Benutzerhandbuch für Dell EMC OpenManage Enterprise Version 3.7

Juli 2021
Rev. A00

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

Tabellen

1

Informationen zu Dell EMC OpenManage Enterprise

OpenManage Enterprise ist eine Webanwendung zum Systemmanagement und -Monitoring, die als virtuelle Appliance bereitgestellt wird. Sie bietet einen umfassenden Überblick über die Dell EMC Server, Gehäuse, Speicher und Netzwerkswitches im Unternehmensnetzwerk. Mit OpenManage Enterprise, einer webbasierten und 1:n-Systemen-Managementanwendung, können Sie Folgendes ausführen:

- Ermitteln von Geräten in einer Rechenzentrumsumgebung
- Anzeigen des Hardwarebestands und Monitoring des Funktionszustands von Geräten
- Anzeigen und Managen der von der Appliance empfangenen Warnungen und Konfigurieren von Warnungsrichtlinien
- Monitoring von Firmware-/Treiberversionen und Managen von Firmware/Treiber-Updates auf Geräten mit Firmware-Baselines
- Managen von Remote-Tasks (z. B. Energieverwaltung) auf Geräten
- Managen von Konfigurationseinstellungen über Geräte hinweg mithilfe von Bereitstellungsvorlagen
- Managen von virtuellen Identitätseinstellungen über Geräte hinweg mithilfe intelligenter Identitäts-Pools
- Erkennen und Beheben von Konfigurationsabweichungen über Geräte hinweg mithilfe von Konfigurations-Baselines
- Abrufen und Monitoring von Gewährleistungsinformationen für Geräte
- Gruppieren von Geräten in statische oder dynamische Gruppen
- Erstellen und Verwalten von OpenManage Enterprise-Nutzern

ANMERKUNG:

- Das Systemmanagement und die -Überwachung von OpenManage Enterprise ist am besten für Enterprise-LANs geeignet und wird nicht zur Verwendung über WANs empfohlen.
- Informationen zu unterstützten Browsern finden Sie in der OpenManage Enterprise Supportmatrix auf der Support-Website.

Dies sind einige der Sicherheitsfunktionen von OpenManage Enterprise:

- Rollenbasierter Zugriff mit Einschränkungen für Konsoleneinstellungen und Geräteaktionen.
- Die bereichsbasierte Zugriffskontrolle ermöglicht es Administratoren, die Gerätegruppen zu beschränken, auf die Geräte-Manager zugreifen und die sie verwalten können.
- Optimierte Appliance mit Security-Enhanced Linux (SELinux) und einer internen Firewall.
- Verschlüsselung sensibler Daten in einer internen Datenbank.
- Verwendung verschlüsselter Kommunikation außerhalb der Appliance (HTTPS).
- Erstellen und Durchsetzen von firmware- und konfigurationsbezogenen Richtlinien.
- Vorsorge für die Konfiguration und Aktualisierung der Bare-Metal-Server

OpenManage Enterprise bietet eine auf Domänenaufgaben basierte GUI, in der die Navigation die Aufgabenreihenfolge berücksichtigt, die von einem Administrator und Device-Manager vorherrschend verwendet wird. Wenn Sie ein Gerät zu einer Umgebung hinzufügen, erkennt OpenManage Enterprise automatisch die Geräteeigenschaften, platziert es in die relevante Gerätegruppe und ermöglicht Ihnen die Verwaltung des Geräts: Die typische Reihenfolge von Aufgaben, die von OpenManage Enterprise-Nutzern ausgeführt werden:

- Installieren von OpenManage Enterprise auf Seite 20
- OpenManage Enterprise mithilfe der textbasierten Benutzeroberfläche konfigurieren auf Seite 27
- Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41
- Geräte und Gerätegruppen verwalten auf Seite 55
- Überwachen Sie Geräte mit dem OpenManage Enterprise-Dashboard auf Seite 38
- Geräte in Gruppen organisieren auf Seite 55
- Verwalten der Geräte-Firmware und -Treiber auf Seite 77
- Anzeigen und Konfigurieren einzelner Geräte auf Seite 68
- Überwachen und Verwalten von Gerätewarnungen auf Seite 118
- Anzeigen und Erneuern der Gerätegewährleistung auf Seite 139
- Verwalten von Gerätebereitstellungsvorlagen auf Seite 86
- Verwalten der Device-Konfigurations-Compliance auf Seite 110
- Verwalten von Compliance-Vorlagen auf Seite 111
- Überwachen von Auditprotokollen auf Seite 127
- Verwalten von OpenManage Enterprise-Geräteeinstellungen auf Seite 148

- Sofortiges Ausführen eines Bestandsaufnahme-Jobs auf Seite 75
- Verwalten der Gerätegewährleistung auf Seite 138
- Berichte auf Seite 140
- Verwalten von MIB-Dateien auf Seite 145
- Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16
- Integration von Verzeichnisdiensten in OpenManage Enterprise auf Seite 157

Themen:

Was ist neu in dieser Version?

- CloudIQ-Plug-in-Unterstützung – Gerätegruppen können ausgewählt werden, um Daten zum Monitoring an CloudIQ zu senden.

Verbesserungen

- Möglichkeit zur Anzeige von Geräten, die aufgrund von Authentifizierungsfehlern von der Seite „Alle Geräte" getrennt wurden.
- Text User Interface-Funktionen (TUI) zur selektiven Aktivierung oder Deaktivierung der Debug-Protokollierung für Appliance- und Plug-in-Services.

Weitere nützliche Informationen

Zusätzlich zu diesem Handbuch können Sie auf die folgenden Dokumente zugreifen, die weitere Informationen über OpenManage Enterprise und andere zugehörige Produkte enthalten.

Tabelle 1. Weitere nützliche Informationen

Dokument	Beschreibung	Verfügbarkeit
Dell EMC OpenManage Enterprise Support Matrix	Führt die Geräte auf, die von OpenManage Enterprise unterstützt werden.	1. Gehen Sie zu Dell.com/OpenManageManuals. 2. Klicken Sie auf **Dell OpenManage Enterprise** und wählen Sie die erforderliche Version von OpenManage Enterprise. 3. Klicken Sie auf **Dokumentation**, um auf diese Dokumente zuzugreifen.
Versionshinweise zu Dell EMC OpenManage Enterprise	Stellt Informationen zu bekannten Problemen und Workarounds in OpenManage Enterprise bereit.	
Dell EMC OpenManage Mobile Benutzerhandbuch	Enthält Informationen zur Installation und Verwendung der OpenManage-Mobile-Anwendung.	
Dell EMC Repository Manager Benutzerhandbuch	Stellt Informationen zur Verwendung des Repository Manager zur Verwaltung von Systemaktualisierungen bereit	
Dell EMC OpenManage Enterprise and OpenManage Enterprise – Modular Edition RESTful API Handbuch	Enthält Informationen zur Integration von OpenManage Enterprise mithilfe von REST-APIs (Representational State Transfers) sowie Beispiele für die Verwendung von REST APIs zum Ausführen gängiger Aufgaben.	
Dell EMC OpenManage Enterprise Services-(vormals SupportAssist Enterprise-)Benutzerhandbuch	Stellt Informationen zur Installation, Konfiguration, Verwendung und zum Troubleshooting von OpenManage Enterprise Services bereit	Dell.com/ServiceabilityTools
Dell EMC OpenManage Enterprise Power Manager	Stellt Informationen zur Installation, Konfiguration, Verwendung und zum Troubleshooting von OpenManage Enterprise Power Manager bereit	https://www.dell.com/support/home/en-yu/products/software_int/software_ent_systems_mgmt/ent_sys_mgmt_power_manager

Tabelle 1. Weitere nützliche Informationen (fortgesetzt)

Dokument	Beschreibung	Verfügbarkeit
Dell EMC OpenManage Enterprise Update Manager	Stellt Informationen zur Installation, Konfiguration, Verwendung und zum Troubleshooting von OpenManage Enterprise Update Manager bereit	https://www.dell.com/support/home/en-yu/products/software_int/software_ent_systems_mgmt/ent_sys_mgmt_openmanage_enterprise_update_manager
Dell EMC CloudIQ	Stellt Informationen zur Installation, Konfiguration, Verwendung und zum Troubleshooting von CloudIQ bereit	

Kontaktaufnahme mit Dell EMC

ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell EMC Produktkatalog finden.

