Dell EMC OpenManage Enterprise-Modular Edition, Version 1.10.20 für PowerEdge MX7000-Gehäuse

Benutzerhandbuch

March 2020
Rev. A01

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.

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 unterstützt:

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

Unterstützte Plattformen

OME - Modular unterstützt die folgenden Plattformen und Komponenten:

Plattformen:

- PowerEdge MX7000
- PowerEdge MX740c
- 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 Ethernet-Switch
- Dell EMC MX7116n Fabric Expander Module
- Fibre-Channel-Switch-Modul Dell EMC MXG610s
- PowerEdge MX9002m Managementmodul

Unterstützte Web-Browser

OME – Modular wird von den folgenden Web-Browsern unterstützt:

- Google Chrome Version 63
- Google Chrome Version 64
- Mozilla Firefox Version 57
- Mozilla Firefox Version 58
- Microsoft EDGE
- Microsoft Internet Explorer 11
- Safari Version 11

Damit die OME – Modular-Webschnittstelle ordnungsgemäß in den Webbrowser geladen wird, stellen Sie sicher, dass die Active X/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 REST-API-Handbuch	Dieses Dokument enthält Informationen zur Integration Ihrer Anwendungen mit OpenManage Enterprise Modular unter Verwendung der Restful-API-Befehle.

Tabelle 1. Liste mit weiteren Dokumenten zu Referenzzwecken (fortgesetzt)

Name des Dokuments	Kurze Einführung in das Dokument
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 OpenManage-Dokumente – **Www.dell.com/openmanagemanuals**
  - Für Dokumente zu iDRAC und Lifecycle Controller – **Www.dell.com/idracmanuals**
  - Für alle Enterprise-System-Verwaltungsdokumente – **unter www.dell.com/esmmanualsDell.com/SoftwareSecurityManuals**
  - Für OpenManage Connections Enterprise-System-Verwaltungsdokumente – **unter www.dell.com/esmmanuals**
  - Für Dokumente zu Serviceability Tools – **https://www.dell.com/serviceabilitytools**
  - Für Client Command Suite-System-Verwaltungsdokumente – **Www.dell.com/omconnectionsclient**
- 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

Managementmodul-Firmware aktualisieren

In diesem Kapitel werden die Methoden zur Aktualisierung der Management Modul-Firmware und der MX7000-Firmware-Komponenten beschrieben.

Führen Sie in der MCM-Umgebung die Firmware-Aktualisierung für alle Geräte vom Hauptgehäuse aus durch. Wählen Sie außerdem für eine erfolgreiche Firmwareaktualisierung die EAMs und Speicherschlitten als einzelne Geräte und nicht als Gehäusekomponenten aus.

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 REST-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 die Firmwareaktualisierung 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. Nach der OME – Modular-Aktualisierung sollten Sie 3-5 Minuten warten, bis die Konsole einen stabilen Zustand erreicht.

Themen:

Firmware unter Verwendung der Katalog-basierten Compliance-Methode aktualisieren

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

1. Laden Sie das DUP über die Website **www.dell.com/support/drivers** herunter.
2. Erstellen Sie mit dem Dell Repository Manager (Repository Manager) die Datei `catalog.xml`.
3. Legen Sie die mit Repository Manager erstellte Datei `catalog.xml` in einem freigegebenen Verzeichnis ab.
4. Navigieren Sie zur Seite **Konfigurationsfirmware**, um den Katalog und die Baseline zu erstellen.
5. In der OME – Modular-Webschnittstelle navigieren Sie zur Seite **Geräte** > **Gehäuse**.
6. Klicken Sie auf die Option **Firmware aktualisieren**. Die Seite **Firmwarequelle auswählen** wird angezeigt.
7. Wählen Sie die Option **Baseline**, und wählen Sie die erforderlichen Baseline aus dem Drop-Down-Menü aus.
8. Wählen Sie die OME – Modular-Komponente aus dem Vergleichsbericht aus.
   Die unterstützten Komponenten werden angezeigt.
9. Wählen Sie die gewünschten Komponenten aus, zum Beispiel: OME – Modular, und klicken Sie auf **Aktualisieren**, um die Firmwareaktualisierung zu starten:

10. Gehen Sie zur Seite **Überwachen** > **Jobs**, um den Jobstatus anzeigen.

ANMERKUNG: Verwenden Sie die Option Hinzufügen unter Konfiguration > Firmware > Katalogverwaltung, um den Katalog von der Website https://www.dell.com/support herunterzuladen.

MX7000-Komponenten mit OME-Modular 1.10.20 aktualisieren

Sie können die folgenden Komponenten von MX7000 unter Verwendung von OME-Modular 1.10.20 aktualisieren. In der folgenden Tabelle sind die neuen Versionen der MX7000-Komponenten aufgeführt:

Tabelle 2. MX7000 – OME-Modular 1.10.20-Lösungs-Baselines

Komponente	Version
iDRAC mit Lifecycle Controller	4.11.11.11
Dell EMC Server BIOS PowerEdge MX740c	2.5.4
Dell EMC Server BIOS PowerEdge MX840c	2.5.4
Fibre Channel-Adapter der QLogic 26XX-Serie	15.05.12
Fibre Channel-Adapter der QLogic 27XX-Serie	15.05.12
Adapter der QLogic 41xxx-Serie	15.05.14
Mellanox ConnectX-4 Lx Ethernet-Adapter-Firmware	14.25.80.00
Intel NIC-Produktreihe Version 19.5.x, Firmware für X710-, XXV710- und XL710-Adapter	19.5.12
Emulex Fibre Channel-Adapter-Firmware.	03.02.18
OpenManage Enterprise Modular	1.10.20
MX9116n Fabric Switching Engine OS10	10.5.0.5
MX5108n Ethernet-Switch OS10	10.5.0.5

Überprüfen Sie vor der Aktualisierung 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: 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: Möglicherweise ist ein Aus- und Einschalten (Hardwarestart) des MX7000-Gehäuses nach der Aktualisierung aller zutreffenden Lösungskomponenten erforderlich. Weitere Informationen finden Sie unter Stromversorgung des Gehäuses steuern.

Komponenten-Aktualisierungsreihenfolge

Lesen Sie die Anweisungen zur Aktualisierung vor der Implementierung des Aktualisierungsverfahrens. Sammeln Sie die aktuellen Versionen der MX7000-Komponenten in Ihrer Umgebung und notieren Sie die speziellen Anweisungen, die im Aktualisierungsverfahren genannt werden können.

Wenden Sie sich an Dell Support, um Unterstützung bei der Durchführung eines Upgrades der MX7000-Komponenten zu erhalten. **Es wird empfohlen, dass Sie alle Komponenten im geplanten einzelnen Wartungszeitfenster aktualisieren.**

Bevor Sie mit der Aktualisierung 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. iDRAC mit Lifecycle Controller mithilfe von OME-Modular
2. PowerEdge MX740c BIOS und PowerEdge MX840c Server-BIOS
3. Aktualisieren Sie die Betriebssystemtreiber des Geräteadapters, gefolgt von der Firmware des Geräteadapters.

   Adapter – QLogic Fibre Channel der 27XX-Serie, QLogic Fibre Channel der 26XX-Serie, QLogic 41xxx-Serie, Mellanox ConnectX-4 Lx-Ethernet-Adapter-Firmware, Intel X710, XXV710 und XL710 Emulex Fibre Channel
4. OME-Modular
5. Fabric Switching Engine MX9116n und/oder Ethernet-Switch MX5108n

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

iDRAC mit Lifecycle Controller mithilfe von OME-Modular 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 **Firmware aktualisieren**.
5. Wählen Sie im Popup-Assistenten das einzelne Paket aus und klicken Sie auf **Durchsuchen**, um das **iDRAC mit Lifecycle Controller**-DUP auszuwählen.
6. Nachdem das DUP hochgeladen wurde, klicken Sie auf **Weiter** und aktivieren Sie das Kontrollkästchen **Compliance**.
7. Klicken Sie auf **Fertig stellen**, um die Aktualisierung auf allen Rechnern zu starten.
8. Warten Sie, bis der Vorgang abgeschlossen ist, bevor Sie mit der Aktualisierung der Komponenten *Dell EMC Server-BIOS PowerEdge MX740c* und *Dell EMC Server-BIOS PowerEdge MX840c* fortfahren.

ANMERKUNG: Als alternative Methode zum Aktualisieren von Rechner-Hosts können Sie Katalog-basierte Aktualisierungen implementieren, sobald die Kataloge mit den Baseline-Versionen aktualisiert wurden. Weitere Informationen finden Sie unter Kataloge verwalten.

PowerEdge MX740c BIOS und PowerEdge MX840c Server-BIOS aktualisieren

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 und Dell EMC Server-BIOS PowerEdge 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 Schritte, die im Abschnitt *iDRAC mit Lifecycle Controller mithilfe von OME-Modular aktualisieren* beschrieben sind, um *Fibre Channel-Adapter der QLogic 26XX-Serien*, *Fibre Channel-Adapter der QLogic 27XX-Serie*, *Adapter der QLogic 41xxx-Serie*, *Mellanox ConnectX-4 LX-Ethernet-Adapter-Firmware*, *Firmware der Intel NIC-Produktreihe Version 19.5.x für X710-, XXV710- und XL710-Adapter* sowie *Emulex Picard-16/Picard-32-Adapter* nach Bedarf zu aktualisieren. Gehen Sie zu Dell.com, um die neuesten Gerätetreiber für die jeweilige Firmwareaktualisierung herunterzuladen.

OME-Modular aktualisieren

1. Wenn OME-Modular eine Gehäusegruppe verwaltet, melden Sie sich bei OME-Modular des Hauptgehäuses an.
2. Wenn die aktuelle Version 1.10.00, 1.10.01 oder 1.10.10 ist, fahren Sie mit Schritt 4 fort.
3. Wenn die aktuelle Version 1.00.01 oder 1.00.10 ist, aktualisieren Sie OME-Modular auf 1.10.00 oder 1.10.10 vor der Aktualisierung auf 10.10.20.

   Führen Sie folgende Schritte aus, um eine Aktualisierung auf 1.10.10 durchzuführen:

ANMERKUNG: Eine Aktualisierung auf 1.10.x kann zu einer Warnungsprotokollwarnung HWC7522 führen. Möglicherweise müssen Sie auf dem MX7116n oder den Passthrough-Modul (PTM)-IOMs das System neu einsetzen.

a. Klicken Sie auf **Geräte** > **Gehäuse**.
Eine Liste der verfügbaren Gehäuse wird angezeigt.
b. Aktivieren Sie das Kontrollkästchen in der Kopfzeile der Liste, um alle Gehäuse auf der aktuellen Seite auszuwählen. Wenn die Liste mehrere Seiten umfasst, gehen Sie zu jeder Seite und aktivieren Sie das Kontrollkästchen.
c. Klicken Sie nach Auswahl aller Gehäuse auf **Firmware aktualisieren**.
d. Wählen Sie im Pop-up-Assistenten das einzelne Paket aus und klicken Sie auf **Durchsuchen**, um das **OpenManage Enterprise-Modular-1.10.10**-DUP auszuwählen.
e. Nachdem das DUP hochgeladen wurde, klicken Sie auf **Weiter** und aktivieren Sie das Kontrollkästchen **Compliance**.
f. Klicken Sie auf **Fertig stellen**, um die Aktualisierung auf allen Gehäusen zu starten.
g. Warten Sie, bis der Vorgang abgeschlossen ist und die Gerätekommunikation in der MCM-Gruppe wiederhergestellt ist.
h. Melden Sie sich bei OME-Modular an und vergewissern Sie sich, dass alle Mitgliedsgehäuse der Gruppe im MCM-Dashboard verfügbar sind.
i. Navigieren Sie in der OME-Modular-Webschnittstelle des Hauptgehäuses zur Seite **Übersicht** aller Mitgliedsgehäuse und vergewissern Sie sich, dass die Grafiken der Gehäuse und der Gehäuse-Untersysteme geladen werden.
j. Rufen Sie die Seite **Warnmeldungen** > **Warnungsprotokoll** auf und überprüfen Sie, ob ein Warnungssturm stattfindet.
Als einen Warnungssturm bezeichnet man eine Situation, in der mehrere Warnmeldungen pro Sekunde erzeugt werden. Wenn ein Warnungsstopp stattfindet, warten Sie, bis er abgeschlossen ist.
k. Fahren Sie mit dem Aktualisieren der anderen OME-Modular-Firmware fort.

