit DNS** aktiviert ist, können Sie die Option **VLAN aktivieren** nicht ändern.
3. Geben Sie den **DNS-Namen** ein. Ein DNS-Name darf maximal 58 Zeichen enthalten. Das erste Zeichen muss ein alphanumerisches Zeichen (a-z, A-Z, 0-9) sein, gefolgt von einem numerischen Zeichen oder einem Bindestrich (-).
4. Aktivieren oder deaktivieren Sie die Option **DHCP für den Domänennamen verwenden** und aktivieren oder deaktivieren Sie die **Automatische Verhandlung**.

   Wenn die Option **DHCP für den DNS-Domänennamen verwenden** deaktiviert ist, geben Sie den **DNS-Domänennamen** ein.

   **ANMERKUNG:** Sie können **DHCP für den DNS-Domänennamen verwenden** nur aktivieren, wenn für IPv4 oder IPv6 DHCP konfiguriert ist. OME – Modular erhält seinen DNS-Domänennamen von einem DHCP- oder DHCPv6-Server, wenn **DHCP für den DNS-Domänennamen verwenden** aktiviert ist.

   Wenn **Automatische Verhandlung** falsch oder deaktiviert ist, können Sie die Geschwindigkeit des Netzwerkanschlusses wählen.

   **ANMERKUNG:** Das Einstellen der **Automatischen Verhandlung** auf „falsch“ und die Auswahl einer Netzwerk-Port-Geschwindigkeit kann dazu führen, dass das Gehäuse die Verbindung zum Netzwerkswitch in der Oberseite des Racks oder zum Nachbargehäuse verliert, wenn MCM ausgeführt wird. Es wird empfohlen, die **Automatische Verhandlung** für die meisten Anwendungsfälle auf „richtig“ einzustellen.

**Tabelle 9. Supportmatrix für Oberseite des Racks für Managementmodul und Management-Modul-Uplink**

| Switch-Konfiguration für Oberseite des Racks | Konfiguration des Managementmoduls | Unterstützt für Management Modul Uplink (Ja oder Nein) |
|---|---|---|
| 100 Mbit/s (Automatische Aushandlung AUS) | 100 Mbit/s (Automatische Aushandlung AUS) | JA |
| 10 Mbit/s (Automatische Aushandlung AUS) | 10 Mbit/s (Automatische Aushandlung AUS) | JA |
| Aut. Aushandlung EIN | Automatische Aushandlung EIN | JA |

**Tabelle 9. Supportmatrix für Oberseite des Racks für Managementmodul und Management-Modul-Uplink (fortgesetzt)**

| Switch-Konfiguration für Oberseite des Racks | Konfiguration des Managementmoduls | Unterstützt für Management Modul Uplink (Ja oder Nein) |
|---|---|---|
| 100 Mbit/s (Automatische Aushandlung AUS) | Automatische Aushandlung EIN | NEIN |
| 10 Mbit/s (Automatische Aushandlung AUS) | Automatische Aushandlung EIN | NEIN |
| Automatische Aushandlung EIN | 100 Mbit/s (Automatische Aushandlung AUS) | NEIN |
| Automatische Aushandlung EIN | 10 Mbit/s (Automatische Aushandlung AUS) | NEIN |

5. Im Abschnitt **IPv4-Einstellungen** konfigurieren Sie Folgendes:
   - **IPv4 aktivieren**
   - **DHCP aktivieren**
   - **IP-Adresse**
   - **Subnetzmaske**
   - **Gateway**
   - **DHCP zum Abrufen von DNS-Serveradressen verwenden**
   - **Statisch, bevorzugter DNS-Server**
   - **Statisch, alternativer DNS-Server**
6. Im Abschnitt **IPv6-Einstellungen** konfigurieren Sie Folgendes:
   - **IPv6 aktivieren**
   - **Autokonfiguration aktivieren**
   - **IPv6-Adresse**
   - **Präfixlänge**
   - **Gateway**
   - **DHCPv6 zum Abrufen von DNS-Serveradressen verwenden**
   - **Statisch, bevorzugter DNS-Server**
   - **Statisch, alternativer DNS-Server**

   **ANMERKUNG:** Die statische IPv6-IP-Adresse, die bereits konfiguriert wurde, wird in OME-Modular angewendet und angezeigt, wenn die Konfiguration von statischer zu DHCP-IP geändert wird.
7. Aktivieren oder deaktivieren Sie das VLAN für das Gehäuse. Sie können die VLAN-Einstellungen nur dann konfigurieren, wenn das Kontrollkästchen **Mit DNS registrieren** deaktiviert ist.

   Sie können von einem VLAN-Netzwerk auf ein nicht-VLAN-Netzwerk oder von einem nicht-VLAN-Netzwerk auf ein VLAN-Netzwerk verschieben, jedoch nur wenn **Mit DNS registrieren** nicht markiert ist.

   Standardmäßig sind die IPv4-Einstellungen aktiviert und die DNS-Registrierung ist mit einem Standardnamen deaktiviert. Sie können den Namen unter Verwendung einer beliebigen lokalen Schnittstelle wie z. B. OpenManage Mobile ändern.

   **ANMERKUNG:** Stellen Sie sicher, dass beim Ändern des VLAN-Status das Netzwerkkabel an den richtigen Anschluss angeschlossen ist, damit die Änderung wirksam wird.

   Isolieren Sie die Gehäuseverwaltung vom Netzwerk, da die Betriebszeit eines Gehäuses, das nicht ordnungsgemäß in Ihre Umgebung integriert ist, nicht unterstützt oder garantiert werden kann. Wegen des möglichen Datenverkehrs im Datennetzwerk sind die Verwaltungsschnittstellen im internen Verwaltungsnetzwerk vom für Server bestimmten Datenverkehr überlastet. Dies führt zu Verzögerungen in der Kommunikation von OME – Modular und iDRAC. Diese Verzögerungen können zu einem unvorhersehbaren Gehäuseverhalten führen, wie etwa die Anzeige von OME – Modular durch iDRAC als offline, obwohl es arbeitet, was wiederum weiteres unerwünschtes Verhalten verursacht. Falls es nicht möglich ist, das Verwaltungsnetzwerk physisch zu isolieren, besteht noch die Möglichkeit, den OME – Modular- und iDRAC-Datenverkehr auf ein separates VLAN umzuleiten. Die OME – Modular- und einzelnen iDRAC-Netzwerkschnittstellen können für die Verwendung eines VLAN konfiguriert werden.

   **ANMERKUNG:** Jede Änderung der Attributeinstellungen führt zu einem Verlust der IP-Adresse oder einer vorübergehenden Nichtverfügbarkeit der OME – Modular-Webschnittstelle. Die OME – Modular-Webschnittstelle wird jedoch automatisch wiederherstellt.

8. Klicken Sie auf **Anwenden**, um die Gehäusenetzwerkeinstellungen zu speichern.

## Gehäusenetzwerkdienste konfigurieren

Die Konfiguration der Gehäusenetzwerkdienste umfasst SNMP-, SSH- und Remote-RACADM-Einstellungen.

So konfigurieren Sie die Netzwerkdienste:

1. Klicken Sie auf **Geräte** > **Gehäuse** > **Details anzeigen** > **Einstellungen** > **Netzwerkdienste**.
   Der Abschnitt **Netzwerkdienste** wird erweitert.
2. Aktivieren Sie im Abschnitt **SNMP-Einstellungen** das Kontrollkästchen **Aktiviert**, um die SNMP-Einstellungen zu aktivieren, und wählen Sie die **Portnummer** aus.
   Die Portnummer kann zwischen 10 und 65535 liegen.
   **ANMERKUNG:** Für SNMP-Vorgänge konfigurieren Sie die Timeout-Parameter auf dem Client, um die erfolgreiche Fertigstellung der Task zu vereinfachen. Möglicherweise müssen Sie die Timeout-Parameter basierend auf der Netzwerklatenz anpassen.
3. Geben Sie den SNMP **Community-Namen** ein. Der Community-Name darf maximal 32 Zeichen enthalten.
4. Laden Sie die **MIB-Datei (Management Information Base)** auf ein lokales Laufwerk auf Ihrem System herunter.
5. Markieren Sie im Abschnitt **SSH-Einstellungen** das Kontrollkästchen **Aktiviert**, um die SSH-Einstellungen zu aktivieren, und wählen Sie die maximale Anzahl von SSH-Sitzungen aus.
   Standardmäßig kann ein Gehäuse eine maximale Anzahl von vier SSH-Sitzungen haben.
6. Wählen Sie **Max. Authentifizierungsversuche**, um die Anzahl der Versuche festzulegen, falls die SSH-Sitzung nicht erfolgreich ist. Standardmäßig beträgt die maximale Anzahl der Versuche für die Autorisierung drei, kann aber auf bis zu neun erhöht werden.
7. Geben Sie das **Idle Timeout** in Sekunden ein, die sich eine SSH-Sitzung im Leerlauf befinden kann. Die SSH-Sitzung läuft basierend auf der Timeout-Konfiguration ab und das standardmäßige Inaktivitäts-Timeout beträgt 30 Minuten. Wenn eine Änderung im Gehäusemanagementnetzwerk erfolgt, werden alle aktiven Sitzungen, die auf der Seite „Benutzersitzungen“ aufgeführt sind, nicht automatisch beendet.
   Der Standard- oder Mindestwert für die
   Autorisierungsversuche ist drei und der Höchstwert neun.
   **ANMERKUNG:** Die Auditprotokolle werden nicht erzeugt, wenn die Sitzung basierend auf dem Inaktivitäts-Timeout abläuft.
8. Geben Sie die SSH **Portnummer** an. Die Portnummer kann zwischen 10 und 65535 liegen.
   Die Standardportnummer ist 22.
9. Aktivieren Sie die Remote-RACADM-Sitzung für das Gehäuse.
   Sie können die Remote-RACADM-Option in der Weboberfläche nur dann anzeigen, wenn Sie über Rechte als Gehäuseadministrator verfügen.
   **ANMERKUNG:** Ein Protokoll für die Remote-RACADM-Sitzung (Anmeldung oder Abmeldung) wird auf der Seite **Auditprotokolle** angezeigt, unabhängig vom Remote-RACADM-Status. Wenn die Option "Remote RACADM" deaktiviert ist, funktioniert die Funktion nicht.
   **ANMERKUNG:** Jede Änderung der Attributeinstellungen führt zu einem Verlust der IP-Adresse oder einer vorübergehenden Nichtverfügbarkeit der OME – Modular-Weboberfläche. Die OME – Modular-Weboberfläche wird jedoch automatisch wiederherstellt.
10. Klicken Sie auf **Anwenden**, um die Einstellungen für die Gehäusenetzwerkdienste zu speichern.

## Konfigurieren von OME-Modular für die Verwendung von Befehlszeilenkonsolen

Dieser Abschnitt enthält Informationen zu den Funktionen der OME-Modular-Befehlszeilenkonsolen (serielle oder SSH-Konsole). Weitere Informationen zum Einrichten des Systems für die Durchführung von Systemverwaltungsaufgaben über die Konsole finden Sie im White Paper, https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/servers-solution-resources_white-papers22_en-us.pdf. Informationen zur Verwendung von RACADM-Befehlen in OME-Modular über die Befehlszeilenkonsole finden Sie im *Dell EMC OpenManage Enterprise Modular für PowerEdge MX7000 Gehäuse RACADM Befehlszeilen-Referenzhandbuch*.

## OME-Modular: Funktionen der Befehlszeilenkonsole

OME-Modular unterstützt die folgenden Funktionen von seriellen und SSH-Konsolen:

- RACADM-Support
- Integrierter connect-Befehl zum Anschließen an die serielle Konsole von Servern und E/A-Modulen; auch als `racadm connect` verfügbar.
- Maximal vier SSH-Sitzungen
- Mindestens drei und maximal neun Wiederholungen der Authentifizierung für die SSH-Sitzung

## OME-Modular: Befehle der Befehlszeile

Wenn Sie zur OME-Modular Befehlszeile verbinden, können Sie folgende Befehle eingeben:

**Tabelle 10. OME-Modular: Befehle der Befehlszeile**

| Befehl | Beschreibung |
|---|---|
| `racadm` | RACADM-Befehle beginnen mit dem Schlüsselwort `racadm` gefolgt von einem Unterbefehl. Weitere Informationen finden Sie im *Dell EMC OpenManage Enterprise Modular für PowerEdge MX7000 Gehäuse RACADM Befehlszeilen-Referenzhandbuch*. |
| `connect` | Verbindung mit der seriellen Konsole eines Servers oder eines E/A-Moduls. Weitere Informationen finden Sie im *Dell EMC OpenManage Enterprise Modular für PowerEdge MX7000 Gehäuse RACADM Befehlszeilen-Referenzhandbuch*.<br>**ANMERKUNG:** Sie können auch den RACADM-Befehl `connect` verwenden. |
| `exit`, `logout` und `quit` | Alle Befehle führen die gleiche Maßnahme aus. Sie beenden die aktuelle Sitzung und kehren zur Anmeldeaufforderung zurück. |

So beenden Sie eine Sitzung:

- Auf Systemen, die Windows als Client-Host ausführen, verwenden Sie die Tasten [Strg]+[A] [Strg]+[X].
- Auf Systemen, die Linux als Client-Host ausführen, verwenden Sie die Tasten [Strg]+[A] [Strg]+[A] [Strg]+[X].

Um eine Binärsitzung in der seriellen Konsole von OME-Modular zu beenden, verwenden Sie die Tasten, [Strg] + ]. Verwenden Sie für EAMs [STRG] + \.

Um eine nicht-binäre Sitzung zu beenden, melden Sie sich an der OME-Modular-Schnittstelle an und gehen zu **Alle Geräte** > **Gehäuse** > **Übersicht** > **Troubleshooting** und klicken auf **Serielle Verbindung beenden**.

# Lokalen Zugriff konfigurieren

Sie können den Netzschalter des Gehäuses, Quick Sync, KVM, LCD und USB-Zugriffe für ein Gehäuse konfigurieren.

So konfigurieren Sie die lokalen Zugriffseinstellungen in einem Gehäuse:

1. Klicken Sie auf **Geräte** > **Gehäuse** > **Details anzeigen** > **Einstellungen** > **Konfiguration des lokalen Zugriffs**.
   Der Abschnitt **Konfiguration des lokalen Zugriffs** wird erweitert.
2. Wählen Sie **Gehäusenetzschalter aktivieren** aus, um das Gehäuse aus- oder einzuschalten.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Stromstatus des Gehäuses nicht mehr über den Gehäusenetzschalter geändert werden.
3. Wählen Sie **LCD-Überschreiben-PIN**, um die <LCD-Überschreiben-PIN einzugeben.

   Diese Option wird nur angezeigt, wenn Sie das Kontrollkästchen **Netzschalter des Gehäuses aktivieren** deaktivieren. Ist das Kontrollkästchen deaktiviert, können Sie die LCD-Überschreiben-PIN nicht eingeben.
4. Geben Sie im Textfeld **Schaltfläche für LCD-Überschreiben-PIN deaktiviert** die sechsstellige PIN ein, um den Stromzustand des Gehäuses zu ändern.

   Nur der Gehäuse-Administrator kann die LCD-Überschreiben-PIN erzeugen. Die PIN zum Überschreiben wurde entwickelt, um zu verhindern, dass andere Benutzer unbefugten Zugriff auf das Gehäuse erhalten. Wenn andere Benutzer Zugriff zur Ausführung von Aufgaben benötigen, kann der Gehäuse-Administrator die sechsstellige PIN bereitstellen.

**ANMERKUNG:** Wenn die PIN nicht gültig ist, wird eine Fehlermeldung angezeigt. Sie können den Vorgang maximal drei Mal wiederholen.

5. Wählen Sie **Quick Sync-Zugriffstyp** aus.

   Folgende Optionen stehen zur Verfügung:

   - Nur-Lesen – Ermöglicht den schreibgeschützten Zugriff auf WLAN und Bluetooth-Low Energy (BLE). Sie können keine Konfigurationsinformationen mit Quick Sync schreiben.
   - Lese-/Schreibzugriff – Ermöglicht das Speichern der Konfiguration unter Verwendung von Quick Sync.
   - Deaktiviert – Deaktiviert das Lesen oder Schreiben der Konfiguration unter Verwendung von Quick Sync.

   **ANMERKUNG:** Die Quick Sync-Funktion verwendet eine niedrigere Hochfrequenz (HF) bei der Werbung und erhöht die HF-Leistung nach der -Zeritfikatauthentifizierung. Der HF-Bereich basiert auf der Umgebung und kann variieren.

6. Aktivieren Sie **Inaktivitäts-Timeout aktivieren**, um das Inaktivitäts-Timeout zu aktivieren, und geben Sie die **Zeitüberschreitungsbegrenzung** ein.

   Timeout ist die Leerlaufzeit (inaktive Zeit), wenn kein Wi-Fi-Datenverkehr stattfindet. Geben Sie das Zeitlimit des Inaktivitäts-Timeout in Sekunden an. Das Timeout kann zwischen zwei und 60 Minuten liegen.

   **ANMERKUNG:** Die Option **Zeitüberschreitungsbegrenzung** ist nur dann verfügbar, wenn **Inaktivitäts-Timeout aktivieren** ausgewählt ist.

7. Wählen Sie **Leseauthentifizierung aktivieren** aus, um sich über Ihre Nutzerzugangsdaten zum Lesen des Bestands in einem sicheren Rechenzentrum anzumelden.

   Standardmäßig ist die Option ausgewählt. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie nicht auf das sichere Rechenzentrum zugreifen.

8. Wählen Sie **Quick Sync-Wi-Fi aktivieren** aus, um für die Kommunikation mit dem Gehäuse Wi-Fi zu verwenden. Standardmäßig ist das Kontrollkästchen **Quick Sync-Wi-Fi aktivieren** markiert.
9. Markieren Sie das Kontrollkästchen **KVM-Zugriff aktivieren**, um die Quick Sync-Einstellung unter Verwendung von KVM zu konfigurieren. Sie können auch die Befehle RACADM oder Redfish zum Aktivieren oder Deaktivieren von KVM verwenden. Weitere Informationen finden Sie im *OME - Modular für PowerEdge MX7000-Gehäuse RACADM CLI – Handbuch* verfügbar unter https://www.dell.com/openmanagemanuals.

   Sie können den DisplayPort im Gehäuse verwenden, um das Video im KVM zu streamen. Wenn der externe DP-zu-Video Graphics Array (VGA)-Konverter verfügbar ist, können Sie das KVM-Video auch im VGA streamen.

10. Aktivieren Sie die Option **LCD-Zugriff** für Quick Sync.

    Folgende Optionen stehen zur Verfügung:

    - Deaktiviert
    - Nur Ansicht
    - Ansicht und Modifizieren

    **ANMERKUNG:** Die Option **LCD-Zugriff** wird nur dann angezeigt, wenn ein System mit LCD im Gehäuse verfügbar ist.

11. Geben Sie im Textfeld **Benutzerdefiniert** den Text ein, der auf dem LCD-Startbildschirm angezeigt werden soll. Der LCD-Startbildschirm wird angezeigt, wenn das System auf die Werkseinstellungen zurückgesetzt wird. Der Text darf maximal 62 Zeichen lang sein und unterstützt eine begrenzte Anzahl UTF-8-Zeichen. Wenn ein nicht unterstütztes UTF-8-Zeichen im Text verwendet wird, wird anstelle des Zeichens ein Kästchen angezeigt. Die Standardzeichenfolge ist die Service-Tag-Nummer des Systems.
12. Wählen Sie aus der Drop-Down-Liste **LCD Sprache** die Sprache aus, in der der Text auf dem LCD-Bildschirm angezeigt werden soll.

    Folgende Optionen stehen zur Verfügung:

    - Englisch
    - Französisch
    - Spanisch
    - Deutsch
    - Japanisch
    - Chinesisch

    Standardmäßig wird der Text auf Englisch angezeigt.

13. Wählen Sie das **Gehäuse-Direktzugriff aktivieren**-Textfeld, um den Zugriff auf das MX7000-Gehäuse von einem Host wie z. b. einem Laptop oder Server unter Verwendung eines USB-On-the-Go (OTG)-Kabels zu aktivieren.

    Wenn das Kontrollkästchen **Gehäuse-Direktzugriff aktivieren** nicht aktiviert ist, werden die vorhandenen Chassis-Direct-Sitzungen getrennt und die Chassis-Direct-LED erlischt. Wenn die Funktion deaktiviert ist, können Sie den Laptop nicht mit dem Gehäuse verbinden. Auf die URL `https://ome-m.local` kann nicht zugegriffen werden. Nachdem Sie die Funktion aktiviert haben,

schließen Sie das USB-Kabel wieder an und warten Sie, bis die Gehäuse-Direkt-LED grün leuchtet, um auf das Gehäuse-Telefonbuch zuzugreifen. Weitere Informationen finden Sie im Abschnitt Chassis Direct.

14. Klicken Sie auf **Anwenden**, um die Quick-Sync-Einstellungen zu speichern.

## Chassis Direct

Die Chassis-Direct-Funktion in OME-Modular ermöglicht Nutzern den Zugriff auf Verwaltungskonsolen, wie z. b. iDRAC und das Managementmodul von Geräten im Gehäuse. Das MX7000-Gehäuse verfügt über mehrere USB-Ports. Das Rechte Bedienfeld (RCP) an der Vorderseite des Gehäuses hat drei USB-Anschlüsse. Zwei Ports sind normal dimensionierte USB-A-Ports, für Tastaturen und Maus, die für die KVM des Gehäuse-Levels verwendet werden. Der dritte Port ist ein Micro-AB-Port, der USB OTG unterstützt. Zum Verwenden von Chassis Direct verbinden Sie den USB OTG-Port mit einem Laptop. Der Prozessor auf dem Verwaltungsmodul emuliert eine USB-Netzwerkschnittstelle und stellt eine Netzwerkbrücke in das Management-VLAN bereit. Das Netzwerk ist identisch mit QuickSync-2-Brücken für Wi-Fi-Zugriff zu OpenManage Mobile.

Wenn die Einstellung für das Netzwerkzeitprotokoll nicht aktiviert ist, wird die Systemzeit durch die RCP-Ersetzung nicht wiederhergestellt. Die Echtzeituhr auf dem neuen RCP wird dann als Systemzeit des Hauptgehäuses verwendet und mit allen Mitgliedsgehäusen synchronisiert, was zu einem Neustart des Mitglieds-MSM und für einige Zeit zum Verlust der MM-Redundanz führen kann. Die Redundanz sollte nach wenigen Minuten erfolgreich wiederhergestellt werden.

Entfernen Sie das USB-Kabel, das an der Vorderseite angeschlossen ist, und schalten Sie das Gehäuse komplett aus und wieder ein.

Mit dem System, das mit dem USB OTG-Port auf dem Gehäuse verbunden ist, können Sie auf die MM-Nutzeroberfläche und die iDRAC Nutzeroberfläche oder KVM zugreifen. Sie können Zugriff erhalten, indem Sie einen Browser auf dem Laptop starten und die URL `https://ome-m.local` eingeben. Eine Gehäuse-Telefonbuchseite, die eine Liste der Einträge der verfügbaren Geräte auf dem Gehäuse enthält, wird angezeigt. Diese Option bietet eine bessere Erfahrung als die Frontblende KVM, die nur Zugriff auf die Befehlszeilen-Eingabeaufforderung für OME-Modular ermöglicht.

Wählen Sie das Kontrollkästchen, um den Zugriff auf das MX7000-Gehäuse von einem Host, wie z.B. einem Laptop oder Server, unter Verwendung eines USB-On-the-Go (OTG)-Kabel zu aktivieren. Verbinden Sie den Host mithilfe des USB-OTG-Kabels mit dem Mikro-USB-Anschluss auf der Frontblende (rechtes Bedienfeld) des MX7000-Gehäuses. Bei erfolgreicher Verbindung wird die LED unter dem Micro-USB auf dem rechten Bedienfeld des MX7000-Gehäuses grün und der USB Ethernet-Adapter wird auf dem Host angezeigt. Das Gehäuse wird automatisch mit einer IPv4- und einer IPv6-Adresse konfiguriert. Öffnen Sie einen Webbrowser, nachdem Sie sichergestellt haben, dass die Adressen konfiguriert sind, und geben Sie die URL `https://ome-m.local` in die Adressleiste ein.

Wenn auf Laptops unter Windows der IPV6-Datenverkehr blockiert ist, überprüfen Sie die RvIS-Schnittstelle (Remote Network Driver Interface Specification) der IPv6-Adresse. Möglicherweise können Sie über IPv4 auf die Telefonbuchseite des Gehäuses zugreifen, auf iDRAC- und OME-Modular-Webkonsolen kann jedoch nicht zugegriffen werden. Aktivieren Sie in diesem Fall den IPv6-Datenverkehr auf dem System.

Wenn Sie die Chassis Direct-Funktion in OME-Modular aktivieren oder deaktivieren, werden folgende Fehlercodes angezeigt:

Die Chassis Direct-Funktion in OME-Modular hat eine gegenseitige Exklusivität mit der Quick Sync-Funktion. Bevor Sie die Management Modul-Firmware von der Version 1.10.00 auf eine frühere Version zurückstufen, entfernen Sie das USB-Kabel, das mit der Frontblende des Gehäuses verbunden ist. Wenn das USB-Kabel nicht entfernt wird und die Firmware 1.10.00 heruntergestuft wird, ist die Quick Sync-Funktion möglicherweise heruntergestuft. Um Quick Sync wieder in Betrieb zu nehmen, schalten Sie das Gerät komplett aus und wieder ein.

- Das Gehäuse verfügt über eine Quick Sync-Funktion und die Chassis Direct-Funktion ist aktiviert. Das bedeutet, dass das USB-Kabel am USB-Anschluss auf der Frontblende befestigt ist.
- Die Version des Managementmoduls wird von 1.10.00 auf eine frühere Version zurückgestuft.

### Tabelle 11. Chassis Direct – LED-BLINK-Status und Beschreibung

| Fehlercode | LED-Blinkstatus des Gehäuses | Beschreibung und Lösung |
|---|---|---|
| 1 | Gelb | Die USB-Netzwerkverbindung ist inaktiv, da die Chassis Direct-Funktion deaktiviert ist.<br>**Lösung** – aktivieren Sie Chassis Direct und verbinden Sie das USB-Kabel erneut, um auf das Gehäuse-Telefonbuch zuzugreifen. |
| 2 | Gelb | Die USB-Netzwerkverbindung wird nicht gestartet, wenn der interne USB-Vorgang des Gehäuses fehlgeschlagen ist. |

**Tabelle 11. Chassis Direct – LED-BLINK-Status und Beschreibung (fortgesetzt)**

| Fehlercode | LED-Blinkstatus des Gehäuses | Beschreibung und Lösung |
|---|---|---|
| | | **Lösung** – wenn das Problem weiterhin besteht, schließen Sie das USB-Kabel an den Laptop an oder schalten Sie das Gehäuse aus und wieder ein. |
| 3 | Gelb | Die USB-Netzwerkverbindung kann aufgrund eines Problems mit dem Host-Laptop nicht hergestellt werden.<br>**Lösung** – wenn das Problem weiterhin besteht, schließen Sie das USB-Kabel wieder an. |
| 4 | Ausgeschaltet | Die USB-Netzwerkverbindung ist nicht aktiv, da das USB-Kabel nicht angeschlossen ist.<br>**Lösung** – schließen Sie das USB-Kabel wieder an, damit die Verbindung hergestellt werden kann. |

Wenn die Chassis Direct-Funktion deaktiviert ist und das USB-Kabel eingesetzt ist, leuchtet die LED von Chassis Direct gelb und die Warnmeldung USR0197 wird auf der OME-Modular-Weboberfläche angezeigt. Sie können die Warnmeldung nur anzeigen, wenn Sie sich bei OME Modular über das öffentliche Netzwerk angemeldet haben. Wenn Sie die Aktion in einem kurzen Intervall wiederholen, wird die Warnmeldung nicht angezeigt. Die Chassis Direct-LED bleibt jedoch gelb, wenn das MM aufeinanderfolgende doppelte Warnmeldungen unterdrückt.

**ANMERKUNG:** Bei Verwendung des Internet Explorers für den Zugriff auf die Telefonbuchseite führt ein nutzerdefiniertes Zertifikat mit einer Größe von mehr als 46 KB zu einem TLS-Fehler. Ändern Sie das Zertifikat oder verwenden Sie einen anderen Browser.

# Gehäuseposition konfigurieren

So konfigurieren Sie den Standort des Gehäuses:

1. Klicken Sie auf **Geräte** > **Gehäuse** > **Details anzeigen** > **Einstellungen** > **Standort**.
   Der Abschnitt **Standortkonfiguration** wird erweitert.
2. Geben Sie die Standortnamen für **Rechenzentrum**, **Raum**, **Gang** und **Rack** ein.
   **Rechenzentrum**, **Raum**, **Gang** und **Rack** unterstützen bis zu 128 Zeichen.
3. Geben Sie die Nummer des **Rack-Steckplatzes** und den Namen des **Standorts** ein, an dem sich das Rack befindet.
   **Rack-Steckplatz** unterstützt 1-255 numerische Zeichen.
   **Speicherort** unterstützt bis zu 128 Zeichen. Es wird Abwärtskompatibilität unterstützt. Diese Eigenschaft wird durch Rechenzentrums-, Gang-, Rack- und Rack-Steckplatz-Eigenschaften ersetzt. Verwenden Sie diese Eigenschaften, um den physischen Speicherort des Gehäuses zu bestimmen.
4. Klicken Sie auf **Anwenden**, um die Standort-Einstellungen zu speichern.

# Konfiguration von Quick Deploy-Einstellungen

Die **Quick Deploy**-Funktion ermöglicht Ihnen die Konfiguration des Kennworts für den Zugriff auf die iDRAC-Nutzeroberfläche, EAMs und IPv4- und IPv6-Einstellungen. Diese Einstellungen können unmittelbar auf vorhandene Rechnerschlitten oder EAM-Geräte angewendet werden. Sie können **Quick Deploy**-Einstellungen auf Rechnerschlitten anwenden, wenn diese in das Gehäuse eingesetzt werden oder auch später. Sie können die **Quick Deploy**-Einstellungen jedoch nicht auf IOMs anwenden, die später eingefügt werden.

Quick Deploy-Einstellungen werden überprüft, wenn der Job ausgeführt wird. Wenn ein ungültiger Parameter verwendet wird, schlägt der Quick Deploy-Job fehl. Die Parameter für den **Quick Deploy**-Job werden nicht ausgewertet, da sie einen beliebigen Wert enthalten können, der während der Ausführung des Jobs delegiert wird.

Das Aktivieren und Deaktivieren von **Quick Deploy** ist eine Funktion der Webschnittstelle, um festzustellen, ob die Steuerelemente zum Konfigurieren der Quick Deploy-Einstellungen aktiviert sind. Das Back-End verarbeitet nur Anforderungen von der Webschnittstelle.

**ANMERKUNG:** Nachdem die Quick Deploy-Einstellungen auf den Rechnerschlitten angewendet wurden, wird die IP-Konfiguration beim Aktualisieren der Bestandsaufnahme in der OME – Modular-Webschnittstelle angezeigt.

**ANMERKUNG:** Wenn IPv4 für IPv6 für FC-IOMs deaktiviert ist, werden die IPv4- und die IPv6-Adresse des Geräts auf der Seite **Quick Deploy** für IOMs nicht angezeigt. Für Netzwerk-EAMs sind die IPv4- und IPv6-Geräteadressen jedoch **::** und **0.0.0.0**.

So konfigurieren Sie die **Quick Deploy**-Einstellungen:

1. Klicken Sie auf **Geräte** > **Gehäuse** > **Details anzeigen** > **Einstellungen** > **Quick Deploy**.
   Der Abschnitt **Quick Deploy-Konfiguration** wird erweitert.
2. Geben Sie das neue Kennwort ein und bestätigen Sie es für den Zugriff auf die iDRAC-Nutzeroberfläche.
   Das Kennwort kann bis zu 20 Zeichen umfassen.
   **ANMERKUNG:** Wenn eine iDRAC IP-Konfiguration geändert wird, ist das SSO für die Schlitten in der OME-Modular-Konsole erst dann funktionsfähig, wenn der standardmäßige Bestandsaufnahme-Task oder die manuelle Bestandsaktualisierung abgeschlossen ist.
3. Wählen Sie im Abschnitt **Management IP IPv4 aktiviert** aus, um die IPv4-Netzwerkeinstellungen zu aktivieren, und wählen Sie den **IPv4-Netzwerktyp** aus.
   Folgende Optionen stehen zur Verfügung:
   - Statisch
   - DHCP
4. Geben Sie die **IPv4-Subnetzmaske** und das **IPv4-Gateway** ein.
   **ANMERKUNG:** Die Optionen **IPv4-Subnetzmaske** und **IPv4-Gateway** werden nur angezeigt, wenn der **IPv4-Netzwerktyp** „Statisch“ ist.
5. Wählen Sie **IPv6 aktiviert** aus, um die IPv6-Netzwerkeinstellungen zu aktivieren, und wählen Sie den **IPv6-Netzwerktyp** aus.
   Folgende Optionen stehen zur Verfügung:
   - Statisch
   - DHCP
6. Wenn der **IPv6-Netzwerktyp** „Statisch“ ist, wählen Sie die **IPv6-Präfixlänge** und geben das **IPv6-Gateway** ein.
7. Aktivieren Sie in der Liste der angezeigten Steckplätze das Kontrollkästchen neben der Steckplatznummer, auf die Sie die **Quick Deploy**-Einstellungen anwenden möchten.
8. Geben Sie im Abschnitt **Einstellungen für Netzwerk IOM** das Passwort ein, um sich bei der IOM Oberfläche anzumelden.
9. Wählen Sie **IPv4 aktiviert** aus, um die IPv4-Netzwerkeinstellungen zu aktivieren, und wählen Sie den **IPv4-Netzwerktyp** aus.
   Folgende Optionen stehen zur Verfügung:
   - Statisch
   - DHCP
10. Geben Sie die **IPv4-Subnetzmaske** und das **IPv4-Gateway** ein.
    **ANMERKUNG:** Die Optionen **IPv4-Subnetzmaske** und **IPv4-Gateway** werden nur angezeigt, wenn der **IPv4-Netzwerktyp** „Statisch“ ist.
11. Wählen Sie **IPv6 aktiviert** aus, um die IPv6-Netzwerkeinstellungen zu aktivieren, und wählen Sie den **IPv6-Netzwerktyp** aus.
    Folgende Optionen stehen zur Verfügung:
    - Statisch
    - DHCP
12. Wenn der **IPv6-Netzwerktyp** „Statisch“ ist, wählen Sie die **IPv6-Präfixlänge** und geben das **IPv6-Gateway** ein.
13. Klicken Sie auf **Anwenden**, um die **Quick Deploy**-Einstellungen zu speichern.

# Gehäuse verwalten

Sie können die Liste der Gehäuse und die Gehäusedetails auf der Seite **Gehäuse** anzeigen. Die Details sind: Funktionszustand, Stromzustand, Name, IP-Adresse, Service-Tag-Nummer und Modell des Gehäuse. Sie können auch ein Gehäuse auswählen, um eine grafische Darstellung und Zusammenfassung des Gehäuses im rechten Bereich der Seite **Gehäuse** anzuzeigen.

Auf der Seite **Gehäuse** können Sie auch folgende Aufgaben ausführen:

- Die Stromversorgung des Gehäuses steuern

- Aktualisieren Sie die Firmware.
- Blink LED
- Die Gehäuse-Bestandsaufnahme aktualisieren
- Die Gehäuseliste filtern

**ANMERKUNG:** Wenn ein Gehäuse aus- und wieder eingeschaltet wird, wird die Bestandsliste der Rechnerschlitten und EAMs nach drei bis fünf Minuten in der OME – Modular-Webschnittstelle angezeigt.

**ANMERKUNG:** Halten Sie zwischen dem Entfernen und Einsetzen jedes Geräts ein Mindestintervall von zwei Minuten ein.

**ANMERKUNG:** Nach einem Ausschalten des Gehäuses werden die Rechnerschlitten basierend auf dem Ereignis aus dem Gehäuse abgefragt. Jedes Ereignis aus dem Gehäuse löst eine Zustandsabfrage aus. Sie sehen möglicherweise mehrere Verbindungsverlust-Ereignisse von den Rechnerschlitten.

## Gehäusefilter erstellen

Sie können die Liste der Gehäuse, die auf der Seite **Geräte** > **Gehäuse** angezeigt werden, unter Verwendung von Filtern sortieren.

So erstellen Sie Filter:

Klicken Sie auf der Seite **Gehäuse** auf **Erweiterte Filter** zum Anzeigen der Filteroptionen.
Die folgenden Optionen werden angezeigt:

- **Funktionszustand**
- **Zustand**
- **Name enthält**
- **IP-Adresse enthält**
- **Service-Tag enthält**
- **Modell**

## Gehäuseübersicht anzeigen

Auf der Seite **Übersicht** für das Gehäuse können Sie zum Anzeigen der Rechnerschlitten-Steckplatzdetails auf **Steckplatzinformationen anzeigen** klicken. Eine grafische Darstellung des Gehäuses wird auf der linken Seite angezeigt. Informationen über das Gehäuse werden unterhalb der grafischen Darstellung angezeigt. Diese Angaben umfassen: FIPS-Status des Gehäuses, Name, Modell, Service-Tag-Nummer, Bestands-Tag, Express-Servicecode, Management-IP-Adresse, Firmware-Version, Stromzustand und Maximalstrom des Gehäuses. Klicken Sie auf **Geräte anzeigen**, um die Liste aller Geräte auf der Seite **Alle Geräte** anzuzeigen.

Sie finden auch Informationen in den entsprechenden folgenden Abschnitten:

- **Gehäuse-Untersysteme** – Zeigt den Funktionszustand der Gehäusekomponenten wie Batterie, Lüfter, EAMs und Netzteil an.

  Informationen zur Fabric-Konsistenzprüfung (FCC) und zu Änderungen des Funktionszustands werden unter **Gehäuse-Untersysteme** angezeigt. Die FCC-Details des Rechnerschlittens werden jedoch nicht in der grafischen Darstellung des Gehäuses und auf der Seite Rechner-**Übersicht** angezeigt.

- **Umgebung** – Zeigt die Stromverbrauchseinheiten und die Temperatur des Gehäuses an. Klicken Sie auf **Stromstatistik anzeigen**, um Details zum Stromverbrauch des Gehäuses anzuzeigen, wie z. B. den aktuellen Redundanzzustand, Spitzen-Aussteuerungsreserve und Stromverbrauch des Systems. Klicken Sie auf **Zurücksetzen**, um die Energieversorgungs-Statistiken und den Start des Überwachungszeitraums zurückzusetzen. Klicken Sie auf **Stromverbrauch**, um Details über das Netzteil des Gehäuses auf der Seite **Gehäuse** > **Hardware** > **Gehäusenetzteile** anzuzeigen. Wenn ein Failover oder Managementmodul-Neustart durchgeführt wird, dann wird der letzte Reset-Stromstatistik-Zeitstempel basierend auf dem Failover- oder Managementmodul-Neustart-Zeitstempel aktualisiert.

  Klicken Sie auf **Temperaturstatistik anzeigen**, um Informationen wie Dauer, Datum und Uhrzeit des Beginns der Aufzeichnung von Temperaturdetails, Spitzentemperatur, Zeitstempel, Mindesttemperatur und Zeitstempel anzuzeigen. Klicken Sie auf **Zurücksetzen**, um die Temperaturstatistiken und den Start des Überwachungszeitraums zurückzusetzen.

  **ANMERKUNG:** Der Stromverbrauchswert für den Rechnerschlitten wird abgerundet und kann weniger als minimalen Stromverbrauch anzeigen.

  **ANMERKUNG:** Der Temperaturstatistik-Zeitstempel bleibt nach einem Failover oder einem Neustart des Verwaltungsmoduls unverändert.

- **Letzte Warnungen** – Zeigt die Anzahl sowie Details der im Rechnerschlitten durchgeführten Tasks an. Klicken Sie auf **Alle anzeigen**, um eine Liste aller Warnungen in Bezug auf den Rechnerschlitten auf der Seite **Gehäuse** > **Warnungen** anzuzeigen.

- **Kürzlich durchgeführte -Aktivitäten** – Zeigt den Status der im Rechnerschlitten durchgeführten Jobs an.
- **Server-Untersysteme** – Zeigt eine Zusammenfassung der Informationen über die Server-Untersysteme an. Die Informationen umfassen den Funktionszustand der Komponenten wie Akku, Speicher, Prozessor und Spannung.

Wenn Sie über Rechte als Gehäuseadministrator verfügen, können Sie auf dieser Registerkarte die folgenden Aufgaben ausführen:

- **Stromsteuerungs**-Tasks
  - **Ausschalten (nicht ordnungsgemäß)**: Schaltet den Serverstrom aus, was dem Drücken des Netzschalters entspricht, wenn das Gehäuse eingeschaltet ist. Diese Option ist deaktiviert, wenn das Gehäuse bereits abgeschaltet ist. Es erfolgt keine Benachrichtigung des Serverbetriebssystems.
  - **System aus- und einschalten (Kaltstart)**: schaltet das Gehäuse aus und anschließend wieder ein (Kaltstart). Diese Option ist deaktiviert, wenn das Gehäuse bereits abgeschaltet ist.

    In der Befehlszeilenschnittstelle führt die Aktion zum Aus- und Wiedereinschalten zu einem ordnungsgemäßen Neustart des Gehäuses.

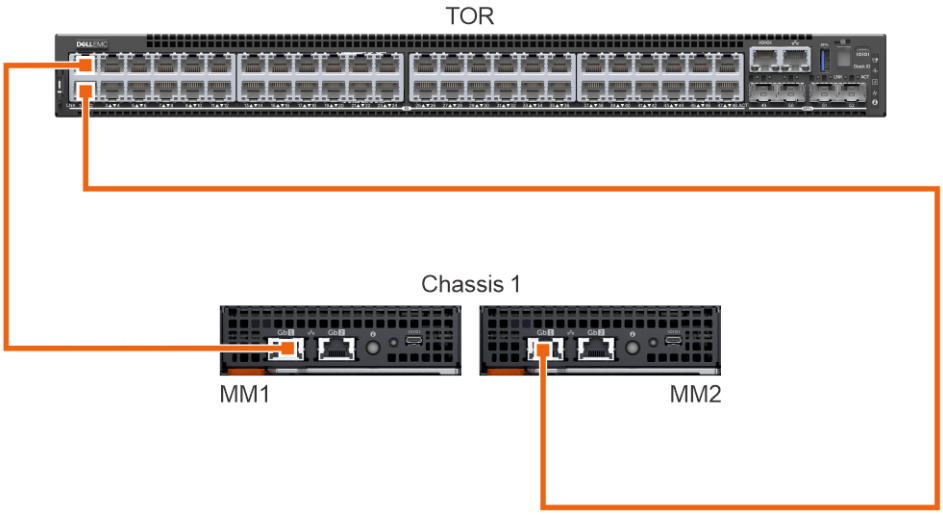
    **ANMERKUNG:** Wenn das Gehäuse aus- und wieder eingeschaltet wird, werden alle Geräte im Gehäuse ebenfalls aus- und wieder eingeschaltet. Das Managementmodul wird nicht aus- und wieder eingeschaltet. Die protokollierten Warnmeldungen können jedoch enthalten, dass die Verbindung aufgrund eines Aus- und Einschaltvorgangs unterbrochen wurde.
  - **Ausschalten (ordnungsgemäß)**: Benachrichtigt das Serverbetriebssystem, dass das Gehäuse ausgeschaltet werden soll. Diese Option ist deaktiviert, wenn das Gehäuse bereits abgeschaltet ist.
- Konfigurations-Tasks:
  - **Neue Gehäusegruppe erstellen**
  - **Gehäusegruppe beitreten**
  - **Erstkonfiguration**
- Troubleshooting-Tasks:
  - Protokoll extrahieren
  - Diagnosebefehle
  - Gehäuseverwaltungsmodul zurücksetzen
  - Serielle Verbindung beenden
- Schalten Sie die LEDs über **Blink LED** ein und aus.
- Sichern, wiederherstellen und exportieren Sie das Gehäuseprofil, und führen Sie ein Failover durch.

**ANMERKUNG:** Nach einem Ausschalten des Gehäuses werden die Rechnerschlitten basierend auf dem Ereignis aus dem Gehäuse abgefragt. Jedes Ereignis aus dem Gehäuse löst eine Zustandsabfrage aus. Sie sehen möglicherweise mehrere Verbindungsverlust-Ereignisse von den Rechnerschlitten.

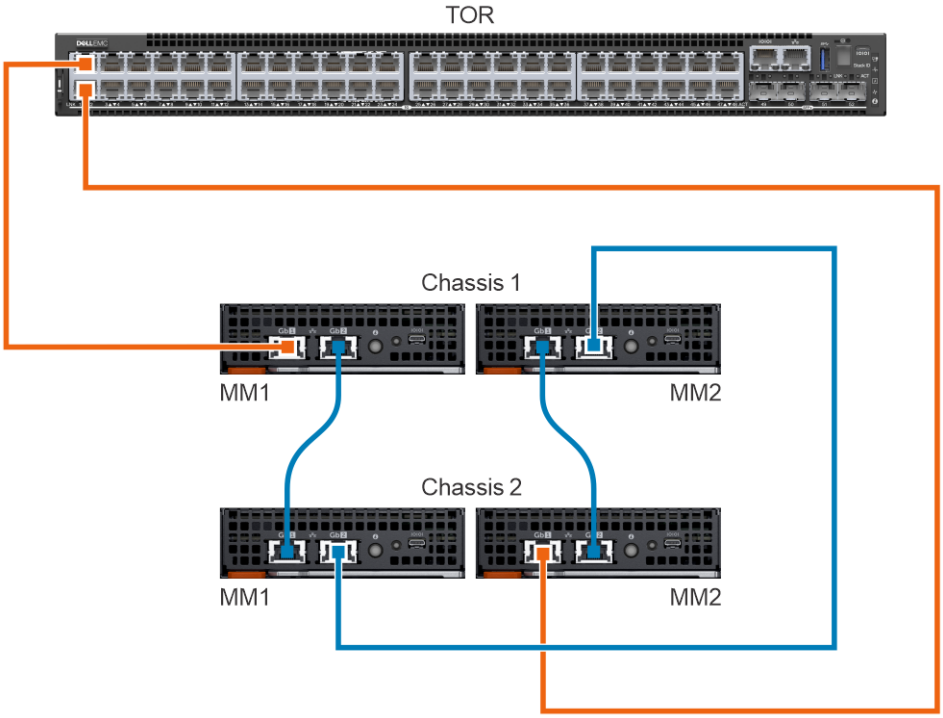
# Verkabelungsgehäuse

Die Funktionen zur automatischen Uplink-Erkennung und Netzwerkschleifenprävention in OME-Modular ermöglichen die Verbindung mehrerer Gehäuse mit Kabeln. Die Verkabelung speichert die Port-Nutzung in den Rechenzentrums-Switches und greift auf jedes Gehäuse im Netzwerk zu. Die Verkabelung des Gehäuses auf diese Weise wird als Stack bezeichnet.

Verbinden Sie während der Verkabelung eines Gehäuses ein Netzwerkkabel von jedem Verwaltungsmodul mit dem Top-of-Rack-Switch (ToR) des Rechenzentrums. Stellen Sie sicher, dass beide Ports auf dem ToR aktiviert sind und sich im selben Netzwerk und VLAN befinden. Die folgende Abbildung ist eine Darstellung der individuellen Gehäuseverkabelung:




Die folgende Abbildung ist eine Darstellung der Zwei-Gehäuse-Verkabelung:




# Gehäusegruppen

Sie können viele Gehäuse zu einer Multi-Gehäuseverwaltung (MCM)-Gruppe zusammenfassen. Eine MCM-Gruppe kann ein Haupt- und 19 Mitgliedsgehäuse umfassen. Sie können jedes Managementmodul zum Erstellen einer MCM-Gruppe verwenden. Das Managementmodul, das für die Erstellung der MCM-Gruppe verwendet wird, ist standardmäßig das Hauptgehäuse der Gruppe. In der MCM-Gruppe sind die Gehäuse über einen redundanten Port am Managementmodul kabelgebunden oder linear verkabelt. Das von Ihnen für die Erstellung der Gruppe ausgewählte Gehäuse muss mit mindestens einem Gehäuse linear verkabelt sein. Sie können eine Liste verkabelter Gehäuse anzeigen und alle oder eine erforderliche Anzahl von Gehäusen zur Erstellung der MCM-Gruppe auswählen.

**ANMERKUNG:** Sie müssen über die Berechtigung als Gehäuseadministrator verfügen, um eine MCM-Gruppe erstellen zu können:

Sie können die folgenden Aufgaben unter Verwendung einer MCM-Gruppe durchführen:

- Den Zustand der MCM-Gruppe und der Mitgliedsgehäuse anzeigen.
- Die Einstellungen des Hauptgehäuses automatisch auf die Mitgliedsgehäuse anwenden.
- Jeden Gehäusevorgang auf der MCM-Gruppe ausführen.

Sie können Mitgliedsgehäuse auf zwei Arten zu einer MCM-Gruppe hinzufügen:

- Automatisch – Ermöglicht den automatischen Einschluss des Mitglieds in die Gehäusegruppe. Der automatische Einschlussprozess erfordert keine Genehmigung des Gehäuseadministrators.
- Manuell – Erfordert die Genehmigung durch den Gehäuseadministrator zum Einschluss des Mitgliedsgehäuses in die Gehäusegruppe.

## Voraussetzungen für das Erstellen einer kabelgebundenen Gruppe

Im Folgenden sind die Voraussetzungen zum Erstellen einer kabelgebundenen oder linear verkabelten Gehäusegruppe dargelegt:

- Liste der kabelgebundenen, verketteten Gehäuse – Das gesamte Gehäuse muss sich in dem privaten Stack befinden. Sie brauchen kein Kennwort einzugeben, da die Maschine-zu-Maschine-Authentifizierung verwendet wird.
- Stellen Sie sicher, dass Sie das Mitgliedsgehäuse unter Verwendung der automatischen oder manuellen Methode zur Gruppe hinzugefügt haben.
- Stellen Sie sicher, dass die Gehäuseeinstellungen ausgewählt sind, damit sie auf das andere Gehäuse angewendet werden können. Dazu gehören: Strom, Benutzerauthentifizierung, Warnungsziel, Uhrzeit, Proxy, Sicherheit, Netzwerkdienste, lokaler Zugriff.
- Stellen Sie sicher, dass "Automatische Verhandlung" in allen Gehäusen, die mit einer MCM-Gruppe verbunden sind, auf "wahr" gesetzt ist. Weitere Informationen finden Sie unter Konfigurieren des Gehäusenetzwerks.
- Bevor Sie das Gehäuse zum Erstellen einer Gruppe oder zum Hinzufügen neuer Mitglieder zu einer vorhandenen Gruppe stapeln, stellen Sie sicher, dass alle Gehäuse dieselbe OME-Modular-Firmware-Version aufweisen.