Dell EMC bietet verschiedene Optionen für Online- und Telefonsupport an. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar. So erreichen Sie den Vertrieb, den Technischen Support und den Kundendienst von Dell EMC:

1. Rufen Sie die Website Dell.com/support auf.
2. Wählen Sie Ihre Supportkategorie.
3. Wählen Sie das Land bzw. die Region in der Drop-Down-Liste **Land oder Region auswählen** am unteren Seitenrand aus.
4. Klicken Sie je nach Bedarf auf den entsprechenden Service- oder Support-Link.

OpenManage Enterprise Advanced-Lizenz

ANMERKUNG: Für die Installation und Verwendung von OpenManage Enterprise ist keine *OpenManage Enterprise Advanced* Lizenz notwendig. Nur die Serverkonfigurationsverwaltungsfunktion – Bereitstellung von Gerätekonfigurationen und Überprüfung der Konfigurationskonformität auf Servern – erfordert, dass die *OpenManage Enterprise Advanced* Lizenz auf Zielservern installiert ist. Diese Lizenz ist für die Erstellung von Bereitstellungsvorlagen von einem Server aus nicht erforderlich.

Die *OpenManage Enterprise Advanced* Lizenz ist eine unbefristete Lizenz für die gesamte Lebensdauer eines Servers und kann jeweils nur einmal an eine Service-Tag-Nummer eines Servers gebunden werden. OpenManage Enterprise bietet einen integrierten Bericht zum Anzeigen der Liste der Geräte und deren Lizenzen. Wählen Sie **OpenManage Enterprise** > **Überwachung** > **Berichte** > **Lizenzbericht** und dann auf **Ausführen.** Informationen dazu finden Sie unter Berichte ausführen auf Seite 141.

ANMERKUNG: Für die Aktivierung der Funktion zur Serverkonfigurationsverwaltung in OpenManage Enterprise ist keine separate Lizenz notwendig. Wenn die *OpenManage Enterprise Advanced* Lizenz auf einem Zielserver installiert ist, können Sie die Funktion zur Serverkonfigurationsverwaltung auf diesem Server verwenden.

OpenManage Enterprise Advanced Lizenz – Unterstützte Server

Sie können die *OpenManage Enterprise Advanced* Lizenz auf folgenden PowerEdge-Servern bereitstellen:

- YX3X-Server mit iDRAC8 2.50.50.50 oder höher. Die YX3X-Firmwareversionen sind abwärtskompatibel und können auf YX2X-Hardware installiert werden. Informationen dazu finden Sie unter Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.
- YX4X-Server mit iDRAC9 3.10.10.10 oder höher. Siehe . Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187

OpenManage Enterprise Advanced Lizenz

Sie können die *OpenManage Enterprise Advanced* Lizenz beim Kauf eines Servers oder von Ihrem Vertriebsmitarbeiter erwerben. Sie können die gekaufte Lizenz aus dem Software-Lizenzverwaltungsportal unter Dell.com/support/retail/lkm herunterladen.

Überprüfen der Lizenzinformationen

OpenManage Enterprise bietet einen integrierten Bericht zum Anzeigen der Liste der von OpenManage Enterprise überwachten Geräte und deren Lizenzen. Klicken Sie auf **OpenManage Enterprise** > **Überwachen** > **Berichte** > **Lizenzberichte**. Klicken Sie auf **Ausführen**. Informationen dazu finden Sie unter Berichte ausführen auf Seite 141.

Sie können überprüfen, ob die *OpenManage Enterprise Advanced* Lizenz auf einem Server installiert ist, durch:

- Sie können auf allen Seiten von OpenManage Enterprise in der oberen rechten Ecke auf das Symbol **i** und dann auf **Lizenzen** klicken.
- Lesen Sie im Dialogfeld **Lizenzen** die Meldung und klicken Sie auf entsprechende Links, um Open-Source-Dateien oder andere Open-Source-Lizenzen im Zusammenhang mit OpenManage Enterprise zu betrachten und herunterzuladen.

Lizenz-basierte Funktionen in OpenManage Enterprise

Die *OpenManage Enterprise Advanced* Lizenz ist für die Verwendung der folgenden Funktionen von OpenManage Enterprise erforderlich:

- Bereitstellung der Serverkonfiguration.
- Erstellung und Wartung der Richtlinientreue-Baseline der Serverkonfiguration.
- Starten Sie in ISO.
- Aktivieren Sie die verfügbaren Plug-ins, wie z. B. Power Manager, um die Funktionalität der Appliance zu erweitern.

ANMERKUNG: Um auf Funktionen von OpenManage Enterprise zuzugreifen, z. B. die Funktion "Virtual Console Support", die vom iDRAC abhängig ist, benötigen Sie die iDRAC Enterprise-Lizenz. Weitere Informationen finden Sie in der *iDRAC-Dokumentation* auf der Support-Website.

2

Sicherheitsfunktionen in OpenManage Enterprise

Dies sind einige der Sicherheitsfunktionen von OpenManage Enterprise:

- Die rollenbasierte Zugriffskontrolle ermöglicht verschiedene Gerätemanagementfunktionen für verschiedene Nutzerrollen (Administrator, Geräte-Manager, Viewer).
- Die bereichsbasierte Zugriffskontrolle ermöglicht es einem Administrator, die Gerätegruppen festzulegen, die Geräte-Manager verwalten sollen.
- Optimierte Appliance mit Security-Enhanced Linux (SELinux) und einer internen Firewall.
- Verschlüsselung sensibler Daten in einer internen Datenbank.
- Verwendung verschlüsselter Kommunikation außerhalb der Appliance (HTTPS).
- Es werden nur Browser mit 256-Bit-Verschlüsselung unterstützt. Weitere Informationen finden Sie unter Mindestsystemanforderungen für die Bereitstellung von OpenManage Enterprise auf Seite 21

WARNUNG: Nicht autorisierte Benutzer können Zugriff auf Betriebssystemebene auf das OpenManage Enterprise-Gerät erhalten, unter Umgehung der Dell EMC Sicherheitseinschränkungen. Eine Möglichkeit ist, VMDK an eine andere Linux VM als Sekundärlaufwerk anzuhängen und so Zugriff auf die Betriebssystempartition zu erhalten, wobei die Anmeldeinformationen auf Betriebssystemebene möglicherweise geändert werden können. Dell EMC empfiehlt, dass Kunden das Laufwerk (Abbild-Datei) verschlüsseln, um den unbefugten Zugriff zu erschweren. Kunden müssen außerdem sicherstellen, dass sie für verwendete Verschlüsselungsmechanismen Dateien später entschlüsseln können. Anderenfalls kann das Gerät nicht gelöscht werden.

ANMERKUNG:

- Alle Änderungen an der Benutzerrolle werden sofort wirksam und die betroffenen Benutzer werden von der aktiven Sitzung abgemeldet.
- AD und LDAP Verzeichnisbenutzer können importiert werden und einer der OpenManage Enterprise-Rollen zugewiesen werden (Admin, DeviceManager oder Betrachter).
- Ausführung von Gerätemanagementaufgaben erfordert ein Konto mit den entsprechenden Berechtigungen auf dem Gerät.