4. Wenn die aktuelle Version 1.10.00 oder 1.10.10 ist:
a. Klicken Sie auf **Geräte** > **Gehäuse**.
Eine Liste der verfügbaren Gehäuse wird angezeigt.
b. Aktivieren Sie das Kontrollkästchen in der Kopfzeile der Liste, um alle Gehäuse auf der aktuellen Seite auszuwählen. Wenn die Liste mehrere Seiten umfasst, gehen Sie zu jeder Seite und aktivieren Sie das Kontrollkästchen.
c. Klicken Sie nach Auswahl aller Gehäuse auf **Firmware aktualisieren**.
d. Wählen Sie im Pop-up-Assistenten das einzelne Paket aus und klicken Sie auf **Durchsuchen**, um das **OpenManage Enterprise-Modular-1.10.20**-DUP auszuwählen.
ANMERKUNG: IOMs der MX9116n- und/oder MX5108n-Version 10.5.0.3 werden bei einer Aktualisierung von OME Modular möglicherweise neu gestartet.
e. Nachdem das DUP hochgeladen wurde, klicken Sie auf **Weiter** und aktivieren Sie das Kontrollkästchen **Compliance**.
f. Klicken Sie auf **Fertig stellen**, um die Aktualisierung auf allen Gehäusen zu starten.
g. Warten Sie, bis der Vorgang abgeschlossen ist.

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.

Fabric Switching Engine und Ethernet-Switch aktualisieren

Sammeln Sie die folgenden Informationen, die zum Ausführen der Aktualisierungen erforderlich sind.

ANMERKUNG: Überspringen Sie die Schritte 1 und 2 für die Netzwerk-Switch-Versionen 10.4.0.R3S und 10.4.0.R4S und fahren Sie mit Schritt 3 fort.

1. Identifizieren und notieren Sie die Switch-Service-Tag-Nummer und ihre Rolle im Smart Fabric-Cluster, indem Sie den Befehl `show smartfabric cluster` auf der Switch-CLI ausführen.
Führen Sie diesen Befehl auf allen Switches in einem einzigen Gehäuse oder einer Gehäusegruppe aus.

Beispielausgabe von einem Gehäusegruppen-Mitglied:

```
IOM# show smartfabric cluster
-------------------------------------------------------------
CLUSTER DOMAIN ID : 159
VIP : fde1:53ba:e9a0:de14:0:5eff:fe00:1159
ROLE : BACKUP
SERVICE-TAG : MXWV011
MASTER-IPV4 : 100.69.101.170
PREFERRED-MASTER :
```

Beispielausgabe von einem Gehäusegruppen-Master:

```
IOM# show smartfabric cluster
-------------------------------------------------------------
CLUSTER DOMAIN ID : 159
VIP : fde1:53ba:e9a0:de14:0:5eff:fe00:1159
ROLE : MASTER
SERVICE-TAG : MXWV122
MASTER-IPV4 : 100.69.101.170
PREFERRED-MASTER :
```

2. Führen Sie auf dem Netzwerk-Switch mit der Rolle „Master“ den Befehl `show smartfabric cluster member` aus, um die Details aller ermittelten Switches in der OME-Modular-Gehäusegruppe abzurufen.

   Diese Befehlsausgabe enthält eine Referenz für das Upgradeverfahren.

```
IOM# show smartfabric cluster member
Service-tag  IP Address  Status         Role        Type          Chassis-Service-Tag
Chassis-Slot
MXWV122  xxxxxxxxxxx   ONLINE   MASTER     MX9116n  SKYMX02             A2
MXLE103    xxxxxxxxxxx   ONLINE   BACKUP     MX9116n  SKYMX10               B2
MXLE093   xxxxxxxxxxx   ONLINE    BACKUP     MX9116n  SKYMX09               B1
MXWV011  xxxxxxxxxxx   ONLINE   BACKUP     MX9116n  SKYMX01             A1
```

3. Aktualisieren Sie alle Netzwerk-Switches (MX9116n und MX5108n) in der OME-Modular-Gehäusegruppe auf 10.5.0.5. Ändern Sie während dieses Upgrades keine Konfigurationen in der Gehäusegruppe.

   Führen Sie den folgenden Befehl aus, um die IOM mit der Rolle „Master“ zu identifizieren. Die IOM mit der Rolle „Master“ muss **zuletzt** aktualisiert werden.

```
OS10# system bash
root@HRA0017:~# python /opt/dell/os10/bin/rest-service/tool/dnv_cli.py
DNV Command Line Interface
['/opt/dell/os10/bin/rest-service/tool/dnv_cli.py']
dnv$show cluster
http://127.0.0.1:8000/cluster/238
vip: fde1:53ba:e9a0:de14:0:5eff:fe00:1238
my_role: BACKUP
Master_node: fde1:53ba:e9a0:de14:2204:fff:fe21:e749
slot_number: 1
ip_address: fde1:53ba:e9a0:de14:2204:fff:fe21:9f49

        Chassis Tag ARH0009
        IOM Service Tag HRA0036
        Role BACKUP
        IP Address fde1:53ba:e9a0:de14:2204:fff:fe20:56c9


        Chassis Tag ARH0005
        IOM Service Tag HRA0017
        Role BACKUP
        IP Address fde1:53ba:e9a0:de14:2204:fff:fe21:9f49


        Chassis Tag ARH0010
        IOM Service Tag HRA0037
        Role BACKUP
        IP Address fde1:53ba:e9a0:de14:2204:fff:fe12:e8c3
```

```
        Chassis Tag ARH0005
        IOM Service Tag HRA0020
        Role MASTER
        IP Address fde1:53ba:e9a0:de14:2204:fff:fe21:e749


dnv$
```

Dieser Befehl gilt für Netzwerk-Switches 10.4.0.R3S und 10.4.0.R4S.

4. Für das Upgrade des Netzwerk-Switch von 10.4.0E (R3S oder R4S) gilt Folgendes:
   a. Aktualisieren und laden Sie die VLT-Nodes gleichzeitig während des Wartungszeitfensters, da der Datenverkehr während des Upgrades möglicherweise betroffen ist.
   b. Verwenden Sie für das Upgrade die CLI, wie im Abschnitt Netzwerk-Switch-CLI aktualisieren erläutert.

   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 Änderungen an der Konfiguration vornehmen.

   Verwenden Sie für das Upgrade der Netzwerk-Switches von 10.5.0.x auf 10.5.0.5 die CLI, wie im Abschnitt Netzwerk-Switch-CLI aktualisieren beschrieben.

5. Überprüfen Sie, ob alle erwarteten Datenpfad-Links eingerichtet sind und Datenverkehr weiterleiten. Wenn Probleme mit der Netzwerkverbindung oder Performance auftreten, schalten Sie das MX7000-Gehäuse aus und wieder ein. Weitere Informationen finden Sie unter Stromversorgung des Gehäuses steuern.

Netzwerk-Switch-CLI aktualisieren

1. Führen Sie ein Upgrade des Master-Netzwerk-E/A-Moduls durch, nachdem alle Mitglieder in der Gehäusegruppe aktualisiert wurden.
2. Wenn die Gehäusegruppe über MX5108n und MX9116n verfügt, aktualisieren Sie die MX5108n Netzwerk-E/A-Module zuerst (nicht-Master), gefolgt von der Aktualisierung der MX9116n Netzwerk-E/A-Module.
3. Wenn Sie mehrere Netzwerk-E/A-Module aktualisieren möchten, stellen Sie sicher, dass nicht mehr als zwei Netzwerk-E/A-Module gleichzeitig aktualisiert werden. Außerdem müssen alle Netzwerk-E/A-Module Teil verschiedener Fabrics sein.

   Beim Aktualisieren von IOMs mit 10.4.x auf 10.5.05 müssen Sie beide IOMs in der Fabric aktualisieren und sie gleichzeitig neu starten.
4. 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 3. 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 4. 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 5. Befehlsbeschreibung

Befehl	Beschreibung

`OS10# image download file-url`
Beispiel:
`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 Software-Downloadstatus im Ausführungsmodus (EXEC) an.

Tabelle 6. Befehlsbeschreibung

Befehl	Beschreibung
`OS10# show image status`	Zeigen Sie den aktuellen Software-Downloadstatus an.

e. Installieren Sie das 10.5.0.5-Software-Image im Ausführungsmodus (EXEC).

Tabelle 7. Befehlsbeschreibung

Befehl	Beschreibung

`OS10# image install image-url`
Beispiel:
`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 8. 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 Standby-Partition. Verwenden Sie den aktiven Parameter, um die nächste Startpartition von Standby auf Active zu ändern.

Tabelle 9. Befehlsbeschreibung

Befehl	Beschreibung
`OS10# boot system standby`	Ändern Sie die nächste Startpartition zu Standby.

h. **(Optional)** Überprüfen Sie, ob die nächste Startpartition im Ausführungsmodus (EXEC) zu Standby geändert wurde.

Tabelle 10. 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 11. 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#
```

5. Führen Sie den Befehl `smartfabric-Cluster-Mitglied anzeigen` im Master-Netzwerk-Switch aus. Vergewissern Sie sich, dass der `STATUS` des aktualisierten Switch nach dem erneuten Laden `ONLINE` in der Ausgabe des Befehls lautet.