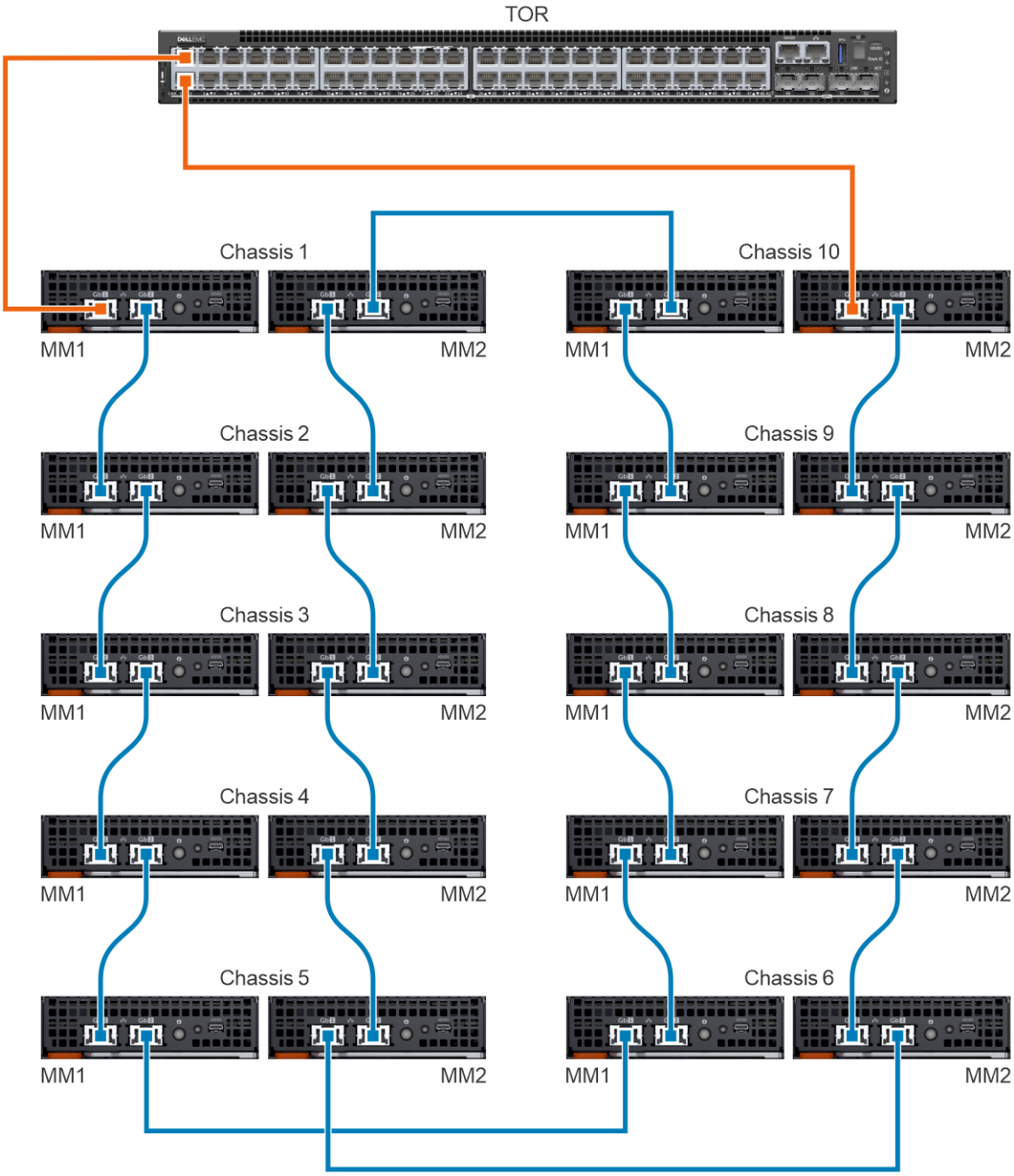
Vor dem Erstellen einer MCM-Gruppe stellen Sie sicher, dass die MX7000-Verwaltungsnetzwerke zu einer Stapelkonfiguration verdrahtet sind. Der Konfiguration als Stack hilft, folgende Situationen zu überwinden:

- Ausfall eines einzelnen Netzwerkkabels
- Ausfall eines einzelnen Verwaltungsmoduls
- Stromverlust aufgrund irgendwelcher Gehäuse im Stapel
- Failover eines Gehäuses im Stapel

**ANMERKUNG:** Wenn eines der oben aufgeführten Probleme auftritt, kann der Managementnetzwerkzugriff auf alle Komponenten in der linear verkabelten Gruppe für bis zu 10 Minuten unterbrochen werden. Die OME-Modular-Webschnittstelle wird automatisch wiederherstellt.

Die verdrahteten Gehäuse werden wie unter **Verfügbare Gehäuse** im **Gruppen-Bereitstellungsassistenten** angezeigt.

Die folgende Abbildung ist eine Darstellung der empfohlenen MCM-Verkabelung:




# Gehäusegruppen erstellen

Um eine Gehäusegruppe zu erstellen:

1. Klicken Sie auf dem Gehäuse-Dashboard auf **Übersicht** > **Konfigurieren** > **Gehäusegruppe erstellen**.
   Der Assistent **Gruppe erstellen und Hauptgehäuse konfigurieren** wird angezeigt.
2. Geben Sie einen Namen und eine Beschreibung für die Gehäusegruppe ein, die Sie erstellen möchten.
   Die Gruppennamen können Buchstaben und Zahlen enthalten und müssen weniger als 48 Zeichen lang sein. Allerdings dürfen die Gruppennamen keine Leerzeichen und Sonderzeichen enthalten.
3. Wählen Sie den Onboarding-Berechtigungstyp.
4. Wählen Sie die Konfigurationseinstellungen aus, die Sie auf das Mitgliedsgehäuse übertragen möchten.
   Die Einstellungen sind:
   - Alle – Wendet alle Einstellungen des Hauptgehäuses auf das Mitgliedsgehäuse an
   - Strom – Stromobergrenze, Redundanz, Priorität des Rechnerschlittens
   - Benutzerauthentifizierung – Verzeichnisdienste, lokale Benutzer

- Warnungsziel – E-Mail, SNMP-Trap, Systemprotokoll
- Proxy-Einstellungen – Alle Einstellungen
- Sicherheitseinstellungen – Anmeldungs-IP-Bereich, Anmeldungs-/Abmeldesperrungs-Richtlinie
- Netzwerkdienste – SNMP, SSH, Remote-RACADM, Webserver
- Lokale Zugriffskonfiguration – Gehäuseschalter, Quick Sync, KVM, LCD serieller Zugriff
- Sitzungsinaktivitätszeitlimit-Konfiguration – Sitzungsinaktivitäts-Timeout

  **ANMERKUNG:** Zeiteinstellungen des Hauptgehäuses werden automatisch mit allen Mitgliedsgehäusen im Stapel synchronisiert.

5. Klicken Sie auf **Weiter**, um die Zusammenfassung der Gruppe anzuzeigen.

   Auf dem Dashboard eines Hauptgehäuses wird eine Zusammenfassung der Zustandsinformationen, der kürzlich durchgeführten Aktivitäten und der letzten Warnungen des Mitgliedsgehäuses angezeigt. Sie können ein Mitgliedsgehäuse auswählen, um dessen Details anzuzeigen.

   Die aktuelle Mitglieds-ID des Gehäuses wird auf der linken Seite angezeigt.

# Mitgliedsgehäuse zu Gruppen hinzufügen

Sie können Mitglieder zu Gehäusegruppen hinzufügen aus:

- Der Seite **Übersicht** des Hauptgehäuses oder des Mitgliedergehäuses.
- Der Option **Gruppenkonfiguration** im MCM-Dashboard.

## Mitgliedsgehäuse vom Hauptgehäuse hinzufügen

So fügen Sie ein Mitgliedsgehäuse vom Hauptgehäuse aus zur Gruppe hinzu:

1. Auf der Seite **Übersicht** des Hauptgehäuses klicken Sie auf **Konfigurieren** > **Mitglied hinzufügen**.
   Das Fenster **Gruppenmitglieder ändern** wird angezeigt. Die ermittelten Gehäuse werden unter **Verfügbare Gehäuse** angezeigt.
2. Wählen Sie die Anzahl der Gehäuse aus, die Sie der Gehäusegruppe hinzufügen möchten, und klicken Sie auf **Hinzufügen**.
   Die Liste der hinzugefügten Gehäuse wird unten im Fenster angezeigt.
3. Klicken Sie auf **Fertigstellen**.

### Ein einzelnes Gehäuse zu Gehäusegruppen hinzufügen

So fügen Sie ein einzelnes Gehäuse zur Gehäusegruppe hinzu:

1. Auf der Seite **Übersicht** des Gehäuses klicken Sie auf **Konfigurieren** > **Gehäusegruppe beitreten**.

   **ANMERKUNG:** Der Job **Gehäusegruppe beitreten** schlägt fehl, wenn die Management-Modul-Firmware auf eine frühere Version zurückgestuft wird.

   Das Fenster **Gruppe beitreten** mit allen vorhandenen MCM-Gruppen im Stapel wird angezeigt.
2. Wählen Sie aus der Drop-Down-Liste **Gruppe auswählen** die Gehäuse- oder MCM-Gruppe aus, zu der Sie das Mitgliedsgehäuse hinzufügen möchten.
3. Klicken Sie auf **Fertigstellen**.

   Wenn die MCM-Gruppe mit manueller Onboarding-Richtlinie erstellt wurde, wird die Beitrittsanfrage in der Liste „Ausstehend“ angezeigt. Das Hauptgehäuse muss das Hinzufügen des Mitgliedsgehäuses bestätigen. Das Hauptgehäuse kann die Anfrage genehmigen oder ablehnen.

   Wenn die MCM-Gruppe mit der automatischen Onboarding-Richtlinie erstellt wird, ist keine Genehmigung vom Hauptgehäuse erforderlich. Das einzelne Gehäuse wird automatisch zur MCM-Gruppe hinzugefügt und wird so zum Mitgliedsgehäuse.

4. Melden Sie sich am Hauptgehäuse an, und genehmigen Sie die Anfrage des Mitgliedsgehäuses, der Gehäusegruppe beizutreten.

### Gehäuse aus Gehäusegruppe entfernen

So fügen Sie ein einzelnes Gehäuse zur Gehäusegruppe hinzu:

1. Auf der Gehäuseseite **Übersicht** klicken Sie auf **Konfigurieren** > **Mitglied hinzufügen**.
   Das Fenster **Gruppenmitglieder ändern** wird angezeigt. Die ermittelten Gehäuse werden unter **Verfügbare Gehäuse** angezeigt.
2. Wählen Sie das Gehäuse aus der Liste **Aktuelle Mitglieder** aus.

3. Klicken Sie auf **Gehäuse entfernen**.
4. Klicken Sie auf **Fertigstellen**.

## Zuweisen des Backup-Lead

In einer Umgebung mit mehreren Gehäusen kann das Lead-Gehäuse manchmal zeitweilig ausfallen oder stillgelegt werden. In solchen Fällen muss ein Mitgliedsgehäuse in der MCM-Gruppe als Backup für das Lead-Gehäuse nominiert werden. Das Backup-Lead-Gehäuse wird zum Lead-Gehäuse hochgestuft, wenn das vorhandene Lead-Gehäuse ausfällt oder stillgelegt wird.

1. Klicken Sie im MCM-Dashboard auf **Konfigurieren** > **Backup-Lead Einstellungen bearbeiten**.
   Das Fenster **Backup-Lead Einstellungen bearbeiten** wird angezeigt.

   Wenn ein Backup bereits zugewiesen ist, wird der Name des Backup-Gehäuses im Feld **Aktuelles Backup** angezeigt.
2. Wählen Sie aus der Drop-Down-Liste **Backup zuweisen** den Namen des Mitgliedsgehäuses aus, das Sie als Backup-Lead-Gehäuse auswählen möchten.
3. Wählen Sie aus der Dropdown-Liste **Backup-Synchronisation – Timeout-Warnmeldung** aus.

   Folgende Optionen stehen zur Verfügung:
   - 5 Minuten
   - 10 Minuten
   - 15 Minuten
   - 30 Minuten
   - 60 Minuten
4. Klicken Sie auf **Virtuelle Lead-IP-Konfiguration (optional)** und auf **Weitere Informationen**, um Details zum Aktivieren der virtuellen IP anzuzeigen. Die Details sind:
   - **Das Ändern der Netzwerkeinstellungen wirkt sich möglicherweise auf die virtuelle IP-Konfiguration aus.**
   - **Durch das Deaktivieren der NIC wird auch die virtuelle IP-Adresse deaktiviert.**
   - **Durch das Deaktivieren von IPv4 wird die virtuelle IP-Adresse nicht deaktiviert.**
   - **Wenn Sie VLAN aktivieren, bleibt die virtuelle IP nur innerhalb des angegebenen VLAN zugänglich.**
   - **Durch das Aktivieren/Deaktivieren der DHCP für IPv4 wird die virtuelle IP-Adresse so konfiguriert, dass Sie mit der neuen Subnetzmaske und dem Gateway übereinstimmt.**

   Weitere Informationen finden Sie im Abschnitt Anwendungsfallszenarien.

   Wenn der Job zum Zuweisen eines Mitgliedsgehäuses als Backup-Lead gestoppt wird, wird der Status des Jobs auf der Seite **Jobs** als **Gestoppt** angezeigt. Allerdings wird das Mitgliedsgehäuse als Backup-Lead der Gruppe zugewiesen.
5. Wählen Sie das Kontrollkästchen **Virtuelle IP aktivieren** und geben sie die **statische IPv4-Adresse** ein.

   Wenn die virtuelle IP-Adresse konfiguriert ist, wird die Konsistenz der IP-Adressen erleichtert, wenn die Rolle des Lead-Gehäuses von einem Gehäuse auf ein anderes übertragen wird.

## Hochstufen des Backup-Lead zum Lead

Sie können das Backup-Gehäuse als neues Lead-Gehäuse hochstufen, wenn das vorhandene Lead-Gehäuse ausfällt. Wenn das erste Lead-Gehäuse verfügbar ist, können Sie es auch als Mitgliedsgehäuse zuweisen. Zur Hochstufung des Backup-Gehäuses zum Lead-Gehäuse müssen Sie sich beim Backup-Gehäuse anmelden.

Nach dem Hochstufen des Backup-Gehäuses als Hauptgehäuse:

- Aktualisieren Sie alle Compliance-Berichte für Baselines, die für alle Geräte erstellt werden.
- Trennen Sie alle Profile, die mit einem Steckplatz mit einem Rechnerschlitten verbunden sind, und verbinden Sie sie erneut. Durch das Trennen und erneute Verbinden der Profile wird sichergestellt, dass die Zuweisung dauerhaft ist. Die Aufgabe „Hochstufen“ hat keine Auswirkungen auf Profile, die leeren Steckplätzen zugewiesen sind. Weitere Informationen finden Sie im Abschnitt Anwendungsfallszenarien.

1. Klicken Sie auf der Startseite des Backup-Gehäuses auf **Konfigurieren** > **Zu Lead-Gehäuse hochstufen**.
   Das Fenster **Zu Lead-Gehäuse hochstufen** wird angezeigt.
2. Klicken Sie auf **Hochstufen**.

Nachdem Sie den Backup-Lead als neuen Lead der Gehäusegruppe heraufgestuft haben, führen Sie die folgenden Schritte aus, bevor Sie das alte Lead-Gehäuse wieder in die Produktionsumgebung setzen:

1. Entfernen Sie das alte Lead-Gehäuse aus der Gruppe, um alle Verweise auf das alte Lead-Gehäuse zu entfernen.
2. Entfernen Sie das alte Lead-Gehäuse aus dem Stacking-Netzwerk.

3. Führen Sie eine erzwungene Reset-Aktion mit der REST API aus: `URI:/api/ApplicationService/Actions/ApplicationService.ResetApplication`. Weitere Informationen finden Sie im *Handbuch zu OpenManage Enterprise und OpenManage Enterprise-Modular Edition RESTful API*.

   Der Task „Konfiguration zurücksetzen“ wechselt das alte Gehäuse in ein eigenständiges Gehäuse und kann Teil der Produktionsumgebung sein.

Wenn ein Backup-Lead zum Lead-Gehäuse hochgestuft wird, werden Anforderungen von anderen Mitgliedsgehäusen, die an das frühere Lead-Gehäuse gesendet werden, nicht auf dem MCM-Dashboard des neuen Lead angezeigt. Infolgedessen können bestimmte Mitgliedsgehäuse keine Join-Anforderungen an andere Gruppen im Stapel senden. Um die ausstehenden Anforderungen zu entsperren, führen Sie die folgende API von dem Mitgliedsgehäuse aus aus, von dem die Joining-Anforderungen gesendet wurden, und senden Sie die Anforderungen erneut:

**URI—**`/api/ManagementDomainService/Actions/ManagementDomainService.DeletePendingDomains`

**Method—**`POST`

**Payload—**`empty`

## Lead-Gehäuse stilllegen

Sie können die Stilllegung des vorhandenen Lead-Gehäuses verwenden, um es zu einem Mitgliedsgehäuse der vorhandenen Gruppe oder einem eigenständigen Gehäuse zu machen.

1. Klicken Sie im MCM-Dashboard auf **Konfigurieren** > **Lead-Gehäuse stilllegen**.
   Das Fenster **Lead-Gehäuse stilllegen** wird angezeigt.
2. Wählen Sie eine der folgenden Optionen:
   - Machen Sie es zu einem Mitglied der aktuellen Gruppe.
   - Machen Sie es zu einem eigenständigen Gehäuse.
3. Klicken Sie auf **Stilllegen**.

   Weitere Informationen finden Sie im Abschnitt Anwendungsfallszenarien.

   Alle vorhandenen Firmware-Baselines auf dem alten Hauptgehäuse werden während der Stilllegung in das neue Hauptgehäuse importiert, und ein Job zur Überprüfung der Firmwarecompliance wird initiiert. Aufgrund der Neuerkennung der Anordnung des Gehäuses während der Stilllegung findet ein Onboarding des alten Hauptgehäuses nach Abschluss der Complianceprüfung für importierte Firmware-Baselines statt. Die Bestellung schließt die Geräte im alten Hauptgehäuse aus dem Baseline-Bericht aus. Um diese Einschränkung zu beheben, führen Sie die Complianceprüfung für das heraufgestufte Hauptgehäuse erneut aus, nachdem der Stilllegungsjob abgeschlossen wurde, damit die alten Hauptgeräte im Compliance- oder Baseline-Bericht aufgeführt werden.

   Nach Abschluss der Aufgabe zum Stilllegen des Leads führt das System einige interne Aufgaben durch, um die Zuordnung der Gruppen abzuschließen, was einige Zeit in Anspruch nehmen kann. Eventuelle Unstimmigkeiten bei den Geräteinformationen, nachdem die Aufgabe zum Stilllegen des Leads abgeschlossen wurde, werden nach Abschluss der internen Aufgaben automatisch abgeglichen.

   Wenn Sie ein Hauptgehäuse stilllegen, aktualisieren Sie alle Compliance-Berichte für Baselines, die für alle Geräte erstellt werden.

# Gehäusegruppen bearbeiten

So bearbeiten Sie eine Gehäusegruppe:

1. Klicken Sie auf dem Gehäuse-Dashboard auf **Übersicht** > **Konfigurieren** > **Gehäusegruppe bearbeiten**.
   Der Assistent **Gehäusegruppe bearbeiten** wird angezeigt.
2. Bearbeiten Sie im Bereich **Gruppe definieren** den Gruppennamen und die Beschreibung der Gehäusegruppe, die Sie bearbeiten möchten.

   Die Gruppennamen können Buchstaben und Zahlen enthalten und müssen weniger als 48 Zeichen lang sein. Allerdings dürfen die Gruppennamen keine Leerzeichen und Sonderzeichen enthalten.
3. Wählen Sie die Konfigurationseinstellungen aus, die Sie auf das Mitgliedsgehäuse übertragen möchten und klicken auf **Weiter**.

   Die Einstellungen sind:
   - Alle – Wendet alle Einstellungen des Hauptgehäuses auf das Mitgliedsgehäuse an
   - Benutzerauthentifizierung – Verzeichnisdienste, lokale Benutzer
   - Netzwerkdienste – SNMP, SSH, Remote-RACADM, Webserver
   - Warnungsziel – E-Mail, SNMP-Trap, Systemprotokoll
   - Lokale Zugriffskonfiguration – Gehäuseschalter, Quick Sync, KVM, LCD serieller Zugriff
   - Strom – Stromobergrenze, Redundanz, Priorität des Rechnerschlittens

- Proxy-Einstellungen – Alle Einstellungen
- Sicherheitseinstellungen – Anmeldungs-IP-Bereich, Anmeldungs-/Abmeldesperrungs-Richtlinie
- Sitzungsinaktivitätszeitlimit-Konfiguration – Sitzungsinaktivitäts-Timeout

Der Fensterbereich **Mitglieder hinzufügen** wird angezeigt.

4. Sie können das Gehäuse nach Bedarf hinzufügen oder entfernen. Wählen Sie das Gehäuse aus der Liste „Verfügbare Gehäuse“ aus und klicken Sie auf **Gehäuse hinzufügen**.
5. Klicken Sie auf **Fertigstellen**.

## Gruppen löschen

So löschen Sie eine Gehäusegruppe:

1. Klicken Sie auf dem Gehäuse-Dashboard auf **Übersicht** > **Konfigurieren** > **Gehäusegruppe löschen**.
   Der Assistent **Gruppe löschen** wird angezeigt.
2. Klicken Sie auf **Bestätigen**, um die Gruppe zu löschen.

## MCM-Dashboard

Das MCM-Dashboard wird nur angezeigt, wenn eine Multi-Chassis Management (MCM)-Gruppe erstellt wird. Sie können den Namen der MCM-Gruppe auf der linken Seite des Dashboard anzeigen lassen. Unterhalb des Gruppennamens können Sie die Namen, IPs und Service-Tag-Nummern des Lead- und Mitgliedsgehäuses anzeigen lassen. Das Lead-Gehäuse wird durch „LEAD“ auf der rechten Seite des Gehäusenamens angezeigt und das Backup-Gehäuse wird durch „BACKUP“ angezeigt.

Klicken Sie auf **Topologie anzeigen**, um die Struktur der MCM-Gruppe anzuzeigen.

Klicken Sie auf **Gruppenkonfiguration** für: **Hinzufügen/Entfernen eines Mitglieds Gruppe bearbeiten**, **Gruppen löschen** und **Einstellungen für Backup-Hauptgehäuse bearbeiten**

Im mittleren Abschnitt des MCM-Dashboard wird die Integritäts-Zusammenfassung aller Gehäuse-, Rechner-, Netzwerk-und Speichergeräte in der MCM-Gruppe angezeigt. Sie können die Liste aller Geräte in der Gruppe anzeigen, indem Sie auf **Alle Geräte** in der oberen rechten Ecke des Dashboards klicken.

Unterhalb der Zustandszusammenfassung können Sie die Warnmeldungen anzeigen, die auf der Wichtigkeit der Warnmeldung und des Gerätetyps basieren. Klicken Sie auf **Alle Warnmeldungen**, um die Liste der Warnmeldungen anzuzeigen, die sich auf alle Ereignisse in der MCM-Gruppe beziehen.

Sie können die Details der letzten Aktivitäten, die sich auf die Gruppe beziehen, auf der rechten Seite des Dashboards anzeigen. Die Details bestehen aus dem Namen und dem Status der Aktivität sowie dem Zeitstempel der Aktivität. Klicken Sie auf **Alle benutzerinitiierten Aktivitäten**, um eine Liste aller Aktivitäten anzuzeigen, die mit der Gruppe zusammenhängen, auf der Seite **Jobs** anzuzeigen.

# Stromversorgung des Gehäuses steuern

Sie können das Netzteil des Gehäuses über die OME – Modular-Startseite ein- und ausschalten:

Wenn Sie das Gehäuse manuell ausschalten oder wenn ein Stromnetzausfall zum Ausschalten mehrerer Gehäuse, IOMs und Rechnerschlitten führt, kann das Einschalten aller Gehäuse und Rechnerschlitten zu Fehlern bei Bestandsaufnahme-Jobs für zwei bis drei Stunden führen. Die Bestandsaufnahme-Jobs werden jedoch ohne Auswirkungen auf das Gehäuse und die zugehörigen Komponenten wiederhergestellt.

So steuern Sie die Stromversorgung des Gehäuses:

1. Klicken Sie auf der Startseite auf **Stromsteuerung**, und wählen Sie die gewünschte Option.
   Folgende Optionen stehen zur Verfügung:
   - Ausschalten (nicht ordnungsgemäß)
   - System aus- und wieder einschalten (Hardwareneustart)
   - Abschalten (ordnungsgemäß)

     **ANMERKUNG:** Nach der Anmeldung warten Sie 7 Minuten. Wenn die IP-Adresse nicht verfügbar ist, überprüfen Sie, ob:
     - das Kabel angeschlossen ist.
     - DHCP konfiguriert ist. Stellen Sie sicher, dass das Kabel an einen Top-of-Rack (TOR)-Switch angeschlossen ist, der über eine Verbindung mit dem DHCP-Server verfügt.

   Es wird eine Meldung angezeigt, die Sie dazu auffordert, den Vorgang zu bestätigen.

2. Klicken Sie auf **Bestätigen**, um fortzufahren.

# Gehäuse sichern

Sichern Sie die Gehäuse- und die Rechnerschlitten-Konfiguration für den späteren Gebrauch. Zum Sichern des Gehäuses benötigen Sie Administratorzugriff mit Berechtigung zur Device-Konfiguration. Die Gehäusekonfiguration enthält die folgenden Einstellungen:

- Einrichtung und Konfiguration
- Stromkonfiguration
- Konfiguration des Gehäusenetzwerks
- Konfiguration des Remote-Zugriffs
- Standortkonfiguration
- Steckplatzkonfiguration
- OME – Modular-Netzwerkeinstellungen
- Benutzereinstellungen
- Sicherheitseinstellungen
- Warnungseinstellungen

Sie können die gesicherte Konfiguration in anderen Gehäusen verwenden.

So erstellen Sie eine Gehäuse-Sicherung:

1. Auf der Seite **Übersicht** klicken Sie auf **Weitere Aktionen** > **Sichern**.
   Das Fenster **Gehäuse sichern** wird angezeigt.
2. Unter **Speicherort der Sicherungsdatei** wählen Sie den **Freigabetyp** aus, in dem Sie die Gehäuse-Sicherungsdatei speichern wollen.

   Folgende Optionen stehen zur Verfügung:
   - CIFS
   - NFS
3. Geben Sie die **Netzwerkfreigabeadresse** und den **Netzwerkfreigabepfad** an.
4. Geben Sie einen Namen für die **Sicherungsdatei** ein.

   Der Dateiname kann alphanumerische Zeichen und Sonderzeichen, Bindestrich (-), Punkt (.) und Unterstrich (_) enthalten.
5. Wenn der **Freigabetyp** CIFS ist, geben Sie Angaben für **Domäne**, **Nutzername** und **Kennwort** ein. Andernfalls fahren Sie mit Schritt 5 fort.
6. Unter **Kennwort der Sicherungsdatei** geben Sie das **Verschlüsselungskennwort** und **Verschlüsselungskennwort bestätigen** ein.

   Die Sicherungsdatei ist verschlüsselt und kann nicht bearbeitet werden.
7. Klicken Sie auf **Sichern**.
   Es wird eine Meldung angezeigt, die darauf hinweist, dass die Sicherung erfolgreich abgeschlossen wurde, und die Seite **Übersicht** des Gehäuses wird angezeigt.

   Sie können den Status und die Details des Sicherungsvorgangs auf der Seite **Überwachung** > **Jobs** anzeigen.

# Gehäuse wiederherstellen

Sie können die Konfiguration eines Gehäuses anhand einer Sicherungsdatei wiederherstellen, wenn die gesicherte Konfiguration von ein und demselben Gehäuse stammt. Sie müssen die Administratorrolle mit Berechtigung zur Device-Konfiguration haben, um das Gehäuse wiederherstellen zu können.

So stellen Sie ein Gehäuse wieder her:

1. Auf der Seite **Übersicht** klicken Sie auf **Weitere Aktionen** > **Wiederherstellen**.
   Das Fenster **Gehäuse wiederherstellen** wird angezeigt.
2. Wählen Sie unter **Speicherort der wiederhergestellten Datei** den **Freigabetyp**, um den Speicherort der Konfigurations-Sicherungsdatei anzugeben.
3. Geben Sie die **Netzwerkfreigabeadresse** und den **Netzwerkfreigabepfad** der Sicherungsdatei an.
4. Geben Sie den Namen der **Sicherungsdatei** ein.
5. Wenn der **Freigabetyp** CIFS ist, geben Sie die **Domäne**, den **Nutzernamen** und das **Kennwort** für den Zugriff auf den freigegebenen Speicherort ein. Andernfalls fahren Sie mit Schritt 6 fort.

6. Geben Sie im Abschnitt **Dateikennwort wiederherstellen** das **Verschlüsselungskennwort** zum Öffnen der verschlüsselten Sicherungsdatei ein.
7. Klicken Sie auf **Wiederherstellen**, um das Gehäuse wiederherzustellen.
   Eine Meldung wird angezeigt, dass das Gehäuse erfolgreich wiederhergestellt wurde.

   Sie können den Status und die Details des Wiederherstellungsvorgangs auf der Seite **Überwachung** > **Jobs** anzeigen.

# Gehäuseprofile exportieren

Sie können Gehäuseprofile exportieren, um die Einstellungen auf ein anderes Gehäuse zu klonen.

So exportieren Sie das Gehäuseprofil:

1. Klicken Sie auf der OME – Modular-Startseite auf **Weitere Aktionen** > **Profil exportieren**.
   Das Fenster **Profil exportieren** wird angezeigt.
2. Wählen Sie den **Freigabetyp**.
3. Geben Sie die Adresse und den Pfad der Netzwerkfreigabe ein.
4. Wenn der **Freigabetyp** CIFS ist, geben Sie die **Domäne**, den **Benutzernamen** und das **Kennwort** für den Zugriff auf den freigegebenen Speicherort ein.
5. Klicken Sie auf **Exportieren**.

# Gehäuse-Failover verwalten

Failover gilt bei Managementmodul-Doppelkonfiguration und ist der Prozess der Übertragung der aktiven Rolle an das Standby-Managementmodul. Sie müssen das aktive Managementmodul neu starten und das Standby-Managementmodul zum Übernehmen der aktiven Rolle neu initialisieren. Der Failover-Vorgang nimmt bis zu 10 Minuten in Anspruch. OME – Modular steht während dieses Prozesses nicht zur Verfügung. Sie müssen über die Berechtigung als Gehäuseadministrator verfügen, um ein Failover zu starten.

**ANMERKUNG:** Nach einem Failover kehrt die Leistung der Gehäuseverwaltung nach ein paar Minuten auf die normalen Werte zurück.

**ANMERKUNG:** Bei einem Failover wird der Stromzustand des Gehäuses auf der Benutzeroberfläche von OME – Modular als "Aus" angezeigt. Der ursprüngliche Stromzustand wird angezeigt, nachdem der Bestand aktualisiert wird.

So starten Sie ein Failover:

Klicken Sie auf der Seite **Übersicht** auf **Weitere Aktionen** > **Failover**.
Es wird die Meldung angezeigt, dass während eines Failovers nicht auf das System zugegriffen werden kann.

# Fehlersuche im Gehäuse

Über die Option zur Problembehebung auf der OME – Modular-Startseite können Sie die folgenden Optionen zur Behebung von Störungen verwenden, die im Gehäuse auftreten:

- Protokoll extrahieren – Verwenden Sie diese Option, um die Anwendungsprotokolle zu extrahieren und sie an NFS- oder CIFS-Speicherorten im Netzwerk zu speichern.
- Diagnosebefehle – Verwenden Sie diese Option, um Diagnosebefehle und Parameter zur Fehlerbehebung im Gehäusenetzwerk auszuführen.
- Gehäuseverwaltungsmodul zurücksetzen – Verwenden Sie diese Option, um einen Neustart des Managementmoduls (MM) in einer Konfiguration mit einem einzigen Managementmodul und ein Failover in einer dualen MM-Konfiguration durchzuführen.

  **ANMERKUNG:** Während des Prozesses "Auf Werkseinstellungen zurücksetzen" dauert die Synchronisierung etwa 3-5 Minuten. Während dieses Zeitraums akzeptieren die seriellen, KVM- und Quick Sync-Schnittstellen nicht das Werkseinstellungen-Kennwort und der Anmeldeversuch schlägt fehl.
- Serielle Verbindung beenden – Verwenden Sie diese Option, um die vorhandenen seriellen Sitzungen zu beenden.

# Blinkende LEDs

Sie können mit der Option **Blink LED** auf der OME – Modular-Startseite die Gehäuse-LED aus- oder einschalten.

# Schnittstellen für den Zugriff auf OME – Modular

Nach der Konfiguration der Netzwerkeinstellungen in OME – Modular können Sie über verschiedene Schnittstellen remote auf OME – Modular zugreifen. Die folgenden Tabelle listet die Schnittstellen auf, die Sie für den Remote-Zugriff auf OME – Modular verwenden können.

**Tabelle 12. Verwaltungsmodul-Schnittstellen**

| Schnittstelle | Beschreibung |
|---|---|
| Webschnittstelle | Ermöglicht Remote-Zugriff auf den OME – Modular über eine grafische Benutzeroberfläche. Die Webschnittstelle ist in die OME – Modular-Firmware integriert, und der Zugriff erfolgt von einem unterstützten Webbrowser auf der Management Station über die NIC-Schnittstelle. Die Anzahl der für jede Schnittstelle zulässigen Benutzersitzungen ist:<br>● Webschnittstelle – 6<br>● RESTful API – 32<br>● SSH – 4<br>Eine Liste der unterstützten Web-Browser finden Sie im Abschnitt „Unterstützte Browser“ unter *OME - Modular für PowerEdge MX7000-Gehäuse Versionshinweise* verfügbar unter https://www.dell.com/openmanagemanuals. |
| Remote-RACADM-Befehlszeilenschnittstelle | Verwenden Sie dieses Befehlszeilen-Dienstprogramm, um OME – Modular und dessen Komponenten zu verwalten. Sie können Remote- oder Firmware-RACADM verwenden:<br>● Remote-RACADM ist ein Client-Dienstprogramm, das auf einer Management Station ausgeführt wird. Es verwendet die Out-of-band-Netzwerkschnittstelle, um die RACADM-Befehle auf dem Managed System auszuführen, außerdem wird der HTTPs-Kanal verwendet. Die Option `-r` führt den RACADM-Befehl über ein Netzwerk aus.<br>● Firmware-RACADM kann aufgerufen werden, indem Sie sich über SSH oder Telnet bei OME – Modular anmelden. Sie können die Firmware RACADM-Befehle ausführen, ohne die OME – Modular-IP, den Nutzernamen oder das Kennwort festzulegen. Nach der Eingabe an der RACADM-Eingabeaufforderung können Sie die Befehle ohne das Präfix „RACADM“ direkt ausführen.<br>**ANMERKUNG:** Ein Protokoll für die Remote-RACADM-Sitzung (Anmeldung oder Abmeldung) wird auf der Seite **Auditprotokolle** angezeigt, unabhängig vom Remote-RACADM-Status. Die Funktion kann jedoch nicht ausgeführt werden, wenn die Remote-RACADM-Option deaktiviert ist. |
| LCD | Verwenden Sie die LCD auf der Frontblende, um die folgenden Aktivitäten auszuführen:<br>● Anzeigen von Warnungen, OME – Modular-IP oder MAC-Adresse.<br>● DHCP festlegen<br>● Konfigurieren der statischen IP-Einstellungen für OME – Modular.<br>● Anzeigen der OME – Modular-MAC-Adresse für den aktiven MM.<br>● Anzeigen der an das Ende der OME – Modular-IP angehängten MM-ID, wenn VLAN bereits konfiguriert ist.<br>● At-the-Box-Verwaltung – erstellen Sie eine Gruppe, fügen Sie eine Gruppe hinzu, verlassen Sie die Gruppe oder löschen Sie die Gruppe.<br>● At-the-Box Speicherzuordnungsauflösung für das Wechseln von Rechnerschlitten.<br>**ANMERKUNG:** Die Datenaktualisierung kann abhängig von der Antwort von OME-Modular einige Sekunden dauern. Dies dauert normalerweise 1 bis 5 Sekunden, kann jedoch länger dauern, wenn das OME-Modular ausgelastet ist. Wenn es länger als 30 Sekunden dauert, überprüfen Sie die Antwort von OME-Modular mithilfe der GUI oder RACADM.<br>Weitere Informationen zum LCD-Touchpanel finden Sie im *Installations- und Service-Handbuch des Dell EMC PowerEdge MX7000-Gehäuses*. |
| SSH | Verwenden Sie SSH, um eine Verbindung mit dem MX7000-Gehäuse herzustellen und RACADM-Befehle lokal auszuführen. |
| RESTful API und Redfish | Der Redfish Scalable Platforms Management API-Standard wurde von der Distributed Management Task Force (DMTF) definiert. Redfish ist ein Verwaltungsschnittstellenstandard für Systeme der nächsten Generation, das eine skalierbare, sichere und offene Serververwaltung ermöglicht. Es ist eine neue Schnittstelle, die die RESTful- |

**Tabelle 12. Verwaltungsmodul-Schnittstellen (fortgesetzt)**

| Schnittstelle | Beschreibung |
|---|---|
| | Schnittstellensemantik für den Zugriff auf die im Modellformat definierten Daten für die Out-of-band-Systemverwaltung verwendet. Sie ist für zahlreiche Server geeignet, von eigenständigen Servern bis hin zu Rack-Server- und Blade-Server-Umgebungen, sowie für große Cloud-Umgebungen.<br>Redfish bietet die folgenden Vorteile gegenüber bestehenden Serververwaltungsmethoden:<br>● Einfachheit und Nutzbarkeit<br>● Hohe Datensicherheit<br>● Programmierbare Schnittstelle, für die problemlos Skripte erstellt werden können<br>● Entspricht weit verbreiteten Standards<br>Weitere Informationen finden Sie im *OME und OME - Modular REST-API – Handbuch* verfügbar unter https://www.dell.com/openmanagemanuals. |
| SNMP | Verwenden Sie SNMP zum:<br>1. Herunterladen der OME-Modular-MIB-Datei von https://www.dell.com/support.<br>2. Verwenden des MIB Walker-Tools, um Informationen über OIDs zu erhalten.<br>**ANMERKUNG:** SNMP SET wird nicht unterstützt. |
| Seriell | Sie können die serielle Schnittstelle für den Zugriff auf OME – Modular durch Anschließen des Mikro-USB-Anschluss auf der Rückseite des Managementmoduls an einen Laptop und Öffnen eines Terminalemulators verwenden. Über die Benutzeroberfläche, die nun angezeigt wird, können Sie sich beim Managementmodul, bei Networking-EAMs oder Servern (iDRAC) anmelden. Sie können maximal eine serielle Sitzung auf einmal öffnen. |
| Quick Sync | Sie können maximal eine Quick Sync-Sitzung auf einmal öffnen. |
| KVM | Sie können maximal eine KVM-Sitzung auf einmal öffnen. |
| Chassis Direct | Die Chassis Direct-Funktion ermöglicht Ihnen den Zugriff auf Verwaltungskonsolen, wie z. b. iDRAC und Managementmodule von Geräten auf dem MX7000-Gehäuse. |

# Gehäusehardware anzeigen

Klicken Sie auf der OME – Modular Startseite auf **Hardware**, um Hardwarekomponenten anzuzeigen, die im Gehäuse installiert sind. Durch Klicken auf **Geräte** > **Gehäuse** > **Details anzeigen** > **Hardware** können Sie auch Details zur Gehäusehardware anzeigen. Die Hardwarekomponenten umfassen Gehäusenetzteile, Gehäusesteckplätze, Verwaltungsmodul, Lüfter, Temperatur, FRU, Geräteverwaltungsinformationen, installierte Software und Verwaltungsports.

**ANMERKUNG:** Wenn das Netzteil (PSU) fehlt, werden der Zustand und der Stromstatus des Netzteils nicht auf der Seite **Gehäuse** > **Hardware** > **Gehäusenetzteile** angezeigt.

**ANMERKUNG:** Halten Sie beim Entfernen und Einsetzen eines Geräts ein Mindestintervall von zwei Minuten ein.

## Gehäusesteckplatz-Details

Die Seite **Gehäusesteckplätze** zeigt Details der Steckplätze an, die in das Gehäuse eingesetzt sind. Die Details sind: Anzahl, Typ und Name des Steckplatzes, Name des Geräts, Modell, eindeutiger Identifikationscode des Steckplatzes und Anzahl der VLAN-IDs, die mit dem Steckplatz verknüpft sind. Die Seite zeigt außerdem an, ob ein Serverprofil mit dem Steckplatz verknüpft ist.

Auf der Seite **Gehäuseereignisse** können Sie folgende Aufgaben ausführen:

- System neu einsetzen – Setzt die Rechner- oder Speicherschlitten und IOMs virtuell neu ein. Dieser Vorgang simuliert das physische Entfernen und Wiedereinsetzen eines Geräts.
- iDRAC-Reset – Führt einen Hardware-Reset des Steckplatz-basierten Rechnerschlittens durch. Sie können diese Option verwenden, um Probleme mit einer nicht reagierenden iDRAC zu beheben.

# Gehäusealarme anzeigen

Klicken Sie auf der OME – Modular-Startseite auf **Warnungen**, um Details zu Warnungen anzuzeigen, die für Ereignisse im Gehäuse ausgelöst wurden. Durch Klicken auf **Geräte** > **Gehäuse** > **Details anzeigen** > **Warnungen** können Sie auch Details zur Gehäuse-Hardware anzeigen.

Sie können die Liste der Warnungen auf Basis der folgenden erweiterten Filter sortieren:

- Schweregrad
- Bestätigen
- Startdatum
- Enddatum
- Quellenname
- Kategorie
- Unterkategorie
- Meldung

Wählen Sie eine Warnung aus, um eine Zusammenfassung der Warnung anzuzeigen.

Auf der Seite **Warnungen** können Sie auch folgende Aufgaben ausführen:

- **Bestätigen**
- **Bestätigung aufheben**
- **Ignorieren**
- **Exportieren**
- **Löschen**

# Gehäusehardwareprotokolle anzeigen

Die Protokolle der an Hardwarekomponenten ausgeführten Aktivitäten, die dem Gehäuse zugeordnet sind, werden auf der OME – Modular-Seite **Hardwareprotokolle** angezeigt. Die angezeigten Protokolldetails umfassen Schweregrad, Meldungs-ID, Kategorie, Zeitstempel und Beschreibung. Durch Klicken auf **Geräte** > **Gehäuse** > **Details anzeigen** > **Hardwareprotokolle** können Sie die Gehäusehardwareprotokolle anzeigen.

Auf der Seite **Hardwareprotokoll** können Sie folgende Aufgaben ausführen.

- Klicken Sie auf **Erweiterter Filter**, um Protokolle nach Schweregrad, Meldungs-ID, Startdatum, Enddatum oder Kategorie zu filtern.
- Klicken Sie auf **Exportieren** > **Aktuelle Seite exportieren**, um alle angezeigten Protokolle zu exportieren.
- Wählen Sie ein bestimmtes Protokoll aus, und klicken Sie auf **Exportieren**.

**ANMERKUNG:** Beim Durchführen eines `racrestcfg` wird die Meldung „CMC8709- und CMC8710-Protokolle werden jedes zweimal angezeigt, eines für Steckplatz 1 und das andere für Steckplatz 2“ auf der Seite **Hardwareprotokolle** angezeigt.

# OME – Modular konfigurieren

Über das Menü **Anwendungseinstellungen** auf der Startseite können verschiedene Einstellungen für OME – Modular konfigurieren. Hierzu gehören die folgenden Einstellungen:

- Netzwerk
- Benutzer
- Sicherheit
- Warnungen

## Aktuelle RAID-Konfiguration anzeigen

Klicken Sie auf **Anwendungseinstellungen** > **Netzwerk** > **Aktuelle Einstellungen**.
Die aktuellen Netzwerk-, IPv4- und IPv6-Einstellungen werden angezeigt.

## OME – Modular-IP-Adresse konfigurieren

1. Klicken Sie auf **Anwendungseinstellungen** > **Netzwerk** > **Adresskonfiguration**.
2. Stellen Sie sicher, dass die Option **NIC aktivieren** ausgewählt ist.
3. Aktivieren Sie die gewünschte IP-Version, IPv4 oder IPv6.

   **ANMERKUNG:** Das E/A-Modul und OME – Modular müssen in diesem DNS registriert werden. Andernfalls wird die Meldung „Warning: Unit file of rsyslog.service changed on disk, 'systemctl daemon-reload' recommended.“ angezeigt.

   **ANMERKUNG:** Nach dem Neustart von OME – Modular steht die öffentliche Schnittstelle mit der OME – Modular-IP nach ca. 12 Minuten zur Verfügung.

4. Aktivieren Sie die DHCP-Option und geben die IP-Adresse und die anderen Details ein.

## OME – Modular-Web-Server konfigurieren

1. Klicken Sie auf **Anwendungseinstellungen** > **Netzwerk** > **Web Server-Konfiguration**.
2. Stellen Sie sicher, dass die Option **Web-Server aktivieren** ausgewählt ist.
3. Geben Sie den Timeout-Wert in Minuten ein.
4. Geben Sie die Portnummer für den Web-Server ein.

   Sie können eine Portnummer im Bereich von 10 bis 65535 wählen. Die Standardportnummer ist 443.

   Wenn die https-Porteinstellungen des Webservers vom Hauptgehäuse als Teil der Aufgabe zum Hinzufügen oder Verbinden von Mitgliedern auf das Mitgliedsgehäuse angewendet werden, aktualisieren Sie das Inventar für das Hauptgehäuse manuell, um den richtigen https-Port für das Mitgliedsgehäuse auf der Seite **Hardware** > **Gerätemanagementinformationen** zu sehen. Starten Sie das Mitgliedsgehäuse vom Hauptgehäuse aus, um die Portnummer zu sehen.

   Wenn Sie den HTTPS-Port anpassen, versucht OME-Modular automatisch auf den neuen Port umzuleiten. Allerdings funktioniert die Umleitung aufgrund von Sicherheitseinschränkungen des Browsers möglicherweise nicht. Öffnen Sie in einem solchen Fall ein neues Fenster oder eine Registerkarte im Browser und geben Sie die OME-Modular-URL mit dem benutzerdefinierten Port ein. Beispiel: `https://10.0.0.1:1443`

   **ANMERKUNG:** Die Deaktivierung des OME-Modular-Webservers hat keinen Einfluss auf das Starten der OME-Modular-GUI auf der Telefonbuchseite bei der Verwendung von Chassis USB Direct.

   **ANMERKUNG:** Verwenden Sie zum Aktualisieren des Webdienst-Timeouts und des Sitzungskonfigurations-Timeouts das gleiche Gehäuseprofil. Durch die Verwendung desselben Gehäuseprofils wird sichergestellt, dass das Webservice-Timeout und die Sitzungskonfigurations-Timeout synchronisiert werden. Andernfalls werden die Webdiensteinstellungen überschrieben, wenn das Webservice-Timeout aktualisiert und die Sitzungskonfiguration verarbeitet wird.

## Konfigurieren des Inaktivitäts-Timeout für Sitzungen

1. Aktivieren Sie im Abschnitt **Universelles Timeout** das Kontrollkästchen **Aktivieren** und geben Sie die Zeit in Minuten ein, nach deren Ablauf alle Sitzungen beendet werden müssen. Die Dauer kann 1-1440 Minuten betragen.

   Wenn Sie die Dauer des universellen Inaktivitäts-Timeouts eingeben, werden die Inaktivitätsoptionen für die API, die Weboberfläche, die SSH und seriellen Sitzungen deaktiviert.
2. Geben Sie in den Abschnitten **API**, **Weboberfläche**, **SSH** und **Seriell** die Zeit in Minuten ein, nach deren Ablauf die Sitzungen abgeschlossen werden müssen, und die maximale Anzahl der Sitzungen, die Sie aktivieren möchten.

   Die Timeout-Dauer kann 1 bis 1440 Minuten betragen und die maximale Anzahl von Sitzungen kann zwischen 1 und 100 liegen. Die Dauer des Inaktivitäts-Timeouts kann 1-1440 Minuten für API- und serielle Sitzungen, 1-120 Minuten für Weboberflächensitzungen und 1-180 Minuten für SSH-Sitzungen betragen.

   Die maximale Anzahl an Sitzungen pro Schnittstelle ist wie folgt:

   - API—1-100
   - Weboberfläche: 1-6
   - SSH—1-4
   - Seriell: 1

Wenn Sie die aktuelle Version von OME-Modular auf eine frühere Version zurückstufen, ist die maximale Anzahl der unterstützten API-Sitzungen 32. Wenn Sie jedoch OME-Modular auf die neueste Version aktualisieren, die 100-Sitzungen unterstützt, wird dennoch ein Attributwert der API-Sitzung von 32 angezeigt. Sie können den Attributwert manuell auf 100 Sitzungen festlegen.

## Datums- und Uhrzeiteinstellungen von OME – Modular konfigurieren

1. Klicken Sie auf **Anwendungseinstellungen** > **Netzwerk** > **Zeitkonfiguration**.
2. Markieren Sie das Kontrollkästchen **NTP verwenden**, falls erforderlich, und geben Sie die NTP-Server-Informationen ein.
3. Wählen Sie die gewünschte Zeitzone aus.

**ANMERKUNG:** Jede Änderung der Attributeinstellungen führt zu einem Verlust der IP-Adresse oder einer vorübergehenden Nichtverfügbarkeit der OME – Modular-Weboberfläche. Die OME – Modular-Weboberfläche wird jedoch automatisch wiederherstellt.

**ANMERKUNG:** Einige Zeitzonen, die in OME-M unterstützt werden, werden möglicherweise auf Brocade-FC-EAMs nicht unterstützt.

## Proxy-Einstellungen von OME – Modular konfigurieren

1. Klicken Sie auf **Anwendungseinstellungen** > **Netzwerk** > **Proxy-Konfiguration**.
2. Wählen Sie **HTTP-Proxy-Einstellungen aktivieren** aus.
3. Geben Sie die Proxy-Adresse und die Port-Nummer ein.
4. Wenn für den Proxy Authentifizierung erforderlich ist, wählen Sie **Proxy-Authentifizierung aktivieren** aus und geben die Anmeldeinformationen ein.