Themen:

OpenManage Enterprise-Nutzerrollentypen

ANMERKUNG:

- AD und LDAP Verzeichnisbenutzer können importiert werden und einer der OpenManage Enterprise-Rollen zugewiesen werden (Admin, DeviceManager oder Betrachter).
- Auf den Geräten ausgeführte Aktionen erfordern ein dazu berechtigtes Konto auf dem Gerät.

Tabelle 2. OpenManage Enterprise-Benutzerrollentypen

Benutzer mit dieser Rolle ...	Hat die folgenden Benutzerberechtigungen
Administrator	Hat vollen Zugriff auf alle Aufgaben, die auf der Konsole durchgeführt werden können. ● Uneingeschränkter Zugriff (über GUI und REST) zum Lesen, Anzeigen, Erstellen, Bearbeiten, Löschen, Exportieren und Entfernen von Informationen in Zusammenhang mit Geräten

Tabelle 2. OpenManage Enterprise-Benutzerrollentypen (fortgesetzt)

Benutzer mit dieser Rolle ...	Hat die folgenden Benutzerberechtigungen
	und Gruppen, die von OpenManage Enterprise überwacht werden. ● Kann lokale, Microsoft Active Directory- (AD-) und LDAP-Benutzer erstellen und geeignete Rollen zuweisen ● Aktivieren und Deaktivieren von Benutzern ● Ändern der Rollen der vorhandenen Benutzer ● Löschen von Benutzers ● Ändern des Benutzerkennworts
Geräte-Manager	● Aufgaben, Richtlinien und andere Vorgänge auf den Geräten (Bereich) ausführen, die vom Administrator zugewiesen wurden.
Viewer	● Kann nur Informationen einsehen, die auf OpenManage Enterprise angezeigt werden, und Berichte ausführen. ● Standardmäßig nur Lesezugriff auf die Konsole und alle Gruppen. ● Kann nicht Aufgaben ausführen oder Richtlinien erstellen und verwalten.

ANMERKUNG:

- Wenn ein Betrachter oder ein DM zum Administrator wird, erhält er die vollständigen Administratorrechte. Wenn ein Betrachter zu einem DM wird, erhält der Betrachter die Berechtigungen eines DM.
- Alle Änderungen an der Benutzerrolle werden sofort wirksam und die betroffenen Benutzer werden von der aktiven Sitzung abgemeldet.
- Ein Auditprotokoll wird aufgezeichnet, wenn:
  - Eine Gruppe zugeordnet oder eine Zugangsberechtigung geändert wird.
  - Eine Nutzerrolle geändert wird.

Zugehörige Informationen

Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise

OpenManage Enterprise verfügt über rollenbasierte Zugriffskontrolle (RBAC), die die Nutzerberechtigungen für die drei integrierten Rollen (Administrator, Device Manager und Viewer) eindeutig definiert. Darüber hinaus kann ein Administrator mithilfe der bereichsbasierten Zugriffskontrolle (SBAC) die Gerätegruppen begrenzen, auf die ein Device Manager Zugriff hat. In den folgenden Themen werden die RBAC- und SBAC-Funktionen erläutert.

Berechtigungen der rollenbasierten Zugriffskontrolle (RBAC) in OpenManage Enterprise

Den Nutzern werden Rollen zugewiesen, die ihren Zugriff auf die Appliance-Einstellungen und Geräteverwaltungsfunktionen bestimmen. Diese Funktion wird als rollenbasierte Zugriffskontrolle (RBAC, Role-Based Access Control) bezeichnet. Die Konsole erzwingt die für eine bestimmte Aktion erforderliche Berechtigung, bevor die Aktion zugelassen wird. Weitere Informationen zum Verwalten von Nutzern auf OpenManage Enterprise finden Sie unter Verwalten von OpenManage Enterprise-Nutzern auf Seite 149.

In dieser Tabelle sind die verschiedenen Berechtigungen aufgeführt, die für jede Rolle aktiviert sind.

Tabelle 3. Rollenbasierte Nutzerberechtigungen in OpenManage Enterprise

OpenManage Enterprise – Funktionen	Beschreibung der Berechtigungen	Nutzerebenen für den Zugriff auf OpenManage Enterprise		
		Admin	Device Manager	Viewer
Appliance-Einrichtung	Globale Appliance-Einstellungen, einschließlich der Einrichtung der Appliance.	**J**	N	N
Sicherheitskonfiguration	Sicherheitseinstellungen der Appliance	**J**	N	N
Warnungsverwaltung	Warnungsmaßnahmen/-verwaltung	**J**	N	N
Fabric-Management	Fabric-Aktionen/-Management	**J**	N	N
Netzwerkverwaltung	Netzwerkmaßnahmen/-verwaltung	**J**	N	N
Gruppenverwaltung	Erstellen, Lesen, Aktualisieren und Löschen (CRUD) für statische und dynamische Gruppen	**J**	N	N
Ermittlungsverwaltung	CRUD für Ermittlungsaufgaben, Ausführen von Ermittlungsaufgaben	**J**	N	N
Bestandsverwaltung	CRUD für Bestandsaufnahmeaufgaben, Ausführen von Bestandsaufnahmeaufgaben	**J**	N	N
Trap-Management	MIB-Import, Trap-Bearbeitung	**J**	N	N
Verwaltung der automatischen Bereitstellung	Verwalten der automatischen Bereitstellung von Konfigurationsvorgängen	**J**	N	N
Überwachungskonfiguration	Warnmeldungsrichtlinien, Weiterleitung, SupportAssist usw.	**J**	**J**	N
Betriebsschalter	Neustart/Ein- und Ausschalten der Gerätestromversorgung	**J**	**J**	N
Device-Konfiguration	Device-Konfiguration, Anwendung von Vorlagen, Verwaltung/Migration der IO-Identität, Speicherzuordnung (für Speichergeräte) usw.	**J**	**J**	N
Betriebssystembereitstellung	Bereitstellen des Betriebssystems, Zuordnung zu LUN usw.	**J**	**J**	N
Geräteupdate	Geräte-Firmwareupdates, Anwendung aktualisierter Baselines usw.	**J**	**J**	N
Vorlagenverwaltung	Erstellen/Verwalten von Vorlagen	**J**	**J**	N
Baseline-Management	Erstellen/Verwalten von Firmware/Konfigurations-Baseline-Richtlinien	**J**	**J**	N
Energiemanagement	Festlegen von Energiebudgets	**J**	**J**	N
Jobverwaltung	Jobausführung/-verwaltung	**J**	**J**	N
Berichtsverwaltung	CRUD-Vorgänge für Berichte	**J**	**J**	N
Ausführen von Berichten	Berichte ausführen	**J**	**J**	**J**
Ansicht	Anzeigen aller Daten, Berichtausführung/-verwaltung usw.	**J**	**J**	**J**

Bereichsbasierte Zugriffskontrolle (SBAC) in OpenManage Enterprise

Mithilfe der Funktion der rollenbasierten Zugriffskontrolle (RBAC) können Administratoren Rollen zuweisen, während sie Nutzer erstellen. Die Rollen bestimmen den Zugriff der Nutzer auf die Appliance-Einstellungen und Gerätemanagementfunktionen. Die bereichsbasierte Zugriffskontrolle (SBAC) ist eine Erweiterung der RBAC-Funktion, die es einem Administrator ermöglicht, eine Device Manager-Rolle auf eine Teilmenge von Gerätegruppen, genannt Bereich, zu beschränken.