```
IOM# show smartfabric cluster member
Service-tag  IP Address  Status         Role        Type          Chassis-Service-Tag
Chassis-Slot
MXWV122  xxxxxxxxxxx   ONLINE   MASTER     MX9116n  SKYMX02             A2
MXLE103    xxxxxxxxxxx   ONLINE   BACKUP     MX9116n  SKYMX10               B2
MXLE093   xxxxxxxxxxx   ONLINE    BACKUP     MX9116n  SKYMX09               B1
MXWV011  xxxxxxxxxxx   ONLINE   BACKUP     MX9116n  SKYMX01             A1
```

6. Fahren Sie nach Abschluss von Schritt 5 mit dem Upgrade des nächsten Netzwerk-E/A-Moduls fort.

   Nachdem alle IOMs aktualisiert wurden, ist der Aktualisierungsprozess aller Komponenten im MX7000-Aktualisierungsverfahren abgeschlossen. Überprüfen Sie, ob alle erwarteten Datenpfad-Links eingerichtet sind und Datenverkehr weiterleiten. Wenn Probleme mit der Netzwerkverbindung oder Performance auftreten, schalten Sie das MX7000-Gehäuse aus und wieder ein. Weitere Informationen finden Sie unter Stromversorgung des Gehäuses steuern.

3

Bei OME – Modular anmelden

Sie können sich bei OME – Modular als lokaler, Active Directory- oder allgemeiner LDAP-Benutzer 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 Benutzerkonten.

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

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

- LDAP-Zugang aktivieren
- Ein Verzeichnisdienst-Zertifizierungsstellenzertifikat hochladen und anzeigen
- Während der Konfiguration von LDAP Attribute zuzuweisen Die Attribute sind: LDAP-Serveradresse, LDAP-Serverschnittstelle, Bindungs-DN, Bindungs-Kennwort, Benutzeranmeldeattribut, Gruppenmitgliedschafts-Attribut und Suchfilter
- Eine LDAP-Gruppe mit einer vorhandenen oder neuen Verwaltungsmodul-Rollengruppe verknüpfen

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

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

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

   - Ihr Konto konfigurieren
   - Das Kennwort ändern
   - Das Stammkennwort wiederherstellen

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

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

So fügen Sie einen Verzeichnisdienst hinzu:

1. Klicken Sie in der Menüleiste der OME – Modular-Webschnittstelle auf **Anwendungseinstellungen** > **Benutzer** > **Verzeichnisdienste** > **Hinzufügen**.
   Die Seite **Verbindung zum Verzeichnisdienst** wird angezeigt.
2. Wählen Sie AD oder LDAP aus, und geben Sie die entsprechenden Informationen ein.
3. Wenn der Verzeichnistyp AD und der **Domänen-Controller Lookup**-Typ DNS ist, geben Sie den Domänennamen und die Gruppendomäne ein.

   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 "DNS" **Domain Controller-Lookup**, 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-Lookup**-Typ ausführen.

   Die Funktion **Verbindung testen** ist nur auf den Domänen-Controller-Typ "DNS" anwendbar.

Verzeichnisgruppe importieren

So importieren Sie eine Verzeichnisgruppe:

1. Klicken Sie in der Menüleiste der OME – Modular Webschnittstelle auf **Anwendungseinstellungen** > **Benutzer** > **Verzeichnisgruppe importieren**.
   Das Fenster **Verzeichnis importieren** wird angezeigt.
2. Wählen Sie den Verzeichnisdienst aus, aus dem Sie die Gruppe importieren wollen.
3. Unter **Verfügbare Gruppen** wählen Sie die Gruppe aus und klicken auf >>.
   Die ausgewählte Gruppe wird unter **Zu importierende Gruppen** angezeigt.
4. Weisen Sie den importierten Gruppen eine Rolle zu.

   Sie können Gruppen nach dem Zuweisen von Rollen importieren. Eine Meldung wird angezeigt, nachdem die Gruppen erfolgreich importiert wurden. Benutzer in den importierten Gruppen können mit spezifischen Rollen und Berechtigungen auf OME-Modular zugreifen.

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.

OME – Modular-Startseite

Wenn Sie sich bei OME – Modular anmelden, wird die Startseite angezeigt. Diese Seite zeigt ein Dashboard mit Informationen auf höchster Ebene über das System und die Unterkomponenten an. Verwenden Sie das Suchfeld auf der Seite, um nach den in OME –

Modular verfügbaren Einstellungen zu suchen. 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 unteren linken Ecke der Seite sehen Sie eine Zusammenfassung der Gehäuseinformationen wie z. B. Service-Tag-Nummer, Asset-Tag, Firmware-Versionen und Stromstatus.
- **Gerätezustand** – In der oberen rechten Ecke der Seite sehen Sie den Funktionszustand der Gehäuse-Untersysteme wie Lüfter, Netzteile, Temperatur und Rechner-, Netzwerk-, 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 **Kürzlich durchgeführte Aktivitäten** sehen Sie die letzten Aktivitäten im Gehäuse. Klicken Sie auf **Alle anzeigen**, um alle Aktivitäten auf der Seite **Jobs** zu sehen.

ANMERKUNG: Wenn Sie die Bestandsaufnahme aktualisieren und das Gehäuse nach einem Aus- und Einschalten wieder einschalten, wird die Bestandsliste des Rechnerschlittens und des EAM nach 3-5 Minuten angezeigt.

ANMERKUNG: Wenn das Gehäuse nach einem Aus- und Einschalten nicht eingeschaltet wurde, wird der Bestandsaufnahmestatus als "unbekannt" angezeigt.

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 die Aktualisierung 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 nach einem Aus- und Einschalten wieder einschalten, 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 Firmwareaktualisierung, 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-IPs 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 HTTP-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 Strompriorität 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 Stromquellen mit 110 Volt und 220 Volt.
3. Im Abschnitt **Redundanzkonfiguration** wählen Sie die erforderliche Redundanzregel aus.

   Richtlinien zur Stromredundanz erleichtern die Verwaltung des Energieverbrauchs 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.
   - **Grid-Redundanz:** Bei dieser Richtlinie wird die Strombelastung des Gehäuses auf alle Netzteile verteilt. Die sechs Netzteile sind in zwei Gruppen unterteilt: Grid A besteht aus den Netzteilen 1, 2, 3 und Grid 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 Grid für Grid-Redundanz optimiert ist. Das Grid mit der größten Netzteilkapazität bestimmt die Grenze für die Stromversorgung von Geräten, die zum Gehäuse hinzugefügt werden. Beim Ausfall eines Grids oder Netzteils wird die Strombelastung des Gehäuses zwischen den verbleibenden Netzteilen aufgeteilt mit der Absicht, dass ein einziges funktionsfähiges Grid 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 Netzteileinheit (PSU) unter Berücksichtigung der Gesamtausgabekapazität der PSU niedrig ist. Standardmäßig ist die Hot-Spare-Funktion aktiviert. Wenn die Hotspare-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 Netzwerk-Switch 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 12. Support-Matrix 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/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 12. Support-Matrix 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/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 können die Verwaltungsschnittstellen im internen Verwaltungsnetzwerk vom für Server bestimmten Datenverkehr überlastet werden. Dies führt zu Verzögerungen in der OME – Modular- und iDRAC-Kommunikation. 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. Geben Sie das **Idle Timeout** in Sekunden ein, die sich eine SSH-Sitzung im Leerlauf befinden kann. Die SSH-Sitzung läuft basierend auf der Zeitüberschreitungskonfiguration ab und die standardmäßige Zeitüberschreitung beträgt 30 Minuten. Wenn eine Änderung im Gehäusemanagementnetzwerk erfolgt, werden alle aktiven Sitzungen, die auf der Seite „Benutzersitzungen“ aufgeführt sind, nicht automatisch beendet.
   ANMERKUNG: Die Auditprotokolle werden nicht erzeugt, wenn die Sitzung basierend auf der Zeitüberschreitung abläuft.
7. Geben Sie die SSH **Portnummer** an. Die Portnummer kann zwischen 10 und 65535 liegen.
   Die Standardportnummer ist 22.
8. Aktivieren Sie die Remote-RACADM-Sitzung für das Gehäuse.
   Sie können die Remote-RACADM-Option in der Webschnittstelle nur dann anzeigen, wenn Sie über die Berechtigung 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-Webschnittstelle. Die OME – Modular-Webschnittstelle wird jedoch automatisch wiederherstellt.
9. Klicken Sie auf **Anwenden**, um die Einstellungen für die Gehäusenetzwerkdienste zu speichern.

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 mit dem Netzschalter aus- oder einzuschalten.
   Wenn das Kontrollkästchen deaktiviert ist, kann der Stromstatus des Gehäuses nicht mehr über den Gehäusenetzschalter geändert werden.

3. 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.

4. Aktivieren Sie **Inaktivitätszeitüberschreitung aktivieren**, um die Inaktivitätszeitüberschreitung zu aktivieren, und geben Sie die **Zeitüberschreitungsbegrenzung** ein.

   Zeitüberschreitung ist die Leerlaufzeit (inaktive Zeit), wenn kein WLAN-Datenverkehr stattfindet. Geben Sie das Zeitlimit der Inaktivitätszeitüberschreitung in Sekunden an. Das Zeitlimit kann zwischen zwei und 60 Minuten liegen.

   ANMERKUNG: Die Option Zeitüberschreitungsbegrenzung ist nur dann verfügbar, wenn Inaktivitätszeitüberschreitung aktivieren ausgewählt ist.

5. Wählen Sie **Leseauthentifizierung aktivieren** aus, um sich über Ihre Benutzeranmeldeinformationen 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.

6. Wählen Sie **Quick Sync-WLAN aktivieren** aus, um für die Kommunikation mit dem Gehäuse WLAN zu verwenden. Standardmäßig ist das Kontrollkästchen **Quick Sync-WLAN aktivieren** markiert.
7. 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 *RACADM-CLI-Handbuch zu OME – Modular für PowerEdge MX7000-Gehäuse* verfügbar unter 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)-Converter verfügbar ist, können Sie das KVM-Video auch im VGA streamen.

8. 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.

9. 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.
10. 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.

11. 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.

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

Chassis Direct