   Sie können Proxy-Authentifizierung nur dann aktivieren, wenn die Option **HTTP-Proxy-Einstellungen aktivieren** aktiviert ist.
5. Geben Sie die Proxy-Nutzerzugangsdaten ein.
6. Wählen sie **Zertifikatsprüfung ignorieren**,
7. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern oder auf **Verwerfen**, um die Änderungen zu verwerfen.

### EAM-Synchronisation konfigurieren

Sie können die Zeit- und Warnungszielkonfiguration des Lead-Gehäuses im Netzwerk und in den FC-EAMs replizieren.

So konfigurieren Sie die Zeit und das Warnungsziel:

1. Klicken Sie auf **Anwendungseinstellungen** > **Netzwerk** > **EAM-Synchronisationskonfiguration**.
2. Aktivieren Sie die Kontrollkästchen **Zeitkonfiguration des Gehäuses replizieren** und **Warnungszielkonfiguration des Gehäuses replizieren**.
   - MXG610s unterstützt nur drei SNMP-Ziele, OS10 hingegen vier SNMP-Ziele.
     - Bei Verwendung von SNMP wird die IPV4- und IPV6-Replikation von OME-Modular zu EAM unterstützt.
     - Die Verwendung von SNMP, FQND und Hostname wird nur unterstützt, wenn die DNS-Adresse für FC-EAM (Voraussetzung für die DNS-Konfiguration) „Statische Konfiguration der Verwaltungs-IP-Adresse“ ist.
     - Bei Verwendung von SNMP wird die SNMPV2-Replikation für OS10 und die SNMPV1-Replikation für FC-EAM unterstützt.
   - MXG610s unterstützt ebenso wie MSM vier Syslog-Ziele.
     - Bei Verwendung von Syslog werden nur 514 Portnummern von MSM zu Netzwerk-EAM unterstützt.
     - Bei Verwendung von Syslog werden 10 bis 65535 Portnummern von MSM zu FC-EAM unterstützt. Die Portnummer wird als sicherer Port konfiguriert.
3. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

   In der MCM-Umgebung wird die Konfiguration der IOM-Netzwerksynchronisation nur dann vom Haupt- zum Mitgliedsgehäuse propagiert, wenn die Zeit- und Warnzieloptionen ausgewählt werden, wenn die Gehäusegruppe erstellt wird oder Mitglieder zur Gruppe hinzugefügt werden.

### Einstellung der Gerätebezeichnung ändern

1. Klicken Sie auf **Anwendungseinstellungen** > **Netzwerk** > **Einstellung der Gerätebezeichnung**.

2. Wählen Sie die Gerätenamen-Einstellung aus.

## In OME-Modular unterstützte Ports und Protokolle

In der folgenden Tabelle sind die Protokolle und Ports aufgelistet, die in OME-Modular unterstützt werden.

**Tabelle 13. Ports und Protokolle, die in OME Modular unterstützt werden**

| Portnummer | Protokoll | Port-Typ | Maximale Verschlüsselungsstufe | Quelle | Richtung | Ziel | Verwendung |
|---|---|---|---|---|---|---|---|
| 22 | SSH | TCP | 256-Bit | Externe Anwendung | Eingang | OME-Modular | Nur für eingehende Kommunikation erforderlich, wenn FSD verwendet wird. OME-Modular-Administrator muss diesen Port nur bei der Interaktion mit Dell EMC aktivieren. |
| 25 | SMTP | TCP | Keine | OME-Modular | Ausgang | Externe Anwendung | Zum Empfang von E-Mail-Warnungen von OpenManage Enterprise. |
| 53 | DNS | UDP/TCP | Keine | OME-Modular | Ausgang | Externe Anwendung | Für DNS-Abfragen |
| 80 | HTTP | TCP | Keine | Externe Anwendung | Eingang | OpenManage Enterprise Modular | Die Web-GUI Landing Page. Leitet einen Benutzer zu HTTPS weiter. |
| 123 | NTP | UDP | Keine | OME-Modular | Ausgang | NTP-Server | Zeitsynchronisierung (falls aktiviert). |
| 137, 138, 139, 445 | CIFS | UDP/TCP | Keine | OME-Modular | Ausgang | CIFS-Freigabe | So importieren Sie Firmware-Kataloge von der CIFS-Freigabe: |
| 161* | SNMP | UDP | Keine | Externe Anwendung | Eingang | OpenManage Enterprise Modular | Für SNMP-Abfragen. |
| 162 | SNMP | UDP | Keine | Externe Anwendung | Ein/Aus | OpenManage Enterprise Modular | Senden von SNMP Traps und Erhalt einer informierten Anfrage. |
| 443 | HTTPS | TCP | 128 Bit SSL | Externe Anwendung | Ein/Aus | OpenManage Enterprise Modular | Web-GUI. Zum Herunterladen von |

**Tabelle 13. Ports und Protokolle, die in OME Modular unterstützt werden (fortgesetzt)**

| Portnummer | Protokoll | Port-Typ | Maximale Verschlüsselungsstufe | Quelle | Richtung | Ziel | Verwendung |
|---|---|---|---|---|---|---|---|
| | | | | | | | Aktualisierungen und Serviceinformationen von dell.com. Die 256-Bit-Verschlüsselung wird bei der Kommunikation mit OME-Modular mithilfe des HTTPS-Protokolls für die Web-Schnittstelle aktiviert. |
| 514** | Syslog | TCP | Keine | OME-Modular | Ausgang | Syslog-Server | Zum Senden von Warn- und Überwachungsprotokollinformationen an den Syslog-Server. |
| 546 | DHCP | TCP | Keine | OME-Modular | Ausgang | | Netzwerkkonfiguration |
| 636 | LDAPS | TCP | Keine | OME-Modular | Ausgang | Externe Anwendung | AD-/LDAP-Anmeldung für den globalen Katalog. |
| 3269 | LDAPS | TCP | Keine | OME-Modular | Ausgang | Externe Anwendung | AD-/LDAP-Anmeldung für den globalen Katalog. |

Legende:

- *– Sie können bis zu 65535 Ports konfigurieren, ausschließlich der Portnummer, die bereits zugewiesen wurde.
- **– Konfigurierbare Ports

# Benutzer und Benutzereinstellungen konfigurieren

In OME – Modular können Sie bis zu 64 lokale Benutzer erstellen und ihnen bestimmten Rollen und Berechtigungen zuweisen. Mit den Optionen unter **Anwendungseinstelungen** > **Benutzer** können Sie Benutzer hinzufügen und bearbeiten, eine Verzeichnisgruppe importieren und aktive Benutzersitzungen anzeigen und beenden.

**ANMERKUNG:** Sie können Benutzer nur dann erstellen, löschen, aktivieren oder deaktivieren, wenn Sie über die Berechtigungen für Sicherheitseinstellungen verfügen.

## Nutzerkonten anzeigen und bearbeiten

1. Klicken Sie auf **Anwendungseinstellungen** > **Benutzer**
   Auf dieser Seite können Sie eine Liste von Nutzerkonten und ihre Rollen, Nutzertypen und die Angabe, ob das Konto aktiviert ist oder nicht, anzeigen.
2. Wählen Sie einen Benutzer aus, und klicken Sie rechts auf der Seite auf **Bearbeiten**.
3. Bearbeiten Sie die erforderlichen Einstellungen.

**ANMERKUNG:** Sie können nur das Passwort des standardmäßigen „Root“-Kontos ändern.

## Benutzer hinzufügen

1. Klicken Sie auf **Anwendungseinstellungen** > **Benutzer**
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie den **Nutzernamen** ein.

   Der Standardnutzername lautet „root“ und kann nicht bearbeitet werden. Sie können das Standardkonto nicht deaktivieren oder die dem Standardkonto zugeordnete Rolle bearbeiten. Der Nutzername kann 1 bis 16 Zeichen lang sein und Leerzeichen und alphanumerische Zeichen enthalten. Die Sonderzeichen - §, ", /, :, @, und ` werden nicht unterstützt.

   **ANMERKUNG:** Stellen Sie für die serielle Schnittstelle OME – Modular sicher, dass die Länge des lokalen oder Remotenutzernamens höchstens 35 Zeichen beträgt.

   **ANMERKUNG:** Verwenden Sie nicht „system“ als Nutzernamen.

4. Geben Sie das **Kennwort** und **Kennwort bestätigen** ein.

   Das Kennwort kann 8-32 Zeichen lang sein und muss mindestens eines der folgenden Zeichen enthalten:
   - Nummer
   - Sonderzeichen: Die unterstützten Sonderzeichen sind +, &, ?, >, -, }, |, ., !, (, ', ,, _, [, ", @, #, ), *, ;, $, ], /, §, %, =, <, :, {, I
   - Großbuchstaben
   - Kleinbuchstaben
5. Wählen Sie eine Rolle aus.
6. Wählen Sie **Aktiviert**, um das Konto sofort zu aktivieren, nachdem Sie es erstellt haben.

   **ANMERKUNG:** Weitere Informationen zu den Feldern finden Sie in der integrierte Hilfe in der OME – Modular-Webschnittstelle.

## Benutzer aktivieren, deaktivieren und löschen

1. Klicken Sie auf **Anwendungseinstellungen** > **Benutzer**.
   Eine Liste der Nutzerkonten wird angezeigt.
2. Wählen Sie das Konto aus, und klicken Sie dann auf die erforderliche Option oberhalb der Liste der Konten.

## Kennwörter wiederherstellen

Sie müssen über physischen Zugriff auf das Gehäuse verfügen, um die Anmeldeinformationen auf die Standardeinstellungen zurückzusetzen.

### Kennwörter in einem einzigen OME-Modular-Controller wiederherstellen

1. Entfernen Sie den einzelnen OME-Modular-Controller aus dem Gehäuse.
2. Machen Sie den Jumper ausfindig (siehe Platinen-Speicherort: P57 KENNWORT ZURÜCKSETZEN) und setzen Sie den Jumper ein.
3. Setzen Sie den Controller wieder in den Steckplatz ein.
4. Wenn OME-Modular verfügbar ist, melden Sie sich mit dem Benutzernamen „root“ und dem Kennwort „calvin“ an.
5. Nach der Authentifizierung als Root-Benutzer ändern Sie das Kennwort für den Root-Benutzer über die Seite **Anwendungseinstellungen** > **Benutzer**.
6. Melden Sie sich ab und melden Sie sich erneut mit dem geänderten Kennwort an, um sicherzustellen, dass die Anmeldung erfolgreich ist.
7. Entfernen Sie den Jumper und setzen Sie ihn wieder in die Standardpositionen (2 und 3) ein.

### Kennwörter in Dual-OME-Modular-Controllern wiederherstellen

1. Entfernen Sie beide OME-Modular-Controller aus dem Gehäuse.

2. Machen Sie auf einem der Module den Jumper ausfindig (siehe Platinen-Speicherort: P57 KENNWORT ZURÜCKSETZEN) und setzen Sie den Jumper ein.
3. Setzen Sie nur den Controller, in dem der Jumper installiert ist, in das Gehäuse ein.
4. Wenn OME-Modular verfügbar ist, melden Sie sich mit dem Benutzernamen „root“ und dem Kennwort „calvin“ an.
5. Nach der Authentifizierung als Root-Benutzer ändern Sie das Kennwort für den Root-Benutzer über die Seite **Anwendungseinstellungen** > **Benutzer**.
6. Entfernen Sie den Controller, auf dem der Jumper eingesetzt ist, und ermitteln Sie den Jumper.
7. Setzen Sie den Jumper auf die Standardposition und setzen Sie den Controller wieder in das Gehäuse ein.
8. Wenn OME-Modular verfügbar ist, melden Sie sich mit dem geänderten Kennwort an.
9. Setzen Sie den zweiten Controller ein, um die MM-Redundanz wiederherzustellen.

## Benutzergruppen und Berechtigungen

### Tabelle 14. Benutzergruppen und Berechtigungen

| Benutzerrolle | Gehäuse-Administrator | Rechner-Manager | Storage Manager | Fabric-Manager | Viewer |
|---|---|---|---|---|---|
| Berechtigung | | | | | |
| Anwendungsinformationen anzeigen | Ja | Ja | Ja | Ja | Ja |
| Anwendungen wie z. B. Netzwerk, NTP und Proxy einrichten | Ja | Nein | Nein | Nein | Nein |
| Benutzer, Sicherheit Anmeldungsrichtlinien und Zertifikate einrichten | Ja | Nein | Nein | Nein | Nein |
| Warnungsrichtlinien und Warnungsziele überwachen | Ja | Nein | Nein | Nein | Nein |
| Gerätestromregelung | Ja | Ja | Ja | Ja | Nein |
| Gerätekonfigurationsaktionen<br>z. B. Vorlagen anwenden, Profile migrieren und Speicherzuordnungen verwalten | Ja | Ja | Ja | Ja | Nein |
| Aktualisieren der Gerätefirmware | Ja | Ja | Ja | Ja | Nein |
| Gerätevorlagen, Identitäts-Pools und logische Netzwerke erstellen und verwalten | Ja | Ja | Ja | Ja | Nein |
| Firmwarekataloge und Baseline-Richtlinien verwalten | Ja | Ja | Ja | Ja | Nein |
| Strombudget-Konfiguration und -Verwaltung | Ja | Nein | Nein | Nein | Nein |

## Benutzersitzungen verwalten

Sie können bestehende Benutzersitzungen über die Seite **Benutzersitzungen** anzeigen und beenden, wenn Sie über die Berechtigung als Gehäuseadministrator verfügen.

### Benutzersitzungen anzeigen

Klicken Sie im Fenster **Benutzer** auf **Benutzersitzungen**.
Sie können die Liste sowie die Details der angemeldeten Benutzer anzeigen.

### Benutzersitzungen beenden

1. Klicken Sie im Fenster **Benutzer** auf **Benutzersitzungen**.
   Sie können die Details der angemeldeten Benutzer anzeigen.
2. Wählen Sie einen Benutzer aus der Liste aus, und klicken Sie auf **Beenden**.
   Es wird eine Meldung angezeigt, die Sie dazu auffordert, den Beenden-Vorgang zu bestätigen.

# Sicherheitseinstellungen für die Anmeldung konfigurieren

OME – Modular unterstützt die auf IP-Bereichen basierte Zugriffsbeschränkung. Sie können den Zugriff auf einen angegebenen Bereich von IP-Adressen beschränken. Sie können auch Richtlinien für Anmeldesperrung konfigurieren, die nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche Verzögerungen erzwingen.

## Anmeldungs-IP-Bereich konfigurieren

1. Klicken Sie auf **Anwendungseinstellungen** > **Sicherheiht** > **IP-Anmeldebereich**.
2. Wählen Sie **IP-Bereich aktivieren** aus.
3. Geben Sie den IP-Bereich im Format CIDR ein.
   Für IPv4 geben Sie die IP-Adresse im Format 192.168.100.14/24 ein. Für IPv6 geben Sie die IP-Adresse im Format 2001:db8::/24 ein.

## Richtlinienattribute für Anmeldesperrung konfigurieren

1. Klicken Sle auf **Anwendungseinstellungen** > **Sicherheit** > **Richtlinie für Anmeldesperrung**.
2. Wählen Sie **Nach Benutzernamen**, um die Sperrung basierend auf dem Benutzerkonto zu aktivieren. Wählen Sie **Nach IP-Adresse**, um die Sperrung basierend auf der IP-Adresse zu aktivieren.
3. Geben Sie die Details der Sperrung ein:
   a. Fehlversuche bis Sperrung: Die Anzahl der fehlgeschlagenen Anmeldeversuche. Gültige Werte liegen zwischen 2 und 16.
   b. Fenster für Fehlversuche bis Sperrung: Der Zeitraum, in dem nachfolgende fehlgeschlagene Anmeldeversuche registriert werden. Die gültige Zeitdauer liegt zwischen 2 und 65535 Sekunden.
   c. Sperrdauer: Der Zeitraum, während dessen Anmeldungen beschränkt sind. Die gültige Zeitdauer liegt zwischen 2 und 65535 Sekunden.

Wenn die IP immer noch nicht verfügbar ist, stellen Sie Folgendes sicher:

- Das Netzwerkkabel ist angeschlossen.
- Wenn DHCP konfiguriert ist, stellen Sie sicher, dass das Kabel mit einem ToR-Switch, der Konnektivität zum DHCP-Server bietet, verbunden ist.

## FIPS-Modus aktivieren

USA Regierungsbehörden und Vertragspartner verwenden die FIPS-Standards. FIPS-Modus dient dazu, die Anforderungen von FIPS 140-2 Ebene 1 zu erfüllen.

Zum Aktivieren des FIPS-Modus klicken Sie auf **Anwendungseinstellungen** > **Sicherheit** > **Federal Information Processing Standards (FIPS)**

**ANMERKUNG:** Nach dem Aktivieren des FIPS-Modus oder Zurücksetzen der Konfiguration warten Sie einen Moment, bis sich die Anwendung stabilisiert.

## Verwaltung von Zertifikaten

Sie können Einzelheiten der SSL-Zertifikate im Fenster **Zertifikate** anzeigen. Diese Angaben umfassen folgende Details:

- Die Organisation, an die das Zertifikat ausgestellt wurde.
- Die ausstellende Zertifizierungsstelle des Zertifikats.
- Die Gültigkeit des Zertifikats.

Wenn Sie die Berechtigung für Sicherheitseinstellungen haben, können Sie die folgenden Aufgaben ausführen:

- Die bereitgestellten SSL-Zertifikate anzeigen.
- Eine neue Zertifikatsignierungsanforderung (CSR) erstellen.
- Laden Sie das Serverzertifikat, das auf der generierten CSR basiert, um das standardmäßige oder derzeit verwendete Zertifikat zu ersetzen.

### Zertifikate hochladen

So laden Sie Zertifikate hoch:

1. Klicken Sie auf **Anwendungseinstellungen** > **Sicherheit** > **Zertifikate**.
2. Klicken Sie auf **Hochladen**, um nach dem Zertifikat zu suchen und es hochzuladen.

### Erstellen einer Zertifikatsignierungsanforderung

1. Klicken Sie auf **Anwendungseinstellungen** > **Sicherheit** > **Zertifikate**.
2. Klicken Sie rechts unten auf der Seite auf **Zertifikatsignierungsanforderung erstellen**.
3. Geben Sie die erforderlichen Einzelheiten ein, wie Eindeutiger Name, Unternehmensname, Primärer Alternativer Antragstellername, Sekundärer Alternativer Antragstellername, Tertiärer Alternativer Antragstellername (SAN) und Quaternärer Alternativer Antragstellername.

   SAN muss einen gültigen Domänennamen enthalten. OME-Modular unterstützt keine Platzhaltereinträge für SAN.
4. Klicken Sie auf **Erstellen**.
   - OME – Modular erstellt kein SSL-Zertifikat bei einer Zeitänderung oder bei jedem Systemstart oder bei gleichzeitiger Zeitänderung und Systemstart.
   - OME – Modular generiert ein neues SSL-Zertifikat mit Gültigkeit von build_time bis (build_time +10 Jahre) nur bei Erststart-Szenarien wie z. B. Firmwareupdates, `racresetcfg` und FIPS-Modusänderungen.

   **ANMERKUNG:** Nur Benutzer mit Rechten als Gehäuseadministrator können Zertifikatsignierungsanforderungen erstellen.

# Warnungen konfigurieren

In diesem Abschnitt können Sie die E-Mail-Adresse, SNMP und die Syslog-Einstellungen zum Auslösen von Warnungen konfigurieren.

## E-Mail-Benachrichtigungen konfigurieren

1. Klicken Sie auf **Anwendungseinstellungen** > **Warnungen**.
2. Klicken Sie auf **E-Mail-Konfiguration**.
3. Geben Sie die **SMTP-Server-Netzwerkadresse** ein.

   **ANMERKUNG:** Die SMTP-Server-Netzwerkadresse darf maximal aus 255 Zeichen bestehen.
4. Wenn für den Server Authentifizierung erforderlich ist, markieren Sie **Authentifizierung aktivieren**.

   **ANMERKUNG:** Wenn **Authentifizierung aktivieren** ausgewählt ist, müssen Sie den Nutzernamen und das Kennwort angeben, um auf den SMTP-Server zuzugreifen.

5. Geben Sie die **SMTP-Portnummer** ein.
6. Wenn der SMTP-Server für die Verwendung von SSL konfiguriert ist, aktivieren Sie die Option **SSL**.

## SNMP-Benachrichtigungen konfigurieren

Die SNMP-Warnungen enthalten die Service-Tag-Nummer des Gehäuses als einen der Parameter in der Trap. Konsolen von Drittanbietern können anhand dieser Informationen die Traps mit dem System korrelieren.

Für Netzwerk-EAMs und Rechnerschlitten bezieht OME – Modular Warnungen über interne private VLANs, entweder SNMP oder REST. Für MXG610s Fibre-Channel-Switch-Module wird nur SNMP V1 unterstützt, und Sie können nur vier SNMP-Warnungsziele konfigurieren.

Sie können das SNMP-Warnungsziel für EAMs über die Seite **Anwendungseinstellungen** > **Warnungen** > **SNMP-Konfiguration** konfigurieren. Nach der Konfiguration des SNMP-Ziels gehen Sie zu **E/A-Einstellungen** > **Warnungsziele replizieren**.

Führen Sie zum Konfigurieren der SNMP-Warnungen die folgenden Schritte aus:

1. Wählen Sie im Hauptmenü **Anwendungseinstellungen** > **Warnungen**.
2. Klicken Sie auf **SNMP-Konfiguration**.
3. Zum Aktivieren der Konfiguration wählen Sie **Aktivieren**.
4. Geben Sie die **Zieladresse** ein.

   Sie können bis zu vier SNMP-Ziele konfigurieren.
5. Wählen Sie die **SNMP-Version** aus.

   Die verfügbaren SNMP-Versionen sind:
   - SNMP V1
   - SNMP V2

   **ANMERKUNG:** Für MX9116n oder MX5108n EAMs wird SNMP V2 unterstützt. SNMP V1 unterstützt nur MXG610s FC IOM.

   **ANMERKUNG:** Das MX7000-Gehäuse ermöglicht die Konfiguration von vier SNMP Zielen. Die MXG610s-FC-IOM-Switches unterstützen jedoch nur drei SNMP-Ziele. Wenn das vierte SNMP-Ziel konfiguriert ist, wird es vom IOM ignoriert.
6. Geben Sie den **Communitystring** ein.

   Beim Konfigurieren des Communitystrings für SNMP v1 wird an den Communitystring standardmäßig `|common|FibreChannel11` angehängt.
7. Wählen Sie die **Portnummer** aus, und klicken Sie auf **Senden** zum Testen der SNMP-Traps.

## Systemlog-Warnungen konfigurieren

Sie können bis zu vier Syslog-Ziele konfigurieren.

Zum Konfigurieren der Systemprotokoll-Warnungen führen Sie folgende Schritte aus:

1. Klicken Sie auf **Anwendungseinstellungen** > **Warnungen** > **Syslog-Konfiguration**.
2. Markieren Sie das Kontrollkästchen **Aktiviert** für den jeweiligen Server.
3. Geben Sie die Zieladresse oder den Hostnamen ein.
4. Geben Sie die Schnittstellennummer ein.

# 5

# Rechnerschlitten verwalten

OME – Modular ermöglicht das Zuweisen und Verwalten von Rechnerschlitten zum Ausgleichen der Workload-Anforderungen.

Sie können die Liste und Details der Rechnerschlitten auf der Seite **Rechnerschlitten** anzeigen. Die Details sind: Funktionszustand, Stromzustand, Name, IP-Adresse, Service-Tag-Nummer und Modell des Gehäuse. Sie können auch einen Rechnereinschub auswählen, um eine grafische Darstellung und Zusammenfassung des Rechnerschlittens im rechten Bereich der Seite **Rechnerschlitten** anzuzeigen.

Wählen Sie einen Rechnerschlitten aus der Liste aus, um auf der rechten Seite eine Zusammenfassung des Schlittens anzuzeigen. Die Zusammenfassung enthält Verknüpfungen zum Starten des iDRAC und virtueller Konsolen, den Namen des Rechnerschlittens, Gerätetyp, Service-Tag-Nummer, Management-IP-Adresse, Modell und Funktionszustand.

Wenn Sie über Rechner-Manager-Rechte verfügen, können Sie auf dieser Registerkarte die folgenden Aufgaben ausführen:

- **Stromsteuerungs**-Tasks
  - **Ausschalten (nicht ordnungsgemäß)**
  - **System aus- und wieder einschalten (Hardwareneustart)**
  - **Systemzurücksetzung (Warmstart)**
  - **Abschalten (ordnungsgemäß)**
  - **Systemzurücksetzung**
  - **Einschalten**
- Schalten Sie die LEDs über **Blink LED** ein und aus.
- Aktualisieren Sie die Bestandsaufnahme.

  **ANMERKUNG:** Wenn ein Rechnerschlitten in ein Gehäuse eingesetzt wird, wird mitunter die Meldung „Kein Geräteimage gefunden“ angezeigt. Um dieses Problem zu beheben, aktualisieren Sie manuell die Bestandsaufnahme des Rechnerschlittens.

Nach dem Ausführen einer Power-Operation auf Rechnerschlitten wechseln einige Schlitten nicht sofort in den gewünschten Zustand. In diesem Fall wird der tatsächliche Status des Rechnerschlittens während der nächsten Integritäts- oder Bestandsaktualisierung aktualisiert.

**ANMERKUNG:** Wenn Rechnerschlitten und Fabric-EAM nicht übereinstimmen, wird der Zustandsstatus des Rechnerschlittens oder des EAM im Gehäuse-Subsystem als „Warnung“ angezeigt. Der Funktionszustand wird jedoch nicht in der grafischen Darstellung des Gehäuses auf den Seiten **Gehäuse**, „E/A-Module“ und **Rechnerschlitten** angezeigt.

**ANMERKUNG:** Gelegentlich erhalten Sie Meldungen, die besagen, dass das Gerät offline ist. Diese Meldungen werden protokolliert, wenn die Statusabfrage für das Gerät angibt, dass das Gerät vom eingeschalteten Zustand in den Offline-Status gewechselt ist.

### Themen:



# Rechnerübersicht anzeigen

Auf der Seite Rechner-**Übersicht** können Sie links eine grafische Darstellung des Rechners anzeigen. Die Rechnerinformationen werden unterhalb der grafischen Darstellung angezeigt. Die Informationen beinhalten Details wie iDRAC-DNS-Name, Modell, Service-Tag, Asset-Service-Tag, Express-Servicecode, Management-IP, System-Betriebsdauer, bestückte DIMM-Steckplätze und Gesamtzahl der DIMM-Steckplätze im Rechner. Sie können auch Details zum Betriebssystem und zu den Standortinformationen einsehen.

**ANMERKUNG:** Der angezeigte Wert für **Spitzenstrom** ist der letzte Spitzenwert, unabhängig vom Stromzustand des Geräts oder der Komponente.

Im mittleren Bereich der Seite **Übersicht** wird die Anzahl der verschiedenen ausgelösten **Letzten Warnungen** im Rechner angezeigt. Details zu den Warnungen werden unten angezeigt.

Unterhalb der **Letzten Warnungen** befindet sich der Abschnitt **Kürzlich durchgeführte Aktivitäten**, in dem die Liste der letzten Aktivitäten im Zusammenhang mit dem Rechner angezeigt wird. Status und Zeitstempel des Abschlusses der Aktivitäten werden ebenfalls angezeigt. Klicken Sie auf **Alle anzeigen**, um die Liste aller Aktivitäten auf der Seite **Jobs** anzuzeigen.

**ANMERKUNG:** Die angezeigte Zeit basiert auf der Zeitzone des Systems, von der aus auf OME-Modular zugegriffen wird.

Rechts auf der Seite wird eine grafische Darstellung der Remote-Konsole angezeigt. Unter des Remote-Console-Image finden Sie folgende Links:

- **iDRAC starten**: Zeigt die iDRAC-Nutzeroberfläche an.
- **Virtuelle Konsole starten**: Öffnet die virtuelle Konsole.

Die Optionen **iDRAC starten** oder **Virtuelle Konsole starten** sind basierend auf Folgendem nicht deaktiviert:

- Bereitschaft von iDRAC
- Zustand **Ausgeschaltet** des Rechnerschlittens
- Verfügbarkeit der Express-Lizenz in iDRAC
- Status des Firmwareupdates in iDRAC
- Status der virtuellen Konsole

Internet Explorer und Safari weisen außerdem bestimmte Einschränkungen auf, die die Wiederverwendung von OME – Modular-Sitzungen beschränken. Das heißt, Sie werden aufgefordert, die OME – Modular Nutzerzugangsdaten für den Zugriff auf iDRAC einzugeben.

**ANMERKUNG:** Die Vorschau der virtuellen Konsole ist für Nutzer mit der **Nutzerrolle** „Viewer“ nicht verfügbar.

Eine Zusammenfassung der Informationen über die Server-Subsysteme wird unterhalb des Remote-Konsolen-Bildes angezeigt. Die Informationen umfassen den Funktionszustand der Komponenten wie Akku, Speicher, Prozessor und Spannung.

**ANMERKUNG:** Die **URSACHE** für **SEL/misc** ist möglicherweise leer, wenn die Integrität des **SEL/Misc**-Subsystems nicht OK ist. Es gibt **SEL**-Ereignisse, denen kein unter **URSACHE** angezeigter Fehler zugeordnet ist. Suchen Sie in diesem Fall nach dem Hardwareprotokoll, um Details zum **SEL**-Ereignis zu erhalten.

Der Abschnitt **Umgebung** rechts unten auf der Seite **Übersicht** zeigt die Temperatur- und Netzteilinformationen des Rechners an. Sie können auch Leistungs- und Temperaturstatistiken des Rechners einsehen.

Klicken Sie im Fenster **Stromstatistik** auf **Zurücksetzen**, um die Energieversorgungs-Statistiken und den Start des Überwachungszeitraums zurückzusetzen.

Die Temperaturstatistiken werden möglicherweise nicht angezeigt, wenn der Server ausgeschaltet ist. Warten Sie nach dem Einschalten des Servers mindestens 24 Stunden, bis die Temperaturstatistiken angezeigt werden.

**ANMERKUNG:** Der Temperaturstatistik-Zeitstempel bleibt nach einem Failover oder einem Neustart des Verwaltungsmoduls unverändert.

**ANMERKUNG:** Der angezeigte Wert für **Spitzenstrom** ist der letzte Spitzenwert, unabhängig vom Stromzustand des Geräts oder der Komponente.

Wenn Sie über Rechner-Manager-Rechte verfügen, können Sie auf dieser Registerkarte die folgenden Aufgaben ausführen:

- **Stromsteuerungs**-Tasks
  - **Ausschalten (nicht ordnungsgemäß)**: Schaltet den Serverstrom aus (entspricht dem Drücken des Netzschalters, wenn der Serverstrom eingeschaltet ist). Diese Option ist deaktiviert, wenn der Server bereits aus ist. Es erfolgt keine Benachrichtigung des Serverbetriebssystems.
  - **System aus- und einschalten (Kaltstart)**: Schaltet den Server aus und anschließend wieder ein (Kaltstart). Diese Option ist deaktiviert, wenn der Server bereits aus ist.
  - **Server zurücksetzen (Softwareneustart)**: Startet den Server neu (führt einen Reset des Servers durch), ohne dass er ausgeschaltet werden muss (Softwareneustart).
  - **Ausschalten (ordnungsgemäß)**: Benachrichtigt das Serverbetriebssystem, dass der Server ausgeschaltet werden soll. Diese Option ist deaktiviert, wenn der Server bereits aus ist.

    **ANMERKUNG:** Für das Linux-Betriebssystem: Konfigurieren Sie die für das ordnungsgemäße Herunterfahren und zur Vermeidung von Watchdog-Neustartfehlern erforderlichen Stromversorgungseinstellungen als „Aus“. Weitere Informationen finden Sie unter https://topics-cdn.dell.com/pdf/red-hat-entps-lx-v70_release-notes_en-us.pdf.
  - **System neu einsetzen** – Entfernt den Rechnerschlitten virtuell.
  - **Einschalten**: Schaltet den Serverstrom ein (entspricht dem Drücken des Netzschalters, wenn der Serverstrom ausgeschaltet ist). Diese Option ist deaktiviert, wenn der Server bereits eingeschaltet ist.
- Extrahieren Sie **SupportAssist**-Protokolle, und setzen Sie iDRAC über **Troubleshooting** zurück.

SupportAssist wird verwendet, um Hardware-, Betriebssystem- und RAID-Controller-Protokolle an einem gemeinsam genutzten CIFS- oder NFS-Speicherort zu sammeln und aufzubewahren.

iDRAC-Reset hilft beim Troubleshooting, wenn keine Kommunikation mit iDRAC möglich ist.

- Schalten Sie die LEDs über **Blink LED** ein und aus. Folgende Optionen stehen zur Verfügung:
  - **1 Minute**
  - **10 Minuten**
  - **30 Minuten**
  - **1 Stunde**
  - **Unbestimmt**

# Rechnereinstellungen konfigurieren

Sie können die folgenden Rechnereinstellungen konfigurieren:

- Netzwerk
- Verwaltung

## Rechnernetzwerkeinstellungen konfigurieren

Sobald die "Quick Deploy"-Einstellungen auf einen Rechnerschlitten angewendet werden, werden die Einstellungen möglicherweise nach einiger Zeit aufgrund von Datenaktualisierungen in OME-Modular gemeldet.

So konfigurieren Sie die Rechnernetzwerkeinstellungen:

1. Klicken Sie auf **Geräte** > **Rechner** > **Details anzeigen** > **Einstellungen** > **Netzwerk**.
2. Im Abschnitt **Allgemeinen Einstellungen** markieren Sie das Kontrollkästchen "LAN-Aktivierung", um die Netzwerkeinstellungen zu konfigurieren.
3. Konfigurieren Sie die IPv4-, IPv6- und Verwaltungs-VLAN-Einstellungen.

## Rechnerverwaltungseinstellungen konfigurieren

So konfigurieren Sie die Rechnerverwaltungseinstellungen:

1. Klicken Sie auf **Geräte** > **Rechner** > **Details anzeigen** > **Einstellungen** > **Verwaltung**.
2. Konfigurieren Sie das Kennwort für den Zugriff auf die iDRAC-Konsole, und wählen Sie **IPMI über LAN** aus, um den Zugriff von OME – Modular über das BIOS auf iDRAC zu ermöglichen.

# Rechnerschlitten ersetzen

Mithilfe der Funktion "RIP-and-Replace" von OME-Modular können Sie einen fehlerhaften Rechnerschlitten, Speicherschlitten oder EAM ersetzen und die Konfiguration automatisch anwenden.

**ANMERKUNG:** Stellen Sie beim Austausch von Rechnerschlitten Folgendes sicher:

- Der Rechnerschlitten ist ausgeschaltet und die Rechner-Nodes im Gehäuse enthalten PERC oder HBA Controller.
- SAS EAMs und Speicherschlitten sind im Gehäuse installiert.

- Wenn Sie einen Rechnerschlitten mit einer Service-Tag-Nummer mit einem Rechnerschlitten einer anderen Service-Tag-Nummer ersetzen und die Speicherschlitten dem Rechner-Node-Steckplatz zugeordnet sind, wird die Stromzufuhr zum jeweiligen Rechnerschlitten ausgeschaltet. Eine Option zum Aufheben der Stromunterbrechung wird auf der Seite **Geräte** > **Rechner** > **Übersicht** für den Rechnerschlitten angezeigt.
- Wenn Sie einen Rechnerschlitten entfernen, der einen HBA 330-Controller mit gemeinsam genutzten Zuordnungen enthält, und ihn durch einen Rechnerschlitten ersetzen, der einen PERC-Controller enthält, wird der Schlitten geprüft, um sicherzustellen, dass keine gemeinsam genutzten Zuordnungen vorhanden sind. Wenn gemeinsam genutzte Zuordnungen vorhanden sind, wird auf der Seite **Geräte** > **Rechner** > **Übersicht** für den Rechnerschlitten eine Meldung angezeigt, die Sie dazu auffordert, die Zuordnung zu löschen. Der Rechnerschlitten ist ausgeschaltet.
- Wenn Sie einen Rechnerschlitten mit einem PERC-Controller mit Zuweisungen entfernen und ihn durch einen neuen Rechnerschlitten mit einem HBA 330-Controller mit einer anderen Service-Tag-Nummer ersetzen, wird eine Meldung in **Geräte** > **Rechner**

> **Übersicht** angezeigt, in der Sie aufgefordert werden, die Zuordnung zu löschen oder zu akzeptieren. Allerdings ist der Rechnerschlitten in diesem Szenario eingeschaltet.

Das folgende Flussdiagramm und die folgende Tabelle veranschaulichen das Verhalten von OME-Modular und des LCD-Bereichs auf dem Gehäuse, wenn der Rechnerschlitten ausgetauscht wird:

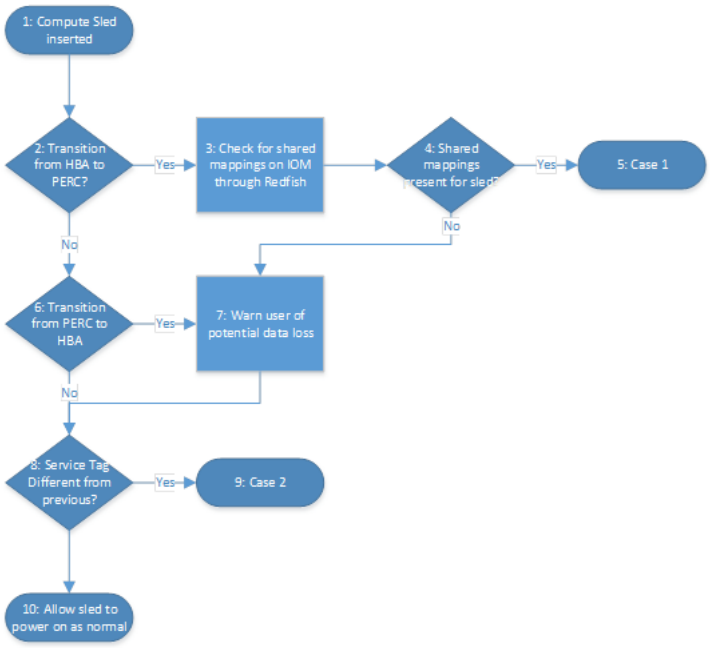



**Abbildung 1. Austausch von Rechnerschlitten – Flussdiagramm**

**Tabelle 15. Austausch des Rechnerschlittens – Verhalten von OME-Modular und des LCD-Bereichs**

| | Verhalten von OME-Modular | Verhalten des LCD |
|---|---|---|
| Fall 1 | Ermöglicht es Benutzern, alle Zuordnungen zum Rechnerschlitten zu löschen. | Ermöglicht es Benutzern, alle Zuordnungen zum Rechnerschlitten zu löschen. |
| Fall 2 | Ermöglicht es Benutzern, alle Zuordnungen zum Rechnerschlitten zu löschen oder zu speichern. | Ermöglicht es Benutzern, alle Zuordnungen zum Rechnerschlitten zu löschen oder zu speichern. |

# Rechnerhardware anzeigen

Sie können die Details der Hardwarekomponenten, die im Rechnerschlitten installiert sind, auf der Seite **Hardware** anzeigen. Die Hardwarekomponenten umfassen Prozessor, Speicher-Controller und FRU.

Die Bereitstellungs- und Konfigurations-Jobs auf dem Rechnerschlitten werden nur zum ersten Mal durchgeführt, wenn das Profil und die Schlitten-Geräte-ID unverändert sind. Wenn der Schlitten entfernt und wieder eingesetzt wird, wird der Bereitstellungs- und Konfigurations-Job nicht ausgeführt. Diese Bedingung gilt auch für die Aufgabe **Profil bearbeiten**.

**ANMERKUNG:** Wenn die Speicher-Controller-Karten in iDRAC nicht vorhanden sind, werden die Details des Speichergehäuses auf der Seite **RechnerDetails anzeigenHardwareSpeichergehäuse** nicht angezeigt.

# Rechnerfirmware anzeigen

Sie können die Firmwareliste für den Rechner auf der Seite **Firmware** anzeigen. Klicken Sie auf **Geräte** > **Rechner** > **Details anzeigen** > **Firmware**.

Die Details umfassen den Namen des Geräts oder der Komponente, eine Auswirkungsabschätzung, die aktuelle Version und die Baseline-Version.

Auf der Seite Firmware können Sie folgende Aufgaben ausführen:

- Wählen Sie aus dem Dropdownmenü **Baseline** eine Baseline aus, um die Liste der Komponenten und ihre aktuellen und Baseline-Firmware-Versionen anzuzeigen. Sie können die Komponente auswählen, für die Sie die Firmware aktualisieren möchten.
- Die vorhandene Firmware auf dem Rechner mit **Firmware aktualisieren** aktualisieren.
- Die aktualisierte Firmwareversion auf die vorhergehende Version mit **Rollback der Firmware** zurückstufen.
- Den Firmware-Baseline-Bericht in einem `.csv`– Format mit der Option **Exportieren** exportieren.

# Rechnerhardwareprotokolle anzeigen

Die Protokolle der an Hardwarekomponenten ausgeführten Aktivitäten, die dem Gehäuse zugeordnet sind, werden auf der Seite **Hardwareprotokolle** angezeigt. Die angezeigten Protokolldetails umfassen Schweregrad, Meldungs-ID, Kategorie, Zeitstempel und Beschreibung.

Zum Anzeigen der Hardwareprotokolle klicken Sie auf **Geräte** > **Rechner** > **Details anzeigen** > **Hardwareprotokolle**.

Auf der Seite **Hardwareprotokolle** können Sie die folgenden Aufgaben ausführen:

- Protokolle mit **Erweiterter Filter** filtern – Sie können Protokolle nach Schweregrad, Meldungs-ID, Startdatum, Enddatum oder Kategorie filtern.
- Protokolle auswählen und Kommentare für diese mit **Kommentar hinzufügen** einschließen.
- Protokolle exportieren, die auf der aktuellen Seite angezeigt werden, oder mit **Exportieren** bestimmte Protokolle exportieren.

# Rechnerwarnungen anzeigen

Sie können die Liste der Warnungen für Rechner auf der Seite **Warnungen** anzeigen.

Zum Anzeigen der Warnungen für Rechnerschlitten klicken Sie auf **Geräte** > **Rechner** > **Details anzeigen** > **Warnungen**.

Sie können die Liste der Warnungen auf Basis der folgenden erweiterten Filter sortieren:

- Schweregrad
- Bestätigen
- Startdatum
- Enddatum
- Kategorie
- Unterkategorie
- Meldung

Sie können eine Warnung auswählen, um im rechten Bereich der Seite **Warnungen** eine Zusammenfassung anzuzeigen.

Auf der Seite **Warnungen** können Sie auch folgende Aufgaben ausführen:

- **Bestätigen**
- **Bestätigung aufheben**
- **Ignorieren**
- **Exportieren**
- **Löschen**

# 6

# Verwalten von Profilen

OME – Modular ermöglicht Ihnen Serverprofile zu erstellen und sie auf Rechnerschlitten oder Steckplätze anzuwenden.

- Sie können folgende für das **Profil** spezifischen Vorgänge ausführen:
  - **Profil erstellen**
  - **Profil anzeigen**
  - **Profil bearbeiten**
  - **Profil zuweisen**
  - **Profil aufheben**
  - **Profil erneut bereitstellen**
  - **Profil migrieren**
  - **Profil löschen**

**Themen:**



## Erstellen eines Profils

Sie können Profile basierend auf den Server-Vorlagen erstellen.

So erstellen Sie ein Profil:

1. Wählen Sie auf der Seite **Profile** ein Profil aus und klicken Sie auf **Erstellen**.
   Der Assistent **Profile erstellen** wird angezeigt.
2. In der Registerkarte **Vorlage** wählen Sie **Vorlage auswählen** und klicken **Weiter**.
   Die Registerkarte **Details** wird angezeigt.
3. Geben Sie auf der Registerkarte **Details Namenspräfix**, **Beschreibung** und **Profilanzahl** für das Profil ein und klicken Sie auf **Weiter**.

   **ANMERKUNG:** Sie können maximal 100 Profile auf einmal erstellen.

   Die Registerkarte **Start auf Netzwerk-ISO** wird angezeigt.
4. Wählen Sie **Start auf Netzwerk-ISO** aus, geben Sie folgende Informationen zur Dateifreigabe ein und klicken Sie auf **Weiter**.
   - **Freigabetyp**: Wählen Sie nach Bedarf CIFS oder NFS.
   - **ISO-Informationen**: Geben Sie den ISO-Pfad ein.
   - **Freigabeinformationen**: Geben Sie die Freigabe-IP-Adresse, die Arbeitsgruppe, den Benutzernamen und das Kennwort ein.
   - **Zeit zum Anfügen der ISO**: Wählen Sie die Dauer des Anhängens von ISO aus dem Dropdown-Menü.
   - **Verbindung testen**: Zeigt den Status der Testverbindung an.

   Die Registerkarte **iDRAC-Management IP** wird angezeigt.
5. Klicken Sie auf **Fertigstellen**.

## Anzeigen des Profils

Mit dieser Funktion können Sie nur Profil- und Netzwerkdetails des ausgewählten Profils anzeigen.

- **Profil anzeigen**: Sie können die Informationen zu „Start auf Netzwerk-ISO“, „iDRAC-Management-IP“, „Zielattribut“ und „Virtuelle Identitäten“ anzeigen, die sich auf das Profil beziehen.
- **Netzwerk anzeigen**: Sie können die Informationen zu Bandbreiten und VLANs anzeigen, die sich auf das Profil beziehen.

Wählen Sie auf der Seite **Profile** ein Profil, klicken Sie auf **Anzeigen** und wählen Sie **Profil anzeigen**aus.
Der Assistent **Profil anzeigen** wird angezeigt.

# Bearbeiten des Profils

Sie können das Profil umbenennen und bearbeiten, um die vorhandenen Einstellungen zu ändern.

## Profil umbenennen

Der Assistent **Profil umbenennen** ermöglicht Ihnen, den Namen des Profils zu ändern.

1. Wählen Sie auf der Seite **Profile** ein Profil, klicken Sie auf **Bearbeiten** und wählen Sie **Umbenennen** aus.
   Der Assistent **Profil umbenennen** wird angezeigt.
2. Ändern Sie den Profilnamen und klicken Sie auf **Fertigstellen**.

## Profil bearbeiten

Mit der Funktion **Profil bearbeiten** können Sie Profilnamen, Netzwerkoptionen, iDRAC-Management-IP-Adresse, Zielattribute und nicht zugewiesene virtuelle Identitäten ändern. Sie können die Profilmerkmale bearbeiten, die für das Gerät oder den Steckplatz spezifisch sind.

1. Wählen Sie auf der Seite **Profile** ein Profil, klicken Sie auf **Bearbeiten** und wählen Sie **Profil bearbeiten** aus.
   Der Assistent **Profil bearbeiten** wird angezeigt.
2. Bearbeiten Sie auf der Registerkarte **Details** den Namen und die Beschreibung des Profils und klicken Sie auf **Weiter**.
   Die Registerkarte **Start auf Netzwerk-ISO** wird angezeigt.
3. Wählen Sie **Start auf Netzwerk-ISO** aus, geben Sie folgende Informationen zur Dateifreigabe ein und klicken Sie auf **Weiter**.
   - **Freigabetyp**: Wählen Sie nach Bedarf CIFS oder NFS.
   - **ISO-Informationen**: Geben Sie den ISO-Pfad ein.
   - **Freigabeinformationen**: Geben Sie die Freigabe-IP-Adresse, die Arbeitsgruppe, den Benutzernamen und das Kennwort ein.
   - **Zeit zum Anfügen der ISO**: Wählen Sie die Dauer des Anhängens von ISO aus dem Dropdown-Menü.
   - **Verbindung testen**: Zeigt den Status der Testverbindung an.

   Die Registerkarte **iDRAC-Management IP** wird angezeigt.
4. Wählen Sie **Ziel-IP-Einstellungen** und klicken Sie auf **Weiter**. Folgende Optionen stehen zur Verfügung:
   - **IP-Einstellungen nicht ändern**: Es werden keine Änderungen gemacht
   - **Als DHCP festlegen**: Wählen Sie **Ipv4 aktivieren** oder **Ipv6 aktivieren** aus
   - **Als statische IP-Adresse festlegen**: Wählen Sie **Ipv4 aktivieren** oder **Ipv6 aktivieren** und geben Sie die entsprechenden Details ein

   Die Registerkarte **Zielattribute** wird angezeigt.
5. Wählen Sie Komponenten der **Zielattribute** und klicken Sie auf **Weiter.**. Folgende Optionen stehen zur Verfügung:
   - **BIOS**
   - **FC**
   - **System**
   - **Netzwerkadapter**
   - **iDRAC**

   Die Registerkarte **Virtuelle Identitäten** wird angezeigt.
6. Zeigen Sie Informationen zu **Virtueller Identitätspool** an und klicken Sie auf **Weiter**.
   Die Registerkarte **Planen** wird angezeigt.
7. Klicken Sie auf **Fertigstellen**.

# Zuweisen eines Profils

Sie können einem Zielgerät ein Profil zuweisen und bereitstellen.

So weisen Sie ein Profil zu:

1. Wählen Sie auf der Seite **Profil** ein Profil aus und klicken Sie auf **Zuweisen**.
   Der Assistent **Profil bereitstellen** wird angezeigt.
2. Überprüfen Sie auf der Registerkarte **Details** die Details und klicken Sie auf **Weiter**.
   Die Registerkarte **Ziel** wird angezeigt.
3. Wählen Sie **An Steckplätze anhängen** oder **Auf Geräten bereitstellen** und klicken Sie auf **Steckplätze auswählen**.
   Der Assistent **Gerät auswählen** wird angezeigt.
4. Wählen Sie das Gerät unter **Alle Geräte**aus, klicken Sie auf **Fertigstellen** und anschließend auf **Weiter**.
   Die Registerkarte **Start auf Netzwerk-ISO** wird angezeigt.
5. Wählen Sie **Start auf Netzwerk-ISO** aus, geben Sie folgende Informationen zur Dateifreigabe ein und klicken Sie auf **Weiter**.
   - **Freigabetyp** – Wählen Sie nach Bedarf CIFS oder NFS.
   - **ISO-Informationen** – Geben Sie den ISO-Pfad ein.
   - **Freigabeinformationen** – Geben Sie die Freigabe-IP-Adresse, die Arbeitsgruppe, den Benutzernamen und das Kennwort ein.
   - **Zeit zum Anfügen der ISO** – Wählen Sie die Dauer des Anhängens von ISO aus dem Dropdown-Menü.
   - **Verbindung testen** – Zeigt den Status der Testverbindung an.