Beim Erstellen oder Aktualisieren eines Device Manager (DM) können Administratoren einen Bereich zuweisen, um den betrieblichen Zugriff des DM auf eine oder mehrere Systemgruppen, nutzerdefinierte Gruppen und/oder Plug-in-Gruppen zu beschränken.

Administrator- und Viewer-Rollen haben einen uneingeschränkten Bereichszugriff. Das bedeutet, dass Sie den betrieblichen Zugriff haben, wie durch RBAC-Berechtigungen für alle Geräte- und Gruppeneinheiten angegeben.

Der Bereich kann wie folgt implementiert werden:

1. Nutzer erstellen oder bearbeiten
2. DM-Rolle zuweisen
3. Bereich zur Beschränkung des betrieblichen Zugriffs zuweisen

Weitere Informationen zum Verwalten von Nutzern finden Sie unter Verwalten von OpenManage Enterprise-Nutzern auf Seite 149.

Wenn ein Device Manager (DM)-Nutzer mit einem zugewiesenen Bereich sich anmeldet, kann der DM nur dem Bereich zugeordnete Geräte anzeigen und verwalten. Außerdem kann der DM Einheiten wie Jobs, Firmware oder Konfigurationsvorlagen und Baselines, Warnungsrichtlinien, Profile und so weiter im Zusammenhang mit Bereichen zugeordneten Geräten anzeigen und verwalten, und zwar nur dann, wenn der DM die Einheit besitzt (DM hat die Einheit erstellt oder die Eigentumsrechte dieser Einheit sind ihm zugewiesen). Weitere Informationen zu den Einheiten, die ein DM erstellen kann, finden Sie unter *Berechtigungen der rollenbasierten Zugriffskontrolle (RBAC) in OpenManage Enterprise*.

Wenn Sie beispielsweise auf **Konfigurationen** > **Vorlagen** klicken, kann ein DM-Nutzer die standardmäßigen und nutzerdefinierten Vorlagen des DM-Nutzers anzeigen. Außerdem kann der DM-Nutzer andere Aufgaben für eigene Vorlagen durchführen, zu denen er von RBAC berechtigt wurde.

Durch Klicken auf **Konfiguration** > **Identitäts-Pools** kann ein DM-Nutzer alle Identitäten sehen, die von einem Administrator oder dem DM-Nutzer erstellt wurden. Der DM kann auch Aktionen für die durch RBAC-Berechtigung angegebenen Identitäten durchführen. Allerdings kann der DM nur die Nutzung der Identitäten anzeigen, die den Geräten im Bereich des DM zugeordnet sind.

In ähnlicher Weise können Sie durch Klicken auf **Konfiguration** > **VLAN-Pools** alle vom Administrator erstellten VLANs sehen und exportieren. Der DM kann keine anderen Vorgänge ausführen. Wenn der DM eine Vorlage hat, kann er die Vorlage bearbeiten, um die VLAN-Netzwerke zu verwenden, aber das VLAN-Netzwerk kann nicht bearbeitet werden.

In OpenManage Enterprise kann der Bereich beim Erstellen eines lokalen oder Importieren eines AD/LDAP-Nutzers zugewiesen werden. Die Bereichszuweisung für OIDC-Nutzer kann nur auf Open-ID Connect (OIDC)-Anbietern erfolgen.

SBAC für lokale Nutzer:

Beim Erstellen oder Bearbeiten eines lokalen Nutzers mit DM-Rolle kann der Administrator eine oder mehrere Gerätegruppen auswählen, die den Bereich für den DM definieren.

Sie können z. B. (als Administrator) einen DM-Nutzer mit dem Namen DM1 erstellen und die Gruppe *G1* in nutzerdefinierten Gruppen zuweisen. Dann hat DM1 nur betrieblichen Zugriff auf alle Geräte in *G1*. Der Nutzer DM1 kann nicht auf andere Gruppen oder Einheiten zugreifen, die mit anderen Geräten in Verbindung stehen.

Außerdem kann DM1 mit SBAC die Einheiten, die von anderen DMs (z. B. DM2) erstellt wurden, nicht in der gleichen Gruppe *G1* sehen. Das bedeutet, dass ein DM-Nutzer nur die Einheiten sehen kann, die im Besitz des Nutzers sind.

Sie können z. B. (als Administrator) einen anderen DM-Nutzer mit dem Namen DM2 erstellen und die gleiche Gruppe *G1* in nutzerdefinierten Gruppen zuweisen. Wenn DM2 Konfigurationsvorlagen, Konfigurations-Baselines oder Profile für die Geräte in *G1* erstellt, hat DM1 keinen Zugriff auf diese Einheiten und umgekehrt.

Ein DM mit Bereich für alle Geräte hat betrieblichen Zugriff, wie durch RBAC-Berechtigungen für alle Geräte- und Gruppeneinheiten im Besitz des DM festgelegt.

SBAC für AD/LDAP-Nutzer:

Beim Importieren oder Bearbeiten von AD/LDAP-Gruppen können Administratoren Bereiche zu Nutzergruppen mit DM-Rolle zuweisen. Wenn ein Nutzer Mitglied mehrerer AD-Gruppen ist, von denen jede eine DM-Rolle hat, und jede AD-Gruppe verschiedene Bereichszuweisungen hat, ist der Bereich des Nutzers die Vereinigung der Bereiche dieser AD-Gruppen.

Beispiel:

- Nutzer DM1 ist Mitglied von zwei AD-Gruppen (*RR5-Floor1-LabAdmins* und *RR5-Floor3-LabAdmins*). Beiden AD-Gruppen wurde die DM-Rolle zugewiesen, wobei die Bereichszuweisungen für die AD-Gruppen wie folgt lauten: *RR5-Floor1-LabAdmins* erhält *ptlab-*

Server und *RR5-Floor3-LabAdmins* erhält *smdlab-Server*. Der Bereich des DM DM1 ist nun die Verbindung von *ptlab-Servern* und *smdlab-Servern*.

- Nutzer DM1 ist Mitglied von zwei AD-Gruppen (*adg1* und *adg2*). Beiden AD-Gruppen wurde die DM-Rolle zugewiesen, wobei die Bereichszuweisungen für die AD-Gruppen wie folgt erfüllt sind: *adg1* erhält Zugriff auf *g1* und *adg2* erhält Zugriff auf *g2*. Wenn *g1* die übergeordnete Menge von *g2* ist, ist der Bereich von DM1 der größere Bereich (*g1*, alle untergeordneten Gruppen und alle untergeordneten Geräte).

Wenn ein Nutzer Mitglied mehrerer AD-Gruppen ist, die über unterschiedliche Rollen verfügen, hat die Rolle mit der höheren Funktionalität Vorrang (in der Reihenfolge Administrator, DM, Viewer).

Ein DM mit uneingeschränktem Bereich hat betrieblichen Zugriff, wie durch RBAC-Berechtigungen für alle Geräte- und Gruppeneinheiten angegeben.

ANMERKUNG: Nach dem Upgrade von OpenManage Enterprise von den Versionen 3.5 oder früher müssen die Geräte-Manager AD/LDAP und OIDC (PingFederate oder KeyCloak) alle Vorgängerversionen neu erstellen, da diese Einheiten nur dem Administrator nach dem Upgrade zur Verfügung stehen. Weitere Informationen finden Sie in den Versionshinweisen unter https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

SBAC für OIDC-Nutzer:

Die Bereichszuweisung für OIDC-Nutzer erfolgt nicht innerhalb der OME-Konsole. Sie können für OIDC-Nutzer in einem OIDC-Anbieter während der Nutzerkonfiguration Bereiche zuweisen. Wenn der Nutzer sich mit den Anmeldeinformationen für den OIDC-Anbieter anmeldet, ist die Rollen- und Bereichszuweisung für OME verfügbar. Weitere Informationen zum Verwalten von Nutzerrollen und Bereichen finden Sie unter Konfigurieren Sie eine OpenID Connect-Anbieterrichtlinie in PingFederate für den rollenbasierten Zugriff auf OpenManage Enterprise auf Seite 162.