Die Chassis-Direct-Funktion in OME-Modular ermöglicht Benutzern 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 Poleg-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 OpenManage mobilen WLAN-Zugang.

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

Mit dem Laptop, der mit dem USB OTG-Port auf dem Gehäuse verbunden ist, können Sie auf die MM-Benutzeroberfläche und die iDRAC Benutzeroberfläche oder KVM zugreifen. Sie können den Zugriff abrufen, 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 Vorderseite (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 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. Aus- und Einschalten des Gehäuses zum Wiederherstellen der Integrität von Quick Sync.

- 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 13. 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. **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. **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. **Lösung** – wenn das Problem weiterhin besteht, schließen Sie das USB-Kabel wieder an.

Tabelle 13. Chassis Direct – LED-BLINK-Status und Beschreibung (fortgesetzt)

Fehlercode	LED-Blinkstatus des Gehäuses	Beschreibung und Lösung
4	Ausgeschaltet	Die USB-Netzwerkverbindung ist nicht aktiv, da das USB-Kabel nicht angeschlossen ist. **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-Webschnittstelle 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.

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-Benutzeroberfläche, 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-IOMs 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-Benutzeroberfläche.
   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, Systemkennnummer, 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 Stromversorgung 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 Energieverbrauch des Systems. Klicken Sie auf **Stromverbrauch**, um Details zum 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.
  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 Berechtigungen als Gehäuseadministrator 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.
    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. Es werden

jedoch Warnungen protokolliert, die darauf hinweisen, dass die Konnektivität zu Geräten aufgrund des Aus- und Einschaltevorgangs verloren geht.

- **Ausschalten (ordnungsgemäß)** – Benachrichtigt das Serverbetriebssystem, dass der Server ausgeschaltet werden soll. Diese Option ist deaktiviert, wenn der Server bereits aus ist.

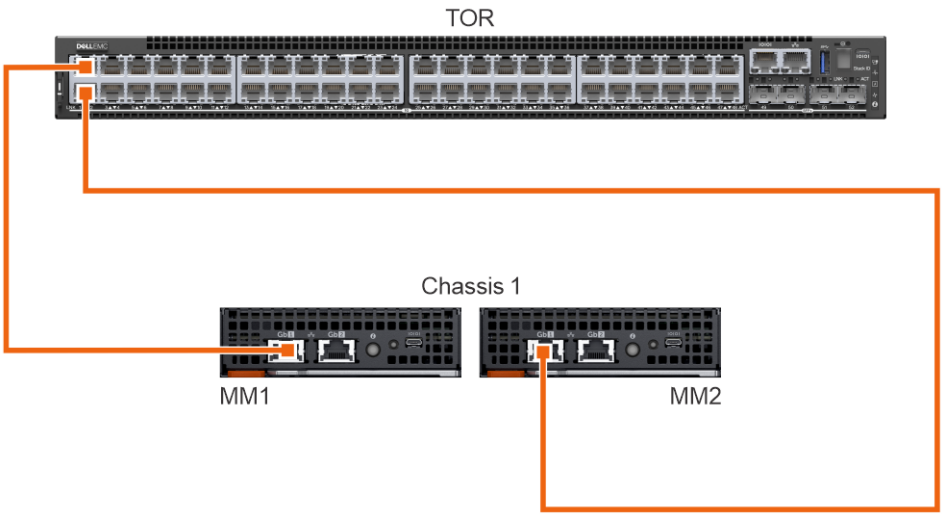
- Konfigurations-Tasks:
  - **Neue Gehäusegruppe erstellen**
  - **Gehäusegruppe beitreten**
  - **Erstkonfiguration**
- Fehlerbehebungs-Tasks:
  - Protokoll extrahieren – Sie können die Protokolle in eine CIFS- oder NFS-Freigabe oder ein lokales Laufwerk Ihres Systems extrahieren.
  - Diagnosebefehle
  - 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.

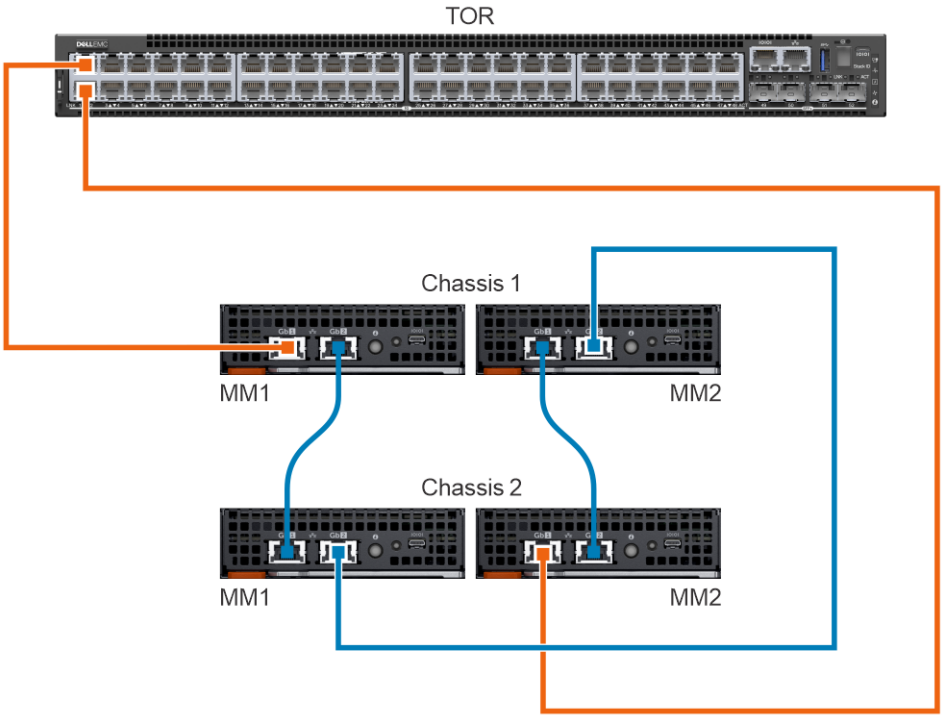
Verkabelungsgehäuse

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.

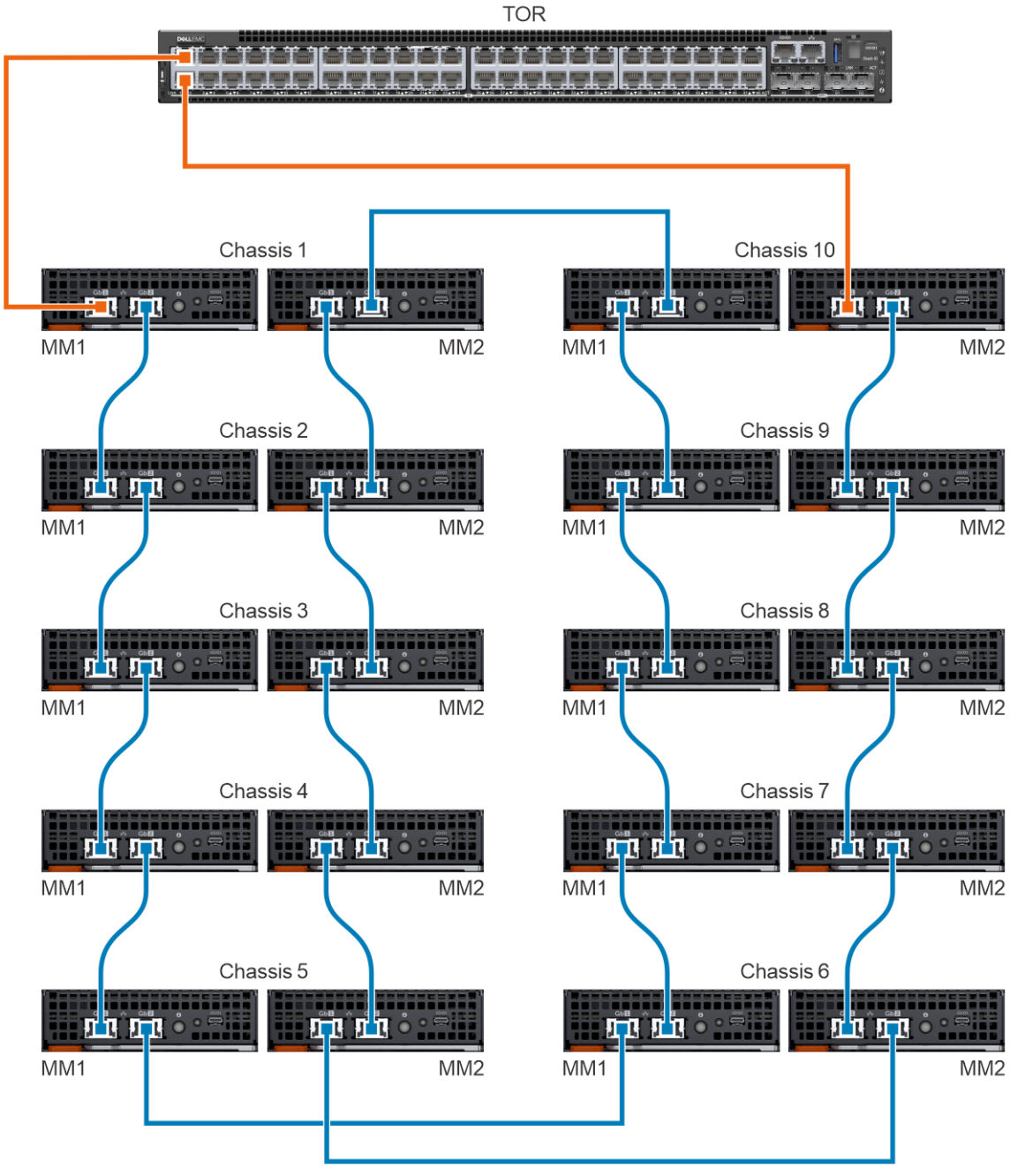
Vor dem Erstellen einer MCM-Gruppe stellen Sie sicher, dass die MX7000-Verwaltungsnetzwerke zu einer Stapelkonfiguration verdrahtet sind. Der Konfiguration als Stack hilft, folgende Situationen zu überwinden:

- 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
   - Zeiteinstellungen – Datum, Uhrzeit, Zeitzone, NTP
   - 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 Zugang
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 über die Seite **Übersicht** des Hauptgehäuses oder über das Mitgliedsgehäuse hinzufügen.

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 **Gehäuse hinzufügen** 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 der manuellen Onboarding-Richtlinie erstellt wird, wird die Beitrittsanfrage in die Warteliste gestellt, damit das Hauptgehäuse das Hinzufügen des Mitgliedsgehäuses bestätigt. 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.

Zuweisen des Backup-Lead

In einer Umgebung mit mehreren Gehäusen kann das Lead-Gehäuse manchmal zeitweilig ausfallen oder sich in den Ruhestand versetzen. 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 in den Ruhestand tritt.

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. Klicken Sie auf die **Virtuelle Lead-IP-Konfiguration (optional)** und aktivieren Sie das Kontrollkästchen **Virtuelle IP aktivieren**.

   Wenn die virtuelle IP-Adresse konfiguriert ist, wird die Gleichmäßigkeit der IP-Adressen erleichtert, wenn die Rolle des Lead-Gehäuses von einem Gehäuse auf ein anderes übertragen wird.
4. Klicken Sie auf **Zusätzliche 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 Anwendungsfall-Szenarien.

   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.

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 eines Backup-Leads zum Lead-Gehäuse lösen Sie alle Profile, die mit einem Steckplatz mit einem Rechnerschlitten verbunden sind, und schließen Sie sie erneut an. 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 Anwendungsfall-Szenarien.

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-Konfiguration mithilfe der REST API `/api/ApplicationService/Actions/ApplicationService.ResetApplication` aus. Weitere Informationen finden Sie im Handbuch *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 den Ruhestand 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 Anwendungsfall-Szenarien.

   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.

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.

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 umfassen den Namen und den Status der Aktivität und den Zeitstempel der Aktivität. Klicken Sie auf **Alle Aktivitäten**, um eine Liste aller Aktivitäten, die mit der Gruppe verknüpft sind, 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 Gerätekonfiguration. 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**, **Benutzername** 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. Unter **Optionale Geräte** wählen Sie die Rechnerschlitten im Gehäuse aus, die Sie sichern möchten.
   Die Anzahl der ausgewählten Geräte wird in der linken unteren Ecke des Fensters **Gehäuse sichern** angezeigt.
8. Klicken Sie auf **Sichern**.
   Es wird eine Meldung angezeigt, die darauf hinweist, dass die Sicherung erfolgreich abgeschlossen wurde, und die Seite **Gehäuseübersicht** 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 Gerätekonfiguration 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 **Benutzernamen** 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 14. 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: • Webschnittstelle – 6 • RESTful API – 32 • SSH – 4 Eine Liste der unterstützten Web-Browser finden Sie im Abschnitt "Unterstützte Browser" unter *Versionshinweise zu OME – Modular für PowerEdge MX7000-Gehäuse* verfügbar unter 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: • Remote-RACADM ist ein Client-Dienstprogramm, das auf einer Management Station ausgeführt wird. Es verwendet die bandexterne 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. • 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 Benutzernamen oder das Kennwort festzulegen. Nach der Eingabe an der RACADM-Eingabeaufforderung können Sie die Befehle ohne das Präfix „racadm“ direkt ausführen. **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: • Anzeigen von Warnungen, OME – Modular-IP oder MAC-Adresse. • DHCP festlegen • Konfigurieren der statischen IP-Einstellungen für OME – Modular. • Anzeigen der OME – Modular-MAC-Adresse für den aktiven MM. • Anzeigen der an das Ende der OME – Modular-IP angehängten MM-ID, wenn VLAN bereits konfiguriert ist. • At-the-Box-Verwaltung – erstellen Sie eine Gruppe, fügen Sie eine Gruppe hinzu, verlassen Sie die Gruppe oder löschen Sie die Gruppe. • At-the-Box Speicherzuordnungsauflösung für das Wechseln von Rechnerschlitten. 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

Tabelle 14. Verwaltungsmodul-Schnittstellen (fortgesetzt)

Schnittstelle	Beschreibung
	für Systeme der nächsten Generation, das eine skalierbare, sichere und offene Serververwaltung ermöglicht. Es ist eine neue Schnittstelle, die die RESTful-Schnittstellensemantik für den Zugriff auf die im Modellformat definierten Daten für die bandexterne 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. Redfish bietet die folgenden Vorteile gegenüber bestehenden Serververwaltungsmethoden: · Einfachheit und Benutzerfreundlichkeit · Hohe Datensicherheit · Programmierbare Schnittstelle, für die problemlos Skripte erstellt werden können · Entspricht weit verbreiteten Standards Weitere Informationen finden Sie im *OME und OME – Modular REST-API-Handbuch* verfügbar unter www.dell.com/openmanagemanuals.
SNMP	Verwenden Sie SNMP zum: 1. Herunterladen der OME-Modular-MIB-Datei von https://www.dell.com/support. 2. Verwenden des MIB Walker-Tools, um Informationen über OIDs zu erhalten. **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 ein Notebook 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:

- Profil bearbeiten – Zeigt das Fenster **Profil bearbeiten** an, in dem Sie die Attribute und Startoptionen des Steckplatzes ändern können.
- Profil anhängen – Zeigt das Fenster **Vorlage auswählen** an, in dem Sie eine Vorlage auswählen und dem Steckplatz beifügen können.
- Profil trennen – Zeigt das Fenster **Profil trennen** an, in dem Sie das an einen Steckplatz angefügte Profil trennen können.
- 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 der Steckplatz-basierten iDRAC-Schnittstelle 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** > **Geräteverwaltungsinformationen** 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 Webschnittstelle, die SSH und seriellen Sitzungen deaktiviert.
2. Geben Sie in den Abschnitten **API**, **Web-Schnittstelle**, **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 1-1440 Minuten betragen und die maximale Anzahl von Sitzungen kann zwischen 1 und 100 liegen. Die Dauer des Inaktivitäts-Timeouts kann 1-100 Minuten für API- und serielle Sitzungen, 1-120 Minuten für Webschnittstellensitzungen und 1-180 Minuten für SSH-Sitzungen betragen.

   Die maximale Anzahl an Sitzungen pro Schnittstelle ist wie folgt:

   - API—1-100