   Die Registerkarte **iDRAC-Management IP** wird angezeigt.
6. Wählen Sie **Ziel-IP-Einstellungen** und klicken Sie auf **Weiter**. Folgende Optionen stehen zur Verfügung:
   - **IP-Einstellungen nicht ändern** – Es werden keine Änderungen gemacht.
   - **Als DHCP festlegen** – Wählen Sie **Ipv4 aktivieren** oder **Ipv6 aktivieren** aus.
   - **Als statische IP-Adresse festlegen** – Wählen Sie **Ipv4 aktivieren** oder **Ipv6 aktivieren** und geben sie die entsprechenden Details ein.

   Die Registerkarte **Zielattribute** wird angezeigt.
7. Wählen Sie Komponenten der **Zielattribute** und klicken Sie auf **Weiter.**. Folgende Optionen stehen zur Verfügung:
   - **BIOS**
   - **FC**
   - **System**
   - **Netzwerkadapter**
   - **iDRAC**

   Die Registerkarte **Virtuelle Identitäten** wird angezeigt.
8. Zeigen Sie Informationen zu **Virtueller Identitätspool** an und klicken Sie auf **Weiter**.
   Die Registerkarte **Planen** wird angezeigt.
9. Wählen Sie die Optionen für **Planen** unter folgenden aus:
   - **Jetzt ausführen** – Wählen Sie diese Option, um das Profil sofort auf dem Server bereitzustellen.
   - **Zeitplan aktivieren** – Wählen Sie diese Option, um das Datum und die Uhrzeit für die Profilbereitstellung auszuwählen.

   **ANMERKUNG:** Die Option **Zeitplan aktivieren** wird für die Bereitstellung des auf Steckplatz basierten Profils nicht unterstützt.

   **ANMERKUNG:** Wenn Sie **Zeitplan aktivieren** auswählen, wird die Profilbereitstellung zur geplanten Zeit ausgeführt, selbst wenn Sie **Jetzt ausführen** vor dem Zeitplan ausgeführt haben. Der Job zum Bereitstellen des Profils schlägt fehl, wenn er zur geplanten Zeit ausgeführt wird, und es wird eine Fehlermeldung angezeigt.
10. Klicken Sie auf **Fertigstellen**.

# Aufheben der Profilzuweisung

Sie können die **Zuweisung** des Profils zu ausgewählten Zielen und damit die Verknüpfung der Profile mit den Zielen aufheben. Sie können nur Profile auswählen, die den Status „zugewiesen“ oder „bereitgestellt“ haben. So heben Sie die Zuweisung des Profils auf:

1. Wählen Sie das aufzuhebende zugewiesene Profil aus.
2. Klicken Sie im Menü „Aktionen“ auf **Zuweisung aufheben**. Das Fenster **Profil aufheben** wird angezeigt.
3. Im Assistenten **Aufheben der Zuweisung** von Profilen ist standardmäßig die Option **Zurückfordern von Identitäten erzwingen** aktiviert. Diese Aktion fordert die Identitäten von diesem Gerät zurück, und der Server wird zwangsweise neu gestartet. Alle auf dem Server konfigurierten VLANs werden entfernt.
4. Klicken Sie auf **Fertigstellen**.

**ANMERKUNG:** Der Job **Profil aufheben** wird nicht erstellt, wenn die Aktion auf das zugewiesene Profil angewendet wird, dessen letzter Jobstatus für gerätebasierte Bereitstellung **Geplant** ist.

# Profil erneut bereitstellen

Sie können Profile, die sich im Status „Bereitgestellt“ befinden, erneut bereitstellen.

Wenn die Einstellungen **Quick Deploy** und **Profil** für den Steckplatz aktiviert sind, wird jedes Mal, wenn ein Schlitten eingesetzt wird, ein Bereitstellungs- und Konfigurationsauftrag erstellt. Wenn das Profil RAID-Attribute enthält, werden die RAID-Einstellungen neu konfiguriert. Deaktivieren Sie **Quick Deploy**, wenn eine RAID-Konfiguration im Profil vorhanden ist.

So stellen Sie das Profil erneut bereit:

1. Wählen Sie auf der Seite **Profile** ein bereitgestelltes Profil aus, das Sie erneut bereitstellen möchten, und klicken Sie auf **Erneut bereitstellen**.
   Der Assistent für die Bestätigungsanforderung wird angezeigt.
2. Klicken Sie auf **Ja**, um das erneute Bereitstellen des Profils zu bestätigen.
   Der Assistent für die erneute Bereitstellung wird angezeigt.
3. Wählen Sie auf der Registerkarte **Attribut-Bereitstellungsoptionen** die Option **Nur geänderte Attribute** oder **Alle Attribute**. Ist ein Neustart erforderlich, wählen Sie die Option **Host-Betriebssystem nicht zwangsweise neu starten, wenn der ordnungsgemäße Neustart fehlschlägt** und klicken Sie auf **Weiter**.
   Die Registerkarte „Planen“ wird angezeigt.
4. Wählen Sie die Planungsoption aus, um das Profil erneut bereitzustellen. Folgende Optionen stehen zur Verfügung: **Jetzt ausführen** und **Zeitplan aktivieren**.
5. Klicken Sie auf **Fertigstellen**.

# Migration eines Profils

Profil migrieren: Sie können ein Profil von einem Server auf einen anderen migrieren. Das System hebt die Zuweisung der Identität des ersten Servers vor der Migration auf. Wenn die Aufhebung fehlschlägt, zeigt das System einen kritischen Fehler an. Sie können den Fehler außer Kraft setzen und die Migration auf einen neuen Server erzwingen.

So migrieren Sie Profileinstellungen:

1. Wählen Sie auf der Seite **Profile** ein Profil aus und klicken Sie auf **Migrieren**.
   Der Assistent **Profil migrieren** wird angezeigt.
2. Klicken Sie im Fenster **Auswahl** auf **Ziel auswählen**.
   Der Assistent **Geräte auswählen** wird angezeigt.
3. Wählen Sie das Gerät oder Gehäuse, auf das Sie das Profil migrieren möchten. Klicken Sie auf **Fertigstellen** und auf **Weiter**.
   Die Registerkarte **Planen** wird angezeigt.
4. Wählen Sie die Option Planen, um die Profileinstellungen zu migrieren. Folgende Optionen stehen zur Verfügung: **Jetzt ausführen** und **Zeitplan aktivieren**.
5. Klicken Sie auf **Fertigstellen**.

# Löschen eines Profils

Sie können Profile löschen, auf denen keine Profilaktionen ausgeführt werden und die sich im Status „Nicht zugewiesenes Profil“ befinden.

So löschen Sie das Profil:

1. Wählen Sie auf der Seite **Profile** die Profils aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
   Der Assistent für die Bestätigungsanforderung wird angezeigt.
2. Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.

# 7

# Speicher verwalten

Dieses Kapitel beschreibt die Speicher- und EAM-Funktionen von OME – Modular. Es enthält außerdem Einzelheiten über das Durchführen verschiedener speicherbezogener Aufgaben. Die SAS-EAMs verwalten die Speichergehäuse. SAS-EAMs erleichtern die Kommunikation zwischen Speicher und Rechnerschlitten und helfen außerdem bei der Zuordnung von Speicher zu den Rechnerschlitten. Sie können Speichergeräte wie folgt zuweisen:

- Als spezifische Laufwerkschächte-Speicher zu Rechnerschlitten
- Als gesamte Speichergehäuse zu Rechnerschlitten

Sie können mit den auf der Seite "Speicher" verfügbaren Optionen Betriebsvorgänge durchführen, die Firmware aktualisieren, Hardware-Einstellungen verwalten und Warnungen für die Speichergeräte konfigurieren.

Weitere Informationen über SAS Speicher finden Sie unter SAS-EAMs verwalten.

**Themen:**



# Speicherübersicht

Auf der Seite **Speicherübersicht** können Sie alle im Gehäuse installierten Speichergehäuse anzeigen. Sie können auch ein virtuelles Neueinsetzen des Speichergehäuses durchführen und ein Blinken der LEDs zum Identifizieren der Speichergehäuse aktivieren.

So zeigen Sie die verfügbaren Speichergehäuse oder Schlitten an:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Speicher** aus.
2. Wählen Sie einen Speicherschlitten aus der Liste der Speichergeräte aus.
3. Klicken Sie auf **Details anzeigen**.

Die Seite **Übersicht** wird angezeigt.

## Neueinsetzen des Speichergehäuses durchführen

Sie können ein Neueinsetzen des Speichergehäuses im Remote-Zugriff über OME – Modular durchführen. Die Option zur Systemzurücksetzung simuliert das Entfernen und die Neuinstallation des Schlittens.

So führen Sie das Neu einsetzen des Speichersystems durch:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Speicher** aus.
2. Wählen Sie den Speicherschlitten aus, Sie neu einsetzen möchten.
3. Klicken Sie auf **Power Control**, und klicken Sie auf **Systemzurücksetzung**.
4. Klicken Sie auf **Bestätigen**.

**ANMERKUNG:** Falls der Speicherschlitten Rechnerschlitten zugewiesen ist, die eingeschaltet sind, führt dies zu einer Unterbrechung der Eingabe/Ausgabe.

## Blinkende LED

Sie können einen Speicherschlitten innerhalb eines Gehäuses ausfindig machen, indem Sie die Schlitten-LED blinken lassen. Dies ist hilfreich bei der Identifizierung eines Systems. So schalten Sie das LED-Blinken ein:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Speicher** aus.
2. Wählen Sie den Speicherschlitten aus.
3. Klicken Sie **Blink LED**, und klicken Sie auf **Einschalten**.

So schalten Sie das LED-Blinken aus:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Speicher** aus.
2. Wählen Sie den Speicherschlitten aus.
3. Klicken Sie auf **Blink LED**, und klicken Sie auf **Ausschalten**.

Sie können die Speicherschlittenschächte aus dem Gehäuse herausziehen, um auf die Speicherschlittenlaufwerke zugreifen zu können. Wenn ein Fach geöffnet ist, befindet sich das Speicherschlittenlaufwerk außerhalb des Gehäuses und hat Kühlungsunterstützung, was dazu führt, dass die Temperatur des Laufwerks einen kritischen Wert erreicht. Wenn das Fach geöffnet ist, zeigt der LCD einen Countdown von fünf Minuten abwärts an. Schließen Sie das Fach innerhalb von fünf Minuten für die Kühlung des Speicherlaufwerks. Wenn ein anderes Fach, das einen Speicherschlitten enthält, geöffnet ist, wird die aktuelle Warnanzeige nicht beeinflusst. Sie können die Anzeige der LCD-Warnmeldung verwerfen.

**ANMERKUNG:** Das LCD-Display der Speicherzuordnung aufgrund von Serveraustausch hat Vorrang vor dem Öffnen des Speicherfachs. Wenn LCD die Anzeige der Speicherzuordnungsmenüs abgeschlossen hat und ein Speicherfach noch geöffnet ist, wird eine Warnung angezeigt, die besagt, dass das Speicherfach geöffnet ist.

## Speicherschlittenzuweisungen bearbeiten

Sie können die Zuordnungen des Geräts mit der Option **Zuweisungen bearbeiten** ändern. So bearbeiten Sie Zuweisungen:

- Auf der Seite **Speicherübersicht** klicken Sie auf **Zuweisungen bearbeiten**.

  Die Seite **Hardware** wird angezeigt.

- Wählen Sie die Hardwarekomponente und ändern die Zuordnung. Weitere Informationen finden Sie unter Laufwerke einem Rechnerschlitten zuweisen.

## Weitere Informationen

Auf der Seite **Hardware** können Sie weitere Informationen zu dem Gerät wie folgt anzeigen:

- **Speichergehäuse-Informationen** – Bietet Informationen über ein Gehäuse, wie z. B. **Name**, **FQDD**, **Modell**, **Service-Tag-Nummer**, **Bestands-Tag**, **Stromzustand**, **Firmware-Version**, **Laufwerksschacht-Zählwert** und **Zuweisungsmodus**
- **Gehäuseinformationen** – Bietet Informationen zu einem Gehäuse, wie z. B. **Gehäuse**, **Steckplatzname** und **Steckplatz**
- **Verbundene E/A-Modulinformationen** – Bietet Informationen zu einem E/A-Modul, wie z. B. **E/A-Modulname** und **Multipfad**
- **Warnungen** – Stellt die Liste der aktuellen Warnungen zur Verfügung
- **Kürzlich durchgeführte -Aktivitäten** – Stellt die Liste der aktuellen Ereignisse zur Verfügung
- **Speichersubsysteme** – Stellt die Liste des Speicher-Subsystems zur Verfügung
- **Umgebung** – Bietet Informationen zum Stromverbrauch

# Hardwaredetails anzeigen

Die Hardwarekomponenten eines Speicherschlittens umfassen Festplatten, Gehäuseverwaltungsmodule (EMMs), Field Replaceable Units (FRUs) und die installierte Software. So können Sie die Details der Hardwarekomponenten im Speicherschlitten anzeigen:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Speicher** aus.
2. Wählen Sie einen Speicher aus der Liste der Speichergeräte aus.
3. Klicken Sie im rechten Fensterbereich auf **Details anzeigen**.
4. Klicken Sie auf **Hardware**, um die Hardwaredetails anzuzeigen. Die Hardwarekomponenten im Speicherschlitten werden im oberen Bereich der Seite **Hardware** angezeigt.

## Energiedetails anzeigen

Um die Liste der Festplatten im Speicherschlitten anzuzeigen, klicken Sie auf **Hardware** > **Festplatten**. Sie können eine Festplatte einem Rechnerschlitten zuweisen.

**ANMERKUNG:** Verwenden Sie die iDRAC-Webschnittstelle, um die Firmware für ein Laufwerk zu aktualisieren.

**Aktueller Modus** – Gibt an, ob die Festplatte einem Gehäuse oder einem einzelnen Serverknoten-Steckplatz zugewiesen ist.

- **Gehäuse zugewiesen** – In diesem Modus können Sie einen ganzen Speicherschlitten einem einzelnen Serverknoten-Steckplatz (oder mehreren) zuweisen.

  **ANMERKUNG:** Speicherzuweisungen sind nicht zulässig, wenn ein redundantes SAS-EAM-Setup temporär in den nicht-redundanten Zustand degradiert wird.

  **ANMERKUNG:** Das Speichergehäuse wird den Steckplätzen der Rechnersteckplätze zugewiesen und nicht dem Schlitten selbst. Wenn ein Rechnerschlitten durch einen anderen Schlitten im gleichen Steckplatz ausgetauscht wird, wird das Speichergehäuse automatisch dem neuen Schlitten zugewiesen. Wenn Sie jedoch den Rechnerschlitten von einem Steckplatz in einen anderen verschieben, müssen Sie den Speicher diesem Schlitten neu zuweisen.
- **Laufwerk zugewiesen** – In diesem Modus können Sie einen Festplattensteckplatz auswählen und einem Serverknoten-Steckplatz zuweisen.

  **VORSICHT: Das Zuweisen eines Festplattenlaufwerks zu einem Rechnerknoten-Steckplatz kann zu Datenverlust führen.**

  **ANMERKUNG:** Wenn das SAS-EAM nicht verfügbar ist, wird für **Aktueller Modus** „Unbekannt“ angezeigt. Dies weist darauf hin, dass ein Kommunikationsfehler vorliegt und keine Zuweisungen durchgeführt werden können.
- **Aktuelle Steckplatzzuweisung(en)**: In diesem Modus wird die Anzahl der Speicher-Rechnerschlitten-Zuweisungen angezeigt.

  **ANMERKUNG:** Wenn ein SAS-EAM aus- und wieder eingeschaltet wird, werden die Informationen zur Speicher-EAM-Zuordnung nach fünf Minuten angezeigt.

  **ANMERKUNG:** Die Zeiten für die Speicherzuweisung variieren je nach Anzahl der ausgewählten Rechnersteckplätze.

  **ANMERKUNG:** Tauschen Sie die Speicherschlitten nacheinander aus, um die Storage-Zuordnung beizubehalten, nachdem ein Schlitten mit einer leeren Service-Tag-Nummer ausgetauscht wurde.

# Festplattenlaufwerke einem Rechnerschlitten zuweisen

Im Modus **Laufwerk zugewiesen** können Sie die Laufwerke in einem Speichergehäuse einem Rechnerschlitten-Steckplatz zuordnen. Wenn der Rechnerschlitten ausfällt, bleibt das Laufwerk dem Steckplatz zugewiesen. Wenn der Schlitten in einen anderen Steckplatz im Gehäuse verschoben wird, müssen Sie die Laufwerke dem neuen Steckplatz neu zuweisen. Zum Konfigurieren von RAID auf den Laufwerken verwenden Sie die iDRAC-Weboberfläche, ein Server-Konfigurationsprofil oder ein Betriebssystem-Bereitstellungsskript, nachdem die Laufwerkzuweisung abgeschlossen ist.

**VORSICHT: Bevor Sie ein Laufwerk einem Steckplatz zuweisen, stellen Sie sicher, dass die Daten aus dem Laufwerk gesichert sind.**

**ANMERKUNG:** Die HBA330-Controllerkarte legt keinen Zustand für die Festplatten fest, wenn die Festplattenlaufwerke aus den Speicherschlitten entfernt werden, nachdem diese Rechnerschlitten zugewiesen wurden.

So weisen Sie ein Laufwerk zu:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Speicher** aus.
2. Wählen Sie einen Speicherschlitten aus der Liste der Speichergeräte aus.
3. Klicken Sie auf **Details anzeigen**.
   Die Seite **Übersicht** wird angezeigt.
4. Klicken Sie auf **Hardware**.
   Das Laufwerksliste wird angezeigt.

   **ANMERKUNG:** Stellen Sie sicher, dass der Modus **Laufwerk zugewiesen** aktiviert ist.
5. Wählen Sie ein oder mehrere Laufwerke aus, und klicken Sie auf **Laufwerkssteckplatz zuweisen**.
   Die Seite **Festplattenlaufwerk einem Rechnerschlitten zuweisen** wird angezeigt.
6. Wählen Sie den Steckplatz aus, und klicken Sie auf **Zuweisen**.

Wenn ein Laufwerk von einem Rechnerschlitten einem anderen zugewiesen wird, bleiben der Gehäusestatus und der hochgefahrene Zustand des Laufwerks gleich. Wenn sich ein Laufwerk im Stromsparmodus befindet, wird der Status des Laufwerks als "Starten" angezeigt.

# Speichergehäuse einem Rechnerschlitten zuweisen

Im Modus **Gehäuse zugewiesen** können Sie ein Speichergehäuse einem oder mehreren Rechnerschlitten mit einer HBA330-Mini-Zusatzkarte zuweisen. Mit diesem Modus können Sie auch ein Speichergehäuse einem leeren Steckplatz zuweisen. Wenn der Schlitten entfernt und in einem anderen Steckplatz installiert wird, muss die Zuordnung erneut durchgeführt werden.

**VORSICHT: Bevor Sie ein Gehäuse einem Steckplatz zuweisen, stellen Sie sicher, dass die Daten aus dem Laufwerk gesichert sind.**

**ANMERKUNG:** Systeme mit H745P MX-Controller unterstützen nur eine einzige Speichergehäusezuweisung.

So weisen Sie ein Gehäuse zu:

1. Wählen Sie in der Drop-Down-Liste **Geräte** die Option **Speicher** aus.
2. Wählen Sie einen Speicherschlitten aus der Liste der Speichergeräte aus.
3. Klicken Sie auf **Details anzeigen**.
   Die Seite **Übersicht** wird angezeigt.
4. Klicken Sie auf **Hardware**, und wählen Sie **Gehäuse zugewiesen** aus.
   Eine Warnmeldung über den Verlust von Daten bei Auswahl dieses Modus wird angezeigt.
5. Wählen Sie **Ich habe zur Kenntnis genommen, dass diese Zuweisung zum Datenverlust führen kann** aus, und klicken Sie auf **Ok**.
6. Wählen Sie den Rechnerschlitten-Steckplätze aus, und klicken Sie auf **Zuweisen**.

   Nach einem Austausch der PERC-Karte sollten Sie eine Weile warten, damit OME – Modular die neuen Bestandsaufnahmedetails vom iDRAC erhält, bevor Sie den Zuweisungsvorgang durchführen. Andernfalls aktualisieren Sie die Bestandsaufnahme auf der Seite **Rechner** manuell.

# Speicherschlitten ersetzen

Wenn Sie einen Speicherschlitten aus einem Steckplatz entfernen und in einen anderen Steckplatz auf dem Gehäuse einsetzen, wird die Zuordnung auf dem neuen Steckplatz für den Speicherschlitten verwendet. Wenn Sie den Speicherschlitten durch einen neuen Schlitten ersetzen, der nicht über ein Service-Tag verfügt, werden das Service-Tag und die Zuordnung des Schlittens, der zuvor im Steckplatz vorhanden war, angewendet. Allerdings wird die Speicherschlitten-Firmware nicht automatisch ausgetauscht.

# Firmware des Gehäuses aktualisieren

Sie können die Speichergehäuse-Firmware unter Verwendung von OME – Modular aktualisieren oder zurückstufen. Verwenden Sie eine der folgenden Methoden, um die Firmware zu aktualisieren:

1. Dell Update Package (DUP)
2. Katalog-basierte Compliance-Methode

**ANMERKUNG:** OME – Modular ist während des Aktualisierungsvorgangs nicht zugänglich.

## Firmware über DUP aktualisieren

1. Laden Sie das DUP von www.dell.com/support/drivers herunter.
2. In der OME – Modular-Webschnittstelle navigieren Sie zur Seite **Geräte** > **Speicher**.
3. Wählen Sie den Speicherschlitten aus, auf dem Sie die Firmware aktualisieren möchten.
4. Klicken Sie auf **Firmware aktualisieren**.
5. Wählen Sie die Option **Einzelnes Paket** aus, und klicken Sie auf **Durchsuchen**, um zum Speicherort des heruntergeladenen DUP zu navigieren.
   Warten Sie, bis der Vergleichsreport die unterstützten Komponenten angezeigt.

6. Wählen Sie die gewünschten Komponenten aus, und klicken Sie auf **Aktualisieren**, um das Firmwareupdate zu starten:
7. Gehen Sie zur Seite **Überwachung** > **Jobs**, um den Jobstatus anzeigen.

## Firmware unter Verwendung der Katalog-basierten Compliance-Methode aktualisieren

1. In der OME – Modular-Webschnittstelle navigieren Sie zur Seite **Geräte** > **Speicher**.
2. Wählen Sie den Speicherschlitten aus, auf dem Sie die Firmware aktualisieren möchten.
3. Klicken Sie auf **Firmware aktualisieren**.
4. Wählen Sie die Baseline aus, und klicken Sie auf **Weiter**.
   Die Seite „Aktualisierung planen“ wird angezeigt.
5. Wählen Sie die **Aktualisierung planen**-Optionen nach Bedarf.
   - **Jetzt aktualisieren** – Wendet die Firmwareupdates sofort an.
   - **Für später planen** – Plant die Firmwareupdates für einen späteren Zeitpunkt. Wählen Sie Datum und Uhrzeit aus.
   - **Serveroptionen**: Wählen Sie, ob Sie das Update nach Bedarf anwenden möchten.
     - **Server sofort neu starten**: Aktivieren Sie dieses Kontrollkästchen, um das Update zu senden und den Server sofort neu zu starten. Sie können die Neustartoptionen aus der Drop-down-Liste auswählen. Die verfügbaren Optionen sind:
       - Ordentlicher Neustart mit erzwungenem Herunterfahren
       - Ordentlicher Neustart ohne erzwungenes Herunterfahren
       - Aus- und Einschalten
     - **Vorbereiten für nächsten Neustart des Servers**: Aktivieren Sie dieses Kontrollkästchen, um das Update an den Server zu senden. Allerdings wird die Aktualisierung erst beim nächsten Neustart des Servers installiert.

   a.

# Speichergehäuse-Firmware zurückstufen

Führen Sie die folgenden Schritte aus, um die Firmware für ein Speichergehäuse zurückzustufen:

1. In der OME – Modular-Webschnittstelle navigieren Sie zur Seite **Geräte Speicher**.
2. Wählen Sie das System aus, und klicken Sie auf **Details anzeigen**.
3. Klicken Sie auf **Firmware zurücksetzen**.
4. Wählen Sie die verfügbaren Version der Firmware aus, und klicken Sie auf **Bestätigen**, um den Vorgang fortzusetzen.

# SAS-EAMs verwalten

Die interne Verbindung des Speicher-Subsystems wird als "Fabric C" bezeichnet. Diese dient als Kommunikationsmodus zwischen Rechnerschlitten und Speichergehäusen. Die "Fabric C" wird für SAS der FC-Speicherkonnektivität verwendet und umfasst eine Mittelplatine. SAS-EAMs ermöglichen das Erstellen von Speicherzuordnungen, in denen Sie Gehäuselaufwerke oder ganze Speichergehäuse Rechnerschlitten zuordnen können. SAS-EAMs bieten Rechnerschlitten Multipath Input Output (MPIO)-Zugriff auf Laufwerkselemente. Das aktive Modul steuert das SAS-EAM und ist zuständig für alle Bestands- und Speicherzuweisungen in der Fabric.

Ein Rechnerschlitten mit einfacher Breite kann eine Fab-C-Zusatzkarte unterstützen, die über einen x4-Link eine Verbindung zu den einzelnen E/A-Modulen herstellt. Jede Lane in dem Link unterstützt 12-Gbit/s-SAS für eine Verbindung von insgesamt 48 Gbit/s für jedes SAS-EAM. In SAS-EAMs werden die Fab-C EAMs verwendet, um SAS-Switching zwischen Rechnerschlitten und internen Speicherschlitten wie z. B. PowerEdge MX5016s zu ermöglichen.

Weitere Informationen zu den Aufgaben, die Sie ausführen können, finden Sie auf der Seite zu E/A-Modulen für SAS unter EAMs verwalten.

## SAS-EAM-Übersicht

Die Seite **SAS-EAM-Übersicht** zeigt Details zu EAM, Gehäuse, die Liste der neuesten Warnungen und aktuelle Aktivitäten an. Die EAM-Informationen umfassen den Namen des Modells, den Leistungszustand, die Firmware-Version, den Fabric-Typ und die Verwaltungsrolle des EAM. Es gibt drei Arten von Verwaltungsrollen:

- Aktiv
- Passiv
- Herabgesetzt

Ein funktionstüchtiges System verfügt über ein „aktives“ und ein „passives“ SAS-EAM.

Die Gehäuseinformationen umfassen den Namen des Gehäuses, den Einschubnamen und die Steckplatznummer.

Informationen über das SAS-EAM-Speichersubsystem werden im rechten Bereich der **Startseite** angezeigt. Die Informationen zum Speichersubsystem umfassen den Namen des Subsystems und den Funktionsstatus. Klicken Sie auf **Details anzeigen**, um die Warnungen und Warnungsdetails anzuzeigen. Die Informationen umfassen die Meldungs-ID, die Meldung, einen Zeitstempel, wann die Warnung ausgelöst wurde und die empfohlene Maßnahme.

So zeigen Sie die EAM-Übersicht an:

1. Klicken Sie in der Menüleiste auf **Geräte** > **E/A-Module**. Die Listenseite **E/A-Module** wird angezeigt.
2. Wählen Sie das Gerät aus, dessen Einzelheiten Sie anzeigen möchten. Eine Zusammenfassung des ausgewählten EAM wird auf der rechten Seite angezeigt. Die Zusammenfassung umfasst Namen des EAM, Gerätetyp, Verwaltungs-IP-Adresse, Modell, Funktionsstatus und Verfügbarkeit.
3. Klicken Sie auf **Details anzeigen**. Die Seite **Übersicht** wird angezeigt.

Auf der Seite **EAM-Übersicht** können Sie die folgenden Aufgaben ausführen:

- Energiesteuerung – Einschalten, Ausschalten, Aus- und Einschalten oder Systemzurücksetzung.
  - Einschalten oder Ausschalten – Nach dem Ausschalten des EAM ist der Status des EAM „Offline“. Als Folge kann der Status des Peer-EAM „Aktiv“ sein. Wenn Sie das EAM aus- und einschalten, erfolgt ein Warmstart des EAM.
  - Aus- und Einschalten – Die Option „Aus- und Einschalten“ leitet einen Warmstart des EAM ein. In diesem Fall wird die Stromzufuhr zum EAM und den Kernsystemen des EAM nicht unterbrochen.
  - System neu einsetzen: Mit der Option „System neu einsetzen“ wird das EAM virtuell entfernt. In diesem Fall wird die Stromzufuhr vom und zum EAM unterbrochen.

    **ANMERKUNG:** Nach dem Neueinsetzen der SAS EAM schaltet sich EAM innerhalb einer Minute ein. Jede Abweichung im Energiestatus des EAM wird durch Aktualisieren des Inventars korrigiert oder automatisch mit dem standardmäßigen Bestandsaufnahme-Task korrigiert.
- Blink LED – Diese sind ein- oder ausgeschaltet zur Identifizierung der EAM-LEDs.
- Konfiguration löschen – Löscht die Speicher-EAM-Konfiguration.
- Protokoll extrahieren – Mit dieser Option extrahieren Sie das EAM-Aktivitätsprotokoll auf einer CIFS- oder NFS-Freigabe.
- Zeigen Sie eine Liste der letzten Warnungen und das Datum und die Uhrzeit, an dem/zu der die Warnungen generiert wurden, im Abschnitt **Letzte Warnungen** an. Zum Anzeigen einer Liste aller Warnungen klicken Sie auf **Alle anzeigen**. Die Seite **Warnungen** mit allen Warnungen, die in einer Beziehung zu dem EAM stehen, wird angezeigt.
- Zeigen Sie eine Liste aller Aktivitäten an, die in einer Beziehung zu dem EAM stehen, den Grad der Fertigstellung der Aktivität, und das Datum und die Uhrzeit, an dem/zu der die Aktivität begann, im Abschnitt **Kürzlich durchgeführte Aktivitäten** an. Zum Anzeigen einer Liste aller Aktivitäten, die in einer Beziehung zu dem EAM stehen, klicken Sie auf **Alle anzeigen**. Die Seite **Jobs** mit einer Liste aller Jobs, die in einer Beziehung zu dem EAM stehen, wird angezeigt.
- Zeigen Sie die Stromstatistik des EAM durch Klicken auf **Stromstatistik anzeigen** im Abschnitt **Umgebung** an. Die Statistiken umfassen den Zeitstempel des Spitzenstroms und den Zeitstempel des minimalen Stromverbrauchs sowie das Datum und die Uhrzeit an dem/zu der die Statistiken aufgezeichnet wurden. Klicken Sie auf **Zurücksetzen**, um die Statistikdaten zum Stromverbrauch zurückzusetzen.

**ANMERKUNG:** Wenn Sie den Vorgang **Löschen** auf einem SAS-EAM durchführen, wird das EAM aktiv, wenn es nicht bereits aktiv ist, und die Speicherkonfiguration auf beiden SAS-EAMs wird gelöscht.

**ANMERKUNG:** Beheben Sie vor der Aktualisierung der Firmware jegliche suboptimalen Funktionszustände des EAM (außer nicht übereinstimmende Firmware). Dieses Vorgehen stellt sicher, dass die Firmware aktualisiert wird, ohne den Funktionszustand des SAS-EAM herabzusetzen.

# Active erzwingen

Sie können **Weitere Aktionen** > **Active erzweingen** zum Durchführen eines Failovers auf einem "passiven" oder "herabgesetzten" Switch verwenden. Das Durchführen eines "Active erzwingen"-Vorgangs auf dem SAS-EAM wird als störender Vorgang angesehen und sollte nur verwendet werden, wenn dies wirklich notwendig ist. Wenn Sie einen "Active erzwingen"-Vorgang durchführen, wird das SAS-EAM "Aktiv", und die zugehörige Speicherkonfiguration wird auf das Gehäuse angewendet.

Sie können die Option **Active erzwingen** in den folgenden Fällen zum Auflösen von Nichtübereinstimmungen verwenden:

- Die Switches wurden zuvor konfiguriert, werden jedoch in ein Gehäuse eingesetzt wird, das zuvor über keine SAS-EAMs verfügte.

- Zwei Switches von zwei verschiedenen Gehäusen werden in ein drittes Gehäuse eingesetzt.

Sie können **Active erzwingen** auch als präventive Maßnahme zur Wartung eines Switch verwenden. Stellen Sie vor dem Entfernen des Switch, der gewartet werden muss, sicher, dass der verbleibende Switch "Aktiv" ist. Dadurch werden Störungen an der Fabric verhindert, die auftreten könnten, wenn ein Switch entfernt wird und der andere Switch "Passiv" ist.

## Konfiguration löschen

Sie können die Speicherkonfiguration der SAS-EAMs über **Weitere Aktionen** > **Löschen** ändern. Wenn Sie auf **Löschen** klicken, wird das SAS-EAM „Aktiv“ und die Speicherkonfiguration wird aus dem Gehäuse gelöscht.

Sie können mit der Option **Löschen** Folgendes ausführen:

- Eine Gehäusekonfiguration in einem Schritt zurücksetzen.
- Ein Problem beheben, bei dem zwei Switches von zwei verschiedenen Gehäusen in ein drittes Gehäuse eingesetzt werden. In diesem Szenario ist es unwahrscheinlich, dass die beiden Switches über die korrekte Konfiguration verfügen. Verwenden Sie die Option **Löschen** zum Löschen der vorhandenen Konfiguration und zum Erstellen einer korrekten Konfiguration.

Verwenden Sie die Optionen **Active erzwingen** und **Löschen**, um auf einige Meldungen der Kategorien „Kritisch“ und „Warnung“ zu reagieren, die in der OME – Modular-Webschnittstelle angezeigt werden, insbesondere bei einer Nichtübereinstimmung bei Konfiguration.

## EAM-Protokolle extrahieren

Sie können ein Protokollpaket für den Support durch Auswahl von **Protokoll extrahieren** erfassen. Das vom SAS-EAM erfasste Protokollpaket enthält außerdem die verbundenen Protokolle von allen Speichergehäusen, die vom EAM ermittelt werden, selbst wenn sie sich derzeit nicht im Gehäuse befinden.

# 8

# Verwalten von Vorlagen

OME – Modular ermöglicht Ihnen die Konfiguration von Servern basierend auf Vorlagen. Eine Servervorlage ist eine Konsolidierung der Konfigurationsparameter, die von einem Server extrahiert und für die schnelle Replikation der Konfiguration auf mehreren Servern verwendet werden. Ein Serverprofil ist eine Kombination von Vorlagen- und Identitätseinstellungen, die auf einen bestimmten oder mehrere Server angewendet oder für die spätere Verwendung gespeichert werden.

Sie müssen über Vorlagenverwaltungs-Berechtigungen verfügen, um Vorlagen erstellen zu können. Eine Servervorlage beinhaltet die folgenden Kategorien:

- BIOS
- SupportAssist
- Netzwerkadapter
- System
- EventFilters
- LifecycleController
- iDRAC

Um die Liste der vorhandenen Vorlagen anzuzeigen, klicken Sie auf **Konfiguration** > **Vorlage**. Die Seite **Bereitstellen** wird angezeigt.

Sie können die Liste der Vorlagen basierend auf dem Namen und dem Status der Vorlage sortieren.

Auf dieser Seite können Sie die folgenden Aufgaben ausführen:

- Vorlage erstellen
- Vorlage bearbeiten
- Vorlage klonen
- Vorlage exportieren
- Vorlage löschen
- Netzwerk bearbeiten
- Vorlage bereitstellen

**Themen:**



# Vorlagendetails anzeigen

So zeigen Sie die Vorlagendetails an:

1. Wählen Sie auf der Seite **Vorlagen** die Vorlage aus, deren Details Sie anzeigen möchten.
   Eine Zusammenfassung der Vorlage wird auf der rechten Seite angezeigt.
2. Klicken Sie auf **Details anzeigen**.
   Die Seite **Vorlagendetails** wird angezeigt.

   Folgende Details werden angezeigt: Name und Beschreibung der Vorlage, Referenzgerät, Zeitpunkt, zu dem die Vorlage zuletzt aktualisiert wurde, und der Name des Benutzers, der sie zuletzt aktualisiert hat. Sie können auch die Konfigurationsdetails anzeigen, wie z. b. BIOS, SupportAssist, NIC, System EventFilters, LifecycleController und iDRAC-Informationen.

   Auf der Seite **Vorlagendetails** können Sie folgende Aufgaben ausführen:

   - Vorlage bereitstellen

- Bearbeiten

# Vorlagen erstellen

Sie können Vorlagen auf folgende Weise erstellen:

- Von einem vorhandenen Server klonen – **Referenzgerät**
- Aus einer externen Quelle importieren – **Aus Datei importieren**

So erstellen Sie eine Vorlage aus einem Referenzgerät:

1. Klicken Sie auf der Seite **Vorlagen** auf **Vorlage erstellen**, und wählen Sie **Von Referenzgerät**.
   Es wird der Assistent **Vorlage erstellen** angezeigt.
2. Geben Sie den Namen und eine Beschreibung für die Vorlage ein, und klicken Sie auf **Weiter**.
   Der Assistent **Referenzgerät** wird angezeigt.
3. Klicken Sie auf **Gerät auswählen**, um die Seite **Geräte auswählen** anzuzeigen, auf der Sie das Gerät oder das Gehäuse auswählen können, auf dessen Basis Sie die Vorlage erstellen möchten.

   Wählen Sie zum Bereitstellen virtueller Identitäten für NIC NIC und iDRAC aus.

   Zum Bereitstellen von virtuellen Identitäten für Fibre Channel müssen Sie iDRAC, NIC und Fibre Channel auswählen.
4. Wählen Sie die Konfigurationselemente aus, die Sie klonen möchten.

## Vorlagen importieren

So importieren Sie eine vorhandene Vorlage:

1. Klicken Sie auf der Seite **Vorlagen** auf **Vorlage erstellen**, und wählen Sie **Aus Datei importieren** aus.
   Das Fenster **Vorlage importieren** wird angezeigt.
2. Geben Sie einen Namen für die Vorlage ein, und **wählen Sie eine Datei aus**, um zu dem Speicherort zu wechseln, an dem die zu importierende Vorlage gespeichert werden soll.

# Vorlagen bearbeiten

Die Funktion **Vorlage bearbeiten** ermöglicht es, Namen und Beschreibung der Vorlage zu ändern.

1. Wählen Sie auf der Seite **Vorlagen** eine Vorlage aus und klicken Sie auf **Bearbeiten**.
   Der Assistent **Vorlage bearbeiten** wird angezeigt.
2. Bearbeiten Sie auf der Registerkarte **Vorlageninformationen** den Namen und die Beschreibung der Vorlage und klicken Sie auf **Weiter**.
   Die Registerkarte **Komponenten bearbeiten** wird angezeigt.
3. Klicken Sie in der Registerkarte **Komponenten bearbeiten** auf **Geführte Ansicht**. Sie können die folgenden Komponenten bearbeiten:
   - **BIOS**: Wählen Sie die Konfigurationsmethode für die BIOS-Einstellungen aus.
   - **Start**: Wählen Sie den Startmodus für die Starteinstellungen aus.
   - **Networking**: Wählen Sie NIC-Teaming aus und klicken Sie auf das Symbol „Bearbeiten“, um die Vorlage zu ändern. Ändern Sie im Assistenten **Vorlage bearbeiten** die folgenden Komponenten und klicken Sie auf **Fertigstellen**.
     - Nicht markiertes Netzwerk
     - Markiertes Netzwerk
     - Bandbreite (Min.)
     - Bandbreite (Max.)
4. Klicken Sie auf **Erweiterte Ansicht**, um die folgenden Komponenten oder Attribute auszuwählen, die in die Vorlage aufgenommen werden sollen, und klicken Sie auf **Weiter**.
   - BIOS
   - SupportAssist
   - Netzwerkadapter
   - System
   - EventFilters
   - Lifecycle Controller

- iDRAC

Die Registerkarte **Zusammenfassung** wird angezeigt.

5. Überprüfen Sie die ausgewählten Komponenten und ihre Konfigurationen auf der Registerkarte **Zusammenfassung**.
6. Klicken Sie auf **Fertigstellen**.

# Cloning von Vorlagen

So erstellen Sie eine Kopie einer Vorlage.

Wählen Sie auf der Seite **Vorlagen** die Vorlage aus, von der Sie eine Kopie erstellen möchten, und klicken Sie auf **Klonen**.

# Vorlagen exportieren

Sie können eine Vorlage auf eine Netzwerkfreigabe oder ein lokales Laufwerk Ihres Systems exportieren.

So exportieren Sie eine Vorlage:

Wählen Sie auf der Seite **Vorlagen** die Vorlage aus, die Sie exportieren möchten, und klicken Sie auf **Exportieren**.
Daraufhin wird eine Meldung angezeigt, um den Exportvorgang zu bestätigen. Die Vorlage wird im Format `.xml` auf ein lokales Laufwerk Ihres Systems exportiert.

# Vorlagen löschen

So löschen Sie Vorlage:

1. Wählen Sie auf der Seite **Vorlagen** die Vorlagen aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
   Es wird eine Meldung angezeigt, die Sie dazu auffordert, den Löschvorgang zu bestätigen.
2. Klicken Sie auf **Ja,** um fortzufahren.

   Wenn eine Vorlage gelöscht wird, werden die nicht zugewiesenen Identitäts-Pools in der Vorlage wieder an den Identitäts-Pool zurückgegeben.

   **ANMERKUNG:** Sie können eine Vorlage nicht löschen, wenn es Profile gibt, die mit dieser Vorlage erstellt wurden.

# Vorlagennetzwerke bearbeiten

So bearbeiten Sie die Vorlagennetzwerkdetails:

1. Wählen Sie auf der Seite **Vorlagen** die Vorlage aus, deren Netzwerkdetails Sie ändern möchten, und klicken Sie auf **Netzwerk bearbeiten**.
   Das Fenster **Netzwerk bearbeiten** wird angezeigt.
2. Ändern Sie den **Identitäts-Pool**, falls erforderlich.
3. Wählen Sie die NIC-Teamingoption für den Port aus.

   NIC-Teaming wird für Redundanz empfohlen, obwohl es nicht erforderlich ist. NIC-Partitionierung (NPAR) kann sich auf die Arbeitsweise von NIC-Teaming auswirken. Basierend auf Einschränkungen, die mit der NIC-Partitionierung in Zusammenhang stehen und von NIC-Anbietern implementiert werden, verhindern bestimmte Konfigurationen bestimmte Arten von Teaming. Die folgenden Einschränkungen gelten für die Full Switch- und SmartFabric-Modi:

   - Wenn NPAR nicht verwendet wird, werden sowohl die Switch-abhängigen (LACP) als auch die anderen (Switch-unabhängigen) Teaming-Methoden unterstützt.
   - Wenn NPAR verwendet wird, wird nur die andere (Switch-unabhängige) Teaming-Methode unterstützt. Switch-abhängiges Teaming wird nicht unterstützt.

   Die NIC-Teaming-Funktion ist auf IOM Versionen 10.5.0 und höher anwendbar.

   Detaillierte NIC-Teaming-Anweisungen finden Sie in der Dokumentation des Netzwerkadapters oder des Betriebssystems.

   Sie können aus den folgenden NIC-Teaming-Optionen auswählen:

   - Kein Teaming – NICs sind nicht verstärkt und bieten keinen Lastenausgleich oder Redundanz.

- LACP – Auch Switch-abhängig, 802.3ad oder dynamische Link-Aggregation genannt. Die LACP-Teaming-Methode verwendet das LACP-Protokoll zum Verständnis der Teaming-Topologie. Sie bietet aktiv-aktiv-Teaming mit Lastenausgleich und Redundanz. Mit dieser Option wird nur die native VLAN auf non-LAG-Schnittstellen programmiert. Alle markierten VLANs warten, bis der LACP LAG auf den NICs aktiviert ist. Die folgenden Einschränkungen gelten für LACP-Teaming:
  - Die Shared LOM-Funktion des iDRAC kann nur verwendet werden, wenn „Failover“ auf dem iDRAC aktiviert ist.
  - Wenn das Hostbetriebssystem Windows ist, muss der LACP-Timer auf „langsam“ (bzw. „normal“) eingestellt werden.
- Sonstige – bezieht sich auf eine NIC Teaming-Methode, bei der der Switch die verwendete Teaming-Technologie nicht kennt. Die Option „Sonstige“ verwendet das Betriebssystem und NIC-Gerätetreiber auf dem Server, um die NICs zu verbinden. Jeder NIC-Hersteller bietet eventuell etwas andere Implementierungen mit unterschiedlichen Vor- und Nachteilen.

4. Aktivieren oder deaktivieren Sie **VLAN-Einstellungen weitergeben**. Wenn Sie diese Option auswählen, werden alle Änderungen an VLAN-Einstellungen auf Schlitten übertragen, für die diese Vorlage zuvor vorgesehen waren.

# Vorlagen bereitstellen

Sie können Vorlagen über die Seiten **Vorlagen bereitstellen** und **Vorlagendetails** bereitstellen.

Wenn Sie nach der Bereitstellung einer Vorlage auf einem oder mehreren Servern zusammen mit VLAN-Konfigurationen einen Fehler machen oder die vorhandenen VLAN-Konfigurationen im Fabric Manager ändern möchten, führen Sie den Bereitstellungsworkflow erneut aus. Im Bereitstellungsworkflow wird der Server bereitgestellt, nachdem das VLAN auf dem Fabric-Manager konfiguriert wurde.

Die systemspezifischen Attribute, die in der Vorlage definiert sind, werden nicht automatisch bereitgestellt. Definieren Sie die Attribute für das Zielsystem neu, das für die Bereitstellung ausgewählt ist. Verwenden Sie **Schnelles Bereitstellen**, um die VLAN-ID für das System festzulegen.

Wenn das Attribut `OneTimeBootMode` deaktiviert ist, können Sie die Attribute `OneTimeUefiBootSeq` oder `OneTimeHddSeq` nicht festlegen.

Bevor Sie die Server-Vorlagen anwenden, stellen Sie Folgendes sicher:

- Die Anzahl der Ports im Profil entspricht der des Servers, auf dem Sie die Vorlage bereitstellen möchten.
- Alle Server-Ports auf den Servern, die über das MX7116n Fabric Expander-Modul verbunden sind, sind ordnungsgemäß mit den IOMs verbunden.

Wenn Sie eine importierte Vorlage bereitstellen, bei der NPAR aktiviert ist, konfiguriert sie die Bandbreiteneinstellungen auf den Fabric-Modus-IOMs nicht.

**ANMERKUNG:** Vorlagen, die in früheren Versionen von iDRAC erstellt wurden, können während der Bereitstellung fehlschlagen, wenn sie in den neuesten Versionen von iDRAC verwendet werden.

**ANMERKUNG:** Der Bereitstellungskonfigurationsjob wird automatisch erstellt, wenn das Profil bereits mit den Steckplätzen verbunden ist, wenn die Aufgabe **SystemErase** auf dem Schlitten ausgeführt wird.

**ANMERKUNG:** Die Option **Arbeitsgruppe** in der Registerkarte **Start von Netzwerk-ISO** ist nur verfügbar, wenn der **Freigabetyp** CIFS ist.

So stellen Sie eine Vorlage über die Seite **Vorlagen** bereit:

1. Wählen Sie die erforderliche Vorlage aus und klicken Sie auf **Vorlage bereitstellen**.
   Wenn die Vorlage Identitätsattribute hat, aber keinem virtuellen Identitäts-Pool zugeordnet ist, wird eine Fehlermeldung angezeigt. Daraufhin wird der Assistent**Vorlagen-Bereitstellung** angezeigt.
2. Wählen Sie den Ziel-Steckplatz oder das Gerät aus, auf dem Sie die Vorlage bereitstellen möchten, geben Sie die ISO-Pfad- und Standortdetails ein, konfigurieren Sie die iDRAC-Management-IP-Einstellungen und wählen Sie die Option **Neustart des Hostbetriebssystems nicht erzwingen, wenn ein ordentlicher Neustart fehlschlägt** aus, wenn ein Neustart erforderlich ist.

   Wenn Sie einen belegten Steckplatz auswählen, wird das Kontrollkästchen **Vorlage direkt auf Rechnerschlitten anwenden** angezeigt. Aktivieren Sie das Kontrollkästchen, um den Rechnerschlitten sofort neu einzusetzen und die Vorlage darauf bereitzustellen.

   Das Aktivieren der Option **Neustart des Hostbetriebssystem nicht erzwingen, wenn ein ordentlicher Neustart fehlschlägt** verhindert einen nicht ordnungsgemäßen Neustart des Rechnerschlittens.

   Der Vorgang „Netzwerk-ISO starten“ wird nicht gestartet, wenn der Bereitstellungsvorlagenjob zu einem Attributfehler führt.

   **ANMERKUNG:** Die Bereitstellung von OME-Modular über den Start von einer ISO schlägt möglicherweise fehl, wenn sich OME-Modular und iDRAC in unterschiedlichen Netzwerken befinden, obwohl die Testverbindung erfolgreich ist. Der Fehler kann auf Einschränkungen des Netzwerkprotokolls zurückzuführen sein.

**ANMERKUNG:** Der Rack-Steckplatz und der Rack-Name werden nicht automatisch ausgefüllt, da es sich um zielspezifische Attribute handelt, die für jedes Gerät unterschiedlich sind. Sie können Rack-Details auswählen und hinzufügen, um iDRAC-Attribute zum ausgewählten Gerät hinzuzufügen. Dies kann auch für andere zielspezifische Attribute gelten.

3. Wählen Sie den virtuellen Identitätspool aus oder klicken Sie auf **Identität reservieren** um den erforderlichen Identitätspool für die Bereitstellung der Vorlagen zu reservieren.
4. Planen Sie die Bereitstellung und klicken Sie dann auf **Fertigstellen**.

## Vorlagen über die Seite „Vorlagendetails“ bereitstellen

So stellen Sie eine Vorlage über die Seite **Vorlagendetails** bereit:

1. Klicken Sie auf der Seite **Vorlagendetails** auf **Vorlage bereitstellen**.
   Wenn die Vorlage Identitätsattribute hat, aber keinem virtuellen Identitäts-Pool zugeordnet ist, wird eine Fehlermeldung angezeigt. Daraufhin wird der Assistent**Vorlagen-Bereitstellung** angezeigt.
2. Wählen Sie den Ziel-Steckplatz oder das Gerät aus, auf dem Sie die Vorlage bereitstellen möchten, geben Sie die ISO-Pfad- und Standortdetails ein, konfigurieren Sie die iDRAC-Management-IP-Einstellungen und wählen Sie die Option **Neustart des Hostbetriebssystems nicht erzwingen, wenn ein ordentlicher Neustart fehlschlägt** aus, wenn ein Neustart erforderlich ist und planen Sie die Bereitstellung.