ANMERKUNG: Wenn PingFederate als OIDC-Anbieter verwendet wird, können nur Administratorrollen verwendet werden. Weitere Informationen finden Sie unter Konfigurieren Sie eine OpenID Connect-Anbieterrichtlinie in PingFederate für den rollenbasierten Zugriff auf OpenManage Enterprise auf Seite 162 und in den Versionshinweisen unter https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

Eigentumsübertragung: Der Administrator kann die Eigentümerressourcen von einem Device Manager (Quelle) zu einem anderen Device Manager übertragen. Ein Administrator kann z. B. alle zugewiesenen Ressourcen von einem Quell-DM1 auf DM2 übertragen. Ein Geräte-Manager mit eigenen Einheiten, z. B. Firmware- und/oder Konfigurations-Baselines, Konfigurationsvorlagen, Warnungsrichtlinien und Profilen, wird als berechtigter Quellnutzer betrachtet. Mit der Eigentumsübertragung werden nur die Einheiten und nicht die Gerätegruppen (Bereich), die Eigentum eines Geräte-Managers sind, übertragen. Weitere Informationen finden Sie unter Eigentumsübertragung von Geräte-Manager-Einheiten auf Seite 156.

Verwandte Verweise

OpenManage Enterprise-Nutzerrollentypen auf Seite 15

3

Installieren von OpenManage Enterprise

Dell EMC OpenManage Enterprise wird als Appliance zur Verfügung gestellt, die Sie auf einem Hypervisor bereitstellen und zum Managen von Ressourcen nutzen können, um Ausfallzeiten auf ein Minimum zu reduzieren. Das virtuelle Gerät kann nach der ersten Netzwerkbereitstellung in der textbasierten Benutzeroberfläche (Text User Interface (TUI)) über die Webkonsole der Anwendung konfiguriert werden. Die Schritte zum Anzeigen und Aktualisieren der Konsolen-Version finden Sie unter Überprüfen und Aktualisieren der Version von OpenManage Enterprise und der verfügbaren Plug-ins auf Seite 170. Dieses Kapitel beschreibt die Installationsvoraussetzungen und Mindestanforderungen.

ANMERKUNG: Informationen zu unterstützten Browsern finden Sie in der *OpenManage Enterprise Supportmatrix* auf der Support-Website.

Themen:

Installationsvoraussetzungen und Mindestanforderungen

Eine Liste der unterstützten Plattformen, Betriebssysteme und Browser finden Sie in der *Dell EMC OpenManage Enterprise-Supportmatrix* auf der Supportseite und unter Dell TechCenter.

Für die Installation von OpenManage Enterprise benötigen Sie Administratorrechte auf dem lokalen System, und das verwendete System muss die unter Minimal empfohlene Hardware und Mindestanforderungen für die Installation von OpenManage Enterprise aufgeführten Kriterien erfüllen.

Minimal empfohlene Hardware

Diese Tabelle beschreibt die minimal empfohlene Hardware für OpenManage Enterprise.

Tabelle 4. Minimal empfohlene Hardware

Minimal empfohlene Hardware	Große Bereitstellungen	Kleine Bereitstellungen
Anzahl der Geräte, die durch die Appliance verwaltet werden können	Bis zu 8000	1000
RAM	32 GB	16 GB
Prozessoren	8 Kerne insgesamt	4 Kerne insgesamt
Festplatte	400 GB	400 GB

Mindestsystemanforderungen für die Bereitstellung von OpenManage Enterprise

Tabelle 5. Mindestanforderungen

Einzelheiten	Mindestanforderungen

Unterstützte Hypervisors	• VMware vSphere-Versionen:
	  ○ vSphere ESXi 5.5 und höher
	• Microsoft Hyper-V wird unterstützt auf:
	  ○ Windows Server 2012 R2 und höher
	• KVM wird unterstützt auf:
	  ○ Red Hat Enterprise Linux 6.5 und höher

Netzwerk	Verfügbares virtuelles NIC, das Zugriff auf die Verwaltungsnetzwerke aller zu verwaltenden Geräte hat, die über OpenManage Enterprise verwaltet sind.
Unterstützte Browser	• Internet Explorer (64-Bit) 11 und höher • Mozilla Firefox 52 und höher • Google Chrome 58 und höher • Microsoft Edge Version 41.16299 und höher
Benutzeroberfläche	Basiert auf HTML 5, JS

ANMERKUNG: Aktuelle Informationen zu den Mindestanforderungen für OpenManage Enterprise finden Sie auf der Support-Website unter *Dell EMC OpenManage Enterprise-Supportmatrix*.

OpenManage Enterprise auf VMware vSphere bereitstellen

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Benutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

ANMERKUNG: Wenn ein sekundärer Adapter hinzugefügt wird, bevor die Appliance zum ersten Mal eingeschaltet wird, wird der Adapter so konfiguriert, dass IPv4 und IPv6 deaktiviert sind. Wenn Sie sich an der Text-Benutzeroberfläche (TUI) angemeldet, die EULA akzeptiert und das Administratorkennwort geändert haben, wird der Adapter als **DEAKTIVIERT** angezeigt und muss vom Benutzer konfiguriert werden.

1. Laden Sie die Datei `openmanage_enterprise_ovf_format.zip` von der Support-Website herunter und extrahieren Sie die Datei an einen Speicherort, auf den der VMware vSphere Client zugreifen kann. Es wird empfohlen, ein lokales Laufwerk oder eine CD/DVD zu verwenden, da die Installation von einem Netzwerkspeicherort bis zu 30 Minuten dauern kann.
2. Wählen Sie im v Sphere-Client**Datei** > **OVF-Vorlage bereitstellen**.
   Daraufhin wird der **OVF-Vorlagen-Bereitstellungsassistent** angezeigt.
3. Klicken Sie auf der Seite **Quelle** auf **Durchsuchen** und wählen Sie dann das OVF-Paket aus. Klicken Sie auf **Weiter**.
4. Prüfen Sie auf der Seite **OVF-Vorlagendetails** die angezeigten Informationen. Klicken Sie auf **Weiter**.
5. Lesen Sie auf der Seite **Endbenutzer-Lizenzvertrag** den Lizenzvertrag und klicken Sie auf **Annehmen**. Klicken Sie auf **Weiter**, um fortzufahren.
6. Geben Sie auf der Seite **Name und Speicherort** einen Namen mit bis zu 80 Zeichen ein und wählen Sie dann einen Bestandsaufnahme-Speicherort, an dem die Vorlage gespeichert werden soll. Klicken Sie auf **Weiter**.
7. Je nach vCenter-Konfiguration wird eine der folgenden Optionen angezeigt:
   - **Falls Ressourcenpools konfiguriert wurden** — Wählen Sie auf der Seite **Ressourcenpool** den Pool der virtuellen Server aus, auf denen die Geräte-VM bereitgestellt wird.
   - **Falls KEINE Ressourcenpools konfiguriert wurden** — Wählen Sie auf der Seite **Hosts/Cluster** den Host oder Cluster aus, auf dem die Geräte-VM bereitgestellt wird.