   - Webschnittstelle: 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-Webschnittstelle. Die OME – Modular-Webschnittstelle wird jedoch automatisch wiederherstellt.

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-Benutzeranmeldedaten ein.

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 15. 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.

Tabelle 15. Ports und Protokolle, die in OME Modular unterstützt werden (fortgesetzt)

Portnummer	Protokoll	Port-Typ	Maximale Verschlüsselungsstufe	Quelle	Richtung	Ziel	Verwendung
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 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

Tabelle 15. Ports und Protokolle, die in OME Modular unterstützt werden (fortgesetzt)

Portnummer	Protokoll	Port-Typ	Maximale Verschlüsselungsstufe	Quelle	Richtung	Ziel	Verwendung
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.

Benutzerkonten anzeigen und bearbeiten

1. Klicken Sie auf **Anwendungseinstellungen** > **Benutzer**
   Auf dieser Seite können Sie eine Liste von Benutzerkonten und ihre Rollen, Benutzertypen 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 **Benutzernamen** ein.

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

   ANMERKUNG: Für die serielle OME – Modular-Schnittstelle stellen Sie sicher, dass die Länge des lokalen oder Remote-Benutzernamens höchstens 35 Zeichen beträgt.

   ANMERKUNG: Verwenden Sie nicht "System" als Benutzernamen.

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 +, &, ?, >, -, }, |, ., !, (, ', ,, _, [, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, l
   - 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 **AnwendungseinstellungenBenutzer**.
   Eine Liste der Benutzerkonten 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 16. 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 Anmeldungsrichtlinie	Ja	Nein	Nein	Nein	Nein

Tabelle 16. Benutzergruppen und Berechtigungen (fortgesetzt)

Benutzerrolle	Gehäuse-Administrator	Rechner-Manager	Storage Manager	Fabric-Manager	Viewer
n und Zertifikate einrichten					
Warnungsrichtlinien und Warnungsziele überwachen	Ja	Nein	Nein	Nein	Nein
Gerätestromregelung	Ja	Ja	Ja	Ja	Nein
Gerätekonfigurationsaktionen 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.

Verzeichnisgruppe importieren

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

So importieren Sie die Active Directory-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, aus der Sie das Active Directory importieren möchten.
3. Unter **Verfügbare Gruppen** können Sie nach Directory-Gruppen suchen.

Eine Liste von Gruppen wird unten angezeigt.

4. Wählen Sie eine Gruppe aus, und klicken Sie auf ">>".
   Die ausgewählte Gruppe wird unter **Zu importierende Gruppen** angezeigt.
5. Klicken Sie auf das Kontrollkästchen neben der Gruppe.
6. Wählen Sie aus dem Drop-Down-Menü **Gruppenrolle zuweisen** die Rolle aus, die Sie der Gruppe zuweisen möchten, und klicken Sie auf **Zuweisen**.

Verzeichnisdienste hinzufügen

Sie können Verzeichnisdienste mit weiteren Details erstellen.

1. Klicken Sie im Hauptmenü auf **Anwendungseinstellungen** > **Benutzer** > **Verzeichnisdienste** > **Hinzufügen**.
   Die Seite **Verbindung zum Verzeichnisdienst** wird angezeigt.
2. Wählen Sie den Verzeichnistyp aus der Dropdown-Liste **Verzeichnistyp** aus.
   Folgende Optionen stehen zur Verfügung:
   - **AD**
   - **LDAP**
3. Geben Sie einen Namen für den Verzeichnisdienst in das Feld **Verzeichnisname** ein.

   ANMERKUNG: Der Verzeichnisname darf maximal 255 Zeichen enthalten.
4. Wählen Sie unter **Domänen-Controller-Lookup** die Option **DNS** oder **Manuell** aus.
5. Geben Sie den DNS-Domänennamen in das Feld **Methode** ein.

   ANMERKUNG: Wenn der Domänen-Controller-Lookuptyp "Manuell" ist, geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Domänen-Controllers ein.

   a. Wenn Sie den Verzeichnistyp als AD ausgewählt haben, geben Sie den Domainnamen in das Feld **Gruppendomäne** ein.

      ANMERKUNG: Diese Option wird nur angezeigt, wenn der Verzeichnistyp AD ist.

      ANMERKUNG: Wenn der Verzeichnistyp AD ist, lautet die unterstützte Server-Portnummer 3269 für den globalen Katalog und 636 für den Domänen-Controller. Wenn Sie andere Anschlüsse für den Active Directory-Dienst konfigurieren, funktioniert der Verzeichnisdienst möglicherweise nicht ordnungsgemäß, da die Kommunikation mit dem AD-Server mit verschiedenen Ports fehlschlägt.

      ANMERKUNG: Wenn der Server-Port 3269 ist, ist die Eingabemethode der Gruppendomäne `example.com` oder `ou=org, dc=example, dc=com`. Wenn der Server-Port 636 bzw. nicht 3269 ist, ist die Eingabemethode der Gruppendomäne `ou=org, dc=example, dc=com`.

   b. Wenn Sie den Verzeichnistyp als LDAP auswählen, geben Sie **Bindungs-DN** und **Bindungskennwort** in die entsprechenden Felder ein.

      ANMERKUNG: Diese Optionen werden nur angezeigt, wenn der Verzeichnistyp LDAP ist.
6. Klicken Sie auf **Erweiterte Optionen** und geben die Details ein.
   a. Wenn Sie AD als Verzeichnistyp ausgewählt haben, geben Sie die folgenden Details ein:
      - **Server-Port**nummer – Die Server-Portnummer kann zwischen 1 und 65535 liegen.
      - **Netzwerkzeitüberschreitung** und **Zeitüberschreitung bei Suche** in Sekunden.
      - Markieren Sie das Kontrollkästchen **Zertifikatsvalidierung**.
      - Klicken Sie auf **Eine Datei auswählen**, um nach einem Zertifikat zu suchen und es hochzuladen.

   b. Wenn Sie LDAP als Verzeichnistyp ausgewählt haben, geben Sie die folgenden Details ein:
      - **Server-Port**nummer – Die Server-Portnummer kann zwischen 1 und 65535 liegen.
      - **Abgegrenzter Basis-Name zur Suche**
      - **Attribut der Benutzeranmeldung**, **Attribut der Gruppenmitgliedschaft** und **Suchfilter**.
      - **Netzwerkzeitüberschreitung** und **Zeitüberschreitung bei Suche** in Sekunden.
      - Markieren Sie das Kontrollkästchen **Zertifikatsvalidierung**.
      - Klicken Sie auf **Eine Datei auswählen**, um nach einem Zertifikat zu suchen und es hochzuladen.

ANMERKUNG: Wenn das Kontrollkästchen Zertifikatvalidierung aktiviert ist, geben Sie den FQDN des Domänencontrollers in das Feld Methode ein. Die Zertifikatvalidierung ist nur erfolgreich, wenn die Details der ausstellenden Zertifizierungsstelle im Zertifikat und der FQDN übereinstimmen.

Verzeichnisdienste löschen

So löschen Sie Verzeichnisdienste:

1. Klicken Sie im Hauptmenü auf**Anwendungseinstellungen** > **Benutzer** > **Verzeichnisdienste**.
2. Wählen Sie den Verzeichnisdienst aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.

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.
- Das Serverzertifikat basierend auf der generierten CSR laden, 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 Informationen ein, und klicken Sie auf **Generieren**.
   - 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. Firmwareaktualisierung, `racresetcfg` und FIPS-Modusänderungen.

   ANMERKUNG: Nur Benutzer mit Berechtigungen 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 Benutzernamen 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 nur SNMP V2 unterstützt.

   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 die **Communityzeichenfolge** ein.
   Beim Konfigurieren der Community-Zeichenkette für SNMP v1 wird an die Community-Zeichenkette 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.

4

Rechnerschlitten verwalten

OME – Modular ermöglicht das Zuweisen und Verwalten von Rechnerschlitten zum Ausgleichen der Arbeitslastanforderungen.

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 die Bestandsaufnahme des Rechnerschlittens manuell.

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-Service-Code, 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.

Sie finden auch Informationen in den entsprechenden folgenden Abschnitten:

- **Informationen zum Betriebssystem** – Zeigt Namen, Version und Hostnamen des auf dem Rechnerschlitten installierten Betriebssystems an.
- **Standortinformationen** – Zeigt die Standortdetails des Rechnerschlittens an.
- **Gehäuseinformationen** – Zeigt die Details des Gehäuses, auf dem sich der Rechnerschlitten befindet, an. Klicken Sie auf **Alle anzeigen**, um die Liste aller Aktivitäten auf der Seite **Jobs** anzuzeigen.
- **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 **Rechner** > **Warnungen** anzuzeigen.
- **Kürzlich durchgeführte -Aktivitäten** – Zeigt den Status der im Rechnerschlitten durchgeführten Jobs an.
- **Remote-Konsole** – Zeigt rechts auf der Seite eine grafische Darstellung der Remote-Konsole an. Unter des Remote-Console-Image finden Sie folgende Links:
  - **iDRAC starten** – Zeigt die iDRAC-GUI an.
  - **Virtuelle Konsole starten** – Öffnet die virtuelle Konsole.

  ANMERKUNG: Die Vorschau der virtuellen Konsole ist für Benutzer mit der Benutzerrolle „Viewer“ nicht verfügbar.
- **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.
- **Umgebung** – Zeigt Informationen zur Temperatur und zur Stromversorgung des Rechners an. Sie können auch Leistungs- und Temperaturstatistiken des Rechners einsehen.

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

ANMERKUNG: 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 der Firmwareaktualisierung 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 Benutzeranmeldeinformationen für den Zugriff auf iDRAC einzugeben.

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.
  - **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 **Fehlerbehebung** 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 bei der Fehlerbehebung, 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**

- **Konfigurationsprofil**-Aufgaben:
  - Steckplatz zuordnen – Sie können Blade-Servern Profile zuordnen. Das Profil wird vom Server extrahiert und dem Steckplatz beigefügt, an dem sich der Server befindet.
  - 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.

    ANMERKUNG: Die Option Profil migrieren wird für die Bereitstellung der auf Steckplatz basierten Vorlage nicht unterstützt.
  - Profil bearbeiten – Sie können die Profilmerkmale bearbeiten, die für das Gerät oder den Steckplatz spezifisch sind. Wenn ein Profil an einen Rechner angebunden ist, wird die aktualisierte Profilkonfiguration auf den Rechner propagiert.
  - Steckplatzzuordnungen entfernen – Sie können das Serverprofil aus dem Steckplatz entfernen.