   Wenn Sie einen belegten Steckplatz auswählen, wird das Kontrollkästchen **Vorlage direkt auf Rechnerschlitten anwenden** angezeigt. Aktivieren Sie das Kontrollkästchen, um den Rechnerschlitten sofort neu einzusetzen und die Vorlage darauf bereitzustellen.

   Das Aktivieren der Option **Neustart des Hostbetriebssystem nicht erzwingen, wenn ein ordentlicher Neustart fehlschlägt** verhindert einen nicht ordnungsgemäßen Neustart des Rechnerschlittens.

3. Wählen Sie den virtuellen Identitätspool aus oder klicken Sie auf **Identität reservieren** um den erforderlichen Identitätspool für die Bereitstellung der Vorlagen zu reservieren.
4. Planen Sie die Bereitstellung und klicken Sie dann auf **Fertigstellen**.

# 9

# Identitäts-Pools verwalten

Identität-Pools werden bei der vorlagenbasierten Bereitstellung von Servern verwendet. Sie erleichtern die Virtualisierung von Netzwerkidentitäten, die für den Zugriff auf Systeme mit Ethernet, iSCSI, FCoE oder Fibre Channel (FC) erforderlich sind.
Sie können die zur Verwaltung der I/O-Identitäten erforderlichen Informationen eingeben. Die Identitäten wiederum werden von Gehäuseverwaltungsanwendungen wie z. B. OME – Modular verwaltet.

Wenn Sie einen Serverbereitstellungsprozess starten, wird die nächste verfügbare Identität aus dem Pool abgerufen, um einen Server aus der Vorlagenbeschreibung bereitzustellen. Sie können das Serverprofil von einem Server auf einen anderen migrieren, ohne den Zugriff auf die Netzwerk- oder Speicherressourcen zu verlieren.

Sie können auch Serverprofile Steckplätzen zuordnen. Das Serverprofil verwendet die reservierte Identität aus dem Pool zur Bereitstellung eines Servers.

Um die Liste der Identitäts-Pools anzuzeigen, klicken Sie auf **Konfiguration** > **Identitäts-Pools**.

Die Seite **Identitäts-Pools** mit einer Liste der verfügbaren Identitäts-Pools und deren wichtigsten Attribute wird angezeigt. Auf der Seite **Identitäts-Pools** können Sie folgende Aufgaben ausführen:

- Identitäts-Pools erstellen
- Identitäts-Pools anzeigen
- Identitäts-Pools bearbeiten
- Identitäts-Pools löschen
- Identitäts-Pools exportieren

Bei Intel-NICs verwenden alle Partitionen auf einem Port denselben IQN. Daher wird auf der Seite **Identitätspools** > **Verwendung** ein doppelter iSCSI-IQN angezeigt, wenn die Option **Anzeigen nach** auf "iSCSI" gesetzt ist.

Sie können auch über die RESTful-API-Befehle Identitäts-Pools erstellen und bearbeiten.

**ANMERKUNG:** Die Seite **Identitäts-Pools** zeigt die MAC-Zuordnung an, auch wenn die bereitgestellte Vorlage für das Zielgerät gelöscht wird.

### Themen:



# Identitäts-Pools erstellen

Sie können bis zu 4096 MAC-Adressen in einem Identitäts-Pool erstellen. In folgenden Fällen wird eine Fehlermeldung angezeigt:

- Es liegen Fehler vor, wie z. B. zeitlich überlappende Identitätswerte mit einem vorhandenen Pool.
- Syntaxfehler bei der Eingabe der MAC-, IQN- oder Netzwerkadressen.

Jeder Identitäts-Pool stellt Informationen zum Zustand der einzelnen Identitäten im Pool bereit. Die Zustände können sein:

- Zugewiesen
- Reserviert

Wenn die Identität zugewiesen ist, werden die Informationen über den zugewiesenen Server und die NIC-Kennung angezeigt. Wenn die Identität reserviert ist, werden die Informationen über den zugewiesenen Steckplatz im Gehäuse angezeigt.

Sie können einen Identitäts-Pool mit nur dem Namen und der Beschreibung erstellen und die Details später konfigurieren.

**ANMERKUNG:** Sie können Identitäten durch Deaktivieren der Option **E/A-Identitätsoptimierung** in iDRAC löschen.

So erstellen Sie Identitäts-Pools:

1. Klicken Sie auf **Konfiguration** > **Identitäts-Pools**.

Die Seite **Identitäts-Pools** mit einer Liste der verfügbaren Identitäts-Pools und deren wichtigsten Attribute wird angezeigt.

2. Klicken Sie auf **Erstellen**.
   Der Assistent **Identitäts-Pool erstellen** wird angezeigt.
3. Geben Sie den Namen und eine Beschreibung für den Identitäts-Pool ein, und klicken Sie auf **Weiter**.
   Die Registerkarte **Ethernet** wird angezeigt.
4. Wählen Sie **Virtuelle Ethernet-MAC-Adressen einschließen** zur Eingabe der **Virtuelle MAC- Start-Adresse**, wählen Sie die gewünschte **Anzahl der virtuellen MAC-Identitäten** aus, und klicken Sie auf **Weiter**.

   Die MAC-Adressen können die folgende Syntax aufweisen:

   - `AA:BB:CC:DD:EE:FF`
   - `AA-BB-CC-DD-EE-FF`
   - `AABB.CCDD.EEFF`

   Sie können Identitäts-Pools aus iSCSI, FCoE oder FC erstellen.

   Die Registerkarte **iSCSI** wird angezeigt.
5. Aktivieren Sie die Option **Virtuelle iSCSI-MAC-Adressen einschließen** zur Eingabe der **Virtuellen MAC-Start-Adresse**, und wählen Sie die **Anzahl der iSCSI-MAC-Adresse** oder die gewünschten IQN-Adressen aus.
6. Wählen Sie **iSCSI-Initiator konfigurieren** aus, und geben Sie dann das **IQN-Präfix** ein.

   Der Pool der IQN-Adressen wird automatisch generiert, indem die generierte Zahl an das Präfix angehängt wird, im Format –`<IQN Prefix>.<number>`
7. Wählen Sie **iSCSI-Initiator-IP-Pool aktivieren**, um **IP-Adressbereich**, **Subnetzmaske**, **Gateway**, **Primärer DNS-Server**, und **Sekundärer DNS-Server** einzugeben.

   Die iSCSI-Initiator-IP-Einstellungen werden nur verwendet, wenn iSCSI für Starten konfiguriert ist und wenn die iSCSI-Initiatorkonfiguration über DHCP deaktiviert ist. Wenn die iSCSI-Initiatorkonfiguration über DHCP aktiviert ist, werden alle diese Werte vom einem ausgewiesenem DHCP-Server erhalten.

   Die Felder "IP-Adressbereich" und "Subnetzmaske" werden verwendet, um einen Pool von IP-Adressen anzugeben, die OME – Modular einem Gerät zuweisen kann. Das Gerät kann die IP in der iSCSI-Initiatorkonfiguration verwenden. Im Gegensatz zu den MAC-Adressenpools ist für den IP-Adressbereich kein Zählwert angegeben. Der Pool von IP-Adressen kann auch dazu verwendet werden, die Initiator-IP zu generieren. OME – Modular unterstützt das IPv4-Format des IP-Adressbereichs in den folgenden Formaten:

   - `A.B.C.D - W.X.Y.Z`
   - `A.B.C.D-E, A.B.C.`
   - `A.B.C.D/E` – Dieses Format ist eine Classless Inter-Domain Routing (CIDR)-Schreibweise für IPv4.

   Maximal 64.000 IP-Adressen sind für einen Pool zulässig.

   OME – Modular verwendet die Werte für Gateway, Primärer DNS-Server und Sekundärer DNS-Server während der Bereitstellung einer Vorlage statt der Werte in der Vorlage.OME – Modular weist die Werte für Gateway, Primärer DNS-Server und Sekundärer DNS-Server nicht vom IP-Adressenpool zu, wenn die Werte innerhalb des angegebenen IP-Adressbereichs liegen. Die Werte für Gateway, Primärer DNS-Server und Sekundärer DNS-Server dienen als Ausnahmen vom angegebenen IP-Adressbereich, sofern zutreffend.
8. Sie können die **FCoE-Identität** zur Eingabe der **FIP-MAC-Adresse** auswählen und die gewünschte **Anzahl der FCoE-Identitäten** angeben.

   Die WWPN/WWNN-Werte werden von der MAC-Adresse generiert. Der WWPN-Adresse wird `0x2001` vorangestellt, während die WWNN-Adresse das Präfix `0x2000` erhält. Dieses Format basiert auf einem den FlexAddresses ähnlichen Algorithmus.
9. Aktivieren Sie die Option **FC-Identität einschließen** zur Eingabe des **Postfix (6 Oktette)**, und wählen Sie die **Anzahl der WWPN/WWNN-Adressen**.

# Anzeigen von Identitäts-Pools

Sie können die Details des Identitäts-Pools anzeigen.

Wählen Sie den erforderlichen Identitäts-Pool aus, um eine Zusammenfassung und Einzelheiten zur Verwendung des Identitäts-Pools anzuzeigen.

- **Zusammenfassung** – Zeigt das Erstellungsdatum, die letzte Aktualisierung und die Protokolldetails der Identitäts-Pools an.
- **Nutzung** – Zeigt die folgenden Details zu den ausgewählten Identitäts-Pools an.
  - Konflikt
  - Virtuelle MAC-Adresse

- Zustand
- Profilname
- Gehäusename
- Steckplatz
- Name
- Verwaltungs-IP
- NIC-Kennung

Sie müssen über die Vorlagenverwaltungs-Berechtigung verfügen, um Identitäts-Pools zu verwalten. Sie können die Nutzungsdetails filtern und anzeigen nach:

- Ethernet
- iSCSI
- FCoE
- FC

# Identitäts-Pools bearbeiten

Sie können die Anzahl der Einträge im Pool ändern. Sie können jedoch nicht die Größe der Identitäten ändern, die bereits zugewiesen oder reserviert sind. Wenn zum Beispiel in einem Pool von 100 MAC-Adressen 94 der Adressen zugewiesen oder reserviert sind, so können Sie die Anzahl der MAC-Adressen nicht auf weniger als 94 reduzieren.

So bearbeiten Sie einen Identitäts-Pool:

1. Wählen Sie auf der Seite **Identitäts-Pools** den Identitäts-Pool aus, und klicken Sie auf **Bearbeiten**.
   Das Fenster **Identitäts-Pool bearbeiten** wird angezeigt.
2. Nehmen Sie ggf. erforderliche Änderungen vor.

# Identitäts-Pools exportieren

Sie können Identitäts-Pools im Format `.csv` auf eine Netzwerkfreigabe oder ein lokales Laufwerk Ihres Systems exportieren.

So exportieren Sie Identitäts-Pools:

Wählen Sie auf der Seite **Identitäts-Pools** die Identitäts-Pools aus, und klicken Sie auf **Exportieren**.

# Identitäts-Pools löschen

Sie können auch die Identitäts-Pools löschen, die nicht zugewiesen oder reserviert sind. Beim Versuch, Identitäts-Pools zu löschen, die einer Basislinie zugeordnet sind, wird eine Fehlermeldung angezeigt.

So löschen Sie Identitäts-Pools:

Wählen Sie auf der Seite **Identitäts-Pools** die Identitäts-Pools aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.

# 10

# Ethernet-E/A-Module

Das MX7000 unterstützt die folgenden Ethernet E/A-Module (EAMs):

- Verwaltete Ethernet-Switches
  - MX9116n Fabric Switching Engine
  - MX5108n Ethernet-Switch
- Nicht verwaltete Geräte:
  - MX7116n Fabric Expander Module
  - PowerEdge MX 25 Gb Ethernet-Passthrough-Modul
  - PowerEdge MX 10GBASE-T Ethernet-Passthrough-Modul

Ethernet EAMs werden in den Fabrics A und B unterstützt Informationen zu den unterstützten EAM-Steckplätzen finden Sie unter Unterstützte Steckplatzkonfigurationen für EAMs.

Ethernet-Switches arbeiten in zwei Modi:

- Full Switch-Modus (Standardeinstellung)
- SmartFabric Services-Modus oder Fabric-Modus

Standardmäßig arbeitet ein Ethernet-Switch im Full-Fabric-Modus.

Im Full-Switch-Modus arbeitet der Switch als voller L2/L3-Switch mit allen Funktionen, die vom OS10 und der zugrunde liegenden Hardware unterstützt werden. Die Switch-Konfiguration erfolgt über die CLI. Weitere Informationen zur Konfiguration eines Switch mit der CLI finden Sie im *OS10 Enterprise Edition Nutzerhandbuch*.

**ANMERKUNG:** Entfernen Sie beim Austausch von EAMs im vollständigen Switch-Modus das EAM, bevor Sie die ISL-Kabel entfernen, um mögliche Split-Brain-Situationen zu vermeiden.

Sie können OME – Modular benutzen, um Folgendes zu tun:

- Konfigurieren Sie Hostname, SNMP und NTP-Einstellungen.
- Port-Kabelpeitschenmodi konfigurieren
- Ports aktiv oder inaktiv einrichten
- Funktionszustand, Protokolle, Warnungen und Ereignisse überwachen
- Firmware aktualisieren und verwalten
- Die physische Topologie anzeigen
- Stromsteuerungsvorgänge ausführen

Es wird empfohlen, den Full Switch-Modus zu verwenden, wenn Sie eine Funktion oder Netzwerkarchitektur benötigen, die mit SmartFabric Services nicht verfügbar ist.

Weitere Informationen zum Fabric-Modus finden Sie unter SmartFabric Services.

## Ethernet-EAMs verwalten

Auf der Seite **E/A-Module** werden der Funktionszustand und Bestandsinformationen von EAMs angezeigt. Wenn Sie über die Fabric Manager-Rolle mit Berechtigungen für Gerätekonfiguration und Stromsteuerung verfügen, können Sie die folgenden Aufgaben auf der Seite **E/A-Modul** ausführen:

- Aus- und Einschalten – Einschalten, Ausschalten oder eine Systemzurücksetzung auf dem EAM durchführen
- Firmware aktualisieren, falls zutreffend
- Blink LED – Die EAM Identifikations-LED aus- oder einschalten
- Bestandsaufnahme aktualisieren

Sie müssen über die Gerätekonfigurationsrechte verfügen, um Netzwerk-EAMs einzurichten und Konfigurationsaufgaben an ihnen durchzuführen.

**ANMERKUNG:** Die unbefristete Lizenz wird standardmäßig mit den werkseitig ausgelieferten EAMs geliefert. Wenn Sie eine ONIE-Installation auf dem EAM durchführen, wird die unbefristete Lizenz entfernt und durch die Evaluierungs-Trail-Lizenz ersetzt. Es wird empfohlen, sich nach Abschluss der ONIE-Installation an den Dell Support für die Installation der unbefristeten Lizenz zu wenden.

**ANMERKUNG:** Wenn ein Switch zwischen Full Switch- und Fabric-Modus wechselt, wird er neu gestartet.

**ANMERKUNG:** Wenn Rechnerschlitten und Fabric-EAM nicht übereinstimmen, wird der Zustandsstatus des Rechnerschlittens oder des EAM im Gehäuse-Subsystem als "Warnung" angezeigt. Der Funktionszustand wird jedoch nicht in der grafischen Darstellung des Gehäuses auf den Seiten **Gehäuse**, "E/A-Module" und **Rechnerschlitten** angezeigt.

**Themen:**



# Hardwaredetails anzeigen

Sie können Informationen zu folgender EAM-Hardware anzeigen:

- FRU
- Gerätemanagementinformationen
- Installierte Software
- Portinformationen

**ANMERKUNG:** Wenn der physische Port als Teil des Portkanals hinzugefügt wird, wird er unter der Portkanalgruppe statt auf dem physischen Port angezeigt.

**ANMERKUNG:** Das Attribut URL wird auf der Seite **Hardware** > **Geräteverwaltung** für FC-IOMs aufgrund von Einschränkungen der Gerätekapazität als „N/V“ angezeigt.

**ANMERKUNG:** Bei Quad-Port-Ethernet-Adaptern muss der zweite Uplink des MX7116n an das EAM angeschlossen werden. Wenn der zweite Uplink verbunden ist, wird die Anzahl der Ports in jedem virtuellen Steckplatz von 8 auf 16 Ports erhöht.

Stellen Sie sicher, dass OME-Modular auf 1.20.10 aktualisiert wurde, bevor Sie den Quad-Port bestücken.

Wenn Sie für **Portinformationen** die automatische Verhandlung aktivieren, tauschen die Peer-Geräte Funktionen, wie z. B. die Geschwindigkeit, untereinander aus und einigen sich auf eine für beide Seiten geeignete Konfiguration. Wenn jedoch die automatische Verhandlung deaktiviert ist, tauschen die Peer-Geräte möglicherweise keine Funktionen aus. Daher empfiehlt Dell Technologies, dass die Konfiguration auf beiden Peer-Geräten identisch ist.

Die Richtlinien für die automatische Verhandlung lauten wie folgt:

- MX9116n-, MX7116n- und MX5108n-EAMs unterstützen nur 25G-Geschwindigkeiten auf Server-seitigen Ports.
- Standardmäßig ist die automatische Verhandlung auf serverseitigen 25G-Ports aktiviert, wie durch den IEEE 802.3-Standard vorgegeben.
- Das Aktivieren oder Deaktivieren der automatischen Verhandlung wird unterstützt. Das Konfigurieren der Geschwindigkeit an serverseitigen Ports wird jedoch nicht unterstützt.
- Wenn die automatische Verhandlung aktiviert ist, zeigen Ethernetswitches als Geschwindigkeitskapazität nur 25G an.

So zeigen Sie die Hardwaredetails an:

Klicken Sie auf **E/A-Module** > **Details anzeigen** > **Hardware**.

# EAM-Einstellungen konfigurieren

Wenn Sie über die Berechtigung zur Konfiguration des EAM-Geräts verfügen, können Sie die folgenden Einstellungen für die MX9116n FSE und die MX5108n Ethernetswitch-EAMs konfigurieren:

- Netzwerk
- Administratorkennwort
- SNMP
- Uhrzeit

Sie müssen über Berechtigungen als Netzwerkadministrator verfügen, um die öffentliche Verwaltungs-IP-Adresse für die EAMs zu konfigurieren. Die öffentliche IP erleichtert die Verwendung der EAM-Befehlszeilenschnittstelle (CLI) für die Konfiguration und Fehlerbehebung der EAMs.

# Konfigurieren der IOM-Netzwerkeinstellungen

Die Netzwerkeinstellungen für EAMs schließen die Konfiguration der öffentlichen Verwaltungs-IP-Adresse für den ausgewählten Management Port ein.

So konfigurieren Sie die Netzwerkeinstellungen:

1. Klicken Sie auf **Alle Geräte** > **E/A-Module** > **Details anzeigen** > **Einstellungen** > **Netzwerk** oder **Geräte** > **E/A-Module** > **Details anzeigen** > **Einstellungen** > **Netzwerk**.
2. Im Abschnitt **IPv4-Einstellungen** wählen Sie **IPv4 aktivieren** aus:
3. Geben Sie die **IP-Adresse**, die **Subnetzmaske** und das **Gateway** für den Verwaltungs-Port ein.

   Die Optionen **IP-Adresse**, **Subnetzmaske** und **Gateway** sind nur dann aktiviert, wenn das Kontrollkästchen **DHCP aktivieren** nicht markiert ist.

   **ANMERKUNG:** Für MX5108n und MX9116n IOMs ist die Standardpräfixlänge der DHCP IP 128 Bit, obwohl der DHCP-Server für 64-Bit konfiguriert ist.
4. Im Abschnitt **IPv6-Einstellungen** wählen Sie **IPv6 aktivieren** aus:
5. Geben Sie die **IPv6-Adresse** ein, und wählen Sie die **Präfixlänge** aus.

   Die Optionen **IPv6-Adresse**, **Präfixlänge** und **Gateway** sind nur dann aktiviert, wenn das Kontrollkästchen **Autokonfiguration aktivieren** nicht markiert ist.
6. Geben Sie das **Gateway** für den Verwaltungs-Port ein.

   Die Optionen **IPv6-Adresse**, **Präfixlänge** und **Gateway** sind nur dann aktiviert, wenn das Kontrollkästchen **Autokonfiguration aktivieren** nicht markiert ist.

   **ANMERKUNG:** Bei einem markierten oder nicht markierten VLAN-Netzwerk verfügen alle IPv6-Einstellungen, die mit OME-Modular konfiguriert wurden, möglicherweise nicht über das Standard-Gateway. Um das Standard-Gateway zu verwenden, gehen Sie zur entsprechenden OS10-CLI und deaktivieren Sie die Stateless Address Autoconfiguration (SLAAC) im jeweiligen markierten oder nicht markierten VLAN.
7. Im Abschnitt **DNS-Servereinstellungen** geben Sie die Adressen von **Bevorzugter DNS-Server**, **Alternativer DNS-Server 1** und **Alternativer DNS-Server 2** ein.

   Für MXG610s-EAMs können Sie die Adressen „Bevorzugter DNS-Server“ und „Alternativer Server 1“ und „Alternativer Server 2“ festlegen. Die Serveradresse für **Alternativer DNS-Server 2** wird jedoch nicht übernommen obwohl die Antwort erfolgreich ist, da MXG610s-EAMs nur zwei Serveradressen für DNS-Einstellungen unterstützen.
8. Im Abschnitt **Verwaltungs-VLAN** wählen Sie **VLAN aktivieren**, und geben Sie die **VLAN-ID** ein.

   Bei MXG610s FC-EAMs funktioniert DHCP nur ohne VLAN, während die statische IP-Adresse mit oder ohne VLAN-Konfiguration funktioniert. So ändern Sie die IP-Konfiguration von DHCP-IP in eine statische IP-Adresse:

   a. Deaktivieren Sie DHCP, konfigurieren Sie die statische IP-Adresse und speichern Sie die Konfiguration.
   b. Aktivieren Sie VLAN, konfigurieren Sie die VLAN-ID und speichern Sie die Konfiguration.

# Konfigurieren der EAM-Managementeinstellungen

Die Managementeinstellungen für EAMs umfassen die Konfiguration des Hostnamens und des Kennworts des Managementsystems.

1. Klicken Sie auf **Alle Geräte** > **E/A-Module** > **Details anzeigen** > **Einstellungen** > **Verwaltung** oder **Geräte** > **E/A-Module** > **Details anzeigen** > **Einstellungen** > **Verwaltung**.
2. Geben Sie im Abschnitt **Hostname** den Namen des Managementsystems ein.
   Wenn Sie die Hostnamen-Einstellungen in der OME-Modular-Webschnittstelle für Fibre-Channel-EAM ändern, wird der geänderte Hostname für Fibre-Channel-EAMs nur in einer neuen Sitzung angezeigt. Melden Sie sich von der Sitzung ab und wieder an, um den geänderten Hostnamen anzuzeigen.
3. Geben Sie das Kennwort für den Zugriff auf das Managementsystem ein.

**ANMERKUNG:** Für Ethernet-EAMs mit OS10-Version 10.5.0.7 und höher und MXG610s wird das Kennwort für das Administratorkonto festgelegt. Für OS10-Versionen, die älter als 10.5.0.7 sind, wird das Passwort für das linuxadmin-Konto festgelegt.

**ANMERKUNG:** Die OS10-Kennwortlänge muss mindestens 9 Zeichen betragen. Es wird empfohlen, mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein numerisches Zeichen und ein Sonderzeichen für ein stärkeres Kennwort zu verwenden. Standardmäßig ist die Mindestanzahl verschiedener Zeicheneinstellungen auf 0 festgelegt. Sie können den Befehl **password-attributes** verwenden, um die gewünschte Kennwortstärke zu konfigurieren.

4. Klicken Sie auf **Anwenden**, um die Verwaltungseinstellungen zu speichern, oder auf **Verwerfen**, um die Änderungen zu löschen und zu den vorherigen Einstellungen zurückzukehren.

## Konfigurieren der EAM-Monitoringeinstellungen

Die Monitoringeinstellungen für EAMs umfassen die Konfiguration der Einstellungen für die Überwachung von SNMP.

1. Klicken Sie auf **Alle Geräte** > **E/A-Module** > **Details anzeigen** > **Einstellungen** > **Überwachung** oder **Geräte** > **E/A Module** > **Details anzeigen** > **Einstellungen** > **Überwachung**.
2. Aktivieren Sie das Kontrollkästchen**SNMP aktivieren**, um SNMP zu aktivieren oder zu deaktivieren.
3. Wählen Sie als **SNMP-Version** die Option **SNMP v1** oder **SNMP v2** aus.
4. Geben Sie den **schreibgeschützten Communitystring** zum Abrufen von Anfragen vom OME-Modular Daemon ein, die an das EAM gerichtet sind.
5. Klicken Sie auf **Anwenden**, um die Monitoringeinstellungen zu speichern, oder auf **Verwerfen**, um die Änderungen zu löschen und zu den vorherigen Einstellungen zurückzukehren.

# Konfigurieren des OS10-Administratorkennworts

Das OS10-Administratornutzerkonto ist das Standardadministratorkonto, mit dem OS10 konfiguriert wird.

So konfigurieren Sie das Kennwort für OS10-Administrator:

1. Klicken Sie auf **Alle Geräte** > **E/A-Module** > **Details anzeigen** > **Einstellungen** > **Verwaltung** oder **Geräte** > **E/A-Module** > **Details anzeigen** > **Einstellungen** > **Verwaltung**.
   Die Seite **E/A-Module** wird angezeigt.
2. Geben Sie den **Hostnamen** und das **Stammkennwort** für das EAM ein.

   **ANMERKUNG:** Für OS10-Versionen 10.5.0.5 und früher hat das obige Verfahren das Kennwort für das OS10 linuxadmin-Konto geändert. Bei OS10-Versionen nach 10.5.0.5 ändert das obige Verfahren das Kennwort für den OS10-Administrator.

# SNMP-Einstellungen konfigurieren

So konfigurieren Sie die SNMP-Einstellungen:

1. Klicken Sie auf **Alle Geräte** > **E/A-Module** > **Details anzeigen** > **Einstellungen** > **Überwachung** oder **Geräte** > **E/A Module** > **Details anzeigen** > **Einstellungen** > **Überwachung**.
2. Wählen Sie **SNMP aktivieren**, um die SNMP-Version und die Communityzeichenfolge zu konfigurieren.

   **ANMERKUNG:** OME-Modular bietet keine Unterstützung für die Deaktivierung von SNMP für OS10. Sie können die Community-Zeichenkette nur auf „leer“ festlegen. Für MX9116n und MX5108n EAMs wird nur SNMP v2 unterstützt, während für MXG610s nur SNMPv1 unterstützt wird.

# Erweiterte Einstellungen konfigurieren

So konfigurieren Sie die erweiterten EAM-Einstellungen:

1. Klicken Sie auf **Alle Geräte** > **E/A-Module** > **Details anzeigen** > **Einstellungen** > **Erweitert** oder **Geräte** > **E/A Module** > **Details anzeigen** > **Einstellungen** > **Erweitert**.
2. Wählen Sie die Optionen aus, um die Zeit- und Warnungseinstellungen des Gehäuses auf dem EAM zu replizieren.

# Ports konfigurieren

Im SmartFabric-Modus können Sie den Breakout- und Admin-Status und die MTU-Größe für IOMs konfigurieren. Sie können Port-Breakout nur für Portgruppen konfigurieren.

Im Full-Switch-Modus ist die Seite **Portinformationen** schreibgeschützt. Verwenden Sie die OS10-CLI, um die Schnittstelleneinstellungen zu ändern.

**ANMERKUNG:** Stellen Sie sicher, dass die Peer-FC-Schnittstelle eine feste Geschwindigkeit hat und mit der Geschwindigkeit der IOM-FC-Schnittstelle übereinstimmt, damit die Verbindung aufgebaut werden kann.

So konfigurieren Sie Breakout:

1. Klicken Sie auf **Geräte** > **E/A-Module** > **Details anzeigen** > **Hardware** > **Portinformationen**.
2. Wählen Sie die Portgruppe aus, und klicken Sie auf **Breakout konfigurieren**.
   Das Fenster **Breakout konfigurieren** wird angezeigt.
3. Wählen Sie den **Breakouttyp** aus.

## Admin-Status konfigurieren

Sie können den Admin-Status umschalten, der für alle Ports standardmäßig aktiviert ist. Sie können den Verwaltungsstatus auf aktiviert oder deaktiviert setzen.

So schalten Sie den Admin-Status ein und aus:

Wählen Sie den Port aus, und klicken Sie auf **Verwaltungsstatus ein/aus**.
Das Fenster **Verwaltungsstatus ein/aus** wird angezeigt.

## Maximum Transmission Unit konfigurieren

Sie können die Maximum Transmission Unit (MTU) für EAMs im Full Switch- und Fabric-Modus konfigurieren.

So konfigurieren Sie die MTU:

1. Klicken Sie auf **Geräte** > **E/A-Module** > **Details anzeigen** > **Hardware** > **Portinformationen**.
2. Wählen Sie den Ethernet-Port aus und klicken Sie auf **MTU**.
   Das Fenster **MTU konfigurieren** wird angezeigt.
3. Wählen Sie die **MTU-Größe** aus.

   Der ungefähre Wert für MTU ist 1500 Byte. Der Standardwert ist 1532 Byte und der maximale Wert ist 9000 Byte. Wenn der Port über FCoE- und Ethernet-Schnittstellen verfügt, ist der Wert 2500 Byte.

## Automatische Verhandlung konfigurieren

Sie können die automatische Verhandlung (AutoNeg) über das Umschalten von **AutoNeg** aktivieren oder deaktivieren.

Die Standardkonfigurationen sind:

- MX9116n/MX5108n: Die automatische Verhandlung ist für DAC-Kabel aktiviert und für AOC- und Fiberoptik-Transceiver deaktiviert.
- MX7116n-Fabric-Expander-Modul: die automatische Verhandlung ist für DAC-Kabel aktiviert und für AOC-und Fiberoptik-Transceiver deaktiviert.
- Server (intelligente automatische Verhandlung): Die NIC durchläuft die möglichen Einstellungen, die mit der Konfiguration auf dem Link-Partner übereinstimmen.

Beim MX7116n können Sie die Konfiguration nicht ändern. Ändern Sie die automatische Verhandlung auf dem EAM daher nicht manuell, um eine Nichtübereinstimmung der Konfiguration zu vermeiden. Die intelligente automatische Verhandlung ist für DAC und Fiberoptik üblich. Es wird empfohlen, für die unterstützten Medien nicht die erzwungene Geschwindigkeit zu aktivieren oder die automatische Verhandlung auf dem Server zu aktivieren. Die folgende Tabelle beschreibt die erwarteten Ergebnisse, wenn die automatische Verhandlung auf dem Switch und den Servern aktiviert oder deaktiviert ist.

| Automatische Verhandlung auf Servern | Automatische Verhandlung auf EAMs | Schnittstellenstatus | Erwartete Ergebnisse |
|---|---|---|---|
| Aktivieren | Aktivieren | Aktiv | Die automatische Verhandlung ist auf allen drei Geräten aktiviert. Der Port ist aktiv. Erwartet. |
| Deaktivieren | Deaktivieren | Down | Die automatische Verhandlung ist auf dem MX7116n Fabric Expander-Modul aktiviert. Die automatische Verhandlung auf EAM und Server wird manuell deaktiviert. Konfiguration stimmt nicht überein. Port ist inaktiv. Erwartet. |

**ANMERKUNG:** Für Switch-Server-Ports ist die automatische Verhandlung standardmäßig aktiviert, um die Verbindung zur Server-Netzwerkkarte bei 25 GbE herzustellen. Das Deaktivieren der automatischen Verhandlung auf dem Server-Port kann den Server-Link zu einem operativen Ausfall zwingen.

So wechseln Sie AutoNeg:

Wählen Sie den Port aus, und klicken Sie auf **AutoNeg ein/aus**.
Das Fenster **AutoNeg ein/aus** wird angezeigt.

Wenn Ethernet-Verbindungen nicht automatisch angezeigt werden, ändern Sie die Einstellung für die automatische Verbindungsaushandlung.

## Konfigurieren der „Forward Error Correction“

Die FEC-Funktion (Forward Error Correction) in OME-Modular hilft, Fehler bei der Datenübertragung zu minimieren. FEC erhöht die Datenzuverlässigkeit.

So konfigurieren Sie FEC:

1. Erweitern Sie auf der Seite **Portinformationen** die physische Portgruppe und wählen Sie den Ethernet-Port aus.
2. Klicken Sie auf „FEC konfigurieren“.
   Das Fenster **Forward Error Correction konfigurieren** wird angezeigt.
3. Wählen Sie den **FEC-Typ** aus.
   Folgende Optionen stehen zur Verfügung:
   - **Automatisch**: wendet FEC basierend auf dem verbundenen Kabel oder optischen Gerät an
   - **Aus**: deaktiviert FEC
   - **CL74-FC**: konfiguriert CL74-RS FEC und unterstützt 25G und 50G.
   - **CL91-RS**: Konfiguriert CL91-RS FEC und unterstützt 100G.
   - **CL108-RS**: Konfiguriert CL108-RS FEC und unterstützt 25G und 50G.
4. Klicken Sie auf „Fertig stellen“, um die Änderungen zu speichern und zur Seite **Portinformationen** zurückzukehren.

# 11

# MX-skalierbare Fabric-Architektur

Die skalierbare Fabric-Architektur verbindet mehrere MX7000-Gehäuse zu einer einzigen Netzwerkdomäne, die sich aus Perspektive des Netzwerks wie ein einzelnes logisches Gehäuse verhält. Die MX-skalierbare Fabric-Architektur bietet Multi-Gehäuse-Ethernet mit folgenden Eigenschaften:

- Mehrere 25-Gb-Ethernet-Verbindungen zu jedem Serverschlitten
- Keine Ost-West-Überzeichnung
- Niedrige Latenzzeit „Beliebig-Beliebig“
- Skalierung auf bis zu 10 MX7000-Gehäuse
- Flexible Uplink-Geschwindigkeiten
- Support für Nicht-PowerEdge-MX-Geräte, wie z. B. Rack-Server

Weitere Informationen finden Sie im *PowerEdge MX-I/O-Handbuch* unter www.dellemc.com.

## Architektonischer Überblick

Eine skalierbare Fabric besteht aus zwei Hauptkomponenten: einem Paar von MX9116n Fabric Switching Engines (FSE) und zusätzliche Paare von MX7116n Fabric Expander Modulen (FEM), mit denen Remote-Gehäuse mit den FSEs verbunden werden. Dies ist eine hardwareaktivierte Architektur und gilt unabhängig davon, ob der Switch im Full-Switch- oder Fabric-Modus ausgeführt wird. Insgesamt zehn MX7000-Gehäuse werden in einer skalierbaren Fabric unterstützt.

## Fabric Switching Engine

Die FSE enthält die Switching-ASIC und das Netzwerk-Betriebssystem. Datenverkehr, der von einem FEM empfangen wird, wird automatisch der richtigen Switch-Schnittstelle zugeordnet. Jeder NIC-Port hat eine dedizierte 25-GbE-Lane von der NIC über das FEM und in die FSE, sodass es keine Port-über-Port-Überzeichnung gibt.

## Fabric Expander Module

Eine FEM nimmt Ethernet-Frames von einem Rechenknoten und sendet sie an die FSE und von der FSE an den Rechenknoten. Auf dem FEM wird keine Switching-ASIC oder ein Betriebssystem ausgeführt, was eine sehr niedrige Latenzzeit ermöglicht. Das FEM ist unsichtbar für die FSE und wird in keiner Weise verwaltet.

Bei der Verwendung von NICs mit zwei Ports muss nur der erste Port auf dem FEM über eine FSE verwaltet werden. Der zweite Port wird nicht verwendet.

Beim Anschließen eines FEM an eine FSE sind die folgenden Regeln zu beachten:

- FEM in Steckplatz A1 wird mit der FSE in Steckplatz A1 oder Steckplatz B1 verbunden
- FEM in Steckplatz A2 wird mit der FSE in Steckplatz A2 oder Steckplatz B2 verbunden
- FEM in Steckplatz B1 wird mit der FSE in Steckplatz A1 oder Steckplatz B1 verbunden
- FEM in Steckplatz B2 wird mit der FSE in Steckplatz A2 oder Steckplatz B2 verbunden

**ANMERKUNG:** Bei Quad-Port-NICs müssen Sie zwei Kabel vom MX7116n-FEM mit der MX9116n-FSE verbinden.

**Themen:**

# Empfohlene physische Topologie

Das empfohlene minimale Design für eine skalierbare Fabric sind zwei Gehäuse mit Fabric A, die mit redundanten EAMs bestückt sind. Im Idealfall sollten sich die zwei Gehäuse für höchste Redundanz in separaten Racks auf separaten Stromkreisen befinden.

Zusätzliche Gehäuse haben nur FEMs und erscheinen wie in der Abbildung unten gezeigt.

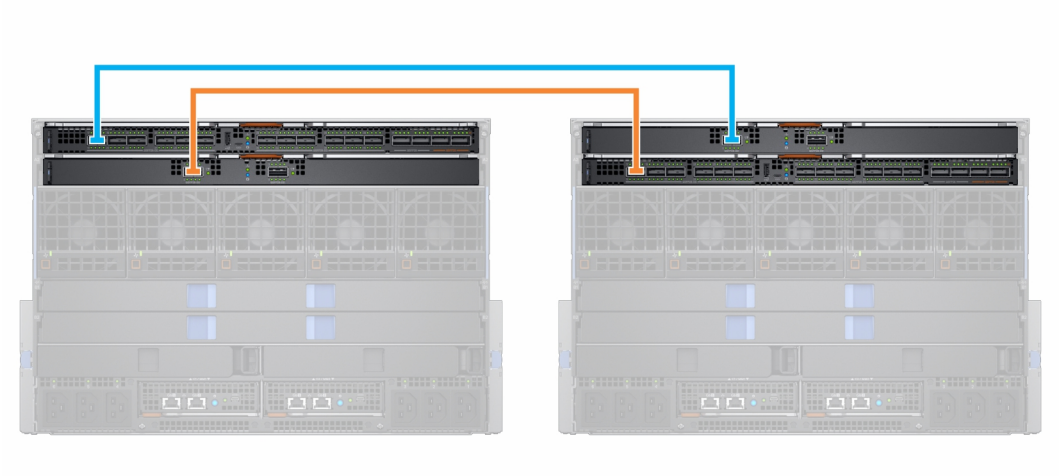


**Tabelle 16. Fabric-Topologie**

| Gehäuse | Steckplatz | Module |
|---|---|---|
| Gehäuse 1 | A1 | MX9116n FSE |
| | A2 | MX7116n FEM |
| Gehäuse 2 | A1 | MX7116n FEM |
| | A2 | MX9116n FSE |
| Gehäuse 3-10 | A1 | MX7116n FEM |
| | A2 | MX7116n FEM |

Sie können auch Fabric B verwenden um eine zweite skalierbare Fabric zu erstellen:

**ANMERKUNG:** Die Firmware-Version 1.20.10 von OME-Modular unterstützt zusätzliche, aber komplexe Topologien und auch Quad-Port-Ethernet-Adapter. Weitere Informationen finden Sie im *Handbuch zur PowerEdge MX-Netzwerkarchitektur* unter https://infohub.delltechnologies.com/t/mx-series-modular-switches-poweredge-mx-7/.

# Einschränkungen und Richtlinien

Die folgenden Einschränkungen und Richtlinien gelten beim Erstellen einer skalierbaren Fabric:

- Das Kombinieren von Switch-Typen derselben Fabric wird nicht unterstützt. Zum Beispiel: MX9116n in Steckplatz A1 und MX5108n in Steckplatz A2
- Das Kombinieren von Switch-Typen über Fabrics hinweg wird unterstützt. Zum Beispiel: MX9116n in den Steckplätzen A1 & A2 und MX5108n in den Steckplätzen B1 und B2
- Alle FSE- und FEM-Module in einer skalierbaren Fabric müssen sich in derselben OME – Modular-MCM-Gruppe befinden. FEMs in einem Gehäuse in MCM-Gruppe 1 können nicht mit FSEs in einem Gehäuse in MCM-Gruppe 2 verbunden werden.

Die folgenden Einschränkungen gelten bei der Implementierung einer skalierbaren Fabric, sowohl in Fabric-Steckplatz A als auch in Fabric-Steckplatz B:

- Die EAM-Platzierung für jede skalierbare Fabric muss innerhalb desselben Gehäuses identisch sein. Wenn sich zum Beispiel die FSE für die erste skalierbare Fabric in Steckplatz A1 befindet, dann muss sich die zweite FSE in Steckplatz B1 im selben Gehäuse befinden usw.
- Für Gehäuse, die nur FEMs enthalten, müssen alle vier FEMs eine Verbindung mit demselben Gehäuse mit den FSEs herstellen. Die FEMs in Fabric B können nicht mit FSEs in einem anderen Gehäuse als Fabric A verbunden werden.

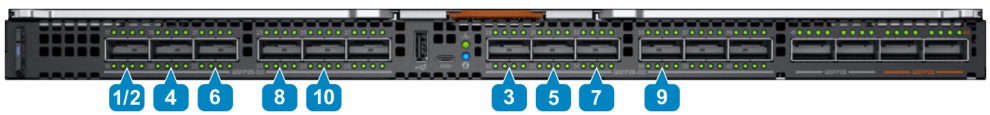
# Empfohlene Reihenfolge der Verbindung

Jeder QSSFP28-DD-Port des MX9116n kann für jeden Zweck verwendet werden. Die folgende Tabelle beschreibt die empfohlene Portreihenfolge für den Anschluss von Gehäusen mit Fabric Expander Modules (FEMs) an den FSE. Die Tabelle enthält Referenz-EAMs in Fabric A, doch die gleichen Richtlinien gelten auf für E/A-Module in Fabric B.

**Tabelle 17. Empfohlene Port-Reihenfolge beim Verbinden von FEMs mit der FSE**

| Gehäuse | FSE-Port (physischer Port) |
|---|---|
| 1 und 2 | FSE-Port 1 (17/18) |
| 3 | FSE-Port 7 (29/30) |
| 4 | FSE-Port 2 (19/20) |
| 5 | FSE-Port 8 (31/32) |
| 6 | FSE-Port 3 (21/22) |
| 7 | FSE-Port 9 (33/34) |
| 8 | FSE-Port 4 (23/24) |
| 9 | FSE-Port 10 (35/36) |
| 10* | FSE-Port 6 (25/26) |

* Standardmäßig ist die Portgruppe 10 nicht für die Unterstützung eines FEM konfiguriert. Wenn Sie einen FEM mit diesem Port verbinden möchten, verwenden Sie die OME-Modular-Schnittstelle, um den Portmodus auf "Fabric Expander" einzustellen.




**ANMERKUNG:** Die Portgruppen 6, 11 und 12 (physische Ports 27/28, 37/38, 39/40) können für weitere Uplinks, ISLs, Rack-Server usw. verwendet werden.

# 12

# SmartFabric Services

SmartFabric Services ist eine Funktion von Dell EMC Networking OS10 Enterprise Edition, die auf Ethernetswitches für die PowerEdge MX-Plattform ausgeführt wird.

Eine SmartFabric ist eine logische Einheit, die eine Sammlung physischer Ressourcen, wie Server und Switches, und logischer Ressourcen, wie Netzwerke, Vorlagen und Uplinks, enthält. Im SmartFabric Services-Modus arbeiten die Switches als ein einfaches Layer 2 Eingabe/Ausgabe-Aggregationsgerät, das die vollständige Interoperabilität mit Herstellern von Netzwerkausrüstung ermöglicht.

Eine SmartFabric bietet:

- Modernisierung des Rechenzentrums
  - E/A-Aggregation
  - Plug-and-Play-Fabric-Bereitstellung
  - Eine einzelne Schnittstelle zur Verwaltung aller Switches in der Fabric wie einen einzigen logischen Switch
- Lebenszyklusmanagement
  - Fabric-weite Planung von Firmware-Upgrades
  - Automatisches oder durch den Nutzer erzwungenes Rollback zu dem zuletzt bekannten Zustand
- Fabric-Automatisierung
  - Garantierte Compliance mit ausgewählter physischer Topologie
  - Richtlinienbasierte Quality of Service (QoS) auf der Grundlage von VLAN- und Prioritätszuordnungen
  - Automatische Erkennung von Fabric-Fehlkonfigurationen und Fehlerbedingungen auf Verbindungsebene
  - Automatische Reparatur der Fabric nach Entfernen eines Fehlerzustands
- Fehlerkorrektur
  - Dynamische Anpassung der Bandbreite über alle Verbindungen zwischen Switches im Falle eines Verbindungsausfalls

Im Gegensatz zum Voll-Switch-Modus erfolgen die meisten Fabric-Konfigurationseinstellungen über OME – Modular.

Weitere Informationen zum automatischen QoS finden Sie unter SmartFabric VLAN-Verwaltung und automatische QoS

## Betriebsmodi ändern

Sowohl im Full Switch- als auch im Fabric-Modus werden alle Konfigurationsänderungen, die Sie unter Verwendung der OME – Modular-Schnittstelle vornehmen, beibehalten, wenn Sie zwischen Modi wechseln. Es wird empfohlen, dass Sie die GUI für alle Switch-Konfigurationen im Fabric-Modus verwenden und die OS10 CLI zum Konfigurieren von Switches im Full-Fabric-Modus.

Um eine MX9116n Fabric Switching Engine oder einen MX5108n Ethernetswitch zwischen Full Switch- und Fabric-Modus umzuschalten, verwenden Sie die OME – Modular GUI und erstellen eine Fabric mit diesem Switch. Wenn dieser Switch zur Fabric hinzugefügt wird, wechselt er automatisch in den Fabric-Modus. Wenn Sie vom Full Switch- in den Fabric-Modus wechseln, werden alle Full Switch CLI-Konfigurationsänderungen gelöscht, außer für eine Untergruppe von Einstellungen, die im Fabric-Modus unterstützt werden.

Um einen Switch vom Fabric- in den Full-Fabric-Modus zu ändern, muss die Fabric gelöscht werden. Anschließend werden alle Fabric GUI-Konfigurationseinstellungen gelöscht. Die Konfigurationen, die von der Untermenge von Fabric CLI-Befehlen unterstützt werden (Hostname, SNMP-Einstellungen usw. ) und die Änderungen, die Sie an Port-Schnittstellen, MTU, Geschwindigkeit und Auto-Negotiation-Modus vornehmen, werden jedoch nicht gelöscht. Die Änderungen an Port-Schnittstellen schließen den Administrator-Status (shutdown/no shutdown) aus.

Beim Austausch von Switches einer Fabric:

- Wenn der Fabric-Name und der Fabric-Beschreibungs-String das Service-Tag des alten Switch enthalten, wird dieses während des Node-Austauschs durch das Service-Tag des neuen Switches ersetzt.
- Wenn der zu ersetzende Switch über die VLT-MAC-Adresse der Fabric verfügt, ist während des Austauschs des Switches VLT-Port-Channel-Flapping zu erwarten oder unvermeidbar. Das liegt daran, dass die VLT-MAC-Adresse auf einen der in der Fabric verfügbaren Switches geändert werden muss.

**Themen:**

- Switch-zu-Switch-Verkabelung
- Vorgeschaltete Netzwerkswitch-Anforderungen
- NIC-Teaming-Einschränkungen
- Verfügbare OS10 CLI-Befehle im SmartFabric-Modus
- Fabrics-Übersicht
- Topologiedetails anzeigen
- Anzeigen von Multicast-VLANs
- VLANs für SmartFabrics und FCoE

# Richtlinien für den Betrieb im SmartFabric-Modus

Während des Betriebs im SmartFabric-Modus gelten die folgenden Richtlinien und Beschränkungen:

- Beim Betrieb mit mehreren Gehäusen müssen Sie darauf achten, dass die Switches in A1/A2 oder B1/B2 in einem Gehäuse nur mit entsprechenden A1/A2- oder B1/B2-Switches verbunden werden. Die Verbindung von Switches, die sich in den Steckplätzen A1/A2 in einem Gehäuse befinden, mit Switches in den Steckplätzen B1/B2 in einem anderen Gehäuse wird nicht unterstützt.
- Uplinks müssen symmetrisch sein. Wenn ein Switch in einer SmartFabric über zwei Uplinks verfügt, muss der andere Switch über zwei Uplinks mit der gleichen Geschwindigkeit verfügen.
- Aktivieren Sie LACP auf den Uplink-Ports, um das Uplinking der Switches zu ermöglichen.
- Sie können ein Paar von Switches im SmartFabric-Modus nicht per Uplink mit einem anderen Paar von Switches in SmartFabric-Modus verbinden. Der Uplink von SmartFabric ist nur mit einem Paar von Switches im Full-Switch-Modus möglich.

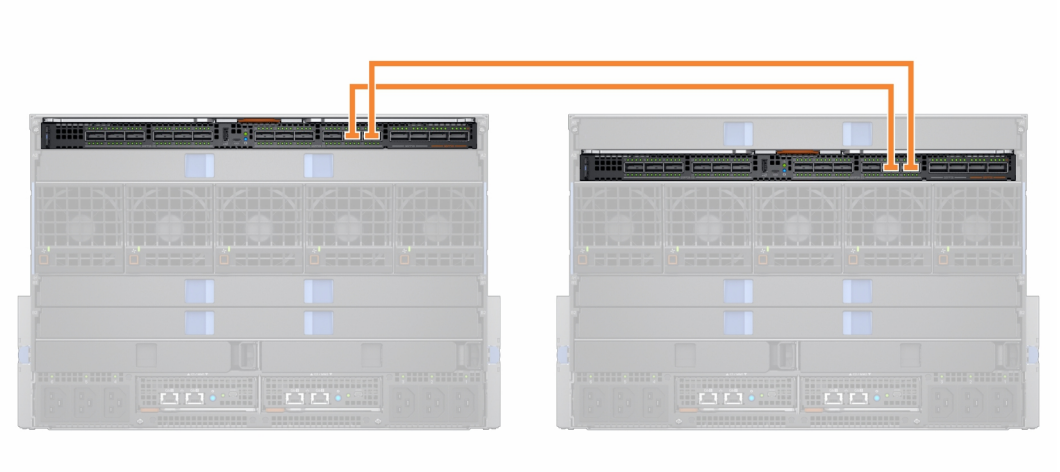
# SmartFabric-Netzwerktopologien

Die SmartFabric Services unterstützen drei Netzwerktopologien mit spezifischen EAM-Anforderungen für die Platzierung.