8. Wenn auf dem Host mehr als ein Datenspeicher vorhanden ist, zeigt die Seite **Datenspeicher** diese Datenspeicher an. Wählen Sie den Speicherort für die Dateien der virtuellen Maschine (VM) aus und klicken Sie anschließend auf **Weiter**.
9. Klicken Sie auf der Seite **Disk-Format** auf **Thick Provision**, um den VMs zum Zeitpunkt der Erstellung des Laufwerks bereits physischen Speicher vorab zuzuweisen.
10. Überprüfen Sie auf der Seite **Für Fertigstellung bereit** Sie die Optionen, die Sie auf den vorherigen Seiten ausgewählt haben, und klicken Sie auf **Fertigstellen**, um den Bereitstellungsjob auszuführen.
    Ein Fenster mit dem Fertigstellungsstatus wird angezeigt, in dem Sie den Fortschritt des Jobs verfolgen können.

OpenManage Enterprise auf Hyper-V 2012 R2 und früheren Hosts bereitstellen

ANMERKUNG:
- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Benutzerberechtigungen verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16
- Wenn ein sekundärer Adapter hinzugefügt wird, bevor die Appliance zum ersten Mal eingeschaltet wird, wird der Adapter so konfiguriert, dass IPv4 und IPv6 deaktiviert sind. Wenn Sie sich an der Text-Benutzeroberfläche (TUI) angemeldet, die EULA akzeptiert und das Administratorkennwort geändert haben, wird der Adapter als **DEAKTIVIERT** angezeigt und muss vom Benutzer konfiguriert werden.
- Nach Installation oder Aktualisierung der Appliance auf Hyper-V: Schalten Sie die Appliance aus, entfernen Sie den Standard-Netzwerkadapter und fügen Sie einen Legacy-Netzwerkadapter hinzu. Schalten Sie die Appliance dann ein.

1. Laden Sie die Datei `openmanage_enterprise_vhd_format.zip` von der Support-Website herunter. Extrahieren Sie die Datei und verschieben oder kopieren Sie dann die beigefügte VHD-Datei in den entsprechenden Speicherort auf Ihrem System, an dem Sie das virtuelle OpenManage Enterprise-Laufwerk speichern wollen.
2. Öffnen Sie **Hyper-V Manager** in Windows Server 2012 R2 oder einer früheren Version. Der Windows Hyper-V sollte unter dem Hyper-V-Manager angezeigt werden. Wenn nicht, klicken Sie mit der rechten Maustaste auf **Hyper-V-Manager** und wählen Sie **Mit Server verbinden** aus.
3. Klicken Sie auf **Aktionen** > **Neu** > **Virtuelle Maschine** zum Starten des **Assistenten für neue virtuelle Maschinen**.
4. Klicken Sie auf **Weiter** auf der ersten Seite von **Bevor Sie beginnen**.
5. Geben Sie auf der **Seite "Name und Speicherort angeben"**
   - den **Namen der virtuellen Maschine** an.
   - (Optional) Aktivieren Sie das Kontrollkästchen **Virtuelle Maschine an einem anderen Ort speichern**, um das Feld **Speicherort** zu aktivieren. Durchsuchen und navigieren Sie zum Erfassen eines Ordners, in dem die VM gespeichert werden soll.

   ANMERKUNG: Wenn das Kontrollkästchen nicht aktiviert ist, wird die VM im Standardordner gespeichert.
6. Klicken Sie auf **Weiter.**
7. Wählen Sie auf der Seite **Generation angeben** die Option **Generation 1** aus und klicken Sie auf **Weiter**.

   ANMERKUNG: OpenManage Enterprise bietet keine Unterstützung für Generation 2.
8. Geben Sie auf der Seite **Speicher zuweisen** den Startspeicher in das Feld **Startspeicher** ein und klicken Sie auf **Weiter**.

   ANMERKUNG: Stellen Sie sicher, dass mindestens 16.000 MB (16 GB) zugewiesen sind.
9. Wählen Sie auf der Seite **Netzwerk konfigurieren** den Netzwerkadapter aus der Dropdown-Liste **Verbindung** aus. Stellen Sie sicher, dass der **virtuelle Switch** mit dem Netzwerk verbunden ist. Klicken Sie auf **Weiter**.

   ANMERKUNG: Wenn diese Option auf **Nicht verbunden** eingestellt ist, funktioniert OME während des ersten Neustarts nicht richtig. In diesem Fall ist eine Neueinrichtung erforderlich.
10. Wählen Sie auf der Seite **Virtuelle Festplatte verbinden** die Option **Ein bestehendes virtuelles Festplattenlaufwerk verwenden** aus und wechseln Sie dann zum Speicherort der VHD-Datei, die Sie in **Schritt 1** kopiert haben. Klicken Sie auf **Weiter**.
11. Folgen Sie den Anweisungen auf dem Bildschirm.

    ANMERKUNG: Stellen Sie sicher, dass Sie eine Mindestspeichergröße von 20 GB haben.
12. Öffnen Sie die **Einstellungen** der neu erstellten VM und schalten Sie die VM ein.
13. Akzeptieren Sie auf dem TUI-Bildschirm die EULA und ändern Sie bei Aufforderung das Kennwort der Appliance und stellen Sie die Netzwerkparameter auf die IP der Appliance ein.

Open Manage Enterprise auf einem Hyper-V 2016-Host bereitstellen

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Benutzerberechtigungen verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16
- Wenn ein sekundärer Adapter hinzugefügt wird, bevor die Appliance zum ersten Mal eingeschaltet wird, wird der Adapter so konfiguriert, dass IPv4 und IPv6 deaktiviert sind. Wenn Sie sich an der Text-Benutzeroberfläche (TUI) angemeldet, die EULA akzeptiert und das Administratorkennwort geändert haben, wird der Adapter als **DEAKTIVIERT** angezeigt und muss vom Benutzer konfiguriert werden.
- Nach Installation oder Aktualisierung der Appliance auf Hyper-V: Schalten Sie die Appliance aus, entfernen Sie den Standard-Netzwerkadapter und fügen Sie einen Legacy-Netzwerkadapter hinzu. Schalten Sie die Appliance dann ein.

1. Laden Sie die Datei **openmanage_enterprise_vhd_format.zip** von der Support-Website herunter. Extrahieren Sie die Datei und verschieben oder kopieren Sie dann die beigefügte VHD-Datei in den entsprechenden Speicherort auf Ihrem System, an dem Sie das virtuelle OpenManage Enterprise-Laufwerk speichern wollen.
2. Starten Sie den **Hyper-V-Manager** unter Windows Server 2016. Der Windows Hyper-V sollte unter dem Hyper-V-Manager angezeigt werden. Wenn nicht, klicken Sie mit der rechten Maustaste auf **Hyper-V-Manager** und wählen Sie **Mit Server verbinden** aus.
3. Klicken Sie auf **Aktionen** > **Neu** > **Virtuelle Maschine** zum Starten des **Assistenten für neue virtuelle Maschinen**.
4. Klicken Sie auf **Weiter** auf der ersten Seite von **Bevor Sie beginnen**.
5. Geben Sie auf der **Seite "Name und Speicherort angeben"**
   - den **Namen der virtuellen Maschine** an.
   - (Optional) Aktivieren Sie das Kontrollkästchen **Virtuelle Maschine an einem anderen Ort speichern**, um das Feld **Speicherort** zu aktivieren. Durchsuchen und navigieren Sie zum Erfassen eines Ordners, in dem die VM gespeichert werden soll.

   ANMERKUNG: Wenn das Kontrollkästchen nicht aktiviert ist, wird die VM im Standardordner gespeichert.
6. Klicken Sie auf **Weiter.**
7. Wählen Sie auf der Seite **Generation angeben** die Option **Generation 1** aus und klicken Sie auf **Weiter**.

   ANMERKUNG: OpenManage Enterprise bietet keine Unterstützung für Generation 2.
8. Geben Sie auf der Seite **Speicher zuweisen** den Startspeicher in das Feld **Startspeicher** ein und klicken Sie auf **Weiter**.