  - Profil trennen – Sie können Profile entfernen, die Blade-Servern zugeordnet sind. Nach dem Trennen des Serverprofils werden die Identitäts-Pools aus den MAC-Adressen-Pools zurückgefordert. Durch das Trennen eines Profils werden die Identitäten von dem Gerät basierend auf der zuletzt bereitgestellten Vorlage oder dem neuesten Profil wieder beansprucht. Wenn die letzte bereitgestellte Vorlage nicht über die MAC-Identitätszuweisung verfügt, werden die MAC-Identitäten, die bereits bereitgestellt wurden, nicht zurückgefordert.

    Wenn in der MCM-Umgebung der Rechnerschlitten auf dem Mitgliedsgehäuse nicht erreichbar ist, können Sie das Profil über die Option **Profil trennen** vom Lead-Gehäuse trennen. Der Status der Aufgabe **Bei der Trennung des Profils Identitäten zurückfordern** auf der Seite **Jobs** im Lead-Gehäuse wird als **Abgeschlossen** angezeigt. Allerdings schlägt der Job **Bei der Trennung des Profils Identitäten zurückfordern** im Mitgliedsgehäuse fehl.

    Wenn der Rechnerschlitten auf dem eigenständigen Gehäuse nicht erreichbar ist und Sie versuchen, das Profil zu trennen, schlägt der Job **Bei der Trennung des Profils Identitäten zurückfordern** fehl.

ANMERKUNG: Die Funktion Identitäten zurückfordern in OME Modular funktioniert in beiden Szenarien.

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.

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:

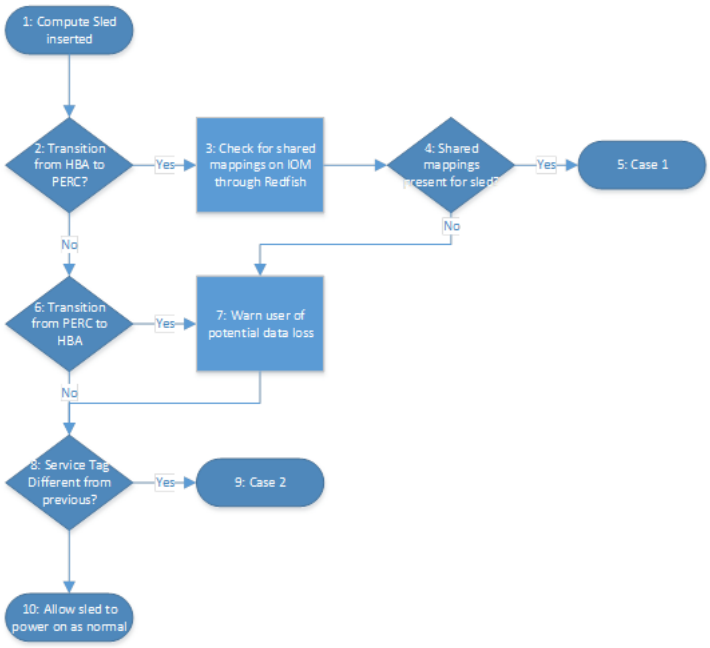


Abbildung 1. Austausch von Rechnerschlitten – Flussdiagramm

Tabelle 17. 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:

- 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**

5

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 die Systemzurücksetzung 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: Die LCD-Anzeige 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**, **Systemkennnummer**, **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 Speichereinschub anzuzeigen, klicken Sie auf **Hardware** > **Festplatten**. Sie können individuelle Festplatten einem Rechnerschlitten zuweisen. Sie können die Firmware dieser Laufwerke über die iDRAC-Webschnittstelle 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.

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 einem HBA330-Mini-Mezzanine-Adapter 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 nagelneuen Schlitten ersetzen, der nicht über eine Service-Tag-Nummer verfügt, werden die Service-Tag-Nummer 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 die Firmwareaktualisierung 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 Firmwareaktualisierungen sofort an.

- **Für später planen** – Plant die Firmwareaktualisierungen für einen späteren Zeitpunkt. Wählen Sie Datum und Uhrzeit aus.

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 Strukturtyp 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.
    - Systemzurücksetzung – Die Option "Systemzurücksetzung" leitet einen Kalt-Neustart des EAM ein. 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.
- Eine schlimmstmögliche Nichtübereinstimmung beheben, bei der 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. Es wird empfohlen, dass Sie mit der Option **Löschen** die vorhandene Konfiguration löschen und eine korrekte Konfiguration erstellen.

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.

6

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:

- iDRAC-Konfiguration – Für iDRAC spezifische Konfiguration
- BIOS-Konfiguration – Satz von BIOS-Attributen
- Speicherkonfiguration – Konfiguration des internen Speichers
- NIC-Konfiguration – Konfiguration der NICs

Um die Liste der vorhandenen Vorlagen anzuzeigen, klicken Sie auf **Konfiguration** > **Bereitstellen**. 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:

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

Themen:

Vorlagendetails anzeigen

So zeigen Sie die Vorlagendetails an:

1. Wählen Sie auf der Seite **Bereitstellen** 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, 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. Serverprofil und BIOS-Informationen.

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

   - Die Vorlage bereitstellen
   - Die Vorlagendetails 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 **Bereitstellen** 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 NIC, iDRAC 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 **Bereitstellen** 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 bereitstellen

Sie können durch Eingabe der für jeden Server eindeutigen Identitätsinformationen Serverprofile von Vorlagen erstellen. Diese Angaben umfassen: Eingabe/Ausgabe-Identitätsinformationen und systemspezifische Attribute wie NIC, RAID iDRAC oder BIOS-Informationen. Sie können Vorlagen über die Seiten **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, müssen Sie den Bereitstellungsworkflow erneut durchführen. 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.

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.

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

1. Wählen Sie die erforderliche Vorlage aus und klicken Sie auf **Vorlage bereitstellen**.
   Wenn die Vorlage Identitätsattribute beinhaltet, die jedoch nicht mit einem virtuellen Identitäts-Pool verknüpft sind, wird eine Meldung angezeigt, die besagt, dass die physischen Identitäten für die Bereitstellung verwendet werden. Andernfalls wird der Assistent**Vorlagen-Bereitstellung** angezeigt.
2. Wählen Sie das Zielgerät aus, auf dem Sie die Vorlage bereitstellen möchten, konfigurieren Sie die iDRAC-IP-Einstellungen und planen Sie die Bereitstellung.

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 beinhaltet, die jedoch nicht mit einem virtuellen Identitäts-Pool verknüpft sind, wird eine Meldung angezeigt, die besagt, dass die physischen Identitäten für die Bereitstellung verwendet werden. Daraufhin wird der Assistent**Vorlagen-Bereitstellung** angezeigt.
2. Wählen Sie das Zielgerät aus, auf dem Sie die Vorlage bereitstellen möchten, konfigurieren Sie die iDRAC-IP-Einstellungen, aktivieren Sie die Option **Keinen Neustart des Host-BS erzwingen** und planen Sie die Bereitstellung.

   Der Rechnerschlitten bootet basierend auf der Auswahl ordnungsgemäß oder nicht ordnungsgemäß.

Vorlagen bearbeiten

Sie können den Namen und die Beschreibung der Vorlage nur über die Seiten **Bereitstellung** und **Vorlagendetails** ändern.

1. Wählen Sie auf der Seite **Bereitstellen** die Vorlage aus, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**. Andernfalls klicken Sie auf der Seite **Vorlagendetails** auf **Bearbeiten**.
   Das Fenster **Vorlage bearbeiten** wird aufgerufen.
2. Nehmen Sie ggf. erforderliche Änderungen vor.

Vorlagennetzwerke bearbeiten

So bearbeiten Sie die Vorlagennetzwerkdetails:

1. Wählen Sie auf der Seite **Bereitstellen** 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-Gruppierungsoption 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-Gruppierungsoptionen auswählen:

   - Kein Teaming – NICs sind nicht verbunden 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 Host-Betriebssystem 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. Wählen Sie die gekennzeichneten und nicht gekennzeichneten VLANs aus, falls erforderlich.

Klonen von Vorlagen

So erstellen Sie eine Kopie einer Vorlage.

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

Vorlagen exportieren

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

So exportieren Sie eine Vorlage:

Wählen Sie auf der Seite **Bereitstellen** 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 **Bereitstellen** die Vorlage 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.

7

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.

Sie müssen über die Vorlagenverwaltungs-Berechtigung verfügen, um Identitäts-Pools zu verwalten. Ein Identitäts-Pool enthält einen Namen, eine Beschreibung und eine Kategorie. Die Kategorie kann die folgenden Typen aufweisen:

- Ethernet
- iSCSI
- FCoE
- FC

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:

- Zusammenfassung und Details des Identitäts-Pools anzeigen
- Identitäts-Pools erstellen
- Identitäts-Pools bearbeiten
- Identitäts-Pools löschen
- Identitäts-Pools exportieren

Wählen Sie einen Identitäts-Pool aus, um eine Zusammenfassung und Einzelheiten zur Verwendung des Identitäts-Pools anzuzeigen. Sie können die Details zur Verwendung durch Auswahl der Kategorie des Identitäts-Pools sortieren.

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 **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`
   - `AA.BB.CC.DD.EE.FF`

   Sie können Identitäts-Pools aus iSCSI, FCoE oder FC erstellen.

   Die Registerkarte **iSCSI** wird angezeigt.
5. Aktivieren Sie die Option **iSCSI-MAC-Adressen einschließen** zur Eingabe der **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 im Format `<IQN Präfix>.<Zahl>` an das Präfix angehängt wird.
7. Aktivieren Sie die Option **iSCSI-Initiator-IP-Pool aktivieren**, um **IP-Adressenbereich**, **Gateway**, **Primärer DNS-Server** und **Sekundärer DNS-Server** einzugeben, und wählen Sie die **Subnetzmaske** aus.

   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-Adresspools 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-Adresspool 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 **MAC-Start-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**.

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**.

8

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 25Gb 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-Fabric-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 Benutzerhandbuch*.

Sie können OME – Modular benutzen, um Folgendes zu tun:

- Hostnamen-, SNMP- und Domain-Einstellungen konfigurieren
- 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: 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
- Geräteverwaltungsinformationen
- 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.

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 annehmbare Konfiguration. Wenn jedoch die automatische Verhandlung deaktiviert ist, tauschen die Peer-Geräte möglicherweise keine Funktionen aus. Daher empfiehlt Dell EMC, 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 Server-seitigen 25G-Ports aktiviert, wie durch den IEEE 802.3-Standard vorgegeben.