- 2 x MX9116n Fabric Switching Engines in unterschiedlichen Gehäusen
- 2 x MX5108n Ethernet-Switches in demselben Gehäuse
- 2 x MX9116n Fabric Switching Engines in demselben Gehäuse

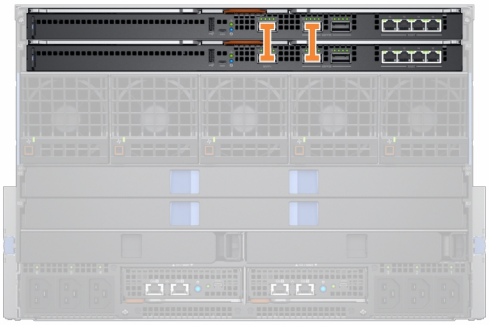
## 2 x MX9116n Fabric Switching Engines in separaten Gehäusen

Diese Platzierung wird während des Erstellens einer SmartFabric auf einer skalierbaren Fabric-Architektur nicht empfohlen. Diese Konfiguration unterstützt die Platzierung im Gehäuse1/A1 und Gehäuse 2/A2 oder Gehäuse1/B1 und Gehäuse 2/B2. Eine SmartFabric darf keinen Switch in Fab A und keinen Switch in Fab B enthalten Wenn eines der Gehäuse ausfällt, sorgt das Platzieren der FSE-Module in einem separaten Gehäuse für Redundanz. Beide Gehäuse müssen sich in der gleichen MCM-Gruppe befinden.



## 2 x MX5108n Ethernet-Switches in demselben Gehäuse

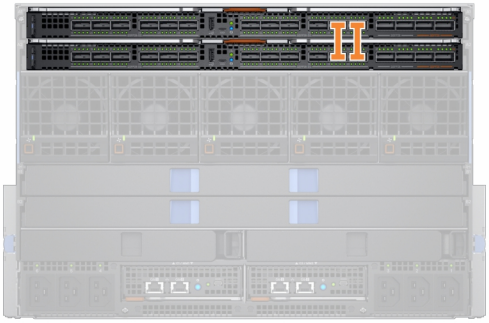
Der MX5108n Ethernet-Switch wird nur in Konfigurationen mit einem einzigen Gehäuse unterstützt. Die Switches müssen in den Steckplätzen A1/A2 oder B1/B2 platziert werden. Eine SmartFabric darf keinen Switch in Fab A und keinen Switch in Fab B enthalten



Im SmartFabric-Modus werden die Ports 9 und 10 automatisch in einem VLT mit 40 GbE Geschwindigkeit konfiguriert. Verwenden Sie für Port 10 ein normales oder optisches Kabel, das 40GbE und nicht 100GbE unterstützt.

## 2 x MX9116n Fabric Switching Engines in demselben Gehäuse

Verwenden Sie diese Platzierung in Umgebungen mit einem einzigen Gehäuse. Die Switches müssen in den Steckplätzen A1/A2 oder B1/B2 platziert werden. Eine SmartFabric darf keinen Switch in Fab A und keinen Switch in Fab B enthalten

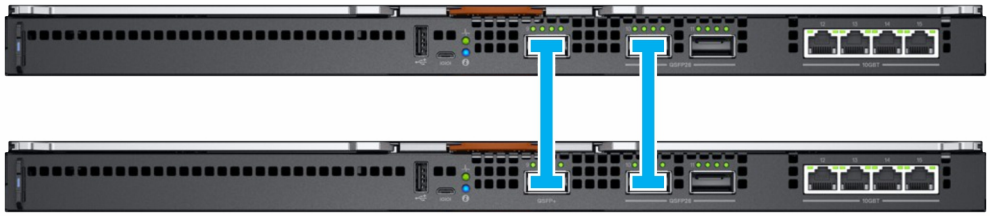


Das Fabric-Design "2 Mx9116n Fabric Switching Engines im selben Gehäuse" wird unterstützt, wird aber nicht empfohlen. Bei Verwendung dieses Designs wird eine Fehlermeldung auf den Seiten **Fabric-Topologie** und **Topologie anzeigen** von OME-Modular angezeigt.

# Switch-zu-Switch-Verkabelung

Beim Betrieb im SmartFabric-Modus besteht zwischen jedem Switch-Paar ein Virtual Link Trunk (VLT)-Link. Für den MX9116n werden die Port-Gruppen 11 und 12 verwendet.

Für den MX5108n werden die Ports 9 und 10 verwendet. Port 10 arbeitet mit 40GbE anstelle von 100GbE, da alle VLT-Links mit der gleichen Geschwindigkeit laufen müssen. Stellen Sie sicher, dass Sie ein Kabel oder Glasfaserkabel verwenden, das 40GbE unterstützt.



**ANMERKUNG:** Sie können die Ports nicht auswählen, und die Verbindungstopologie wird durch SmartFabric Services erzwungen.

**ANMERKUNG:** VLT wird nur auf Ethernet und nicht auf FCoE unterstützt. Für MX5108n- und MX9116n-Switches sind physisch getrennte Uplinks für den LAN- und FCoE-Datenverkehr erforderlich.

# Vorgeschaltete Netzwerkswitch-Anforderungen

Es wird empfohlen, ist aber nicht erforderlich, die PowerEdge MX-Switches zu einem Paar redundanter vorgeschalteter Switches zu verbinden. Wenn Sie ein Switch-Paar im Fabric-Modus mit einem Upstream-Switch-Paar verbinden, stellen Sie Folgendes sicher:

1. Beide vorgeschalteten Switches müssen mithilfe von Technologien wie VLT oder VPC miteinander verbunden werden.
2. Die vorgeschalteten Switch-Ports müssen unter Verwendung von LACP in einen Portkanal verlegt werden.
   **ANMERKUNG:** Die LACP-Option wird nur auf Ethernet-Uplinks unterstützt.
3. Stellen Sie sicher, dass ein kompatibles Spanning Tree-Protokoll konfiguriert ist. Weitere Informationen finden Sie im Abschnitt **Spanning Tree Protocol**.

## Spanning Tree Protocol

OpenManage Modular v1.20.00- und OS10-Versionen nach 10.5.0.5 enthalten einen neuen Ethernet-Uplink-Typ, für den kein STP erforderlich ist. Der Ethernet-Uplink ohne STP ist jetzt der empfohlene Uplink-Typ für alle SmartFabric-Installationen. Anweisungen zur Konfiguration des Upstream-Switch finden Sie im Konfigurations- und Fehlerbehebungshandbuch zu PowerEdge MX SmartFabric.

Der Legacy-Ethernet-Uplink-Typ, für den STP erforderlich ist, wird weiterhin unterstützt. Wenn Sie einen Legacy-Ethernet-Uplink erstellen, achten Sie darauf, dass der richtige STP-Typ ausgewählt ist.

OS10 verwendet standardmäßig RPVST+ als Spanning Tree Protocol. Zum Ändern der STP-Modi verwenden Sie den Spanning-Tree-Modus-Befehl. Verwenden Sie den Spanning-Tree-Modus-Befehl zum Ändern der STP-Modi. Die Schritte sind im *OS10 Enterprise Edition Nutzerhandbuch* erläutert.

**ANMERKUNG:** Wenn auf dem vorgeschalteten Netzwerk RSTP ausgeführt wird, ändern Sie RPVST+ zu RSTP, bevor Sie die Switches physisch mit dem vorgeschalteten Netzwerk verbinden. Andernfalls besteht die Gefahr eines Netzwerkausfalls.

Weitere Informationen zu SmartFabric-Uplinks finden Sie im *Konfigurations- und Fehlerbehebungshandbuch zu PowerEdge MX SmartFabric*.

# NIC-Teaming-Einschränkungen

NIC-Teaming wird für Redundanz empfohlen, es sei denn, eine spezielle Implementierung spricht dagegen. Es gibt zwei wesentliche Arten von NIC-Teaming:

1. Switch-abhängig – Auch als 802.3ad oder dynamische Link-Aggregation bezeichnet. Die switch-abhängige Teaming-Methode verwendet das LACP-Protokoll zum Verständnis der Teaming-Topologie. Diese Teaming-Methode stellt Aktiv-Aktiv-Teaming zur Verfügung und erfordert, dass der Switch LACP-Teaming unterstützt.
2. Switch-unabhängig – Diese Methode verwendet das Betriebssystem und NIC-Gerätetreiber auf dem Server, um die NICs zu verbinden. Jeder NIC-Hersteller bietet eventuell etwas andere Implementierungen mit unterschiedlichen Vor- und Nachteilen.

NIC-Partitionierung (NPAR) kann sich auf die Arbeitsweise von NIC-Teaming auswirken. Basierend auf Einschränkungen, die von NIC-Anbietern in Bezug auf NIC-Partitionierung implementiert werden, schließen bestimmte Konfigurationen bestimmte Arten von Teaming aus.

Die folgenden Einschränkungen gelten für die Full Switch- und SmartFabric-Modi:

1. Wenn NPAR nicht verwendet wird, werden sowohl die switch-abhängigen (LACP) als auch die switchunabhängigen Teaming-Methoden unterstützt.
2. Wenn NPAR verwendet wird, wird nur die Switch-unabhängige Teaming-Methode unterstützt. Switch-abhängiges Teaming wird nicht unterstützt.

Die folgenden Einschränkungen gelten für Switch-abhängiges (LACP) Teaming:

1. Die Shared LOM-Funktion des iDRAC kann nur verwendet werden, wenn „Failover“ auf dem iDRAC aktiviert ist.
2. Wenn das Hostbetriebssystem Windows ist, muss der LACP-Timer auf „langsam“ (bzw. „normal“) eingestellt werden.

   Eine Liste der unterstützten Betriebssysteme finden Sie im *Installations- und Service-Handbuch des Dell EMC PowerEdge MX7000-Gehäuses*.

**ANMERKUNG:** In einem SmartFabric-Modus müssen Sie das gesamte LACP-Team löschen und ein neues LACP-Team mit zwei Ports erstellen, wenn ein LACP-Team mit vier Ports erstellt wurde und Sie zwei Ports aus dem LACP-Team löschen möchten.

Detaillierte NIC-Teaming-Anweisungen finden Sie in der Dokumentation zum Netzwerkadapter oder zum Betriebssystem.

# Verfügbare OS10 CLI-Befehle im SmartFabric-Modus

Beim Betrieb im SmartFabric-Modus wird der Großteil der Switch-Konfiguration über die OME – Modular-GUI verwaltet. Manche OS10-Funktionen, wie z. B. Layer-3-Routing, sind deaktiviert. Ein Switch im Fabric-Modus unterstützt alle **Anzeige**befehle von OS10, jedoch nur eine Teilmenge der CLI-Konfigurationsbefehle: Weitere Informationen zu unterstützten CLI-Konfigurationsbefehlen finden Sie im *Nutzerhandbuch zu Dell EMC SmartFabric OS10*.

# Fabrics-Übersicht

Der MX7000 umfasst zwei Allzweck-E/A-Fabrics, Fabric A und Fabric B. Diese Fabrics werden über eine direkte orthogonale Verbindung zwischen Zusatzkarten verbunden. Es wird auf den Rechnerschlitten an der Vorderseite des Gehäuses und auf den E/A-Fabric-Modulen an der Rückseite des Gehäuses installiert. Das Fehlen einer mittleren Ebene bietet dem Endnutzer eine flexible Möglichkeit, sein E/A-Fabric zu wählen. Sie ermöglicht die Einführung neuer E/A-Technologien, ohne dass die mittlere Ebene aufgerüstet werden muss, was auch die Fehlerpunkte reduziert.

## Fabric-Details anzeigen

So zeigen Sie die Details einer vorhandenen Fabric an:

- Wählen Sie im Drop-Down-Menü **Geräte** die Option **Fabric** aus.
- Wählen Sie in der Tabelle "Fabrics" die Fabric aus, und klicken Sie auf **Details anzeigen**.

Die Seite **Fabric-Details** wird angezeigt.

## Fabric-Details bearbeiten

So bearbeiten Sie die Fabric-Details:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Fabric** aus.
   Die Seite **Fabric** wird angezeigt.
2. Wählen Sie in der Tabelle "Fabrics" die Fabric aus, und klicken Sie auf **Bearbeiten**.
   Die Seite **Fabric bearbeiten** wird angezeigt.
3. Nehmen Sie die erforderlichen Änderungen an den Feldern **Name** und **Beschreibung** vor.

# Ersetzen des Fabric-Switches

Sie können einen fehlerhaften Fabric-Switch in einer SmartFabric problemlos ersetzen. Klicken Sie auf **Geräte** > **Fabric** > **Switch ersetzen**.

Um einen Fabric-Switch zu ersetzen, führen Sie die folgenden Schritte aus:

- **Aktuelle Konfiguration kopieren**: kopiert die Konfiguration des zu ersetzenden Switches.
- **Switch-Hardware ersetzen**: fehlerhaften Switch aus dem Gehäuse entfernen und durch einen neuen Switch ersetzen.
- **Neuen Switch konfigurieren**: Einstellungen anwenden, die vom alten auf den neuen Switch kopiert wurden.
- **Fabric aktualisieren**: geben Sie die Service-Tag-Nummer des alten und des neuen Switches ein, um die Konfiguration des SmartFabric abzuschließen.
- Klicken Sie auf **Fertigstellen**.

# SmartFabric hinzufügen

So fügen Sie eine Fabric hinzu:

1. Klicken Sie auf **Geräte** > **Fabric** .
   Die Seite **Fabric** wird angezeigt.
2. Klicken Sie auf **Fabric hinzufügen**.
   Das Fenster **Fabric erstellen** wird angezeigt.
3. Geben Sie **Name** und **Beschreibung** ein, und klicken Sie dann auf **Weiter**.
4. Wählen Sie den **Designtyp** aus dem Drop-Down-Menü aus.

   Folgende Optionen stehen zur Verfügung:
   - 2x MX5108n Ethernetswitches in demselben Gehäuse
   - 2x MX9116n Fabric Switching Engines in demselben Gehäuse
   - 2x MX9116n Fabric Switching Engines in unterschiedlichen Gehäusen

   Basierend auf dem gewählten Designtyp werden die Optionen zur Auswahl des Gehäuses und der Switches – A und B – angezeigt.
5. Wählen Sie das Gehäuse und die Switches aus.
   Die Verkabelungsdarstellung wird angezeigt.
6. Klicken Sie auf **Weiter**, um die Zusammenfassung der Fabric anzuzeigen.

   Sie können eine Hardcopy der Fabric-Details ausdrucken oder die Details als PDF auf Ihrem System speichern.

   Nachdem die Fabric erstellt wurde, wird der Switch in den SmartFabric-Modus gestellt und das EAM wird neu gestartet.

   **ANMERKUNG:** Nachdem eine Fabric erstellt wurde, ist der Funktionszustand der Fabric kritisch, bis Uplinks erstellt werden.

   **ANMERKUNG:** Die Fabric-Funktionszustandswarnungen werden auf allen Gehäusen in der MCM-Gruppe angezeigt.

## Uplinks hinzufügen

So fügen Sie Uplinks hinzu:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Fabric** aus.
   Die Seite **Fabric** wird angezeigt.
2. Wählen Sie in der Tabelle „Fabrics“ die Fabric aus, und klicken Sie auf **Details anzeigen**.
   Die Seite **Fabric-Details** wird angezeigt.
3. Klicken Sie im Abschnitt **Uplinks** auf **Uplink hinzufügen**.
   Das Fenster **Uplink hinzufügen** wird aufgerufen.
4. Geben Sie einen **Namen**, eine **Beschreibung** und den **Uplink-Typ** ein.

   Folgende Optionen stehen zur Verfügung:
   - **Ethernet – kein Spanning Tree**: Dies ist der empfohlene Uplink-Typ. Sie können einen oder mehrere Ethernet-Ports über EAMs auswählen, um ein LAG für die Verbindung mit dem Upstream-Netzwerk zu bilden. Für diese Art von Uplink ist kein Spanning Tree aktiviert. Für diesen Uplink-Typ muss das Spanning Tree-Protokoll nicht auf dem Upstream-Ethernetswitch konfiguriert werden. Weitere Informationen zum Konfigurieren des Upstream-Ethernetswitch finden Sie im *Konfigurations- und Troubleshootinghandbuch für Dell EMC PowerEdge MX SmartFabric* unter https://infohub.delltechnologies.com/. Bevor Sie einen Uplink über **Ethernet – Kein STP** erstellen können, müssen alle älteren Ethernet-Uplinks, die STP verwenden, gelöscht werden. Es gibt zusätzliche Schritte, die ausgeführt werden müssen, bevor ein Uplink über **Ethernet – Kein STP** auf einer vorhandenen

Fabric erstellt wird, auf der das RSTP-Protokoll nicht ausgeführt wurde. Weitere Informationen finden Sie im Konfigurations- und Troubleshootinghandbuch zu Dell EMC PowerEdge MX SmartFabric unter https://infohub.delltechnologies.com/

- **Ethernet**: Dieser Uplink-Typ wird nicht mehr empfohlen. Sie können einen oder mehrere Ethernet-Ports auf verschiedenen Switches wählen, um ein LAG zu bilden. Der Netzwerktyp kann beliebig sein. Außerdem müssen Sie **Spanning Tree** auf dem Upstream-Netzwerkswitch konfigurieren.
- **FCoE** – Sie können einen oder mehrere Ports aus dem gleichen EAM auswählen und einem einzelnen Netzwerk vom Typ FCoE zuordnen. Dies dient zur FCoE-Konnektivität, mit der eine Verbindung zu einem anderen Switch mit einer Verbindung mit dem FC-Netzwerk hergestellt wird. Sie können für eine einzelne Fabric zwei FCoE-Uplinks haben, eine von jedem E/A-Modul. Beide EAMs müssen sich in unterschiedlichen Netzwerken, d. h. unterschiedlichen FCoE-VLANs, befinden.

  Im FCoE-Modus müssen nicht gekennzeichnete VLANs auf dem Serverport und FCoE-Uplink identisch sein. Dadurch wird sichergestellt, dass die Pakete mit dem Status „untagged FIP VLAN Discovery (L2 Frame)“ auf den nicht markierten VLAN umgeschaltet werden. Der FCoE-Uplink wird verwendet, um den FIP-Snooping-Bridge-Modus (FSB) am Switch zu identifizieren. Um die FCoE-Sitzungen zu überwachen, konfigurieren Sie denselben nicht markierten VLAN auf FCoE-Uplinks und Server-Ports.

  **ANMERKUNG:** Auf dem Uplink FCoE-Switch verwenden Sie nur die fc-map (0efc00).
- **FC Gateway** – Sie können einen oder mehrere Ports aus dem gleichen EAM auswählen und einem einzelnen Netzwerk vom Typ FCoE zuordnen. Diese Art von Uplink dient zur FCoE-Konnektivität mit einem SAN-Switch. Sie können für eine einzelne Fabric zwei FC-Gateway-Uplinks haben, eine von jedem E/A-Modul. Beide EAMs müssen sich in unterschiedlichen Netzwerken, d. h. unterschiedlichen FCoE-VLANs, befinden. Für eine bestimmte Fabric können Sie mindestens einen Uplink vom Typ FC (FCoE-FCDirectAttach oder FC Gateway) haben.

  Im Fabric-Modus können Sie alle nicht markierten VLAN den Ethernet-Server-Ports zuweisen, die zu einem FCoE VLAN gehören, der über ein oder mehrere FC-Gateway-Uplinks verfügt. Der FC-Gateway-Uplink wird verwendet, um den NPG (N-Port-Proxy-Gateway)-Modus am Switch zu identifizieren.
- **FC Direct Attach** – Sie können einen oder mehrere Ports aus dem gleichen EAM auswählen und einem einzelnen Netzwerk vom Typ FCoE zuordnen. Diese Art von Uplink dient zur direkten FC-Speicher-Konnektivität. Sie können für eine einzelne Fabric zwei FC DirectAttach-Uplinks haben, eine von jedem E/A-Modul. Beide EAMs müssen sich in unterschiedlichen Netzwerken, d. h. unterschiedlichen FCoE-VLANs, befinden.

  Im Fabric-Modus können Sie alle nicht markierten VLAN den Ethernet-Server-Ports zuweisen, die zu einem FCoE VLAN gehören, das über ein oder mehrere FC Direct Attach-Uplinks verfügt. Der FC Direct Attach-Uplink wird verwendet, um den F-Port-Modus am Switch zu identifizieren.

5. Wählen Sie **In die Uplink-Fehlererkennungsgruppe aufnehmen**. und klicken anschließend auf **Weiter.**

   Wenn Sie die **Uplink-Fehlererkennung (UFD)** auswählen, wird der Verlust der Upstream-Konnektivität erkannt und dieser Status wird den Servern angezeigt, die mit dem Switch verbunden sind. UFD verknüpft eine Reihe von Downstream-Schnittstellen mit den Uplink-Schnittstellen. Im Falle eines Uplink-Fehlers deaktiviert der Switch die entsprechenden Downstream-Schnittstellen. Auf diese Weise können die Downstream-Server verfügbare alternative Pfade für die Upstream-Konnektivität auswählen.
6. Wählen Sie die erforderlichen **Switch-Ports** aus, und wählen Sie ein beliebiges **gekennzeichnetes Netzwerk**.

   Wenn Sie ein neues Netzwerk konfigurieren müssen, klicken Sie auf **Netzwerk hinzufügen**, und geben Sie die Netzwerkdetails ein. Weitere Informationen finden Sie unter Netzwerk hinzufügen.

## Netzwerk hinzufügen

Sie können mit den Seiten **Fabric** und **Konfigurations-** > **VLANs** Netzwerk hinzufügen. Weitere Informationen finden Sie unter Netzwerke definieren.

So fügen Sie ein neues Netzwerk über die Seite **Fabric** hinzu:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Fabric** aus.
   Die Seite **Fabric** wird angezeigt.
2. Wählen Sie in der Tabelle „Fabrics“ die Fabric aus, und klicken Sie auf **Details anzeigen**.
   Die Seite **Fabric-Details** wird angezeigt.
3. Klicken Sie im Abschnitt **Uplinks** auf **Uplink hinzufügen**.
   Das Fenster **Uplink hinzufügen** wird aufgerufen.
4. Klicken Sie auf **Netzwerk hinzufügen**.
   Das Fenster **Netzwerke definieren** wird angezeigt.
5. Geben Sie **Name**, **Beschreibung** und **VLAN-ID** ein, und wählen Sie den **Netzwerktyp**.

   Weitere Informationen zu Netzwerktypen finden Sie in der *Online-Hilfe*.

## Uplink bearbeiten

So bearbeiten Sie einen vorhandenen Uplink:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Fabric** aus.
   Die Seite **Fabric** wird angezeigt.
2. Wählen Sie in der Tabelle „Fabrics“ die Fabric aus, und klicken Sie auf **Details anzeigen**.
   Die Seite **Fabric-Details** wird angezeigt.
3. Wählen Sie in der Tabelle **Uplinks** den Uplink aus, und klicken Sie auf **Bearbeiten**.
   Die Seite **Uplink bearbeiten** wird angezeigt.
4. Bearbeiten Sie die Felder **Name**, **Beschreibung** und **Uplinktyp** nach Bedarf, und klicken Sie dann auf **Weiter**.
5. Wählen Sie die erforderlichen **Switch-Ports** aus, und wählen Sie beliebige **Markierte Netzwerke** oder **Nicht markierte Netzwerke**.

   Um ein neues Netzwerk zu konfigurieren, klicken Sie auf **Netzwerk hinzufügen**, und geben Sie die Netzwerkdetails ein. Weitere Informationen finden Sie unter Netzwerk hinzufügen.

   **ANMERKUNG:** Sie können die Netzwerke bearbeiten, wenn sich die Uplinks im FCoE-, FC Gateway- oder FC Direct-Attach-Modus befinden. Erstellen Sie den Uplink neu, um die Netzwerke zu ändern.

## Uplinks löschen

So löschen Sie einen Uplink:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Fabric** aus.
   Die Seite **Fabric** wird angezeigt.
2. Wählen Sie in der Tabelle "Fabrics" eine Fabric aus, und klicken Sie auf **Details anzeigen**.
3. Wählen Sie aus der Tabelle "Uplinks" den Uplink aus, den Sie löschen wollen.
4. Klicken Sie auf **Löschen**. Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.

## Fabric löschen

So löschen Sie eine bestehende Fabric:

1. Wählen Sie im Drop-Down-Menü **Geräte** die Option **Fabric** aus.
   Die Seite **Fabric** wird angezeigt.
2. Wählen Sie in der Tabelle der Fabrics die Fabric aus, die Sie löschen möchten.
3. Klicken Sie auf **Löschen**.
   Es wird eine Meldung angezeigt, die Sie dazu auffordert, den Löschvorgang zu bestätigen.
4. Klicken Sie auf **Ja,** um fortzufahren.

   Nachdem die Fabric gelöscht wurde, werden die EAMs im Full-Switch-Modus neu gestartet.

# Topologiedetails anzeigen

Das Fabric-Topologie-Image zeigt nur den Betriebsstatus der Ports an. Wenn der Betriebsstatus "aktiv" ist, wird ein Häkchen angezeigt. Um die grafische Darstellung der Validierungsfehler in einem MCM-Szenario anzuzeigen, gehen Sie zur Seite **Gruppentopologie** der OME – Modular-Webschnittstelle.

So zeigen Sie die Topologiedetails an:

- Wählen Sie im Drop-Down-Menü **Geräte** die Option **Fabric** aus.
- Wählen Sie in der Tabelle "Fabrics" die Fabric aus, und klicken Sie auf **Details anzeigen**.
- Klicken Sie auf der Seite **Fabric-Details** auf **Topologie**.

Die Topologie der Fabric wird angezeigt.

# Anzeigen von Multicast-VLANs

Diese Seite zeigt die Liste der konfigurierten VLANs auf einer Fabric und Multicast-Versionen der IGMP- und MLD-Protokolle auf dem Switch an. Sie können auch VLAN definieren und VLAN zur L2-Multicast-Konfiguration hinzufügen.

So fügen Sie VLANs zu L2-Multicast hinzu:

- Wählen Sie im Drop-Down-Menü **Geräte** die Option **Fabric** aus.
- Wählen Sie in der Tabelle „Fabrics“ die Fabric aus, und klicken Sie auf **Details anzeigen**.
- Klicken Sie auf der Seite **Fabric-Details** auf **Multicast-VLANs** und dann auf **L2-Multicast**.
- Wählen Sie im Assistenten für **L2-Multicast** im Fenster **IGMP** verfügbare VLANs aus.
- Wählen Sie bei Bedarf „Ausgewählte VLANs zur MLD-Konfiguration hinzufügen“. Klicken Sie auf **Weiter**.
- Wählen Sie im Bereich **MLD** verfügbare VLANs aus und klicken Sie auf **Fertigstellen**.

Die ausgewählten VLANs und ihre Details werden angezeigt.

# VLANs für SmartFabrics und FCoE

Erstellen Sie VLANs, bevor Sie die SmartFabric erstellen. Der erste VLAN, der erstellt wird, muss der Standard -oder native VLAN sein, in der Regel VLAN 1. Der Standard-VLAN muss für jeden nicht markierten Datenverkehr erstellt werden, um die Fabric zu überqueren.

Wenn Sie Fibre Channel-Konfigurationen implementieren, können Sie auch VLANs für FCoE konfigurieren. Die Speicher-Arrays verfügen über zwei separate Controller, die zwei Pfade erstellen: SAN Pfad A und SAN Pfad B. Diese Pfade sind mit MX9116n FSE verbunden. Damit der Speicherdatenverkehr redundant ist, werden für diesen Datenverkehr zwei separate VLANs erstellt.

In der folgenden Tabelle sind Beispiele für VLAN-Attribute für FCoE-Datenverkehr aufgeführt:

**Tabelle 18. VLAN-Attribute für FCoE**

| Name | Beschreibung | Netzwerktyp | VLAN-ID | SAN |
|---|---|---|---|---|
| FC A1 | FCOE A1 | Speicher – FCoE | 30 | A |
| FC A2 | FCOE A2 | Speicher – FCoE | 40 | B |

**ANMERKUNG:** Weitere Informationen zu SmartFabric und Fibre Channel finden Sie im *Konfigurations- und Fehlerbehebungshandbuch zu Dell EMC PowerEdge MX SmartFabric* unter https://infohub.delltechnologies.com/

# Definieren von VLANs für FCoE

Gehen Sie wie folgt vor, um VLANs für FcoE zu definieren:

1. Klicken Sie im Menü auf **Konfiguration** > **VLANs**.
2. Klicken Sie im Feld **VLANs** auf **Definieren**.
   Das Fenster **Netzwerke definieren** wird angezeigt.
3. Geben Sie einen **Namen** und eine **Beschreibung** für VLAN ein.
   Die Beschreibung ist optional.
4. Geben Sie die **VLAN-ID** ein und wählen Sie dann den **Netzwerktyp** aus.
   Für FCoE muss der **Netzwerktyp Speicher FCoE** sein.
5. Klicken Sie auf **Fertigstellen**.

# VLANs bearbeiten

Sie können VLANs auf den bereitgestellten Servern in einem SmartFabric hinzufügen oder entfernen.

So fügen Sie VLANs hinzu oder entfernen Sie:

1. Klicken Sie im Menü auf **Geräte** > **Fabric**.
2. Wählen Sie das Fabric aus, für das Sie das VLAN hinzufügen oder entfernen möchten.
3. Wählen Sie im linken Fensterbereich **Server** aus und wählen Sie die erforderlichen Server aus.

4. Klicken Sie auf **Netzwerke bearbeiten**.
5. Wählen Sie eine der folgenden Optionen:
   - **NIC Teaming von LACP**
   - **Kein Teamvorgang**
   - **Andere**
6. Definieren Sie die gekennzeichneten und nicht gekennzeichneten VLANs, um die VLAN-Auswahl nach Bedarf zu ändern.
7. Wählen Sie VLANs auf markierten und nicht markierten Netzwerken für jeden Mezzanine-Karten-Port aus.
8. Klicken Sie auf **Speichern**.

# Richtlinien zur Skalierung von VLAN

Die Anzahl der empfohlenen VLANs unterscheidet sich zwischen den Modi, da der SmartFabric-Modus Netzwerk-Automatisierungsfunktionen bietet, die im vollständigen Switch-Modus nicht verfügbar sind.

Die folgende Tabelle listet die maximale Anzahl der VLANs auf, die pro Fabric, Uplink und Server-Port empfohlen werden:

**Tabelle 19. Maximale Anzahl der VLANs, die im SmartFabric-Modus empfohlen werden**

| OS10-Version | Parameter | Value |
|---|---|---|
| 10.5.2.4 und 10.5.2.6 | Maximale VLANs pro Fabric | 1536 |
| | Maximale VLANs pro Uplink | 1536 |
| | Maximale VLANs pro Serverport | 512 |
| 10.5.1.6-10.5.1.7 | Maximale VLANs pro Fabric | 512 |
| | Maximale VLANs pro Uplink | 512 |
| | Maximale VLANs pro Serverport | 256 |
| 10.5.0.1–10.5.0.7 | Maximale VLANs pro Fabric | 256 |
| | Maximale VLANs pro Uplink | 256 |
| | Maximale VLANs pro Serverport | 64 |
| 10.4.0.R3S<br>10.4.0.R4S | Maximale VLANs pro Fabric | 128 |
| | Maximale VLANs pro Uplink | 128 |
| | Maximale VLANs pro Serverport | 32 |

**ANMERKUNG:** Anweisungen zur Aktivierung der SmartFabric-Services zur Unterstützung einer höheren VLAN-Zahl (mehr als 256 VLANs pro Fabric) finden Sie im Dell EMC PowerEdge MX SmartFabric-Konfigurations- und Troubleshootinghandbuch unter https://infohub.delltechnologies.com/t/mx-series-modular-switches-poweredge-mx-7/.

## Konfigurationsrichtlinien für Spanning Tree zur VLAN-Skalierung

**Tabelle 20. Konfigurationsrichtlinien für VLAN-Skalierung (STP-Variante)**

| Skalieren | STP-Variante |
|---|---|
| Anzahl der in den einzelnen EAMs konfigurierten VLANs beträgt weniger als 100 | RPVST oder RSTP können konfiguriert werden |
| Anzahl der in den einzelnen EAM konfigurierten VLANs beträgt mehr als 100 | Empfohlene Konfiguration ist RSTP |

**Tabelle 21. Konfigurationsrichtlinien für VLAN-Skalierung (VLAN-Konfiguration)**

| Skalieren | Skalierungsprofil-VLAN-Konfiguration |
|---|---|
| Anzahl der Port-VLAN-Kombinationen beträgt weniger als 6144 | Nicht erforderlich |

**Tabelle 21. Konfigurationsrichtlinien für VLAN-Skalierung (VLAN-Konfiguration) (fortgesetzt)**

| Skalieren | Skalierungsprofil-VLAN-Konfiguration |
|---|---|
| Anzahl der Port-VLAN-Kombinationen beträgt mehr als 6144 | Ist erforderlich |

**ANMERKUNG:** Weitere Informationen zu VLAN mit Skalierungsprofil finden Sie im Konfigurations- und Troubleshootinghandbuch zu Dell EMC PowerEdge MX SmartFabric unter https://infohub.delltechnologies.com/t/mx-series-modular-switches-poweredge-mx-7/.

# 13

# Netzwerke verwalten

Sie können für die markierten und nicht markierten VLANs logische Netzwerke konfigurieren, die Ihre Umgebung darstellen. Diese logischen Netzwerke werden für die Bereitstellung der entsprechenden VLANs auf dem zugeordneten Switch-Port für den NIC-Port des physischen Servers verwendet.

**ANMERKUNG:** VLANs werden nur Servern zugewiesen, die im SmartFabric-Modus mit Switches verbunden sind. Für Server, die im Full Switch-Modus mit Switches verbunden sind, werden die VLAN-Informationen ignoriert.

In markierten Netzwerken verarbeitet ein Port mehrere VLANs. Mithilfe markierter VLAN-Netzwerke können Sie leichter identifizieren, welches Paket zu dem VLAN auf der anderen Seite gehört. Ein Paket wird mit einem VLAN-Tag im Ethernet-Frame markiert. Eine VLAN-ID wird in die Kopfzeile gestellt, um das Netzwerk zu identifizieren, zu dem es gehört.

In nicht markierten Netzwerken verarbeitet ein Port nur ein VLAN.

Um die Liste der Netzwerke anzuzeigen, klicken Sie auf **Konfiguration** > **VLANs**. Die Seite **VLANs** mit der Liste der Netzwerke wird angezeigt. Sie können den Namen, die Beschreibung und die VLAN-ID der Netzwerke anzeigen.

Eine Zusammenfassung des ausgewählten Netzwerks wird auf der rechten Seite angezeigt.

Auf der Seite **Netzwerke** können Sie folgende Aufgaben ausführen:

- Netzwerke definieren
- Netzwerke bearbeiten
- Löschen von Netzwerken
- Netzwerke exportieren

**Themen:**



# SmartFabric VLAN-Verwaltung und automatische QoS

Neben dem Zuweisen von VLANs zu Serverprofilen automatisieren SmartFabric Services auch QoS-Einstellungen basierend auf Benutzereingaben. Wenn ein VLAN erstellt wird und Sie den betreffenden Datenverkehrstyp (wie z. B. iSCSI und vMotion) auswählen, weist die SFS Engine diesem VLAN die richtige QoS-Einstellung zu. Sie können auch ein "Metall" wie Gold und Bronze auswählen, um dem Datenverkehr Ihre eigenen Prioritätswerte zuzuweisen.

**Tabelle 22. Netzwerk-Datenverkehrstypen – QoS-Einstellungen**

| Netzwerk-Datenverkehrstyp | Beschreibung | QoS-Einstellung |
|---|---|---|
| Allgemeiner Zweck (Bronze) | Wird für Datenverkehr mit niedriger Priorität verwendet | 2 |
| Allgemeiner Zweck (Silber) | Wird für Datenverkehr mit Standard-Priorität verwendet | 3 |
| Allgemeiner Zweck (Gold) | Wird für Datenverkehr mit hoher Priorität verwendet | 4 |
| Allgemeiner Zweck (Platin) | Wird für Datenverkehr mit extrem hoher Priorität verwendet | 5 |
| Cluster-Interconnect | Wird für Cluster-Heartbeat-VLANs verwendet | 5 |

**Tabelle 22. Netzwerk-Datenverkehrstypen – QoS-Einstellungen (fortgesetzt)**

| Netzwerk-Datenverkehrstyp | Beschreibung | QoS-Einstellung |
|---|---|---|
| Hypervisor-Verwaltung | Wird für Hypervisor-Management-Verbindungen wie z. B. das ESXi-Verwaltungs-VLAN verwendet | 5 |
| Speicher – iSCSI | Wird für iSCSI-VLANs verwendet | 5 |
| Speicher – FCoE | Wird für FCoE-VLANs verwendet | 5 |
| Speicher – Datenreplikation | Verwendet für VLANs, die die Replikation von Speicherdaten wie z. B. für VMware VSAN unterstützen | 5 |
| VM-Migration | Wird für VLANs mit Unterstützung für vMotion und ähnliche Technologien verwendet | 5 |
| VMWare FT-Protokollierung | Wird für VLANs mit Unterstützung für VMware Fault Tolerance verwendet | 5 |

# Definieren von Netzwerken

So konfigurieren Sie ein logisches Netzwerk:

1. Klicken Sie auf **Konfiguration** > **VLANs**.
   Die Seite **VLANs** wird angezeigt.
2. Klicken Sie auf **Definieren**.
   Das Fenster **Netzwerke definieren** wird angezeigt.
3. Geben Sie den Namen, die Beschreibung und die VLAN-ID ein.
   Das Format eines einzelnen VLAN ist ID-123, während für einen ID-Bereich das Format 123-234 lautet.
4. Wählen Sie den **Netzwerktyp** aus.
   Weitere Informationen finden Sie unter SmartFabric VLAN-Verwaltung und automatische QoS. Die folgenden Optionen sind verfügbar:
   - **Allgemeiner Zweck (Bronze)**
   - **Allgemeiner Zweck (Silber)**
   - **Allgemeiner Zweck (Gold)**
   - **Allgemeiner Zweck (Platinum)**
   - **Cluster-Interconnect**
   - **Hypervisor-Verwaltung**
   - **Speicher – iSCSI**
   - **Speicher – FCoE**
   - **Speicher – Datenreplikation**
   - **VM-Migration**
   - **VMware FT-Protokollierung**

   Weitere Informationen finden Sie unter SmartFabric VLAN-Verwaltung und automatische QoS.

# VLANs bearbeiten

So bearbeiten Sie ein Netzwerk:

1. Wählen Sie auf der Seite **VLANs** das Netzwerk aus, das Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
   Das Fenster **Netzwerk bearbeiten** wird angezeigt.
2. Nehmen Sie ggf. erforderliche Änderungen vor.
   Stellen Sie beim Bearbeiten des Netzwerks sicher, dass nur ein VLAN auf beiden Ports konfiguriert ist.
   **ANMERKUNG:** Löschen Sie im Fabric-Modus VLAN nicht aus OME – Modular, wenn das VLAN mit einem Uplink verknüpft ist.

# Exportieren von VLANs

So exportieren Sie die Netzwerkkonfiguration:

Wählen Sie auf der Seite **VLANs** das Netzwerk aus, und klicken Sie auf **Exportieren**. Wählen Sie **Alle als CSV exportieren** oder **Alle als JSON exportieren**.
Der Netzwerkdetails werden wie gewählt im Format `.csv` oder `.json` auf ein lokales Laufwerk Ihres Systems exportiert.

# Importieren von VLANs

So importieren Sie VLANs:

1. Wählen Sie auf der Seite **VLANs** das gewünschte Netzwerk aus, klicken Sie auf **Importieren**und wählen Sie **Aus Datei importieren** aus.
   Der Bildschirm **Aus Datei importieren** wird angezeigt.
2. Klicken Sie auf **Datei auswählen**, um die Datei am Zielort zu suchen und zu importieren. Unterstützte Dateitypen sind `.csv` und `.json`.
3. Klicken Sie auf **Fertigstellen**, um die VLANs zu importieren.

# Löschen von VLANs

So löschen Sie ein VLAN:

Wählen Sie auf der Seite **Netzwerke** das VLAN aus, und klicken Sie auf **Löschen**.
Wenn das Netzwerk einem Fabric-Uplink zugeordnet ist, wird eine Warnmeldung angezeigt, dass das Löschen des Netzwerks zum Verlust der Konnektivität führt.

# 14

# Fibre Channel-EAMs verwalten

Der MXG610s Fibre Channel (FC)-Switch ist für missionskritische Anwendungen ausgelegt, die auf Daten auf einem externen Speicher zugreifen. Er ist optimiert für Flash-Speicher und virtualisierte Serverumgebungen. Der FC-Switch ermöglicht Unternehmen die dynamische Skalierung der Konnektivität und Bandbreiten-Ports-on-Demand (POD). Er verbessert Vorgänge mit konsolidierter Verwaltung und einfacher Server- und Speicherkonnektivität.

OME – Modular macht die Verwaltung des MXG610s einfach. Die SSO-Funktion in OME – Modular erhöht die Sicherheit und Benutzerfreundlichkeit.

So zeigen Sie die GUI des MXG610s FC-Switch an:

1. Auf der Seite **Geräte** > **E/A-Module** klicken Sie auf **EAM UI starten**.

   Die Schnittstelle der MXG610s FC Web-Tools wird angezeigt.

# 15

# Firmware verwalten

Die Firmware-Funktion in OME – Modular hilft Ihnen, die Firmware aller Komponenten im Gehäuse zu aktualisieren. Die Komponenten umfassen Rechnerschlitten, Ethernet-EAMs, Speicher-EAMs und SAS-EAM(s). Die Firmwareaktualisierungen können Quellen von der Dell Website oder ein benutzerdefiniertes Repository sein, das unter Verwendung des Repository Manager eingerichtet wurde.

Sie müssen die Administratorrolle für das Gehäuse und die Aktualisierungsberechtigung für das Gerät haben, um die Firmware auf dem Gehäuse aktualisieren zu können. Zum Aktualisieren der Firmware auf den Komponenten müssen Sie über die Gerätemanager-Rolle und die Berechtigung zum Aktualisieren des Geräts verfügen.

Das MX-Gehäusepaket bezieht sich auf die folgenden Updatepakete:

- Gehäuse-Manager-DUP – Dieses DUP beinhaltet die Firmware von OME – Modular.
- Speicherschlitten-DUP – Dieses DUP enthält Aktualisierungen für die Dell Speicherschlitten im Gehäuse.
- Speicher-EAM-DUP – Dieses DUP enthält Aktualisierungen für die Gehäusespeicher-EAMs.

Die DUPs für Netzwerk-EAMs und Switches sind lizenzierte Software, die als einzelne DUPs zur Verfügung gestellt werden. Für externen Speicher sind die DUPs im Katalog gebündelt. Wenn die Festplattenlaufwerke oder Speichergehäuse einem Rechnerschlitten zugewiesen sind, können Sie sie unter Verwendung des iDRAC aktualisieren. Sie können die zugewiesenen oder nicht zugewiesenen Festplatten jedoch nicht über einen Gehäusekontext aktualisieren. Sie können die Laufwerke einem Server zuweisen, um sie zu aktualisieren.

Das Rechnerschlittenpaket bezieht sich auf die Pakete für die Serverkomponenten: BIOS, NIC, RAID, Festplatten und iDRAC.

Die Firmwareaktualisierung erfordert das Festlegen des Katalogs, das Abholen der Firmware-Bestandsliste, das Überprüfen der Konformität und das Aktualisieren der Firmware.

Alle verfügbaren Baselines werden auf der Seite **Konfiguration** > **Firmware-Compliance** angezeigt. Sie können oben auf der Seite eine Zusammenfassung der Baseline-Übereinstimmung und ein Tortendiagramm anzeigen. Sie können auch die Zusammenfassung der gewünschten Baseline im rechten Bereich der Seite **Firmware-Compliance** anzeigen.

Auf der Seite **Firmware-Compliance** werden die folgenden Basisline-Informationen angezeigt: Compliance, Name der Baseline, Jobstatus, Katalogtyp, Zeitstempel der letzten Verwendung der Baseline.

Der Compliance-Status der Baseline kann die folgenden Typen aufweisen:

- OK
- Kritisch
- Warnung
- Downgrade
- Unbekannt

Auf der Seite **Firmware-Compliance** können Sie folgende Aufgaben ausführen:

- Baseline erstellen
- Baseline bearbeiten
- Bericht anzeigen
- Baseline löschen
- Kataloge verwalten
- Compliance überprüfen

## Themen:

# Kataloge verwalten

Mit der Katalog Verwaltungsfunktion in OME – Modular können Sie die Liste der DUPs auswählen, die mit Baselines zur Bestimmung der Firmware-Compliance verwendet werden sollen.

Die Kataloge können von den folgenden Speicherorten bezogen werden:

- Neueste validierte Stacks der Gehäuse-Firmware auf Dell.com: Komponenten- und Geräte-Firmware für die MX-Lösung werden zusammen als durchgehend validierter Lösungsstack oder als Firmware-Baseline rigoros getestet. Der validierte Stapel entspricht der neuesten Lösungs-Baseline. Weitere Informationen finden Sie in der Tabelle unter *Aktualisieren von MX7000-Komponenten mithilfe von OME-Modular* im https://www.dell.com/OME-modular.

  **ANMERKUNG:** Sie müssen den HTTPS-Proxy wie in der Erstkonfiguration beschrieben konfigurieren.
- Neueste Komponenten-Firmware-Versionen auf Dell.com: Dieser Katalog wird am zweiten und vierten Freitag jedes Monats mit neuer Firmware aktualisiert. Dies kann Versionen von Firmware für Komponenten enthalten, die seit dem letzten validierten Lösungsstack der Gehäuse-Firmware einzeln getestet und freigegeben wurden.
- Netzwerkpfad: Die Netzwerkfreigabe besteht aus NFS, CIFS, HTTP oder HTTPS.

  Sie können mit dem Repository Manager den benutzerdefinierten Katalog erstellen und ihn auf der Netzwerkfreigabe speichern. Die Verzeichnisse mehrerer oder früherer Kataloge können über verschiedene Katalog-Dateipfade verfügbar gehalten werden.

**ANMERKUNG:** Wenn Sie einen Katalog an einem bestimmten Datum erstellen und ihn an den gewünschten Speicherort in Ihrem Netzwerk oder auf Ihrem lokalen Laufwerk herunterladen, ist der Download erfolgreich. Wenn Sie den Katalog jedoch am selben Tag zu unterschiedlichen Zeiten ändern und versuchen, ihn herunterzuladen, wird der geänderte Katalog nicht heruntergeladen. Wenn der Repository-Typ NFS ist und die Katalogdatei auf dem angegebenen NFS-Server nicht verfügbar ist, verwendet das System die Katalogdatei, die zuletzt abgerufen wurde.

So zeigen Sie die Liste der Kataloge an:

Klicken Sie auf der Seite **Firmware-Compliance** auf **Katalogverwaltung**.
Die Seite **Katalogverwaltung** wird angezeigt.

Sie können einen Katalog auswählen, um auf der rechten Seite eine Zusammenfassung anzuzeigen. Die Zusammenfassung umfasst die Anzahl der Bündel im Katalog, Datum und Uhrzeit der Freigabe des Katalogs und den Namen der mit dem Katalog verknüpften Baselines.

Auf der Seite **Katalogverwaltung** können Sie folgende Aufgaben ausführen:

- Kataloge hinzufügen
- Kataloge bearbeiten
- Prüfen Sie auf Katalog-Updates.
- Kataloge löschen

# Kataloge anzeigen

Sie können die folgenden Informationen im Fenster **Katalogverwaltung** anzeigen:

- Name und Downloadstatus des Katalogs
- Den Typ des Repository, von dem der Katalog heruntergeladen wurde.
- Speicherort des Repository
- Name der Katalogdatei `.xml`.
- Zeitstempel der Freigabe des Katalogs

1. Klicken Sie in der Menüleiste auf **Konfiguration** > **Firmware** > **Katalogverwaltung**.
   Die Seite **Katalogverwaltung** wird angezeigt.
2. Wählen Sie einen Katalog aus, um auf der rechten Seite eine Zusammenfassung anzuzeigen.

   Die Zusammenfassung umfasst die Anzahl der Bündel im Katalog, Zeitstempel der Freigabe des Katalogs und den Namen der mit dem Katalog verknüpften Bündel.

# Kataloge hinzufügen

So fügen Sie Kataloge hinzu:

1. Klicken Sie auf der Seite **Katalogverwaltung** auf **Hinzufügen**.
   Das Fenster **Firmwarekatalog hinzufügen** wird angezeigt.

2. Geben Sie einen Namen für den Katalog ein, und wählen Sie die Katalogquelle aus.

   Folgende Optionen stehen zur Verfügung:

   - **Neueste validierte Stapel von Gehäuse-Firmware unter Dell.com** – Die Versionen der Firmware in diesem Katalog wurden zusammen als Teil des neuesten OME Modular Firmware-Release geprüft.

     **ANMERKUNG:** Wenn die Option **validierte Stapel** ausgewählt ist, sind die Details erst verfügbar, wenn die Daten in der Datenbank gespeichert werden.
   - **Neueste Komponenten-Firmware-Versionen auf Dell.com**: Dieser Katalog wird am zweiten und vierten Freitag jedes Monats mit neuer Firmware aktualisiert. Er enthält die Firmwareversionen für Komponenten, die seit dem letzten validierten Lösungsstack der Gehäuse-Firmware individuell getestet und veröffentlicht wurden.
   - **Netzwerkpfad** – Der Ordner, in dem ein Katalog und optional verbundene Aktualisierungen durch Auspacken des geprüften Stapels unter **ftp.dell.com** oder mithilfe von Dell EMC Repository Manager platziert wurden.

3. Wählen Sie den **Freigabetyp**.

   Folgende Optionen stehen zur Verfügung:

   - NFS
   - CIFS
   - HTTP
   - HTTPS

   **ANMERKUNG:** Die Option **Freigabetyp** ist nur verfügbar, wenn Sie **Netzwerkpfad** auswählen.

   **ANMERKUNG:** Die HTTPS-Freigabefunktion mit Proxy funktioniert nicht, wenn die Authentifizierung sowohl für die Proxy- als auch die HTTPS-Freigabe aktiviert ist.

4. Wählen Sie den Modus zum Aktualisieren des Katalogs aus.

   Folgende Optionen stehen zur Verfügung:

   - Manuell
   - Automatisch

   Der Standardmodus ist manuell.

5. Wählen Sie die **Aktualisierungsfrequenz** aus.

   - Täglich
   - Wöchentlich

   Die Zeit kann im Format `HH:MM` angegeben werden.