   ANMERKUNG: Stellen Sie sicher, dass mindestens 16.000 MB (16 GB) zugewiesen sind.
9. Wählen Sie auf der Seite **Netzwerk konfigurieren** den Netzwerkadapter aus der Dropdown-Liste **Verbindung** aus. Stellen Sie sicher, dass der **virtuelle Switch** mit dem Netzwerk verbunden ist. Klicken Sie auf **Weiter**.

   ANMERKUNG: Wenn diese Option auf **Nicht verbunden** eingestellt ist, funktioniert OME während des ersten Neustarts nicht richtig. In diesem Fall ist eine Neueinrichtung erforderlich.
10. Wählen Sie auf der Seite **Virtuelle Festplatte verbinden** die Option **Ein bestehendes virtuelles Festplattenlaufwerk verwenden** aus und wechseln Sie dann zum Speicherort der VHD-Datei, die Sie in **Schritt 1** kopiert haben. Klicken Sie auf **Weiter**.
11. Folgen Sie den Anweisungen auf dem Bildschirm.

    ANMERKUNG: Stellen Sie sicher, dass Sie eine Mindestspeichergröße von 20 GB haben.
12. Öffnen Sie die **Einstellungen** der neu erstellten VM und schalten Sie die VM ein.
13. Akzeptieren Sie auf dem TUI-Bildschirm die EULA und ändern Sie bei Aufforderung das Kennwort der Appliance und stellen Sie die Netzwerkparameter auf die IP der Appliance ein.

Open Manage Enterprise auf einem Hyper-V 2019-Host bereitstellen

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Benutzerberechtigungen verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

- Wenn ein sekundärer Adapter hinzugefügt wird, bevor die Appliance zum ersten Mal eingeschaltet wird, wird der Adapter so konfiguriert, dass IPv4 und IPv6 deaktiviert sind. Wenn Sie sich an der Text-Benutzeroberfläche (TUI) angemeldet, die EULA akzeptiert und das Administratorkennwort geändert haben, wird der Adapter als **DEAKTIVIERT** angezeigt und muss vom Benutzer konfiguriert werden.
- Nach Installation oder Aktualisierung der Appliance auf Hyper-V: Schalten Sie die Appliance aus, entfernen Sie den Standard-Netzwerkadapter und fügen Sie einen Legacy-Netzwerkadapter hinzu. Schalten Sie die Appliance dann ein.

1. Laden Sie die Datei **openmanage_enterprise_vhd_format.zip** von der Support-Website herunter. Extrahieren Sie die Datei und verschieben oder kopieren Sie dann die beigefügte VHD-Datei in den entsprechenden Speicherort auf Ihrem System, an dem Sie das virtuelle OpenManage Enterprise-Laufwerk speichern wollen.
2. Starten Sie den **Hyper-V-Manager** unter Windows Server 2019. Der Windows Hyper-V sollte unter dem Hyper-V-Manager angezeigt werden. Wenn nicht, klicken Sie mit der rechten Maustaste auf **Hyper-V-Manager** und wählen Sie **Mit Server verbinden** aus.
3. Klicken Sie auf **Aktionen** > **Neu** > **Virtuelle Maschine** zum Starten des **Assistenten für neue virtuelle Maschinen**.
4. Klicken Sie auf **Weiter** auf der ersten Seite von **Bevor Sie beginnen**.
5. Geben Sie auf der **Seite "Name und Speicherort angeben"**
   - den **Namen der virtuellen Maschine** an.
   - (Optional) Aktivieren Sie das Kontrollkästchen **Virtuelle Maschine an einem anderen Ort speichern**, um das Feld **Speicherort** zu aktivieren. Durchsuchen und navigieren Sie zum Erfassen eines Ordners, in dem die VM gespeichert werden soll.

   ANMERKUNG: Wenn das Kontrollkästchen nicht aktiviert ist, wird die VM im Standardordner gespeichert.
6. Klicken Sie auf **Weiter.**
7. Wählen Sie auf der Seite **Generation angeben** die Option **Generation 1** aus und klicken Sie auf **Weiter**.

   ANMERKUNG: OpenManage Enterprise bietet keine Unterstützung für Generation 2.
8. Geben Sie auf der Seite **Speicher zuweisen** den Startspeicher in das Feld **Startspeicher** ein und klicken Sie auf **Weiter**.

   ANMERKUNG: Stellen Sie sicher, dass mindestens 16.000 MB (16 GB) zugewiesen sind.
9. Wählen Sie auf der Seite **Netzwerk konfigurieren** den Netzwerkadapter aus der Dropdown-Liste **Verbindung** aus. Stellen Sie sicher, dass der **virtuelle Switch** mit dem Netzwerk verbunden ist. Klicken Sie auf **Weiter**.

   ANMERKUNG: Wenn diese Option auf **Nicht verbunden** eingestellt ist, funktioniert OME während des ersten Neustarts nicht richtig. In diesem Fall ist eine Neueinrichtung erforderlich.
10. Wählen Sie auf der Seite **Virtuelle Festplatte verbinden** die Option **Ein bestehendes virtuelles Festplattenlaufwerk verwenden** aus und wechseln Sie dann zum Speicherort der VHD-Datei, die Sie in **Schritt 1** kopiert haben. Klicken Sie auf **Weiter**.
11. Folgen Sie den Anweisungen auf dem Bildschirm.

    ANMERKUNG: Stellen Sie sicher, dass Sie eine Mindestspeichergröße von 20 GB haben.
12. Öffnen Sie die **Einstellungen** der neu erstellten VM und schalten Sie die VM ein.
13. Akzeptieren Sie auf dem TUI-Bildschirm die EULA und ändern Sie bei Aufforderung das Kennwort der Appliance und stellen Sie die Netzwerkparameter auf die IP der Appliance ein.

Bereitstellen von OpenManage Enterprise mithilfe der Kernel-Based Virtual Machine

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Benutzerberechtigungen verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16
- Wenn ein sekundärer Adapter hinzugefügt wird, bevor die Appliance zum ersten Mal eingeschaltet wird, wird der Adapter so konfiguriert, dass IPv4 und IPv6 deaktiviert sind. Wenn Sie sich an der Text-Benutzeroberfläche (TUI) angemeldet, die EULA akzeptiert und das Administratorkennwort geändert haben, wird der Adapter als **DEAKTIVIERT** angezeigt und muss vom Benutzer konfiguriert werden.

1. Installieren Sie die erforderlichen Virtualisierungspakete während der Installation des Betriebssystems.
2. Laden Sie die Datei `openmanage_enterprise_kvm_format.zip` von der Support-Website herunter. Entpacken Sie die Datei in den entsprechenden Speicherort auf dem System, an dem Sie das virtuelle OpenManage Enterprise-Laufwerk speichern möchten.
3. Starten Sie den virtuellen Manager und wählen Sie **Datei** > **Eigenschaften**.
4. Klicken Sie auf der Seite **Netzwerkschnittstellen** auf **Hinzufügen**.