- Sie können die automatische Verhandlung aktivieren oder deaktivieren, Sie können jedoch nicht die Geschwindigkeit auf Server-seitigen Ports konfigurieren.
- Wenn die automatische Verhandlung aktiviert ist, zeigen Ethernet-Switches als Geschwindigkeitskapazität nur 25G an.

So zeigen Sie die Hardwaredetails an:

Klicken Sie auf **E/A-ModuleDetails anzeigenHardware**.

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 Ethernet-Switch-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 aktivieren 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 des Linux-Administratorkennworts

Das Linux-Administratorkennwort wird nur für das Troubleshooting mithilfe der Shell des Linux-Betriebssystems 10 verwendet.

So konfigurieren Sie das Kennwort für Linux-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: Das Linux-Administratorkennwort wird nur für das Troubleshooting unter Verwendung des Betriebssystems 10 Linux Shell verwendet.

   Verbinden Sie SSH mit dem Switch und melden Sie sich mit dem Standardpasswort "admin" als "admin" an, um das OS10-Admin-Passwort zu ändern. Sie werden vom System aufgefordert, das Admin-Kennwort zu ändern.

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.

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.

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.

   Wenden Sie zuerst "Hardware-Standard" an, und wählen Sie anschließend den erforderlichen Breakout aus.

   ANMERKUNG: Breakouts können nur für EAMs im Fabric-Modus konfiguriert werden.

Admin-Status konfigurieren

Sie können den Admin-Status umschalten, der für alle Ports standardmäßig aktiviert ist. Für die MX9116n FSE-Portgruppen 1/1/15 und 1/1/16 ist der Admin-Status standardmäßig deaktiviert, wenn Sie einen Breakout der Fiber-Channel-Ports durchführen. Aktivieren Sie den Status, falls erforderlich.

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.

Maximale Übertragungseinheit konfigurieren

Sie können die maximale Übertragungseinheit (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) ein- und ausschalten. Für DAC-Verkabelung ist AutoNeg standardmäßig aktiviert. Für AOC (Fiber) ist AutoNeg standardmäßig deaktiviert.

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.

9

MX-skalierbare 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:

- 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 Hardware-aktivierte 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. Dies bedeutet auch, dass keine Firmware aktualisiert werden muss. Die FEM ist unsichtbar für die FSE und muss in keiner Weise verwaltet werden.

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 verbunden
- FEM in Steckplatz A2 wird mit der FSE in Steckplatz A2 verbunden
- FEM in Steckplatz B1 wird mit der FSE in Steckplatz B1 verbunden
- FEM in Steckplatz B2 wird mit der FSE in Steckplatz B2 verbunden

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.

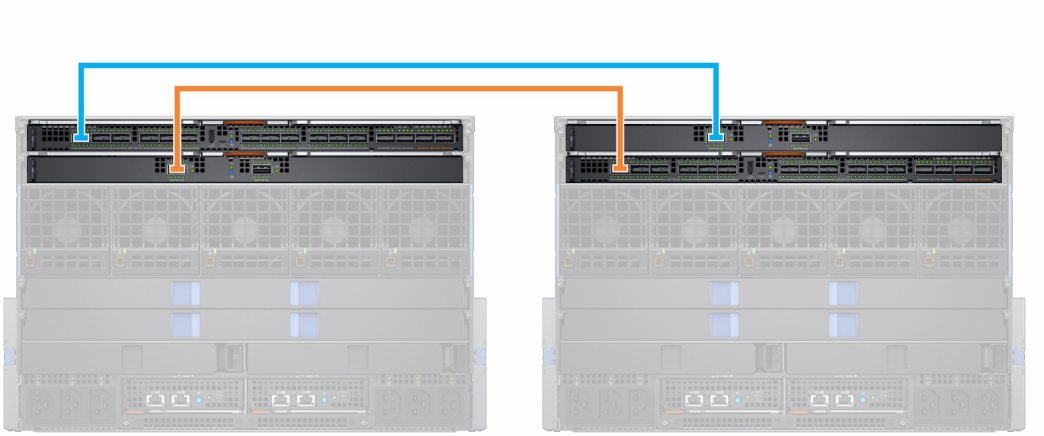
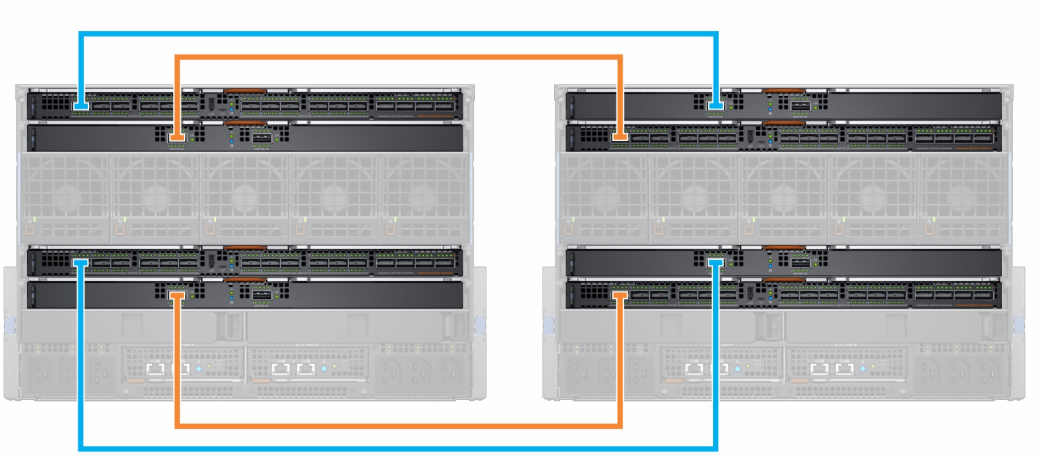


Tabelle 18. Fabric-Topologie

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:



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.

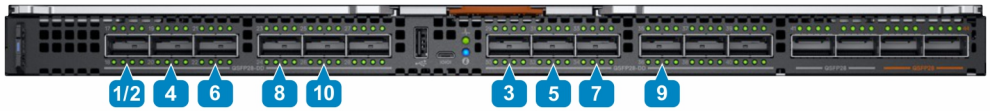
Empfohlene Reihenfolge der Verbindung

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 19. 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.

10

SmartFabric Services

SmartFabric Services ist eine Funktion von Dell EMC Networking OS10 Enterprise Edition, die auf Ethernet-Switches 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
- Lifecycle-Management
  - Fabric-weite Planung von Firmware-Upgrades
  - Automatisches oder durch den Benutzer erzwungenes Rollback zu dem zuletzt bekannten Zustand
- Fabric-Automatisierung
  - Garantierte Compliance mit ausgewählter physischer Topologie
  - Richtlinienbasierte Dienstgüte (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 Ethernet Switch 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. Zu diesem Zeitpunkt 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.

Themen:

- Richtlinien für den Betrieb im SmartFabric-Modus
- SmartFabric-Netzwerktopologien
- Switch-zu-Switch-Verkabelung
- Vorgeschaltete Netzwerk-Switch-Anforderungen
- NIC-Teaming-Einschränkungen
- CLI-Befehle im Fabric-Modus
- Fabric-Details anzeigen
- Fabric hinzufügen

- Fabric löschen
- 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.

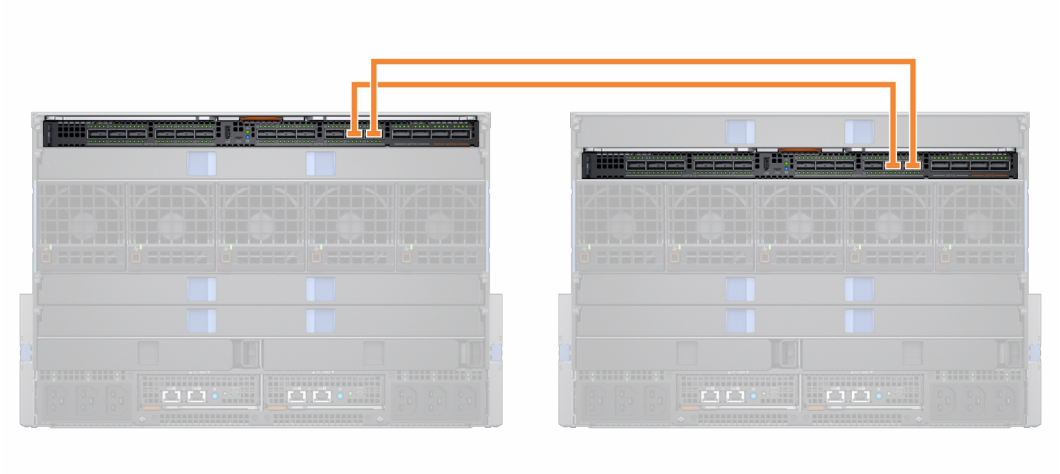
SmartFabric-Netzwerktopologien

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

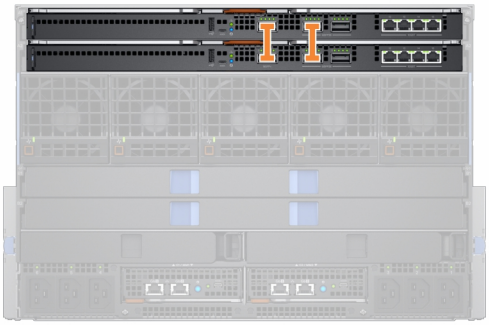
2 x MX9116n Fabric Switching Engines in separaten Gehäusen

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

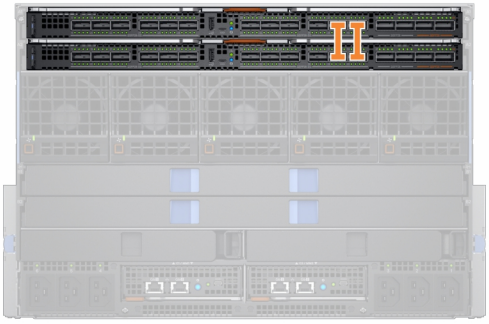
Der MX5108n Ethernet-Switch wird nur in Konfigurationen mit einem einzigen Gehäuse unterstützt. Die Switches müssen in den Steckplätzen A1/A2 oder B1/B2 platziert werden. Eine SmartFabric darf keinen Switch in Fab A und keinen Switch in Fab B enthalten



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

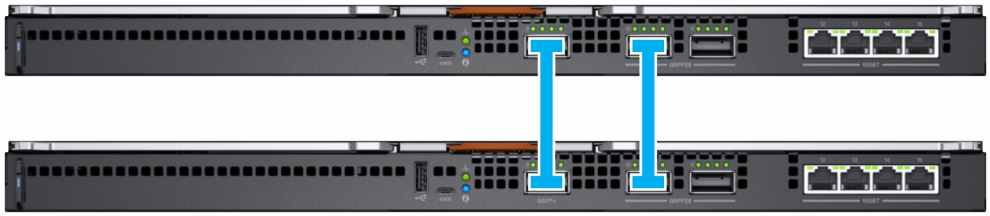


Das Fabric-Design "2 Mx9116n Fabric Switching Engines im selben Gehäuse" wird unterstützt, wird aber nicht empfohlen. Bei Verwendung dieses Designs wird eine Fehlermeldung auf den Seiten **Fabric-Topologie** und **Topologie anzeigen** von OME-Modular angezeigt.

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 Netzwerk-Switch-Anforderungen

Es wird empfohlen, ist aber nicht erforderlich, die PowerEdge MX-Switches zu einem Paar redundanter vorgeschalteter Switches zu verbinden. Wenn Sei ein Paar von Switches im Fabric-Modus zu einem vorgeschalteten Switch-Paar verbinden, **muss** das vorgeschaltete Switch-Paar auf folgende Weise konfiguriert werden:

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 Port-Channel verlegt werden.

   ANMERKUNG: Die LACP-Option wird nur auf Ethernet-Uplinks unterstützt.
3. Stellen Sie sicher, dass ein kompatibles Spanning Tree Protocol konfiguriert ist. Weitere Informationen finden Sie im Abschnitt **Spanning Tree Protocol**.

Spanning Tree Protocol

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 User Guide* (OS10 Enterprise Edition Benutzerhandbuch) 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.

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 Switch-unabhängigen 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 Host-Betriebssystem 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: Im Fabric -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.

CLI-Befehle im Fabric-Modus

Beim Betrieb im Fabric-Modus wird der Großteil der Switch-Konfiguration über die OME – Modular-GUI verwaltet. Manche OS10-Funktionen, wie z. B. Layer 3-Routing, sind deaktiviert. Aufgrund dieser Deaktivierung unterstützt ein Switch im Fabric-Modus alle OS10-Anzeigebefehle, jedoch nur eine Teilmenge der CLI-Konfigurationsbefehle:

- `clock` – Konfigurieren der Uhreinstellungen
- `end` – Beenden in den EXEC-Modus
- `exit` – Beenden vom aktuellen Modus
- `help` – Anzeigen der verfügbaren Befehle
- `hostname` – Legen Sie den System-Hostnamen fest.
- `interface` – Konfigurieren oder Auswählen einer Schnittstelle
- `ip name-server` – Konfigurieren der IP-Adresse von bis zu drei Namensservern
- `logging` – Konfigurieren der Systemprotokollierung
- `management route` – Konfigurieren der IPv4/IPv6-Verwaltungsroute
- `no` – Löschen oder Deaktivieren von Befehlen im Konfigurationsmodus
- `ntp` – Konfigurieren des Netzwerkzeitprotokolls
- `snmp-server` – Konfigurieren des SNMP-Servers
- `username` – Erstellen oder Ändern der Benutzeranmeldeinformationen
- `spanning-tree`
  - `disable` – Globales Deaktivieren des Spanning Tree
  - `mac-flush-timer` – Festlegen der Uhrzeit zum Leeren der MAC-Adressen-Einträge
  - `mode` – Aktivieren eines Spanning-Tree-Modus, wie z. B. RSTP oder MST
  - `mst` – Konfigurieren mehrerer Spanning-Tree (MST)-Modi
  - `rstp` – Konfigurieren des Rapid Spanning-Tree (RSTP)-Modus
  - `vlan` – Konfigurieren des Spanning Tree auf einem VLAN-Bereich.
  - `username` – Erstellen oder Ändern der Benutzeranmeldeinformationen
  - `SupportAssist` – Konfigurieren Sie die Einstellungen von SupportAssist.
  - `Security` – Konfigurieren Sie die Funktionen für die Netzwerksicherheit.
  - `Fibre Channel` – Konfigurieren Sie die Funktionen der Fibre Channel-Schnittstellen.

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 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 Ethernet-Switches 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 **Namen** und **Beschreibung** ein, wählen Sie die Option **Uplinktyp**, und klicken Sie dann auf **Weiter**.
   Folgende Optionen stehen zur Verfügung:
   - **Ethernet** – Sie können einen oder mehrere Ethernet-Ports auf verschiedenen Switches wählen, um ein LAG zu bilden. Der Netzwerktyp kann beliebig sein. Zum Beispiel: Ethernet.
   - **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 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** > **netzwerk** Netzwerke 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 Ports oder Netzwerke bearbeiten, wenn sich die Uplinks im FCoE-, FC Gateway- oder FC Direct-Attach-Modus befinden.

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.

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.

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, wird das EAM neu gestartet.

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 20. 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

Definieren von VLANs

So definieren Sie VLANs:

1. Klicken Sie im Menü auf **Konfiguration** > **Netzwerke**.
2. Klicken Sie im Feld **Netzwerk** 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 21. Maximale Anzahl der VLANs, die im SmartFabric-Modus empfohlen werden

OS10 Version	Parameter	Value
10.5.0	Maximale VLANs pro Fabric	256
	Maximale VLANs pro Uplink	256
	Maximale VLANs pro Serverport	64
10.4.0.R3S 10.4.0.R4S	Maximale VLANs pro Fabric	128
	Maximale VLANs pro Uplink	128
	Maximale VLANs pro Serverport	32

11

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 physikalischen Servers verwendet.