## Kataloge bearbeiten

Sie können nur den Katalognamen, die Netzwerkfreigabeadresse und den Katalog-Dateipfad ändern.

So bearbeiten Sie Kataloge:

1. Wählen Sie auf der Seite **Katalogverwaltung** den Katalog aus, den Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
   Das Fenster **Firmwarekatalog bearbeiten** wird angezeigt.
2. Nehmen Sie ggf. erforderliche Änderungen vor.

## Überprüfen der Katalog-Updates

Sie können auf der Seite **Katalogverwaltung** manuell oder automatisch nach Katalog-Updates suchen und diese herunterladen. Wenn die Überprüfung wöchentlich geplant ist und die Aktualisierung nicht verfügbar ist oder der Standort nicht erreichbar ist, bricht OME-Modular die geplante Prüfung ab. Führen Sie die nächste Prüfung manuell durch. Die manuelle Überprüfung verhindert unnötige Überprüfungen, wenn der Katalog verschoben oder gelöscht wird.

So suchen Sie nach Katalog-Updates:

1. Klicken Sie auf der Seite **Firmware-Compliance** auf **Katalogverwaltung**.
   Die Seite **Katalogverwaltung** mit der Liste verfügbarer Kataloge wird angezeigt.
2. Wählen Sie den Katalog aus, den Sie auf Updates prüfen möchten, und klicken Sie auf **Auf Update überprüfen**.
   Es wird eine Meldung zur Bestätigung der Prüfung angezeigt.

## Kataloge löschen

Sie können nur Kataloge löschen, die keiner Baseline zugeordnet sind. Beim Versuch, einen Katalog zu löschen, der einer Baseline zugeordnet ist, wird eine Fehlermeldung angezeigt.

So löschen Sie einen Katalog:

Wählen Sie auf der Seite **Katalogverwaltung** den Katalog aus, den Sie löschen möchten, und klicken Sie auf **Löschen**.

# Baselines erstellen

So erstellen Sie eine Firmware-Baseline:

1. Klicken Sie auf **Konfiguration** > **Firmware-Compliance** > **Baseline erstellen**.
   Das Fenster **Firmware-Baseline erstellen** wird angezeigt.
2. Wählen Sie den Katalogtyp und geben Sie einen Namen und eine Beschreibung für die Baseline ein.
3. Klicken Sie auf **Hinzufügen**.
   Das Fenster **Firmwarekatalog hinzufügen** wird angezeigt.
4. Wählen Sie die Katalogquelle aus.
5. Im Fenster **Firmware-Baseline erstellen** wählen Sie die Geräte oder Gruppen aus, für die Sie die Baseline erstellen möchten.

   Nachdem die Baseline erstellt wurde, wird eine Meldung angezeigt und eine Compliance-Prüfung für die Baseline durchgeführt. Der Jobstatus wird auf der Seite **Firmware** angezeigt.

   **ANMERKUNG:** Wenn die Baseline aus dem Katalog erstellt wird, werden die Informationen der zugeordneten Baseline angezeigt.

# Baselines bearbeiten

So bearbeiten Sie eine Baseline:

1. Wählen Sie auf der Seite **Firmware-Compliance** die Baseline aus, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
   Es wird das Fenster **Firmware-Baseline bearbeiten** angezeigt.
2. Nehmen Sie ggf. erforderliche Änderungen vor.

# Compliance überprüfen

So überprüfen Sie die Compliance einer Firmware-Baseline:

1. Wählen Sie auf der Seite **Firmware-Compliance** die Baseline aus und klicken Sie auf **Compliance überprüfen**.
   Informationen über die Compliance-Überprüfung werden rechts von der Seite **Firmware-Compliance** angezeigt.
2. Klicken Sie auf **Bericht anzeigen**.
   Daraufhin wird die Seite **Compliance-Report** angezeigt.

   Folgende Details werden angezeigt:

   - Geräte-Compliance
   - Komponenten-Compliance
   - Typ
   - Modell
   - „Gerätename“ enthält
   - „Komponente“ enthält
   - Service-Tag enthält
   - Neustart erforderlich
   - Voraussetzungen
   - Auswirkungseinschätzung
   - „Aktuelle Version“ enthält
   - „Baseline-Version“ enthält

   **ANMERKUNG:** Wenn die Firmware DUP nicht im Katalog vorhanden ist, wird eine Fehlermeldung angezeigt.

**ANMERKUNG:** Die Firmware-Herabstufung für Netzwerk EAMs über DUP wird von OME-M nicht unterstützt. Weitere Informationen finden Sie im *OpenManage Enterprise-Modular Edition for PowerEdge MX7000*-Gehäuse-Benutzerhandbuch oder dem *OS10 Enterprise Edition-Benutzerhandbuch*.

Compliance-Status folgender Typen sind möglich:

- Unbekannt: Die Firmware-Version der Komponente oder des Geräts ist im Katalog nicht verfügbar.
- Kritisch: Die Firmware-Version auf dem Gerät ist älter als die Katalog-Firmware-Version und der Status des Firmwareupdates im Katalog befindet sich in einem kritischen oder dringenden Zustand.
- Warnung: Die Firmware-Version auf dem Gerät ist älter als die Katalog-Firmware-Version und das Firmwareupdate im Katalog befindet sich in einem kritischen Zustand.
- Zurückstufung: Die Firmware-Version auf dem Gerät ist neuer als die Katalog-Firmware-Version.
- Ok: Die Firmware-Version auf dem Gerät und die Katalog-Firmware-Version sind identisch.

Auf der Seite **Compliance-Report** können Sie folgende Aufgaben ausführen:

- **Kompatibel machen** – Aktualisiert die Firmware für das ausgewählte Gerät oder die Komponente innerhalb eines Bundels.
- **Exportieren** – Exportiert den Compliance-Bericht in das Format `.csv` am angegebenen Speicherort.
- **Erweiterte Filter** – Sortiert die Geräteinformationen.

Beim Aktualisieren der Firmware für SAS-EAMs, die als individuelle Komponente und eine Gehäusekomponente verfügbar sind, mithilfe der Compliance-Report-Methode, schlägt die Aktualisierung des Verwaltungsmoduls fehl. Wählen Sie das SAS-EAM aus der Gehäusekomponente oder dem Compliance-Report aus.

3. Klicken Sie auf **Voraussetzungen**, um die Voraussetzungen und Abhängigkeitsanforderungen für die Durchführung des Firmwareupdates anzuzeigen.
   - Voraussetzungen: Zeigt die Aktionen an, die vor der Durchführung des Firmwareupdates ausstehen.
   - Abhängigkeitsanforderungen: Zeigt den Link zum Herunterladen des erforderlichen DUP an. Abhängigkeiten können folgendermaßen klassifiziert werden:
     - Abhängigkeiten zwischen Komponenten: Zeigt die sequenzielle Updatereihenfolge für das Gerät oder die Komponente gemäß der Firmwareupdatematrix an.
     - Interdependenz: Zeigt eine Abhängigkeit zwischen zwei verschiedenen Komponenten oder Geräten an.

# Aktualisieren der Firmware

Bevor Sie die Firmware von einem Gehäuse, Rechner oder Speicherschlitten aktualisieren, stellen Sie sicher, dass alle EAMs und Netzwerkstrukturen funktionsfähig sind.

- Ein Downgrade von OME-M- oder MX7000-Netzwerk-E/A-Komponenten kann zu einem Verlust von Konfigurationsdaten und Funktionen für das Management führen.
- Wenn Sie alle Komponenten auswählen, kann OME-M die Komponentenupdates in der ordnungsgemäßen Reihenfolge durchführen. Während des Updates einer oder mehrerer einzelner Komponenten können Sie in den Readme-Dokumenten nachprüfen, ob alle Voraussetzungen und Sequenzierungsanforderungen erfüllt werden, um Ausfälle zu vermeiden.
- Wenn Sie eine Komponente auswählen, die Teil einer Gruppe mit hoher Verfügbarkeit ist, werden alle anderen Komponenten in der Gruppe aktualisiert, auch wenn sie nicht explizit ausgewählt wurden.
- Wenn Sie für das ONIE-Update ein MX Netzwerk-EAM auswählen, das Teil einer Fabric ist, werden andere Nodes in der Fabric automatisch aktualisiert.
- MX-Speicher-E/A-Module müssen explizit ausgewählt werden, um aktualisiert zu werden.
- Wenn Sie mehrere Netzwerk-EAMs für ein Firmwareupdate auswählen, werden die Mitglied-EAMs zuerst und das Master-EAM später aktualisiert.
- Die OS10-Firmware kann nicht mehr als einen Update-Job gleichzeitig verarbeiten. Wenn ein Update durchgeführt wird, werden alle zusätzlichen Updateanfragen abgelehnt und entsprechende Fehlermeldungen angezeigt.

**ANMERKUNG:** Die Schaltfläche **Firmware aktualisieren** kann während der Bestandsaktualisierung vorübergehend deaktiviert werden, wenn ein Auftrag **Bestandsaufnahme aktualisieren** oder **Standardbestandsaufnahme** ausgeführt wird.

So aktualisieren Sie die Firmware.

1. Wählen Sie auf der Seite **Compliance-Report** das Gerät oder die Komponente aus, für das oder die Sie die Firmware aktualisieren möchten.
   Das Fenster **Firmware aktualisieren** wird angezeigt.
2. Wählen Sie die Option **Jetzt aktualisieren** aus, um die Firmware sofort zu aktualisieren, oder **Für später planen**, um die Firmware am ausgewählten Datum und zu der angegebenen Uhrzeit zu aktualisieren.

**ANMERKUNG:** Wenn das System die lokale Uhrzeit auf der Seite **Zeitkonfiguration** anzeigt, nachdem Sie die NTP-Server konfiguriert haben, konfigurieren Sie die NTP-Server neu.

**ANMERKUNG:** Wenn der aktive MM während des Firmwareupdates neu startet und der Stand-by-MM aktiv ist, werden einige Meldungen auf der Seite **Ausführungsdetails** für das Firmwareupdate nicht angezeigt. Die Meldungen werden aufgrund von Synchronisationsproblemen nicht angezeigt.

**ANMERKUNG:** Während des OME – Modular-Firmwareupdates können mehrere Nutzer das OME – Modular-DUP über jede Schnittstelle hochladen. Es wird jedoch möglicherweise eine Warnmeldung angezeigt, nachdem der Firmwareupdate-Job initiiert wurde.

**ANMERKUNG:** Für Nicht-Standard-VLANs ist die Verwaltungs-IPv6-IP von MX9116n- oder MX5108n-EAMs nicht erreichbar, wenn die DHCP-V6-Konfiguration im ToR-Switch nicht über das IPv6- Standard-Gateway verfügt.

Die Anzahl der EAMs, die aktualisiert werden können, variiert je nach EAM-Versionen. In der folgenden Tabelle wird die Anzahl der EAMs angezeigt, die gleichzeitig aktualisiert werden können.

### Tabelle 23. EAM-Firmwareupdatematrix

| IOM Version | OME-M Version | Anzahl der EAMs |
|---|---|---|
| 10.5.0.5 | 1.10.20 oder höher | 4 |
| 10.5.0.7 | 1.20.00 oder höher | 6 |
| 10.5.1.6 | 1.20.10 oder höher | 6 |
| 10.5.2.4 | 1.30.00 oder höher | Keine Beschränkungen |

Sie müssen die EAMs für das Firmwareupdate je nach Typ des EAM gruppieren. Die folgende Tabelle zeigt ein Beispiel für die Gruppierung von 12 EAMs für ein Firmwareupdate.

### Tabelle 24. EAMs für Firmwareupdate gruppieren

| Beispiel für 12 E/A-Module | Kombination | Gruppe 1 | Gruppe 2 | Gruppe 3 |
|---|---|---|---|---|
| **10.5.0.5** | 6 Fabrics | Fabric 1 und 2 | Fabric 3 und 4 | Fabric 5 und 6 |
| | 12 Full-Switches | EAM 1 bis 4 | EAM 5 bis 8 | EAM 9 bis 12 |
| | 4 Fabrics und 4 Full-Switch | Fabric 1 und 2 | Fabric 3 und 4 | 4 Full-Switch-EAM |
| **10.5.0.7 oder 10.5.1.6** | 6 Fabrics | Fabric 1 bis 3 | Fabric 4 bis 6 | Nicht anwendbar |
| | 12 Full-Switches | EAM 1 bis 6 | EAM 6 bis 12 | Nicht anwendbar |
| | 4 Fabrics und 4 Full-Switch | Fabric 1 bis 3 | Fabric 4 und 4 Full-Switch-EAM | Nicht anwendbar |

Wenn alle EAMs auf den Stack 10.5.2.4 aktualisiert sind, zeigen die Netzwerk-EAMs zwei Softwarekomponenten zum Update an. Folgende Optionen stehen zur Verfügung:

- Dell EMC Networking SmartFabric OS10
- Dell EMC Networking ONIE Firmware

Einschränkungen für ONIE-Firmwareupdates:

- Die Updateoption für die ONIE-Firmware ist nur verfügbar, wenn die OS10-Version 10.5.2.4 oder höher ist.
- Wenn Sie für das ONIE-Update ein Netzwerk-EAM auswählen, das Teil einer Fabric ist, werden andere Nodes in der Fabric automatisch aktualisiert.
- Wenn Sie eine alte Version von EAM einfügen, kann die ONIE-Firmware nicht aktualisiert werden, bis OS10 auf 10.5.2.4 aktualisiert wurde.

**ANMERKUNG:** Die Firmware der ONIE-Komponente wird nicht aktualisiert, da das System nicht in ONIE booten kann, wenn das GRUB-Menü mit seriellen Steuerzeichen angezeigt wird. Dieses Problem wird in der ONIE-Firmwareversion 3.35.1.1-15 behoben. Wenn die ONIE-Aktualisierung fehlschlägt oder ein ONIE-Boot-Problem auftritt, wiederholen Sie das Update der ONIE-Komponenten-Firmware.

# Firmware zurücksetzen

Wenn die Firmwareaktualisierung für ein Gerät oder eine Komponente nicht Ihren Erwartungen entspricht, können Sie ein Rollback der Aktualisierung auf die Version vor der Aktualisierung durchführen. Die Rollback-Option ist nur aktiviert, wenn OME – Modular auf das Firmware-Paket der vorherigen Version zugreifen kann. Der Zugriff kann auf folgende Weisen aktiviert werden:

- Ein Gerät, das die Rollback-Version (oder N-1-Version) hat, die mit der vorherigen Version übereinstimmt. Nicht alle Gerät unterstützen eine Rollback- oder N-1-Version. Die Rollback-Version wird als ein Rollback-Kandidat angezeigt, selbst wenn sie nicht mit dem Version vor der Aktualisierung übereinstimmt.
- Ein importierter Katalog enthält einen Verweis auf die vorherige Katalogversion.
- Sie können nach einem Firmwarepaket mit der vorherigen Version suchen.

Für Netzwerk-IOMs hängt die Verfügbarkeit von Rollback-Informationen vom Status des Netzwerk-IOM (vollständiger Switch oder Fabric) und der Methode der Firmwareaktualisierung ab. Wenn die Firmware auf Knoten in der Fabric aktualisiert wird, sind die Rollback-Informationen auf dem Knoten verfügbar, auf dem die Firmwareaktualisierung initiiert wird. Wenn die Firmware auf den Netzwerk-IOMs der Mitgliedsgehäuse über das Hauptgehäuse aktualisiert wird, sind die Rollback-Informationen nur auf dem Hauptgehäuse verfügbar.

So setzen Sie eine Firmwareaktualisierung zurück:

1. Klicken Sie auf der Seite **Firmware** auf **Rollback für die Firmware**.
   Das Fenster **Rollback für die Firmware** wird angezeigt.
2. Wählen Sie die Komponente aus, für die Sie die Firmware zurücksetzen möchten, und klicken Sie auf **Rollback**.

   **ANMERKUNG:** Das Gerät wird immer mit individuellem DUP aktualisiert und nie als Teil des Katalogs oder der Baselines aktualisiert oder zurückgestuft. Wenn das Gerät jedoch einer Baseline zugeordnet ist und ein Update als Teil dieses Katalogs oder dieser Baseline verfügbar ist, wird standardmäßig die Katalogoption für das Rollback bereitgestellt, da es sich um eine sichere Option handelt.

# Firmware löschen

Sie können die Firmware-Baselines löschen, wenn Sie über die Administratorberechtigung verfügen.

So löschen Sie eine Firmware-Baseline:

Wählen Sie auf der Seite **Firmware** die Baseline aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
Sie werden dazu aufgefordert, den Löschvorgang zu bestätigen.

16

# Warnungen und Protokolle überwachen

Sie können die Warnungen anzeigen und verwalten, die in der Verwaltungssystem-Umgebung generiert werden. Sie können Warnungen filtern und die entsprechenden Maßnahmen ergreifen.

Jedes Gehäuse in der MCM-Gruppe empfängt Fabric-Warnungen, unabhängig davon, ob die im Gehäuse vorhandenen MX5108N- oder MX9116N-IOMs neue MX5108N- oder MX9116N-IOMs aufnehmen können.

Klicken Sie zum Anzeigen der Warnungsseite auf der Menüleiste auf **Warnungen**. Die Seite **Warnungen** wird mit folgenden Registerkarten angezeigt:

- **Warnungsprotokoll**
- **Warnungsrichtlinien**
- **Alarmdefinition**

**Themen:**



# Warnungsprotokoll

Die Seite **Warnungsprotokoll** zeigt die Liste der Warnungsprotokolle für Ereignisse an, die im Gehäuse stattfinden. Klicken Sie in der Menüleiste auf **Warnungen** > **Warnungsprotokoll**. Die Seite **Warnungsprotokoll** wird angezeigt. Sie können die Warnungsdetails anzeigen, wie Schweregrad der Warnung, Zeitstempel, Quelle, Kategorie, Unterkategorie, Meldungs-ID, sowie eine Beschreibung der Warnung.

Auf der Seite **Warnungsprotokoll** werden 30.000 Datensätze angezeigt. Sie können eine Warnung auswählen, um im rechten Bereich der Seite **Warnungsprotokoll** eine Zusammenfassung der Warnung anzuzeigen. Auf der Seite **Warnungsprotokoll** können Sie auch folgende Aufgaben ausführen:

- Warnung bestätigen
- Warnungen nicht bestätigen
- Warnungen ignorieren
- Warnungen exportieren
- Warnungen löschen

Die neuesten unbestätigten Warnungen werden auf der OME – Modular-Startseite angezeigt.

Wenn in den EAMs MX9116N und MX5108N ein Uplink innerhalb von 60 Sekunden vom gleichen Port entfernt und wieder eingesetzt wird, wird die letzte Warnmeldung nicht auf der Seite **Warnungsprotokoll** angezeigt. Der Grund dafür ist, dass das Deduplizierungsintervall auf 60 Sekunden eingestellt ist, um ein erneutes Auftreten von Warnungen zu vermeiden.

## Warnungsprotokolle filtern

So filtern Sie Warnungsprotokolle:

1. Auf der OME – Modular Webschnittstelle navigieren Sie zu **Warnungen** > **Warnungsprotokolle**.
2. Klicken Sie auf **Erweiterte Filter**.
3. Wählen Sie oder aktualisieren Sie basierend auf Ihren Anforderungen die folgenden Angaben:
   - **Schweregrad** – Zur Anzeige aller Warnungen mit einem bestimmten Schweregrad.
   - **Bestätigen** – Zur Anzeige aller Warnungen, die quittiert wurden.
   - **Startdatum** und **Enddatum** – Zur Anzeige der Warnungen aus einen bestimmten Zeitraum.
   - **Quellenname** – Zur Anzeige der Warnungen von einem bestimmten System.
   - **Kategorie** und **Unterkategorie** – Zur Anzeige von Warnungen einer bestimmten Kategorie.
   - **Meldung** – Zur Anzeige von Warnungen, die ein bestimmtes Wort in der Spalte "Meldung" enthalten.

Auswahlen, die an Filtern durchgeführt werden, werden in Echtzeit angewendet.

4. Um die Filter zurückzusetzen, klicken Sie auf **Alle Filter löschen**.

# Warnungsprotokolle bestätigen

Sie können Warnungsprotokolle bestätigen, die noch nicht bestätigt sind. Das Bestätigen einer Warnung verhindert das Speichern des gleichen Ereignisses im System. Wenn ein Gerät zum Beispiel laut ist und mehrere Male das gleiche Ereignis erzeugt, können Sie weitere Aufnahmen der Warnung ignorieren, indem Sie die Ereignisse bestätigen, die vom Gerät empfangen wurden. Daraufhin werden keine weiteren Ereignisse des gleichen Typs aufgezeichnet.

So bestätigen Sie Warnungsprotokolle:

Wählen Sie auf der Seite **Warnungsprotokoll** die Warnungsprotokolle aus, die Sie bestätigen möchten, und klicken Sie auf **Bestätigen**. In der Spalte **Bestätigen** erscheint ein Häkchen für die ausgewählten Warnungsprotokolle.

# Warnungsprotokolle nicht bestätigen

Sie können die Bestätigung von Warnungsprotokollen rückgängig machen. Wenn eine Warnung nicht bestätigt ist, bedeutet dies, dass alle Ereignisse von jedem beliebigen Gerät aufgezeichnet werden, selbst wenn das gleiche Ereignis häufig auftritt. Standardmäßig sind alle Warnungen nicht bestätigt.

So machen Sie die Bestätigung von Warnungsprotokollen rückgängig:

Wählen Sie auf der Seite **Warnungsprotokoll** die Warnungsprotokolle aus, die Sie nicht bestätigen möchten, und klicken Sie auf **Nicht bestätigen**.
Das Kontrollkästchen, das in der Spalte **Bestätigen** für die ausgewählten Warnungsprotokolle angezeigt wird, wird gelöscht. Dies weist darauf hin, dass die ausgewählten Warnungsprotokolle nicht bestätigt sind.

# Warnungsprotokolle ignorieren

Sie können Warnungsprotokolle ignorieren, wenn Sie eine Warnung nicht aufzeichnen möchten. Für alle Ereignisse im Gerät, mit denen die Warnung verknüpft ist, werden keine Maßnahmen initiiert. Warnungsrichtlinien für das ausgewählte Gerät enthalten Details zu Ereignissen, die ignoriert werden müssen.

So ignorieren Sie Warnungsprotokolle:

Wählen Sie auf der Seite **Warnungsprotokoll** die Warnungsprotokolle aus, die Sie ignorieren möchten, und klicken Sie auf **Ignorieren**. Es wird eine Meldung angezeigt, die darauf hinweist, dass eine Warnungsrichtlinie erstellt wurde, um Warnungsprotokolle des ausgewählten Typs zu ignorieren. Die Ignorieren-Richtlinie wird aus dem Gerät oder mehreren Geräten erstellt, für die das Warnungsprotokoll erzeugt wird.

# Warnungsprotokolle exportieren

Sie können Warnungsprotokolle im Format `.csv` auf eine Netzwerkfreigabe oder ein lokales Laufwerk Ihres Systems exportieren.

So exportieren Sie Warnungsprotokolle:

Wählen Sie auf der Seite **Warnungsprotokolle** die Warnungsprotokolle aus, die Sie exportieren möchten, und klicken Sie auf **Exportieren** > **Auswahl exportieren**.

Sie können alle Warnungsprotokolle exportieren, indem Sie auf **Exportieren** > **Alle exportieren** klicken.

Die Warnungsprotokolle werden im Format `.csv` exportiert.

# Warnungsprotokolle löschen

Sie können ein oder mehrere Warnungsprotokolle löschen.

So löschen Sie Warnungsprotokolle:

Wählen Sie auf der Seite **Warnungsprotokoll** die Warnungsprotokolle aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
Es wird eine Meldung angezeigt, die Sie dazu auffordert, den Vorgang zu bestätigen.

# Warnungsrichtlinien

Über die Funktion Warnungsrichtlinien können Sie kritische Warnungen anzeigen und bestimmte Aufgaben ausführen. Um die Liste der Warnungsrichtlinien anzuzeigen, klicken Sie auf **Warnungen** > **Warnungsrichtlinien**. Die Details der Warnungsrichtlinien umfassen den Namen und eine Beschreibung der Warnungsregel, den Status der Warnungsregel, die E-Mail-ID des Administrators und den Syslog.

Auf der Seite **Warnungsrichtlinien** können Sie folgende Aufgaben ausführen:

- Warnungsrichtlinien erstellen
- Warnungsrichtlinien bearbeiten
- Warnungsrichtlinien aktivieren
- Warnungsrichtlinien deaktivieren
- Warnungsrichtlinien löschen

OME – Modular bietet ebenfalls vordefinierte Warnungsrichtlinien zur Überwachung des Systems, nachdem die Warnziele konfiguriert wurden.

## Erstellen von Warnungsrichtlinien

Um Fabrics oder Uplink-Warnmeldungen vom Quell-Fabric-Manager zu erhalten, wählen Sie für die konfigurierten externen Ziele **Netzwerk EAM** oder **Alle Geräte** als **Gruppen** anstelle von **Geräten**, während Sie die Warnungsrichtlinie konfigurieren.

**ANMERKUNG:** Wenn Sie mehrere Warnungsrichtlinien konfigurieren, überprüfen Sie, ob die Informationen wie E-Mail-Adresse und Zieladresse korrekt sind. Wenn falsche Werte eingetragen sind, kann es sein, dass die Warnmeldungen für die Richtlinien länger als erwartet brauchen, um das externe Ziel zu erreichen.

So erstellen Sie eine Warnungsrichtlinie:

1. Klicken Sie in der Menüleiste auf **Warnungen** > **Warnungsrichtlinien** > **Erstellen**.
   Der Assistent **Warnungsrichtlinie erstellen** wird angezeigt.
2. Geben Sie einen Namen und eine Beschreibung für die Warnungsrichtlinie ein.
3. Wählen Sie **Richtlinie aktivieren**, um die Warnmeldungsrichtlinie zu aktivieren, und klicken Sie auf **Weiter**.
   Die Registerkarte **Kategorie** wird angezeigt.
4. Wählen Sie alle Warnungskategorien aus, oder wählen Sie die erforderliche Option aus und klicken auf **Weiter**. Die verfügbaren Kategorien sind:
   - Anwendung
   - Gehäuse
   - iDRAC
   - Netzwerk-EAMs
   - Speicher-EAMs

   Sie können jede Kategorie erweitern, um Unterkategorien anzuzeigen und auszuwählen.

   Die Registerkarte **Geräte** wird angezeigt.
5. Wählen Sie die erforderlichen Geräte oder Gerätegruppen aus, und klicken Sie auf **Weiter**.
   Die Registerkarte **Datum und Uhrzeit** wird angezeigt.
6. Wählen Sie Datum, Uhrzeit und Tage aus, an denen bzw. zu der die Warnungen erstellt werden müssen, und klicken Sie auf **Weiter**.
   Die Registerkarte **Schweregrad** wird angezeigt.
7. Wählen Sie den Schweregrad aus, und klicken Sie auf **Weiter**.
   Folgende Optionen stehen zur Verfügung:
   - Alle
   - Unbekannt
   - Info
   - Normal
   - Warnung
   - Kritisch

   Die Registerkarte **Aktionen** wird angezeigt.
8. Wählen Sie die Warnungsmaßnahme aus und klicken Sie auf **Weiter**. Folgende Optionen stehen zur Verfügung:
   - **E-Mail (Aktivieren)** – Klicken Sie auf **Aktivieren**, um das Fenster **E- Mail-Konfiguration** anzuzeigen. Dort können Sie die E-Mail-Einstellungen für die Warnung konfigurieren.

- **SNMP-Trap-Weiterleitung (Aktivieren)** – Klicken Sie auf **Aktivieren**, um das Fenster **SNMP-Konfiguration** anzuzeigen. Dort können Sie die SNMP-Einstellungen für die Warnung konfigurieren.
- **Syslog (Aktivieren)** – Klicken Sie auf **Aktivieren**, um das Fenster **Syslog -Konfiguration** anzuzeigen. Dort können Sie die Syslog -Einstellungen für die Warnung konfigurieren.
- **Ignorieren**

Sie können die Attribute der Warnungsrichtlinie auf der Registerkarte **Zusammenfassung** anzeigen.

## Aktivieren von Warnungsrichtlinien

Sie können Warnungsrichtlinien aktivieren, die deaktiviert sind. Es können mehrere Warnungsrichtlinien gleichzeitig aktiviert werden.

So aktivieren Sie Warnungsrichtlinien:

Wählen Sie auf der Seite **Warnungsrichtlinien** die Warnungen aus, die Sie aktivieren möchten, und klicken Sie auf **Aktivieren**.
Eine Bestätigungsmeldung wird angezeigt.

## Bearbeiten von Warnungsrichtlinien

Sie können Warnungsrichtlinien bearbeiten.

So bearbeiten Sie Warnungsrichtlinien:

Wählen Sie auf der Seite **Warnungsrichtlinien** die Warnungen aus, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
Eine Bestätigungsmeldung wird angezeigt.

## Deaktivieren von Warnungsrichtlinien

Sie können Warnungsrichtlinien deaktivieren, die aktiviert sind. Sie können mehrere Warnungsrichtlinien gleichzeitig deaktivieren.

So deaktivieren Sie Warnungsrichtlinien:

Wählen Sie auf der Seite **Warnungsrichtlinien** die Warnungen aus, die Sie deaktivieren möchten, und klicken Sie auf **Deaktivieren**.
Eine Bestätigungsmeldung wird angezeigt.

## Löschen von Warnungsrichtlinien

Sie können Warnungsrichtlinien löschen, die aktiviert sind. Sie können mehrere Warnungsrichtlinien gleichzeitig löschen.

So löschen Sie Warnungsrichtlinien:

1. Wählen Sie auf der Seite **Warnungsrichtlinien** die Warnungen aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
   Es wird eine Meldung angezeigt, die Sie dazu auffordert, den Vorgang zu bestätigen.
2. Klicken Sie auf **Ja,** um fortzufahren.

# Warnungsdefinitionen

Sie können auf der Seite **Warnungsdefinition** eine Beschreibung der Warnungsprotokolle anzeigen, die für Ereignisse im Zusammenhang mit dem Gehäuse bzw. Geräten und Komponenten im Gehäuse generiert wurden. Die folgenden Warnungsinformationen werden angezeigt:

- Schweregrad der Warnung
- Meldungs-ID der Warnung
- Alarmmeldung
- Kategorie der Warnung
- Unterkategorie der Warnung

Sie können die Liste der Warnungen auf Basis der **Erweiterten Filter** sortieren:

- **Meldungs-ID enthält**
- **Meldung enthält**
- **Kategorie**

- **Unterkategorie**
- **Schweregrad**

Sie können auch eine Warnung auswählen, um im rechten Bereich der Seite**Warnungsdefinition** Details dazu anzuzeigen. Die Details sind: Detailliertere Beschreibung, Empfohlene Maßnahme, Informationen zur Ereignisquelle und Wichtigkeit.

## Warnungsdefinitionen filtern

So filtern Sie Warnungsdefinitionen:

1. Auf der OME – Modular Webschnittstelle navigieren Sie zu **Warnungen** > **Warnungsdefinitionen**.
2. Klicken Sie auf **Erweiterte Filter**.
3. Wählen Sie oder aktualisieren Sie basierend auf Ihren Anforderungen die folgenden Angaben:
   - **Meldung enthält** – Zur Anzeige von Warnungen, die ein bestimmtes Wort in der Spalte "Meldung" enthalten.
   - **Meldung** – Zur Anzeige von Warnungen, die ein bestimmtes numerisches oder alphanumerisches Zeichen enthalten.
   - **Kategorie** und **Unterkategorie** – Zur Anzeige von Warnungen einer bestimmten Kategorie.
   - **Schweregrad** – Zur Anzeige aller Warnungen mit einem bestimmten Schweregrad.

   Auswahlen, die an Filtern durchgeführt werden, werden in Echtzeit angewendet.
4. Um die Filter zurückzusetzen, klicken Sie auf **Alle Filter löschen**.

# 17

# Überwachungsprotokolle überwachen

Die Prüfprotokoll-Funktion in OME – Modular ermöglicht Ihnen die Überwachung von Protokolleinträgen in Bezug auf:

- Anmeldeversuche
- Appliance-Einrichtung
- Änderung der Gehäusekonfiguration über die RESTful-API
- Änderung in der Konfiguration von Warnungsfiltern

Auf der Seite **Überprüfungsprotokoll** können Sie die folgenden Aufgaben ausführen:

- Die Überwachungsprotokolle anhand von erweiterten Filtern sortieren.
- Alle Überprüfungsprotokolle im Format `.csv` auf eine Netzwerkfreigabe oder ein lokales Laufwerk Ihres Systems exportieren.

Quick Deploy-Überwachungsprotokolle werden als ein allgemeiner Vorgang aufgezeichnet, sobald sie erstellt oder aktualisiert werden. Die Details der Quick Deploy-Überwachungsprotokolle ähneln den Details jedes anderen Jobs, der im System erstellt oder aktualisiert wird.

So zeigen Sie die Seite **Überwachungsprotokoll** an:

Klicken Sie in der Menüleiste auf **Überwachen** > **Überwachungsprotokolle**.
Die Seite **Überwachungsprotokoll** wird angezeigt.

### Themen:



# Überwachungsprotokolle filtern

So filtern Sie Überwachungsprotokolle:

1. Erweitern Sie auf der Seite **Überwachungsprotokolle** die Option **Erweiterte Filter**.
2. Wählen Sie oder aktualisieren Sie basierend auf Ihren Anforderungen die folgenden Angaben:
   - **Schweregrad** – Zum Anzeigen von Überwachungsprotokollen der Schweregrade **Info**, **Warnung**, **Kritisch**, oder **Alle**.
   - **Startzeit** und **Endzeit** – Zum Anzeigen der Überwachungsprotokolle eines bestimmten Zeitraums.
   - **Benutzer**-zum Anzeigen von Prüfprotokollen für einen bestimmten Benutzer.
   - **Quelladresse** – Zum Anzeigen der Überwachungsprotokolle für ein bestimmtes System.
   - **Kategorie** – Zum Anzeigen der Überwachungsprotokolle für einen bestimmen Überwachungs- oder Konfigurationstyp.
   - **Beschreibung** – Zum Anzeigen der Überwachungsprotokolle, die ein bestimmtes Wort in der Spalte **Beschreibung** enthalten.
   - **Meldungs-ID** – Zum Anzeigen der Überwachungsprotokolle, die eine bestimmte Zahl oder ein bestimmtes Zeichen enthalten.

   An Filtern vorgenommene Änderungen werden in Echtzeit angewendet. Um die Filter zurückzusetzen, klicken Sie auf **Alle Filter löschen**.

# Überwachungsprotokolle exportieren

Sie können ausgewählte oder alle Überwachungsprotokolle im Format `.csv` auf ein lokales Laufwerk Ihres Systems oder eine Netzwerkfreigabe exportieren.

So exportieren Sie Überwachungsprotokolle:

1. Wählen Sie auf der Seite **Überwachungsprotokolle** die Überwachungsprotokolle aus, die Sie exportieren möchten.
2. Klicken Sie auf **Exportieren**, und wählen Sie **Ausgewählte exportieren** aus.
   Alternativ können Sie auf **ExportierenAlle exportieren** klicken, um alle Überwachungsprotokolle zu exportieren.

# Jobs überwachen

Sie können auf der Seite **Jobs** den Status und die Details von Jobs überwachen, die im Gehäuse und seinen Unterkomponenten initiiert wurden. Die Jobs umfassen Firmwareupdate und Aktualisierung der Bestandsaufnahme für Geräte.

Um die **Jobs** über die Menüleiste anzuzeigen, klicken Sie auf **Überwachen** > **Jobs**.

Auf der Seite **Jobs** können Sie folgende Aufgaben ausführen:

- Jobs unter Verwendung von **Erweiterter Filter** filtern
- Eine Zusammenfassung des Jobs anzeigen
- Jobs ausführen
- Jobs beenden
- Jobs aktivieren
- Jobs deaktivieren
- Jobs löschen

Der Jobstatus ist „Mit Fehlern abgeschlossen“, wenn eine oder mehreren untergeordnete Aufgaben fehlschlagen und die Anforderung und der Status auf „Warnung“ gesetzt sind. Wenn alle untergeordneten Aufgaben fehlschlagen, ist der entsprechende Status „Fehlgeschlagen“. Wenn alle Aufgaben erfolgreich abgeschlossen wurden, wird der Status als „Abgeschlossen“ angezeigt.

Ein Job zur schnellen Bereitstellung hat Vorrang vor einem Steckplatz-basierten Bereitstellungs-Job. In Konflikt stehende Einstellungen, falls vorhanden, werden auf die Einstellung für die schnelle Bereitstellung zurückgesetzt.

**ANMERKUNG:** Wenn der „Lockdown-Modus“ auf dem iDRAC aktiviert ist, wird der Jobstatus**Blink LED** für iDRAC auf der Seite OME – Modular **Jobs** als „Fehlgeschlagen“ angezeigt, obwohl der Job auf dem iDRAC erfolgreich ist.

## Jobs filtern

So filtern Sie Jobs:

1. Klicken Sie auf der Seite **Jobs** auf **Erweiterte Filter**.
2. Wählen Sie oder aktualisieren Sie basierend auf Ihren Anforderungen die folgenden Angaben:
   - **Status** – Zum Anzeigen von Jobs anhand des Status. Folgende Optionen stehen zur Verfügung:
     - Alle
     - Geplant
     - In Warteschlange
     - Wird gestartet
     - Wird ausgeführt
     - Abgeschlossen
     - Fehlgeschlagen
     - Neu
     - Mit Fehlern abgeschlossen
     - Abgebrochen
     - Angehalten
     - Angehalten
     - Annuliert
   - **Zustand** – Zum Anzeigen von Jobs anhand des Zustands. Folgende Optionen stehen zur Verfügung:
     - Alle
     - Aktiviert
     - Deaktiviert
   - **Job-Typ** – Zum Anzeigen von Jobs anhand des Typs. Folgende Optionen stehen zur Verfügung:
     - Alle
     - Backup
     - Gehäuseprofil
     - Datensynchronisation
     - Debug-Protokolle
     - Geräteaktion
     - Gerätekonfiguration
     - VLAN-Definitionen importieren

- Bestandsaufnahme
- MCM-Backup Lead zuweisen
- MCM-Gruppe
- MCM-OffBoarding
- MCM-Onboarding
- MCM-Backup Lead heraufstufen
- MCM-Backup-Lead neu zuweisen
- Synchronisationsaufgabe für MCM-Sicherheitseinstellungen
- MCM-Stilllegen-Lead
- MCM-Einstellungen propagieren
- Zuweisung für MCM-Backup-Lead aufheben
- Profil aktualisieren
- Quick Deploy
- Wiederherstellen
- Einstellungen aktualisieren
- Software-Rollback
- SyncronizeDate-Aufgabe
- Zeiteinstellungen
- Aktualisierung

**ANMERKUNG:** Die Option zur Datensynchronisation ist für das Troubleshooting vorgesehen und nur in der RESTful API-Schnittstelle verfügbar. Sie können diese Option mit Hilfe des technischen Supports verwenden.

**ANMERKUNG:** Wenn der Bestandsaufnahme-Job gestartet wird, versucht er, die Inventardetails vom Gerät abzurufen. Die für diesen Job konfigurierte maximale Dauer beträgt zwei Stunden und der Job schlägt fehl, wenn er die konfigurierte Zeit überschreitet. Der Bestandsaufnahme-Job schlägt vor der Höchstzeit nur dann fehl, wenn es andere wichtige Probleme gibt, z. B. Verbindungsprobleme mit einem Gerät oder oauth-Fehler.

- **Startdatum der letzten Ausführung** und **Enddatum der letzten Ausführung** – Zum Anzeigen von Jobs anhand des letzten Ausführungszeitraums.
- **Quelle** – Zum Anzeigen von Jobs anhand der Quelle. Folgende Optionen stehen zur Verfügung:
  - Alle
  - Nutzergeneriert
  - Systemgeneriert

Auswahlen, die an Filtern durchgeführt werden, werden in Echtzeit angewendet. Um die Filter zurückzusetzen, klicken Sie auf **Alle Filter löschen**.

Die Synchronisationsaufgabe für die MCM-Sicherheitseinstellungen wird nur in den folgenden Szenarien erstellt:

- Wenn ein neues Mitgliedsgehäuse mit OIDC-Anbieter zum Hauptgehäuse hinzugefügt wird. Die OIDC-Einstellungen werden vom Hauptgehäuse zum neuen Mitgliedsgehäuse propagiert.
- Wenn das Gehäuse während des Workflows **Gehäuse stilllegen** oder **zum Hauptgehäuse hochstufen** zum Hauptgehäuse hochgestuft wird.

**ANMERKUNG:** Die Aufgabe zum **Synchronisieren der MCM-Sicherheitseinstellungen** wird nicht im Rahmen der Propagierung der OIDC-Anbietereinstellungen von Haupt- zum Mitgliedsgehäuse erstellt.

# Details zu einem Job anzeigen

Das Fabric-Manager-On-Boarding wird initiiert, wenn ein Fabric Manager-Failover im IOM-Cluster auftritt. Wenn ein neuer Fabric Manager ermittelt wird, initiiert OME-Modular den On-Boarding-Prozess, um die Kommunikation mit dem EAM-Cluster wiederherzustellen. In bestimmten Szenarien können innerhalb einer kurzer Zeitspanne mehrere Switchover auftreten, was zu einem Fehlschlagen der bereits laufenden Aufgaben führt. Nur die letzte Aufgabe wird erfolgreich abgeschlossen. Im Folgenden sind die Szenarien aufgeführt, in denen mehrere Switchovers auftreten können:

- MM-Reset
- MM-Upgrade oder Switchover
- Entfernen der Verbindung zwischen den Gehäusen bei eingeschaltetem System
- Entfernen von MM bei eingeschaltetem System
- IOM Haupt-Update
- IOM Haupt-Reset

- Fab-D-Überlastung: Grund für die Überlastung ist das Herunterladen riesiger Dateien, die dazu führen, dass FAB-D anderen Datenverkehr abbricht.

Die Details der zugewiesenen MAC-Adressen für die jeweiligen NIC-Partitionen werden auf der Seite **Job-Details** basierend auf den Konfigurationsergebnissen von iDRAC angezeigt.

So zeigen Sie die Details eines Jobs an:

1. Wählen Sie auf der Seite **Jobs** den Job aus, dessen Details Sie anzeigen möchten.
   Eine Zusammenfassung des Jobs wird im rechten Bereich der Seite **Jobs** angezeigt.
2. Klicken Sie auf **Details anzeigen**.
   Die Seite **Jobdetails** wird angezeigt.

   Die Details, einschließlich Name, Beschreibung, Ausführungsdetails und die Details des Systems, auf dem der Job ausgeführt wurde, werden angezeigt.

   Auf der Seite **Jobdetails** können Sie die folgenden Aufgaben ausführen:

   - Den Job **neu starten**.
   - Details zu dem Job im Format `.csv` auf ein lokales Laufwerk Ihres Systems oder eine Netzwerkfreigabe **exportieren**.

   **ANMERKUNG:** Die **Neustart**-Option für den MCM-Onboarding-Task zum Hinzufügen eines Mitgliedsgehäuses ist unabhängig vom Jobstatus deaktiviert.

   Mitunter wird nach einer Firmwareaktualisierung, `racreset` oder dem Ausfall des Verwaltungsmoduls eine Meldung angezeigt, die darüber informiert, dass die Warnungen nicht abgerufen werden konnten. Die angezeigte Meldung hat keinen Einfluss auf die Funktionalität von OME – Modular.

## Exportieren von Details zur Jobausführung

Sie können die Details der Jobausführung im `.txt`-Format auf ein lokales Laufwerk Ihres Systems exportieren.

So exportieren Sie die Job-Details:

Klicken Sie auf der Seite **Job-Details** unter der Registerkarte **Ausführungsdetails** auf **Exportieren**.
Die Ausführungsdetails werden auf ein lokales Laufwerk auf Ihrem System im `.txt`-Format heruntergeladen.

Die Jobausführungsdetails sind: Start- und Enddatum des Jobs, Status, verstrichene Zeit, Zielsystem, auf dem der Job ausgeführt wird, und die Nachricht des Jobs.

**ANMERKUNG:** Laden Sie den Bericht immer im .txt-Format herunter. Das Zeitformat im Bericht zeigt GMT 24-Stunden-Format an, während die Benutzeroberfläche das 12-Stunden-Format anzeigt.

# Jobs ausführen

Wenn ein Job länger als 24 Stunden ausgeführt wird, stoppen Sie den Job nach der Analyse der Jobdetails. Führen Sie den Job bei Bedarf erneut aus.

Sie können über die Seite **Jobs** Jobs sofort ausführen.

So führen Sie Jobs aus:

Wählen Sie auf der Seite **Jobs** die Jobs aus, die Sie ausführen möchten, und klicken Sie auf **Jetzt ausführen**.
Es wird eine Meldung angezeigt, um zu bestätigen, dass die Task neu gestartet wurde.

# Jobs stoppen

Sie können zurzeit laufende Jobs stoppen.

So stoppen Sie Jobs:

Wählen Sie auf der Seite **Jobs** die laufenden Jobs aus, die Sie stoppen möchten, und klicken Sie auf **Stoppen**.
Es wird eine Meldung angezeigt, die Sie dazu auffordert, den Vorgang zu bestätigen.

# Jobs aktivieren

Sie können Jobs aktivieren, die deaktiviert sind.

So aktivieren Sie Jobs:

Wählen Sie auf der Seite **Jobs** die deaktivierten Jobs aus, die Sie aktivieren möchten, und klicken Sie auf **Aktivieren**.
Eine Bestätigungsmeldung wird angezeigt, und der Status der ausgewählten Jobs ändert sich zu "Aktiviert".

## Jobs deaktivieren

Sie können Jobs deaktivieren, die aktiviert sind.

So deaktivieren Sie Jobs:

Wählen Sie auf der Seite **Jobs** die aktivierten Jobs aus, die Sie deaktivieren möchten, und klicken Sie auf **Deaktivieren**.
Eine Bestätigungsmeldung wird angezeigt und der Status der ausgewählten Jobs ändert sich zu "Deaktiviert".

## Jobs löschen

So löschen Sie Jobs:

Wählen Sie auf der Seite **Jobs** die Jobs aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
Es wird eine Meldung angezeigt, die Sie dazu auffordert, den Vorgang zu bestätigen.

# 18

# Anwendungsszenarien

Anwendungsfall-Szenarien für die Funktion "Backup-Lead Gehäuse" werden in diesem Kapitel beschrieben.

**Themen:**



# Zuweisen von Backups zum MCM-Lead

Die Funktion "Backup-Lead-Gehäuse" ermöglicht die Verwaltung von Systemen in der Gehäusegruppe, wenn das vorhandene Lead-Gehäuse ausfällt. Das Managen einer Gehäusegruppe umfasst die folgenden Aufgaben:

- Zuweisen – ermöglicht die Zuweisung eines Mitglieds der Gehäusegruppe als Backup zum vorhandenen Lead-Gehäuse.
- Aufheben der Zuweisung – ermöglicht die Auswahl eines anderen Gehäuses in der Gruppe, um das vorhandene Backup-Gehäuse zu ersetzen.
- Hochstufen – ermöglicht es dem Backup-Gehäuse, als Lead-Gehäuse zu übernehmen, wenn das vorhandene Lead-Gehäuse ausfällt.
- Stilllegen – ermöglicht die Übernahme des Backups als Lead-Gehäuse, wenn das vorhandene Lead-Gehäuse stillgelegt werden muss.

Weitere Informationen finden Sie unter Gehäusegruppen.

## Lebenszyklus des Backups

Der Lebenszyklus der Backup-Funktion umfasst die folgenden Phasen:

1. Phase 1: Erstellen einer Gehäusegruppe mit Backup-Lead
2. Phase 2: Überwachen des Funktionszustands von Lead und Backup
3. Phase 3: Ersetzen des primären Lead-Gehäuses mit einem Backup-Lead oder Stilllegen des Lead-Gehäuses.

# Erstellen einer Gehäusegruppe mit Backup-Lead

Führen Sie die folgenden Schritte aus, um eine Gehäusegruppe zu erstellen und dem Lead-Gehäuse ein Backup zuzuweisen:

1. Stapeln Sie das Gehäuse im Gestell.
2. Verbinden Sie mehrere Gehäuse im Gestell. Weitere Informationen finden Sie unter Verkabelung des Gehäuses und Voraussetzungen für die Erstellung einer verteilten Gruppe.
3. Erstellen Sie eine Gehäusegruppe und fügen Sie Mitglieder zur Gruppe hinzu. Weitere Informationen finden Sie unter Gehäusegruppen.

   Die Konfiguration einer virtuellen IP-Adresse ist optional. Die virtuelle IP-Adresse ermöglicht eine sekundäre IP-Adresse auf dem Lead, der mit dem Lead verbleibt. Wenn das Backup als neuer Lead übernimmt, wird die sekundäre IP automatisch auf den neuen Lead verschoben.
4. Konfigurieren Sie die Gruppe aus dem Lead-Gehäuse.

   Wenn auf dem Mitgliedsgehäuse Einstellungen und Konfigurationen vorhanden sind, die mit dem Lead in Konflikt geraten könnten, deaktivieren Sie diese Konfigurationen, bevor der Lead seine Konfiguration auf die Gruppe übertragen hat. Gehen Sie bei Bedarf wie folgt vor:
   a. Gehäuseeinstellungen konfigurieren.
   b. Die Firmware aktualisieren
   c. Konfigurieren der Firmware-Baselines.
   d. Warnungsrichtlinien konfigurieren.
   e. Konfigurieren Sie Vorlagen- und Identitäts-Pools und stellen Sie sie für Geräte oder Steckplätze bereit.
   f. Konfigurieren Sie andere Einstellungen.
5. Weisen Sie ein Mitglied der Gehäusegruppe als Backup-Lead zu.

Die Erstkonfiguration der Datensynchronisation vom Lead-Gehäuse zum Backup-Gehäuse wird fortgesetzt, auch wenn der Assign-Job abgeschlossen ist. Das Lead- und das Backup-Gehäuse melden die Integrität des Backup-Gehäuses.

Zunächst wird der Status der Backup-Integrität als "kritisch" angezeigt, während die Konfigurationsdaten synchronisiert werden, und wechselt dann auf "OK". Warten Sie, bis die Backup-Integrität auf "OK" wechselt, bevor Sie fortfahren. Wenn die Backup-Integrität auch nach Ablauf von 30 Minuten nach Zuweisung der Aufgabe weiterhin "kritisch" oder "Warnung" angezeigt, ist dies ein Hinweis darauf, dass persistenten Kommunikationsproblemen bestehen. Heben Sie die Zuweisung des Backups auf und wiederholen Sie Schritt 5, um ein anderes Mitglied als neues Backup auszuwählen. Außerdem empfiehlt Dell EMC, dass Sie eine Warnungsrichtlinie auf Lead erstellen, um Benachrichtigungsmaßnahmen per E-Mail, SNMP Trap, Systemprotokoll, für Backup-Integritätswarnungen zu ergreifen. Backup-Integritätswarnungen sind Teil der Gehäusekonfiguration und der Kategorie Systemintegrität.

6. Konfigurieren Sie das Mitgliedsgehäuse, das als Backup festgelegt ist.

   Es ist zwingend erforderlich, dass das Backup-Gehäuse über eine eigene Verwaltungsnetzwerk-IP verfügt. Die IP-Adresse ermöglicht dem Backup die Weiterleitung von Warnmeldungen zur Integrität des Backup.

   Erstellen Sie eine Warnungsrichtlinie für das Backup, um Benachrichtigungsmaßnahmen (E-Mail, SNMP Trap, Systemprotokoll) für Backup-Integritätswarnungen zu ergreifen. Warnmeldungen zur Integrität des Backups sind Teil der Kategorie Gehäuse (Konfiguration, System Zustand). Das Backup-Gehäuse löst Warnmeldungen oder kritische Warnmeldungen aus, wenn es feststellt, dass der Status der Backupsynchronisierung aufgrund von Kommunikation oder anderen nicht rückgängig machbaren Fehlern schlecht ist.

# Überwachen der MCM-Gruppe

1. Schließen Sie alle Konfigurationsaufgaben ab, bevor Sie den Backup-Lead zuweisen. Wenn Sie jedoch die Konfiguration nach dem Zuweisen des Backups ändern müssen, werden die Änderungen automatisch in das Backup kopiert. Der Prozess des Kopierens der Änderungen am Backup kann je nach Konfigurationsänderung bis zu 90 Minuten in Anspruch nehmen.
2. Der Backup-Synchronisierungsstatus des Lead- und des Backup-Lead-Gehäuses sind an den folgenden Orten der GUI verfügbar:
   a. Auf dem Lead-Gehäuse.
      - **Start** Seite –**Backup-Sync** Status unter dem Mitglied (Backup)
      - Seite Lead **Übersicht**: Redundanz- und Backup-Synchronisierungsstatus unter **Gruppeninformationen**

   b. Auf dem Backup-Gehäuse:
      - **Startseite** > **Übersicht** Seite:**Backup Sync** Status unter den **Gruppeninformationen**.
3. Interpretieren der Backup-Integrität:
   - Wenn die Backup-Synchronisierung funktionsfähig ist, wird der Status als "OK" angezeigt und es sind keine weiteren Aktionen erforderlich.
   - Wenn die Backup-Synchronisierung nicht funktionsfähig ist, wird der Status "Warnung" oder "Kritisch" angezeigt. Die "Warnung" weist auf ein Problem mit der momentanen Synchronisierung hin, das automatisch gelöst wird. Der Status "Kritisch" zeigt ein permanentes Problem an und erfordert eine Benutzeraktion.
   - Wenn sich der Backup-Synchronisierungsstatus in "Warnung" oder "Kritisch" ändert, werden die zugehörigen Warnmeldungen unter Warnungskategorien des Gehäuses (Konfiguration, Systemintegrität) automatisch erzeugt. Diese Warnmeldungen werden unter **Home** > **Hardwareprotokolle** und **Warnungen** > **Warnungsprotokoll** protokolliert. Die Warnmeldungen werden auch im MM-Subsystem als Fehler unter **Home** > **Gehäuse-Subsysteme** (obere rechte Ecke) angezeigt. Wenn eine Warnungsrichtlinie konfiguriert ist, werden die Aktionen gemäß der Konfiguration in der Richtlinie durchgeführt.
4. Erforderliche Benutzermaßnahmen, wenn die Backup-Integrität "Warnung" oder "Kritisch" ist:
   - Warnung – ein vorübergehender Status, der auf "OK" oder "Kritisch" übergehen muss. Wenn der Status weiterhin "Warnung" für mehr als 90 Minuten meldet, empfiehlt Dell EMC, dass Sie ein neues Backup zuweisen.
   - Kritisch – ein permanenter Status, der auf Probleme mit dem Backup oder dem Lead hinweist. Ermitteln Sie die zugrunde liegenden Probleme und führen Sie die nachfolgend beschriebenen Schritte aus:
     - Der Integritätsstatus ist aufgrund der Warnung CDEV4006 kritisch: das Lead-oder Mitgliedsgehäuse hat seine Firmwareversion geändert, was zu einer Lead-/Backup-Inkompatibilität geführt hat. Es wird empfohlen, dass die Firmware des Lead- oder Mitgliedsgehäuses wieder auf dieselbe Version (1.10.00 oder höher) gebracht wird.
     - Der Funktionszustand ist aufgrund der Warnung CDEV4007 kritisch: eines der verschiedenen zugrunde liegenden Probleme trägt zu diesem Status bei. Weitere Informationen zu diesem Status finden Sie im folgenden Flussdiagramm, um die Ursache zu ermitteln und die empfohlene Maßnahme zu ergreifen.

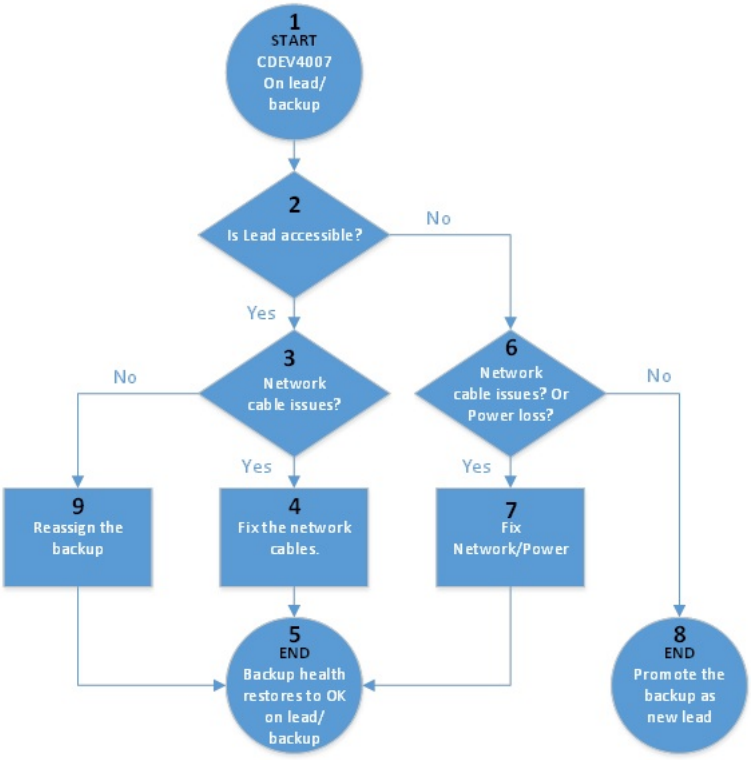



**Abbildung 2. Netzwerk-und Stromausfall – Flussdiagramm**

Die Warnmeldung CDEV4007 steht im Zusammenhang mit Netzwerk-oder Stromproblemen, die wie folgt klassifiziert werden können:

- **Intermittierende/wiederherstellbare Probleme:** Momentane Stromversorgungs- oder Netzwerkausfälle. Der Administrator kann diese Arten von Fehlern identifizieren und Wiederherstellungsmaßnahmen lokal oder remote durchführen. Sie können den Backup-Lead nicht hochstufen. Erlauben Sie dem Lead-Gehäuse, die Verbindung automatisch wiederherzustellen, oder der Administrator repariert die Stromversorgungs- oder Netzwerkprobleme.
- **Partieller Fehler:** Beide Managementmodule sind ausgefallen oder weisen Fehler auf. Aber die übrigen Gehäusekomponenten funktionieren. Stufen Sie den Backup-Lead zum Lead-Gehäuse hoch, um die Gruppenmanagementfunktion über den neuen Lead wiederzuerlangen. Weitere Informationen über das Hochstufen des Backups und die Wiederherstellung des fehlgeschlagenen Lead-Gehäuses im Produktionsstatus finden Sie im Abschnitt Disaster Recovery von Lead-Gehäusen.
- **Vollständiger Fehler:** Katastrophale Ausfälle. Alle Gehäusekomponenten, einschließlich der Managementmodule, sind fehlerhaft oder reagieren nicht mehr. Stufen Sie den Backup-Lead zum Lead-Gehäuse hoch, um die Gruppenmanagementfunktion über den neuen Lead wiederzuerlangen. Informationen zum Hochstufen des Backup-Leads und zum Löschen von Referenzen auf das fehlgeschlagene Lead-Gehäuse finden Sie im Abschnitt Disaster Recovery von Lead-Gehäusen.

# Szenarien, in denen der Backup-Lead als Lead-Gehäuse übernehmen kann

Dieser Abschnitt beschreibt die Situationen, in denen ein Backup-Lead als Lead-Gehäuse der Gehäusegruppe übernehmen kann.

## Disaster Recovery des Lead-Gehäuses

Katastrophale Ausfälle wie Stromausfall, Netzwerkverlust und Ausfall beider MMS können dazu führen, dass das Lead-Gehäuse nicht zugänglich oder nicht verfügbar ist. In solchen Fällen können Sie das Backup zur Übernahme des fehlgeschlagenen Lead-Gehäuses auf die kontinuierliche Verwaltung von Systemen hochstufen.

**ANMERKUNG:** Das Hochstufen des Backup-Leads zum neuen Lead stellt die Gruppenmanagement-Funktion für die Mitgliedsgehäuse wieder her, die nicht von Ausfällen betroffen sind. Es gibt jedoch Einschränkungen hinsichtlich des Umfangs der Funktionen, die auf dem fehlerhaften Lead-Gehäuse wiederhergestellt werden können. Die Wiederherstellung basiert auf dem Schweregrad der Ausfälle im fehlerhaften Lead-Gehäuse.

Beachten Sie Folgendes, wenn Sie das Lead-Gehäuse wiederherstellen:

1. Vor der Ausführung der Aufgabe „Hochstufen“ auf dem Backup-Lead-Gehäuse:
   a. Die Aufgabe „Hochstufen“ ist ein unterbrechungsfreier Vorgang und darf nur ausgeführt werden, wenn es keine Möglichkeit zur Wiederherstellung des nicht zugänglichen Lead-Gehäuses gibt. Bei partiellen Ausfällen des Lead-Gehäuses – z. b. wenn nur die Managementmodule nicht reagieren, die Rechner jedoch funktionieren – werden durch Ausführen der Hochstufung die Workloads unterbrochen, die noch auf den Rechnern des Lead-Gehäuses ausgeführt werden. Weitere Informationen über die Verlagerung der Arbeitskomponenten, Rechner- und Netzwerkswitches vom fehlgeschlagenen Lead, finden Sie im Listenelement 3. c, „Schritte, die erforderlich sind, um den fehlgeschlagenen Lead wiederherzustellen, bevor Sie ihn in die Produktion versetzen.“
   b. Nachdem Sie festgestellt haben, dass das Lead-Gehäuse ausgefallen und nicht mehr zugänglich ist, müssen Sie die Stromversorgung zum Lead-Gehäuse per Remote-Zugriff ausschalten oder das Gehäuse physisch aus dem Stapel entfernen, bevor Sie die Aufgabe „hochstufen“ auf dem Backup ausführen. Wenn das Lead-Gehäuse vor der Hochstufung nicht ausgeschaltet oder aus dem Stapel entfernt wurde, kann das fehlgeschlagene oder teilweise fehlgeschlagene Lead-Gehäuse nach der Hochstufung des Backups wiederhergestellt werden und mehrere Leads verursachen. Mehrere Leads können Verwechslungen und Störungen bei der Verwaltung der Gruppe verursachen.
2. Ausführen der Aufgabe „Hochstufen“ auf dem Backup-Lead-Gehäuse:
   a. Wenn das Lead-Gehäuse aktiv ist, sperrt die Webschnittstelle des Backup-Gehäuses die Aufgabe „Hochstufen“. Stellen Sie sicher, dass der Lead ausgefallen ist und nicht mehr zugänglich ist, bevor Sie die Aufgabe „Hochstufen“ für das Backup initiieren. Das Backup kann fälschlicherweise die „Hochstufung“ blockieren, wenn der Lead über das private Netzwerk zugänglich ist, aber möglicherweise im öffentlichen Nutzerverwaltungsnetzwerk nicht erreichbar ist. In solchen Fällen kann die OME-Modular RESTful API verwendet werden, um das Hochstufen zwangsweise auszuführen. Weitere Informationen finden Sie im RESTful API-Handbuch.
   b. Ein Job wird erstellt, nachdem der Vorgang „Hochstufen“ gestartet wurde. Der Job kann 10 bis 45 Minuten dauern, basierend auf der Anzahl der Gehäuse in der Gruppe und der Menge der wiederherzustellenden Konfiguration.
   c. Wenn das Lead-Gehäuse für die Weiterleitung von Warnmeldungen an externe Ziele (E-Mail, Trap, Systemprotokoll) konfiguriert ist, sind alle Warnmeldungen, die Komponenten in der Gruppe erzeugen, während der Lead ausgefallen ist, nur lokal in ihren jeweiligen Hardware-oder Warnungsprotokollen verfügbar. Während des Lead-Ausfalls können die Leads nicht an konfigurierte externe Ziele weitergeleitet werden. Der Ausfall ist der Zeitraum zwischen dem Ausfall des Leads und der erfolgreichen Hochstufung des Backups.
3. Erwartetes Verhalten nach der Aufgabe „Hochstufen“:
   a. Das Backup-Gehäuse wird zum Lead und alle Mitgliedsgehäuse sind wie auf dem früheren Lead-Gehäuse zugänglich. Nach der „Hochstufung“ bestehen Verweise auf das alte Lead-Gehäuse als Mitglied der gleichen Gruppe. Die Referenzen werden erstellt, um eine Unterbrechung der Arbeitsrechner im alten Lead in einer MM-Fehlersituation im Lead-Gehäuse zu vermeiden.

      Die Aufgabe „Hochstufen“ erkennt alle Mitglieder der Gruppe erneut und wenn ein Mitgliedsgehäuse nicht mehr zugänglich ist, wird das Gehäuse weiterhin auf der Lead-Startseite mit einer unterbrochenen Verbindung und den verfügbaren Reparaturoptionen aufgelistet. Sie können die Option „Reparieren“ verwenden, um das Mitgliedsgehäuse erneut hinzuzufügen oder das Gehäuse aus der Gruppe zu entfernen.

   b. Alle Firmware-Baselines oder -Kataloge, Warnungsrichtlinien, Vorlagen, Identitäts-Pools und Fabrics-Einstellungen werden so wiederhergestellt, wie sie auf dem fehlerhaften Lead-Gehäuse waren. Im Folgenden werden jedoch einige Ausnahmen und Einschränkungen aufgeführt:
      i. Alle letzten Konfigurationsänderungen auf dem fehlgeschlagenen Lead in einem Fenster von 90 Minuten, die für das Kopieren in das Backup erforderlich sind, werden möglicherweise nicht vollständig in das Backup kopiert und nach der Aufgabe „Hochstufen“ nicht vollständig wiederhergestellt.
      ii. Die in Bearbeitung befindlichen und teilweise kopierten Jobs, die Vorlagen/Identitäts-Pools zugeordnet sind, werden weiterhin ausgeführt. Sie können einen der folgenden Aufgaben durchführen:
         i. Beenden Sie den ausgeführten Job.
         ii. Fordern Sie alle Identitäts-Poolzuweisungen zurück.
         iii. Starten Sie den Job neu, um die Vorlage erneut bereitzustellen.
      iii. Jede Vorlage, die mit einem belegten Steckplatz durch die Führung verbunden ist, bevor das Backup als neuer Lead übertragen wird, wird beim Entfernen oder Wiedereinsetzen nicht auf dem vorhandenen Schlitten bereitgestellt. Damit die Bereitstellung funktioniert, muss der Administrator die Vorlage aus dem Steckplatz herausnehmen, die Vorlage wieder mit dem Steckplatz verbinden und den vorhandenen Schlitten entfernen oder wieder einsetzen. Oder Sie legen einen neuen Schlitten ein.
      iv. Alle Firmware-Kataloge, die mit dem automatischen Aktualisierungskatalog nach einem Zeitplan erstellt werden, werden als manuelle Aktualisierungen wiederhergestellt. Bearbeiten Sie den Katalog und stellen Sie die automatische Aktualisierungsmethode mit Aktualisierungshäufigkeit bereit.
      v. Warnungsrichtlinien mit veralteten oder ohne Verweise auf Geräte auf dem alten Lead werden nicht auf dem neuen Lead wiederhergestellt.
   c. Schritte, die erforderlich sind, um den fehlgeschlagenen Lead wiederherzustellen, bevor Sie ihn in die Produktion versetzen:
      i. Schalten Sie das Gehäuse auf dem neuen Lead ferngesteuert aus, bevor Sie die Aufgabe „Hochstufen“ für das Backup durchführen. Wenn das Gehäuse nicht ausgeschaltet ist, kann der teilweise fehlgeschlagene Lead online geschaltet werden und mehrere Leads verursachen. Es gibt nur eingeschränkte Unterstützung bei der automatischen Erkennung und Recovery

dieser Situation. Wenn der frühere Lead online ist und eine automatische Wiederherstellung möglich ist, wird der frühere Lead gezwungen, der Gruppe als Mitglied beizutreten.

ii. Entfernen Sie auf dem neuen Lead das frühere Lead-Gehäuse aus der Gruppe, um die Referenzen zu entfernen.

iii. Verschaffen Sie sich auf dem alten Lead physischen Zugang zum Lead-Gehäuse mit dem Fehler und heben Sie die Stapelung auf. Wenn Vorlagen mit Identitäts-Poolzuweisungen vorhanden sind, die für alle Rechner auf dem alten Lead bereitgestellt werden, fordern Sie die Identitäts-Poolzuweisungen der Rechner wieder zurück. Das Zurückfordern der Identitäts-Poolzuweisungen ist erforderlich, um eine Netzwerkidentitätskollision zu verhindern, wenn das alte Gehäuse wieder in die Produktion versetzt wird.

iv. Löschen Sie keine Fabrics des alten Lead-Gehäuses, da das Löschen der Fabrics zu Netzwerkverlust führen kann, sobald der alte Lead wieder zum Netzwerk hinzugefügt wird.

v. Führen Sie auf dem alten Lead die Option „Konfiguration zurücksetzen“ mithilfe der folgenden Rest API-Payload aus:

**URI:** `/api/ApplicationService/Actions/ApplicationService.ResetApplication`

**Method:** `POST`

**Payload:**
```
{"ResetType": "RESET_ALL", "ForceReset": true}
```

d. Verlagern Sie die funktionsfähigen Komponenten des alten Leads zu anderen Gehäusen in der Gruppe:

i. Verlagern Sie die Netzwerkswitches vom alten Lead in das neue Lead- oder Mitgliedsgehäuse der Gruppe, um die Integrität der Fabrics wiederherzustellen.

ii. Verlagern Sie Rechner vom alten Lead auf das neue Lead- oder Mitgliedsgehäuse in der Gruppe. Neue Vorlagen oder Identitäten müssen auf den Rechnern bereitgestellt werden, bevor Workloads wieder aufgenommen werden, die auf dem alten Lead-Gehäuse ausgeführt wurden.

## Lead-Gehäuse stilllegen

Mit der Option „Stilllegen“ kann ein Backup-Gehäuse als Leiter einer Gehäusegruppe übernommen werden, wenn das Lead-Gehäuse über einen längeren Zeitraum ausgeführt wird und vorübergehend oder dauerhaft aus der Produktionsumgebung entfernt werden muss. Das Lead-Gehäuse kann von der Gruppe ordnungsgemäß abgetrennt werden. Die Option „Stilllegen“ erleichtert es, den Lead stillzulegen, aber dennoch ein Mitglied der Gruppe zu bleiben.

1. Führen Sie die Aufgabe „Stilllegen“ vom Lead-Gehäuse aus:
   a. Ein Job wird erstellt, wenn die Aufgabe „Stilllegen“ gestartet wird. Der Job kann 10-45 Minuten dauern, basierend auf der Anzahl der Gehäuse in der Gruppe und der Menge der wiederherzustellenden Konfiguration.
   b. Wenn das Lead-Gehäuse für die Weiterleitung von Warnmeldungen an externe Ziele (E-Mail, Trap, Systemprotokoll) konfiguriert ist, sind alle Warnmeldungen, die die Komponenten in der Gruppe erzeugen, nur lokal auf ihrer jeweiligen Hardware verfügbar. Außerdem wird eine Warnmeldung protokolliert, wenn die Aufgaben zum Stilllegen des Lead-Gehäuses und Aktivieren das Backup-Gehäuses durchgeführt werden. Nach Abschluss der Aufgabe „Stilllegen“ und vor der Hochstufung des Backups erfolgt ein Ausfall im Gruppenmanagement. Der Ausfall umfasst die Weiterleitung von Warnmeldungen an konfigurierte externe Ziele.
2. Erwartetes Verhalten des Backups nach Abschluss der Aufgabe „Stilllegen“:
   a. Das Backup-Gehäuse wird zum neuen Lead und alle Mitgliedsgehäuse sind wie auf dem stillgelegten Lead-Gehäuse zugänglich. Das neue Lead-Gehäuse erkennt alle Mitglieder der Gruppe erneut und wenn ein Mitgliedsgehäuse nicht zugänglich ist, werden die Mitglieder weiterhin auf der **Startseite** des Lead-Gehäuses mit getrennter Verbindung und verfügbaren Reparaturoptionen aufgelistet. Verwenden Sie die Option „Reparieren“ zum erneuten Hinzufügen oder Entfernen des Mitgliedsgehäuses aus der Gruppe.
   b. Alle Firmware-Baselines oder Kataloge, Warnungsrichtlinien, Vorlagen, Identitäts-Pools und Fabrics-Einstellungen werden wiederhergestellt, wie sie sich auf dem stillgelegten Lead-Gehäuse befanden.
3. Erwartetes Verhalten von alten Lead-Gehäusen nach Abschluss der Aufgabe „Stilllegen“:
   a. Wenn der alte Lead als eigenständiges Gehäuse ausgewählt wurde, wird die Konfiguration der Vorlagen/Identitäts-Pools weiterhin übertragen. Führen Sie die folgenden Schritte aus, um die Konfiguration zu löschen, um Konflikte mit dem neuen Lead zu vermeiden.
      i. Stapeln Sie den früheren Lead aus der Gruppe.
      ii. Fordern Sie alle Identitäts-Pool-IO-Identitäten zurück, die für die Rechner auf dem alten Lead bereitgestellt werden.
      iii. Löschen Sie keine Fabrics des alten Lead-Gehäuses, da das Löschen der Fabrics zu Netzwerkverlust führen kann, sobald der alte Lead wieder zum Netzwerk hinzugefügt wird.
      iv. Erzwingen Sie einen „Reset der Konfiguration“ mithilfe der folgenden REST API-Payload:

**URI:** `/api/ApplicationService/Actions/ApplicationService.ResetApplication`

**Method:** `POST`

**Payload:**
```
{"ResetType": "RESET_ALL", "ForceReset": true}
```

b. Wenn der alte Lead als Mitglied der aktuellen Gruppe stillgelegt wird, trägt er nicht mehr die Identitäts-Poolkonfiguration. Er enthält jedoch die Konfiguration der Vorlagen und Profile. Er enthält jedoch die Konfiguration der Vorlagen und Profile. Um Konflikte mit dem neuen Lead zu vermeiden, sollten diese Konfigurationen nicht geändert oder gelöscht werden, bis dieses Gehäuse die MCM-Gruppe verlässt.

# 19

# Fehlerbehebung

Dieser Abschnitt beschreibt die Aufgaben für die Fehlerbehebung und Behebung von Problemen mit der OME – Modular-Benutzeroberfläche.

- Firmwareupdate schlägt fehl
- Speicherzuweisung schlägt fehl
- Verwaltungs-Rolle der EAMs ist zurückgestuft
- EAM-Funktionszustand ist zurückgestuft
- Laufwerke am Rechnerschlitten sind nicht sichtbar
- Speicherschlitten können nicht auf E/A-Module übernommen werden
- Laufwerke in OpenManage sind nicht sichtbar
- iDRAC-Laufwerksinformationen stimmen nicht mit den OpenManage-Laufwerksinformationen überein
- Der Zuweisungsmodus des Speicherschlittens ist unbekannt

**ANMERKUNG:** Weitere Informationen zum Troubleshooting finden Sie im *Dell EMC PowerEdge MX SmartFabric-Konfigurations- und Troubleshooting-Handbuch* unter /infohub.delltechnologies.com.

**Themen:**



# Speicher

Dieser Abschnitt beschreibt die Probleme im Zusammenhang mit Speicherschlitten und Schritte, um die Probleme zu beheben.

## Firmwareaktualisierung schlägt fehl

1. Die Firmwareaktualisierung kann fehlschlagen, wenn eine oder mehrere Unterkomponenten während der Firmwareaktualisierung nicht in den Flash-Speicher ausgelagert werden können.
2. Wenn ein EAM aufgrund einer Nichtübereinstimmung des Gehäuses oder defekter Unterkomponenten heruntergestuft ist, schlägt die Firmware Aktivierung fehl.

## Speicherzuweisung schlägt fehl

Eine Speicherzuweisung schlägt in den folgenden Fällen fehl:

1. Diese EAMs sind derzeit zurückgestuft.
2. Es ist nur ein EAM vorhanden.
3. Es ist nur ein hot-swap-fähiger Expander in einem Speicherschlitten vorhanden.

## SAS IOM-Status ist zurückgestuft

Beide SAS IOMs sind zurückgestuft, wenn ein:

1. Peer-SAS IOM erkannt wird, aber keine Kommunikation mit ihm möglich ist.
2. Nicht übereinstimmende Firmware ermittelt wird.
3. Gehäuse-Nichtübereinstimmung festgestellt wird.

## SAS-IOM-Funktionszustand ist zurückgestuft

Der SAS-IOM-Funktionszustand wird in den folgenden Fällen zurückgestuft:

1. Eine oder mehrere Unterkomponenten sind defekt.
2. Ein nicht-SAS-EAM wird erkannt.
3. In der Firmware der Subkomponente wird eine Inkonsistenz erkannt.

## Laufwerke am Rechnerschlitten sind nicht sichtbar

1. Wenn der Rechnerschlitten mit einem PERC-Controller konfiguriert ist und die Laufwerke neu eingesetzt oder verschoben wurden, werden diese als "Fremd" neu ermittelt.
2. Wenn die Laufwerke aus dem Speicherschlitten entfernt wurden, können sie nicht ermittelt werden.
3. Wenn ein Speicherschlitten ersetzt wird, kann die Speicherkonfiguration des früheren Schlitten nicht auf den ersetzten Schlitten angewendet werden.

## Speicherkonfiguration kann nicht auf SAS IOMs übertragen werden

1. Wenn ein Speicherschlitten ersetzt wird, kann die Speicherkonfiguration des früheren Schlitten nicht auf den ersetzten Schlitten angewendet werden.
2. Wenn beim Start des SAS IOM eine nicht übereinstimmende Firmware erkannt wird, wird die Speicherkonfiguration nicht angewendet.
3. Wenn beim Start des SAS IOM eine Gehäuse-Nichtübereinstimmung erkannt wird, wird die Speicherkonfiguration nicht angewendet.
4. Wenn keine Kommunikation mit dem Speicherschlitten möglich ist oder ein Expander-Fehler vorliegt, kann das SAS IOM die jeweilige Speicherkonfiguration nicht anwenden.

## Laufwerke in OpenManage sind nicht sichtbar

1. Beim Speicherschlitten ist möglicherweise ein Expander-Ausfall aufgetreten, der verhindert, dass die Laufwerke inventarisiert werden.
2. Um die Laufwerke anzuzeigen, aktualisieren Sie die Bestandsaufnahme für den Speicherschlitten.

## iDRAC- und OpenManage-Laufwerksinformationen stimmen nicht überein

Die Laufwerksinformationen von iDRAC und OpenManage stimmen aufgrund der Mechanismen, die iDRAC und das SAS-EAM zum Abrufen und Erkennen der Speicherdetails für Speicherschlitten verwenden, möglicherweise nicht überein.

## Der Zuweisungsmodus des Speicherschlittens ist unbekannt

1. Wenn die EAM-Verwaltungsrolle derzeit zurückgestuft ist, kann der Speicherschlitten-Zuweisungsmodus derzeit nicht gelesen werden.
2. Möglicherweise müssen Sie die Seite **Speicherschlitten**-Bestandsaufnahme aktualisieren.
3. Wenn der Zustand des Speicherschlittens nicht optimal ist, kann der Zuweisungsmodus zurückgestuft werden.

# Kein Zugriff auf OME-Modular mit Chassis Direct

Auf Systemen, auf denen Linux Betriebssysteme ausgeführt werden, können Sie möglicherweise nicht mit dem Webbrowser auf `ome-m.local` zugreifen. Dies kann auf eine fehlende IP-Adresse auf der USB-Netzwerkverbindung auf dem System zurückzuführen sein. Um dieses Problem zu beheben, führen Sie einen der folgenden Schritte aus, während das USB-Kabel an das System und das Gehäuse angeschlossen ist.

- Navigieren Sie auf dem System zu **Einstellungen** > **Netzwerk** und aktivieren Sie **USB Ethernet**.
- Auf der rechten obere Ecke des Bildschirms klicken Sie auf **Verbinden**.

# Fehlerbehebung bei Lead-Gehäusefehlern

Wenn sich ein Lead-Gehäuse nach einem Ausfall in der Phase "Online" befindet, muss der Übergang automatisch erkannt werden. Wenn Sie das Backup-Lead-Gehäuse als neues Lead-Gehäuse hochgestuft haben, stellen Sie sicher, dass das frühere Lead-Gehäuse ordnungsgemäß wechselt, bevor Sie es wieder in die Produktionsumgebung setzen.

Bevor Sie das frühere Lead-Gehäuse wieder in die Produktion versetzen, führen Sie die folgenden Schritte aus:

1. Trennen Sie das Stacking-Kabel.
2. Führen Sie die RESTful API aus, um das Zurücksetzen auf die Standardeinstellung zu erzwingen.
   Das Lead-Gehäuse wird zu einem eigenständigen Gehäuse.
3. Verbinden Sie das Stacking-Kabel und fügen Sie das eigenständige Mitglied derselben oder einer anderen Gehäusegruppe hinzu.

A

# Empfohlene Steckplatzkonfigurationen für EAMs

Die untenstehende Tabelle enthält die empfohlene EAM-Steckplatzkonfigurationen.

**Tabelle 25. Empfohlene EAM-Steckplatz-Matrix**

| Steckplatz A1 | Steckplatz A2 | Steckplatz B1 | Steckplatz B2 |
|---|---|---|---|
| MX9116n | MX9116n | Leer | Leer |
| MX5108n | MX5108n | Leer | Leer |
| MX7116n | MX7116n | Leer | Leer |
| 25G PTM | 25G PTM | Leer | Leer |
| 10GBT PTM | 10GBT PTM | Leer | Leer |
| MX9116n | MX9116n | MX9116n | MX9116n |
| MX5108n | MX5108n | MX5108n | MX5108n |
| MX7116n | MX7116n | MX7116n | MX7116n |
| MX9116n | MX7116n | Leer | Leer |
| MX7116n | MX9116n | Leer | Leer |
| MX9116n | MX7116n | MX9116n | MX7116n |
| MX7116n | MX9116n | MX7116n | MX9116n |
| 25G PTM | 25G PTM | 25G PTM | 25G PTM |
| 10GBT PTM | 10GBT PTM | 10GBT PTM | 10GBT PTM |

**Themen:**



# Unterstützte Steckplatzkonfigurationen für EAMs

Die untenstehende Tabelle enthält die unterstützten EAM-Steckplatzkonfigurationen.

**Tabelle 26. Unterstützte EAM-Steckplatz-Matrix**

| Steckplatz A1 | Steckplatz A2 | Steckplatz B1 | Steckplatz B2 |
|---|---|---|---|
| MX9116n | Leer | Leer | Leer |
| MX5108n | Leer | Leer | Leer |
| MX7116n | Leer | Leer | Leer |
| 25G PTM | Leer | Leer | Leer |
| 10GBT PTM | Leer | Leer | Leer |
| MX9116n | Leer | MX9116n | Leer |
| MX5108n | Leer | MX5108n | Leer |

### Tabelle 26. Unterstützte EAM-Steckplatz-Matrix (fortgesetzt)

| Steckplatz A1 | Steckplatz A2 | Steckplatz B1 | Steckplatz B2 |
|---|---|---|---|
| MX7116n | Leer | MX7116n | Leer |
| 25G PTM | Leer | 25G PTM | Leer |
| 10GBT PTM | Leer | 10GBT PTM | Leer |
| MX9116n | MX9116n | MX9116n | Leer |
| MX5108n | MX5108n | MX5108n | Leer |
| MX7116n | MX7116n | MX7116n | Leer |
| 25G PTM | 25G PTM | 25G PTM | Leer |
| 10GBT PTM | 10GBT PTM | 10GBT PTM | Leer |
| MX9116n | MX9116n | MX5108n | MX5108n |
| MX9116n | MX9116n | 25G PTM | 25G PTM |
| MX9116n | MX9116n | 10GBT PTM | 10GBT PTM |
| MX9116n | MX7116n | MX5108n | MX5108n |
| MX7116n | MX9116n | MX5108n | MX5108n |
| MX9116n | MX7116n | 25G PTM | 25G PTM |
| MX7116n | MX9116n | 25G PTM | 25G PTM |
| MX9116n | MX7116n | 10GBT PTM | 10GBT PTM |
| MX7116n | MX9116n | 10GBT PTM | 10GBT PTM |
| MX7116n | MX7116n | MX5108n | MX5108n |
| MX7116n | MX7116n | 25G PTM | 25G PTM |
| MX7116n | MX7116n | 10GBT PTM | 10GBT PTM |
| MX5108n | MX5108n | MX9116n | MX9116n |
| MX5108n | MX5108n | MX7116n | MX7116n |
| MX5108n | MX5108n | MX9116n | MX7116n |
| MX5108n | MX5108n | MX7116n | MX9116n |
| MX5108n | MX5108n | 25G PTM | 25G PTM |
| MX5108n | MX5108n | 10GBT PTM | 10GBT PTM |
| 25G PTM | 25G PTM | MX9116n | MX9116n |
| 25G PTM | 25G PTM | MX7116n | MX7116n |
| 25G PTM | 25G PTM | MX9116n | MX7116n |
| 25G PTM | 25G PTM | MX7116n | MX9116n |
| 25G PTM* | 25G PTM* | 10GBT PTM* | 10GBT PTM* |
| 10GBT PTM | 10GBT PTM | MX9116n | MX9116n |
| 10GBT PTM | 10GBT PTM | MX7116n | MX7116n |
| 10GBT PTM | 10GBT PTM | MX9116n | MX7116n |
| 10GBT PTM | 10GBT PTM | MX7116n | MX9116n |
| 10GBT PTM* | 10GBT PTM* | 25G PTM* | 25G PTM* |

**Legende:**

* Die Kombination von zwei Arten von Pass-Through-Modulen (PTMs) wird unterstützt.

B

# Erstellen einer validierten Firmware-Lösungs-Baseline mit dem Dell Repository Manager

Mit dem Dell Repository Manager (DRM) können Sie ein Repository erstellen und auf Kataloge von OME-M zugreifen, die später über CIFS, NFS oder HTTPS importiert werden können.

## Hinzufügen eines Repositorys für die Baseline

Nachdem Sie den DRM installiert und gestartet haben, fügen Sie ein Repository für die zu standardisierende Baseline hinzu. Sie können die getätigte Version aus dem Index-Katalog auswählen, und die Liste der Lösungs-Baselines ist im validierten MX-Stack-Katalog unter Kataloggruppen verfügbar. Die Versionen sind im Format Datum-Jahr-Monat-Zahl nummeriert. Zum Beispiel ist der Katalog JULYCY20 die Version 20-07-00. Für weitere Informationen über Firmwareversionen siehe MX7000 Solution Baselines.

So fügen Sie ein Repository hinzu:

1. Klicken Sie auf der DRM-Startseite auf **Repository hinzufügen**.
2. Geben Sie den **Repository-Namen** und die **Beschreibung** des Repositorys ein.
3. Wählen Sie den Basiskatalog aus der Drop-Down-Liste aus. Standardmäßig ist die Option **Enterprise Server-Katalog** ausgewählt. Folgende Optionen stehen zur Verfügung:
   a. Enterprise Server-Katalog
   b. Index-Katalog
   c. Validierter MX-Stack-Katalog

   Das Fenster **Basiskatalog** wird angezeigt, wenn Sie den Indexkatalog für frühere Versionen des validierten **Stack-Katalogs** auswählen.
4. Wählen Sie im Fenster **Basiskatalog** den erforderlichen Katalog aus der Drop-Down-Liste **Kataloge** aus.
5. Klicken Sie auf **Hinzufügen**.

## Herunterladen des Katalogs und Erstellen des Repositorys

Nachdem Sie das Repository hinzugefügt haben, müssen Sie einen Speicherort auswählen, an dem der Katalog und die Dell Update Packages (DUPs) gehostet werden. Der ausgewählte Speicherort muss eine Netzwerkfreigabe sein, auf die OpenManage - Modular auf dem Chassis zugreifen kann, das die Baseline verwendet. Die Downloads werden im Hintergrund über einen Job ausgeführt.

So laden Sie den Katalog herunter:

1. Wählen Sie auf der DRM-Startseite den von Ihnen erstellten Katalog aus und klicken Sie auf Herunterladen.

   Das Fenster **Komponenten herunterladen** wird angezeigt.
2. Klicken Sie auf **Durchsuchen**. Das Durchsuchen-Fenster wird angezeigt.
3. Wählen Sie einen freigegebenen Ordner und klicken Sie auf Öffnen, um die Baseline herunterzuladen.

   **ANMERKUNG:** Der freigegebene Ordner muss für OME-M über CIFS, NFS oder HTTPS vom Chassis aus zugänglich sein, um die Baseline zu verwenden.

## Zugriff auf den Katalog von OME-Modular aus

So greifen Sie auf den Katalog zu:

1. Klicken Sie auf der OME-M-Startseite auf **Konfiguration** > **Firmwarekonformität** > **Katalogverwaltung**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im Assistenten **Update-Katalog hinzufügen Namen** ein.

4. Wählen Sie Netzwerkpfad, geben Sie die entsprechenden Netzwerkdetails ein.
5. Klicken Sie auf **Jetzt testen**, um die Testverbindung zu überprüfen.
6. Klicken Sie auf **Fertigstellen**.

C

# Netzwerkswitch über unterschiedliche OS10 DUP-Versionen aktualisieren

In den folgenden Abschnitten finden Sie Informationen zum Upgrade von OS10 mit verschiedenen DUP-Versionen.

**ANMERKUNG:** Wenn Sie während des Wartungszeitfensters ein Upgrade von VLT-Peers von 10.4.0E (R3S oder R4S) auf 10.5.0.1 oder höher durchführen, kann dies den Datenverkehr während des Upgrades beeinträchtigen.

**ANMERKUNG:** Das DUP-Update-Verfahren wird empfohlen, um OS10 auf MX9116n und MX5108n zu aktualisieren.

**Themen:**



## Update des Netzwerk-Switches auf 10.5.0.7 oder 10.5.0.9 mit DUP

Gehen Sie folgendermaßen vor, um den Netzwerkswitch mit DUP zu aktualisieren:

1. Laden Sie die neueste DUP-Datei für den Switch von https://www.dell.com/support herunter.
2. Gehen Sie in der OME-Modular-Weboberfläche zu **Geräte** > **E/A-Module**.
3. Wählen Sie das EAM-Modul aus, auf dem Sie das OS10-Upgrade durchführen möchten.
4. Klicken Sie auf **Firmware aktualisieren**.
5. Wählen Sie die Option „Einzelnes Paket“ aus und klicken Sie auf **Durchsuchen**, um zum Speicherort des heruntergeladenen DUP zu navigieren. Warten Sie, bis der Compliance-Bericht abgeschlossen ist, anschließend werden die unterstützten Komponenten angezeigt.
6. Wählen Sie die gewünschten Komponenten aus und klicken Sie auf **Update**, um das Update zu starten.
7. Gehen Sie zur Seite **Monitoring-** > **Jobs**, um den Jobstatus anzeigen.

## Voraussetzungen für das Upgrade von früheren Versionen als 10.5.0.5

- Stellen Sie beim Update sicher, dass die EAMs in Gruppen mit nicht mehr als vier pro Upgrade-Job aktualisiert werden.
- Wenn sich in einem VLT mit Full-Switch-Modus zwei Switches befinden, sollte jeder Switch aus Redundanzgründen Teil eines anderen Upgrade-Batches sein.
- Wenn zwei Switches in einer SmartFabric vorhanden sind, wählen Sie nur einen Switch aus. Der andere Switch wird automatisch aktualisiert und in dieser Upgrade-Gruppe als „2“ gezählt.
- Aktualisieren Sie das Haupt- oder die Peer-Fabric-EAM in der letzten Gruppe.

**ANMERKUNG:** Führen Sie das Skript für das X.509v3 Zertifikat-Upgrade aus, bevor Sie eine Betriebssystemversion aktualisieren. Weitere Informationen finden Sie unter OS10 Firmwareupdate-Matrix.

So identifizieren Sie das Haupt-EAM:

1. Melden Sie sich bei einem beliebigen EAM-Switch an.
2. Gehen Sie zu Linux-Eingabeaufforderung mit den folgenden Befehlen:
   a. `system bash`

b. `sudo -i`

3. Gehen Sie mit dem folgenden Befehl zur SmartFabric Services-CLI-Eingabeaufforderung:

```
python /opt/dell/os10/bin/rest-service/tool/dnv_cli.py
```

4. Rufen Sie das Service-Tag des Haupt-EAM mit dem folgenden Befehl ab:

```
show cluster
```

# Voraussetzungen für das Upgrade von 10.5.0.5

- Stellen Sie beim Update sicher, dass die EAMs in Gruppen mit nicht mehr als vier pro Upgrade-Job aktualisiert werden.
- Wenn sich in einem VLT mit Full-Switch-Modus zwei Switches befinden, sollte jeder Switch aus Redundanzgründen Teil eines anderen Upgrade-Batches sein.
- Wenn zwei Switches in einer SmartFabric vorhanden sind, wählen Sie nur einen Switch aus. Der andere Switch wird automatisch aktualisiert und in dieser Upgrade-Gruppe als „2“ gezählt.

**ANMERKUNG:** Führen Sie das Skript für das X.509v3 Zertifikat-Upgrade aus, bevor Sie eine Betriebssystemversion aktualisieren. Weitere Informationen finden Sie unter OS10 Firmwareupdate-Matrix.

# D

# Netzwerkswitch über CLI aktualisieren

**ANMERKUNG:** Aktualisieren Sie die MX9116n- und MX5108n-Switches nur dann auf 10.5.1.9 oder 10.5.2.6, wenn auf den Switches 10.5.0.9 oder das Zertifikat 10.5.0.7 installiert ist. Weitere Informationen unter OS10 Firmwareupdate-Matrix.

**ANMERKUNG:** Aktualisieren Sie die Switches MX9116n und MX5108n nur dann auf 10.5.1.X, wenn die Switches 10.5.0.7 oder höher ausführen. Stellen Sie während der Aktualisierung sicher, dass nicht mehr als sechs EAMs in der Gruppe pro Upgrade-Job vorhanden sind.

**ANMERKUNG:** Um den Netzwerkswitch von 10.4.0E (R3S oder R4S) zu aktualisieren, aktualisieren und laden Sie beide VLT-Nodes gleichzeitig neu. Führen Sie das Update während des Wartungszeitfensters durch, da der Datenverkehr während des Upgrades möglicherweise betroffen ist.

## Wichtige Hinweise für das Upgrade:

- Versionen 10.5.0.1 und höher: Aktualisieren Sie bei Fabrics oder VLTs ein EAM und fahren Sie dann nach Fertigstellung des ersten EAM mit seinem Peer fort.
- Version 10.4.0E(R4S) und frühere bis 10.5.0.7: Aktualisieren Sie die beiden EAMs einer Fabric oder eines VLT und starten Sie sie gleichzeitig neu.
- Version 10.5.0.7/10.5.0.9-Upgrade von bis zu maximal sechs IOMs gleichzeitig.
- Frühere Versionen als 10.5.0.7: Führen Sie ein Upgrade von bis zu maximal vier EAMs zusammen durch.

1. Führen Sie die folgenden Schritte aus, um das Netzwerk-E/A-Modul zu aktualisieren.
   a. **(Optional)** Sichern Sie die derzeit ausgeführte Konfiguration in der Startkonfiguration im Ausführungsmodus (EXEC).

**Tabelle 27. Befehlsbeschreibung**

| Befehl | Beschreibung |
|---|---|
| `OS10# copy running-configuration startup-configuration` | Sichern Sie die ausgeführte Konfiguration in der Startkonfiguration. |

   b. Sichern Sie die Startkonfiguration im Ausführungsmodus (EXEC).

**Tabelle 28. Befehlsbeschreibung**

| Befehl | Beschreibung |
|---|---|
| `OS10# copy config://startup.xml config://<backup file name>` | Sichern Sie die Startkonfiguration im Ausführungsmodus (EXEC). |

   c. Laden Sie das neue Software-Image von der Dell Support-Website herunter, extrahieren Sie die bin-Dateien aus der tar-Datei und speichern Sie die Datei im Ausführungsmodus (EXEC).

**Tabelle 29. Befehlsbeschreibung**

| Befehl | Beschreibung |
|---|---|
| `OS10# image download file-url`<br>Beispiel:<br>`OS10# image download ftp://userid:passwd@hostip:/filepath` | Laden Sie das neue Software-Image herunter. |

**ANMERKUNG:** Einige Windows-Entpackungsanwendungen fügen zusätzliche Zeilenumbrüche (CR) oder Zeilenvorschübe (LF) ein, wenn sie den Inhalt einer .tar-Datei extrahieren, was das heruntergeladene OS10-Binär-Image beschädigen kann. Deaktivieren Sie diese Option, wenn Sie ein Windows-basiertes Tool verwenden, um eine OS10 Binärdatei zu extrahieren.

   d. **(Optional)** Zeigen Sie den aktuellen Status des Softwaredownloads im EXEC-Modus an.

**Tabelle 30. Befehlsbeschreibung**

| Befehl | Beschreibung |
|---|---|
| `OS10# show image status` | Zeigen Sie den aktuellen Softwaredownloadstatus an. |

e. Installieren Sie das 10.5.0.5-Software-Image im Ausführungsmodus (EXEC).

**Tabelle 31. Befehlsbeschreibung**

| Befehl | Beschreibung |
|---|---|
| `OS10# image install image-url`<br>Beispiel:<br>`OS10# image install image://filename.bin` | Installieren Sie das Software-Image. |

f. **(Optional)** Zeigen Sie den Status der aktuellen Softwareinstallation im Ausführungsmodus (EXEC) an.

**Tabelle 32. Befehlsbeschreibung**

| Befehl | Beschreibung |
|---|---|
| `OS10# show image status` | Zeigen Sie den Status der aktuellen Softwareinstallation an. |

g. Ändern Sie die nächste Startpartition im Ausführungsmodus (EXEC) zur Stand-by-Partition. Verwenden Sie den aktiven Parameter, um die nächste Startpartition von Stand-by auf Active zu ändern.

**Tabelle 33. Befehlsbeschreibung**

| Befehl | Beschreibung |
|---|---|
| `OS10# boot system standby` | Ändern Sie die nächste Startpartition zu Stand-by. |

h. **(Optional)** Überprüfen Sie, ob die nächste Startpartition im Ausführungsmodus (EXEC) zu Stand-by geändert wurde.

**Tabelle 34. Befehlsbeschreibung**

| Befehl | Beschreibung |
|---|---|
| `OS10# show boot detail` | Überprüfen Sie, ob die nächste Startpartition geändert wurde. |

i. Laden Sie das neue Software-Image erneut im Ausführungsmodus (EXEC).

**Tabelle 35. Befehlsbeschreibung**

| Befehl | Beschreibung |
|---|---|
| `OS10# reload` | Laden Sie die neue Software erneut. |

j. Nachdem die Installation abgeschlossen ist, geben Sie den Befehl „show version“ ein, um zu überprüfen, ob die neueste Version der Software, die Sie installiert haben, im System ausgeführt wird.

Das folgende Beispiel zeigt, dass die 10.5.0.5-Software auf dem System installiert ist und ausgeführt wird.

```
OS10# show version
MX9116N-A2# show version
Dell EMC Networking OS10 Enterprise
Copyright (c) 1999-2020 by Dell Inc. All Rights Reserved.
OS Version: 10.5.0.5
Build Version: 10.5.0.5.661
Build Time: 2020-02-15T00:45:32+0000
System Type: MX9116N-ON
Architecture: x86_64
Up Time: 1 day 20:37:53
MX9116N-A2#
```

2. Führen Sie den Befehl `show smartfabric cluster member` im Haupt-Netzwerkswitch aus. Vergewissern Sie sich, dass der `STATUS` des aktualisierten Switch nach dem erneuten Laden `ONLINE` in der Ausgabe des Befehls lautet. Die Netzwerkswitches mit Version 10.5.01 und höher nutzen SFS-CLI, während frühere Versionen wie 10.4.0E(R3S) und 10.4.0E(R4S) den „show cluster“-Befehl `python /opt/dell/os10/bin/rest-service/tool/dnv_cli.py` verwenden. Schritte zur Identifizierung des Master-EAM finden unter Upgrade von früheren Versionen als 10.5.0.5.

**ANMERKUNG:** Während des Image-Upgrade-Prozesses in einem VLT-Setup bei dem VLT-Peers unterschiedliche Softwareversionen ausführen, sollten keine Konfigurationsänderungen in einem der VLT-Peers durchgeführt werden. Stellen Sie sicher, dass beide Nodes auf die gleiche Version aktualisiert wurden, bevor Sie Konfigurationsänderungen vornehmen.

```
IOM# show smartfabric cluster member
Service-tag  IP Address  Status         Role        Type          Chassis-Service-Tag
Chassis-Slot
MXWV122  xxxxxxxxxxx   ONLINE   MAIN     MX9116n  SKYMX02             A2
MXLE103    xxxxxxxxxxx   ONLINE   BACKUP     MX9116n  SKYMX10             B2
MXLE093   xxxxxxxxxxx   ONLINE    BACKUP     MX9116n  SKYMX09             B1
MXWV011  xxxxxxxxxxx   ONLINE   BACKUP     MX9116n  SKYMX01             A1
```