ANMERKUNG: VLANs werden nur Servern zugewiesen, die im Fabric-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** > **Netzwerke**. Die Seite **Netzwerke** 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

Tabelle 22. Netzwerk-Datenverkehrstypen – QoS-Einstellungen (fortgesetzt)

Netzwerk-Datenverkehrstyp	Beschreibung	QoS-Einstellung
Cluster-Interconnect	Wird für Cluster-Heartbeat-VLANs verwendet	5
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** > **Netzwerke**.
   Die Seite **Netzwerke** 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 (Platin)**
   - **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.

Netzwerke bearbeiten

So bearbeiten Sie ein Netzwerk:

1. Wählen Sie auf der Seite **Netzwerke** 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.

Netzwerkkonfigurationen exportieren

So exportieren Sie die Netzwerkkonfiguration:

Wählen Sie auf der Seite **Netzwerke** das Netzwerk aus, und klicken Sie auf **Exportieren**.
Der Netzwerkdetails werden im Format `.csv` auf ein lokales Laufwerk Ihres Systems exportiert.

Netzwerkkonfigurationen löschen

So löschen Sie ein Netzwerk:

Wählen Sie auf der Seite **Netzwerke** das Netzwerk 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.

12

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.

13

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 umfasst 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** 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** anzeigen.

Auf der Seite **Firmware** werden die folgenden Basisline-Informationen angezeigt: Compliance, Name der Baseline, Jobstatus, Katalogtyp, Zeitstempel der letzten Verwendung der Baseline.

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

- Baseline erstellen
- Baseline bearbeiten
- Bericht anzeigen
- Baseline löschen
- Kataloge verwalten
- Compliance überprüfen

Themen:

Baselines erstellen

So erstellen Sie eine Firmware-Baseline:

1. Klicken Sie auf **Konfiguration** > **Firmware** > **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 Übereinstimmungsprüfung 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.

Compliance überprüfen

So überprüfen Sie die Compliance einer Firmware-Baseline:

1. Wählen Sie auf der Seite **Firmware** die Baseline aus, und klicken Sie auf **Compliance überprüfen**.
   Informationen über die Compliance-Überprüfung werden rechts von der Seite **Firmware** angezeigt.
2. Klicken Sie auf **Bericht anzeigen**.
   Daraufhin wird die Seite **Übereinstimmungsreport** angezeigt.

   Sie können Einzelheiten wie z. B. den Namen des Katalogs und die Baseline, Status der Compliance, Art der Baseline, Name des Geräts, Modell, Service-Tag-Nummer des Geräts, aktuelle aktualisierte Version und Baseline-Version anzeigen.

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

   - Aktualisieren Sie die Firmware.
   - Exportiert den Bericht im Format `.csv` auf ein lokales Laufwerk auf Ihrem System.
   - Die Geräteinformationen mit **erweiterten Filtern** sortieren

   Beim Aktualisieren der Firmware für SAS-EAMs, die als individuelle Komponente und eine Gehäusekomponente verfügbar sind, mithilfe der Übereinstimmungsreport-Methode, schlägt die Aktualisierung des Verwaltungsmoduls fehl. Wählen Sie das SAS-EAM aus der Gehäusekomponente oder dem Übereinstimmungsreport aus.

Baselines bearbeiten

So bearbeiten Sie eine Baseline:

1. Wählen Sie auf der Seite **Firmware** 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.

Kataloge verwalten

Anhand der Katalogverwaltungsfunktion in OME – Modular können Sie den Speicherort des Katalogs konfigurieren und Firmware-Baselines erstellen. Eine Katalogdatei enthält Metadaten zu Bündeln und einzelnen DUPs oder Paketen. Die Bündel stellen Sätze von Paketen dar, die zusammen geprüft und zertifiziert wurden.

Die Kataloge können von den folgenden Speicherorten bezogen werden:

- Dell Website – Sie können die Proxyparameter angeben, um die Anwendung zu aktivieren, um über Ihr Netzwerk auf das Internet zuzugreifen. Die Proxy-Parameter beinhalten die Netzwerkadresse und optionale Anmeldeinformationen wie Benutzername und Kennwort. Die Proxy-Einstellungen werden bei der Ersteinrichtung oder auf der Seite **Anwendungseinstellungen** konfiguriert.

  Auf der Dell Website sind eventuell mehrere Kataloge veröffentlicht.
- Netzwerkfreigabe oder Website-Standort in Ihrem Netzwerk – Die Netzwerkfreigabe umfasst NFS, CIFS, HTTP oder HTTPS.

  Sie können mit dem Repository Manager den Katalog erstellen und ihn auf der Netzwerkfreigabe speichern. Wenn Sie über die Berechtigung als Gehäuse-Administrator verfügen, können Sie die Liste der Kataloge anzeigen und grundlegende Verwaltungsaufgaben wie z. B. das Bearbeiten und Löschen von Katalogen durchführen. Sie können einen Katalog löschen, der einer Baseline zugeordnet ist. Wenn ein Katalog nicht mehr zugänglich ist, wird das Betriebsstatus-Symbol für den Katalog angezeigt.

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** 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
- 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.
   - **Neueste Komponenten-Firmware -Versionen unter Dell.com** – Dieser Katalog enthält möglicherweise Firmware-Versionen für Komponenten, die seit dem letzten validierten Stapel von Gehäuse-Firmware individuell freigegeben 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.

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**.

Aktualisieren der Firmware

Bevor Sie die Firmware von einem Gehäuse, Rechner oder Speicherschlitten aktualisieren, stellen Sie sicher, dass alle EAMs und Netzwerkstrukturen funktionsfähig sind. Sie können nur sechs IOMs gleichzeitig aktualisieren.

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 **Übereinstimmungsreport** 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 der Firmwareaktualisierung neu startet und der Standby-MM aktiv ist, werden einige Meldungen auf der Seite Ausführungsdetails für die Firmwareaktualisierung nicht angezeigt. Die Meldungen werden aufgrund von Synchronisierungsproblemen nicht angezeigt.

   ANMERKUNG: Während der OME – Modular-Firmwareaktualisierung können mehrere Benutzer das OME – Modular-DUP über jede Schnittstelle hochladen. Es wird jedoch möglicherweise eine Warnmeldung angezeigt, nachdem der Firmwareaktualisierungs-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.

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.

14

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.

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

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**.

15

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 Firmwareaktualisierung 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 JobstatusBlink 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. Die verfügbaren Optionen sind:
     - Geplant
     - In Warteschlange
     - Wird gestartet
     - Wird ausgeführt
     - Abgeschlossen
     - Fehlgeschlagen
     - Neu
     - Mit Fehlern abgeschlossen
     - Abgebrochen
     - Angehalten
     - Angehalten
     - Abgebrochen
   - **Zustand** – Zum Anzeigen von Jobs anhand des Zustands. Die verfügbaren Optionen sind:
     - Aktiviert
     - Deaktiviert
   - **Job-Typ** – Zum Anzeigen von Jobs anhand des Typs. Die verfügbaren Optionen sind:
     - Debug-Protokolle
     - Einstellungen aktualisieren
     - Software-Rollback
     - Geräteaktion
     - Wiederherstellen
     - Gerätekonfiguration
     - Gehäuseprofil
     - Bestandsaufnahme
     - Aktualisierung

- MCM-OffBoarding
- Backup
- Profil aktualisieren
- Quick Deploy
- MCM-Onboarding
- MCM-Gruppe

- **Startdatum der letzten Ausführung** und **Enddatum der letzten Ausführung** – Zum Anzeigen von Jobs anhand des letzten Ausführungszeitraums.

An Filtern vorgenommene Änderungen werden in Echtzeit angewendet. Um die Filter zurückzusetzen, klicken Sie auf **Alle Filter löschen**.

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 IOM-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-Master-Upgrade
- IOM-Master-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.

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.

16

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.

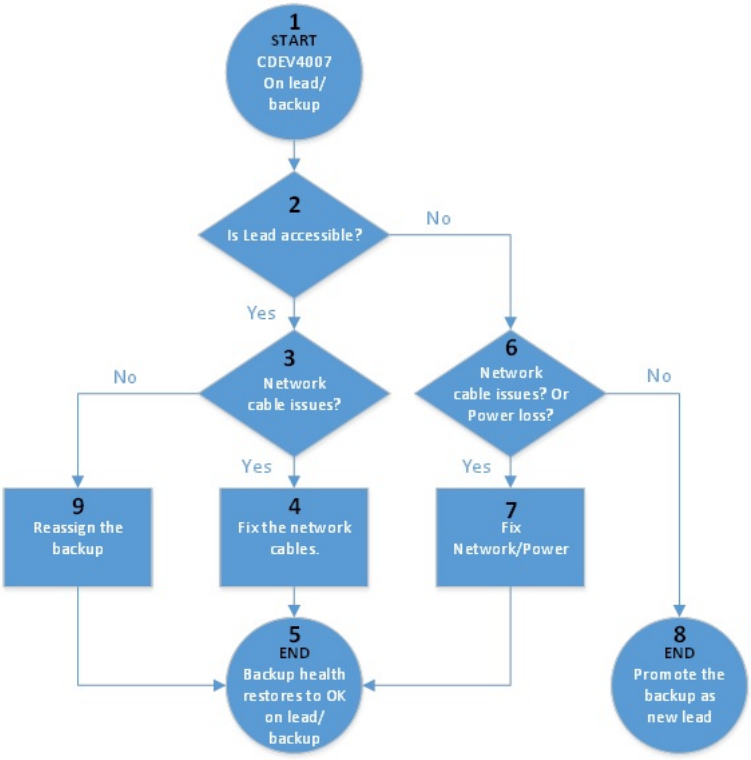


Abbildung 2. Netzwerk-und Stromausfall – Flussdiagramm

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 Netzwerk-Switches 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 Benutzerverwaltungsnetzwerk 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 in 10-45 Minuten durchgeführt werden, basierend auf der Anzahl der Gehäuse in der Gruppe und der Menge der Konfiguration, die wiederhergestellt werden muss.
   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-Nutzlast 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 Netzwerk-Switches 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 von den Komponenten in der Gruppe erzeugt werden, nur lokal in ihren jeweiligen Hardware- oder Warnungsprotokollen verfügbar, während die Aufgabe "Stilllegen" und die Übernahme des Lead-Gehäuses durch das Backup durchgeführt wird. 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 ausgefallenen 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 Lesen 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 im Ruhestand befindlichen 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 Vorlagenkonfiguration. Um Konflikte mit dem neuen Lead zu vermeiden, löschen Sie die Vorlagenkonfiguration mithilfe von **Konfiguration** > **Bereitstellen** > **Löschen**.

17

Fehlerbehebung

Dieser Abschnitt beschreibt die Aufgaben für die Fehlerbehebung und Behebung von Problemen mit der OME – Modular-Benutzeroberfläche.

- Firmwareaktualisierung 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

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 23. 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

Unterstützte Steckplatzkonfigurationen für EAMs

Die untenstehende Tabelle enthält die unterstützten EAM-Steckplatzkonfigurationen.

Tabelle 24. 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
MX7116n	Leer	MX7116n	Leer

Tabelle 24. Unterstützte EAM-Steckplatz-Matrix (fortgesetzt)

Steckplatz A1	Steckplatz A2	Steckplatz B1	Steckplatz B2
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.