5. Wählen Sie als Schnittstellentyp die Option **Überbrücken** aus und klicken Sie auf **Vor**.
6. Setzen Sie den Startmodus auf **Beim Start** und aktivieren Sie das Kontrollkästchen **Jetzt aktivieren**.
7. Wählen Sie aus der Liste die Schnittstelle aus, zu der eine Verbindung erstellt werden soll, und stellen Sie sicher, dass die Eigenschaften mit dem Host-Gerät übereinstimmen, und klicken Sie dann auf **Abschließen**.
   Daraufhin wird eine virtuelle Schnittstelle erstellt und Sie können die Firewall-Einstellungen über das Terminal konfigurieren.
8. Klicken Sie auf dem Virtual Machine Manager auf **Datei** > **Neu**.
9. Geben Sie einen Namen für den VM ein und wählen Sie die Option **Vorhandenes Festplatten-Abbild importieren** und klicken Sie dann auf **Vor**.
10. Navigieren Sie im Dateisystem und wählen Sie die in Schritt 1 heruntergeladene QCOW2-Datei aus und klicken Sie dann auf **Vor**.
11. Weisen Sie dem Speicher 16 GB zu und wählen Sie zwei Prozessorkerne aus und klicken Sie dann auf **Vor**.
12. Weisen Sie der VM den erforderlichen Speicherplatz zu und klicken Sie auf **Vor**.
13. Stellen Sie unter **Erweiterte Optionen** sicher, dass das überbrückte Host-Gerätenetzwerk und KVM als Virtualisierungstyp ausgewählt ist.
14. Klicken Sie auf **Fertigstellen**.
    OpenManage Enterprise Appliance ist jetzt mithilfe der KVM bereitgestellt. Informationen zum Einstieg mit OpenManage Enterprise erhalten Sie unter Bei OpenManage Enterprise anmelden auf Seite 27.

Programmgesteuertes Bereitstellen von OpenManage Enterprise

OpenManage Enterprise kann programmgesteuert (unter Verwendung eines Skripts) auf VMware ESXi Version 6.5 oder höher bereitgestellt werden.

ANMERKUNG: Die programmgesteuerte/skriptbasierte Bereitstellung wird nur über die primäre Schnittstelle unterstützt.

ANMERKUNG: Wenn ein sekundärer Adapter hinzugefügt wird, bevor die Appliance zum ersten Mal eingeschaltet wird, wird der Adapter so konfiguriert, dass IPv4 und IPv6 deaktiviert sind. Wenn Sie sich an der Text-Benutzeroberfläche (TUI) angemeldet, die EULA akzeptiert und das Administratorkennwort geändert haben, wird der Adapter als **DEAKTIVIERT** angezeigt und muss vom Benutzer konfiguriert werden.

ANMERKUNG: Für die programmgesteuerte Bereitstellung müssen Sie über die aktuellsten Versionen von OVF Tool und Python 3.0 oder höher verfügen.

Für das programmgesteuerte Bereitstellen von OpenManage Enterprise gehen Sie wie folgt vor:

1. Laden Sie die Datei `openmanage_enterprise_ovf_format.zip` herunter und extrahieren Sie sie oder laden Sie die folgenden OVF-Dateien einzeln von der Support-Website herunter:
   - `openmanage_enterprise.x86_64-0.0.1-disk1.vmdk`
   - `openmanage_enterprise.x86_64-0.0.1.mf`
   - `openmanage_enterprise.x86_64-0.0.1.ovf`
   - `openmanage_enterprise.x86_64-0.0.1.vmx`
   - `ovf_properties.config`
   - `update_ovf_property.py`
2. Öffnen Sie die Datei `ovf_properties.config` und legen Sie die folgenden Parameter fest:

Tabelle 6. Parameter für `ovf_properties.config`

Parameter	Zulässige Werte	Beschreibung
bEULATxt	Wahr oder falsch	Durch das Setzen dieses Werts auf "true", stimmen Sie den Bedingungen in der Endbenutzer-Lizenzvereinbarung (EULA) zu. Die EULA finden Sie unten in der Datei ovf_properties.config.
adminPassword	Muss mindestens ein Zeichen in Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Zum Beispiel Dell123$	Geben Sie ein neues Administrator-Kennwort für OpenManage Enterprise ein.

Tabelle 6. Parameter für `ovf_properties.config` (fortgesetzt)

Parameter	Zulässige Werte	Beschreibung
bEnableDHCP	Wahr oder falsch	Setzen Sie den Wert auf "true", wenn die Appliance IPv4-DHCP aktivieren und das statische IPv4 ignorieren soll.
bEnableIpv6AutoConfig	Wahr oder falsch	Setzen Sie den Wert auf "true", wenn die Appliance die automatische IPv6-Konfiguration aktivieren und das statische IPv6 ignorieren soll.
staticIP	Statische IP im CIDR-Format	Kann IPv4 oder IPv6 sein. (Sie können nicht gleichzeitig den Typ IPv4 und IPv6 festlegen.)
gateway	IPv4 oder IPv6	Sie können das statische Gateway nicht gleichzeitig als Typ IPv4 und IPv6 festlegen.

3. Führen Sie das Skript `update_ovf_property.py` aus.

   Dieses Skript ändert die Datei `openmanage_enterprise.x86_64-0.0.1.ovf` für die Bereitstellung in Übereinstimmung mit den Werten in der Datei ovf_properties.config. Wenn die Ausführung des Skripts abgeschlossen ist, wird der Beispielbefehl "ovftool" angezeigt. Er enthält Tags wie z. B. `<DATASTORE>, <user>, <password>, <IP address>` usw., die Sie entsprechend Ihrer Implementierungsumgebung ersetzen müssen. Diese Einstellungen definieren die Ressourcen, die auf dem ESXi-Zielsystem verwendet werden, sowie die Anmeldeinformationen und die IP-Adresse des Zielsystems.

   ANMERKUNG: Denken Sie daran, das gesamte Tag einschließlich der Symbole < und > zu ersetzen.

4. Führen Sie den modifizierten Befehl ovftool aus dem vorherigen Schritt aus.

   ANMERKUNG: Der Befehl ovftool muss mit den Flags --X: injectOvfEnv und --powerOn ausgeführt werden, da sie für die programmgesteuerte Bereitstellung erforderlich sind.

Nachdem der Befehl ovftool ausgeführt wurde, wird das Manifest bestätigt und die Bereitstellung beginnt.

4

Einstieg in OpenManage Enterprise

Themen:

Bei OpenManage Enterprise anmelden

Wenn Sie das System zum ersten Mal von der textbasierten Benutzeroberfläche starten, werden Sie dazu aufgefordert, die Endnutzer-Lizenzvereinbarung zu akzeptieren und dann das Administratorkennwort zu ändern. Wenn Sie die Anmeldung bei OpenManage Enterprise zum ersten Mal durchführen, müssen Sie die Nutzeranmeldedaten über die textbasierte Benutzeroberfläche (Text User Interface, TUI) einrichten. Informationen dazu finden Sie unter OpenManage Enterprise mithilfe der textbasierten Benutzeroberfläche konfigurieren auf Seite 27.

VORSICHT: Ein vergessenes Administratorkennwort kann von OpenManage Enterprise Appliance nicht wiederhergestellt werden.

1. Starten Sie den unterstützten Browser.
2. Geben Sie in das Feld **Adresse** die IP-Adresse des OpenManage Enterprise-Geräts ein.

   Auf der Anmeldeseite werden das OpenManage Enterprise-Logo und ein Sicherheitshinweis mit der Meldung „Mit dem Zugriff auf den Computer bestätigen Sie, dass dieser Zugriff der Sicherheitsrichtlinie Ihres Unternehmens entspricht" angezeigt. Der Sicherheitshinweis kann von den Administratoren mithilfe der API angepasst werden. Weitere Informationen finden Sie im OpenManage Enterprise-API-Benutzerhandbuch.
3. Geben Sie auf der Anmeldeseite die Zugangsdaten ein und klicken Sie dann auf **Anmelden**.

   ANMERKUNG: Die Standardeinstellung für den Nutzernamen lautet `admin`.

Wenn Sie sich zum ersten Mal bei OpenManage Enterprise anmelden, wird die Seite **Willkommen bei OpenManage Enterprise** automatisch angezeigt. Klicken Sie auf **Anfangseinstellungen** und führen Sie das grundlegende Konfigurations-Setup aus. Informationen dazu finden Sie unter OpenManage Enterprise konfigurieren auf Seite 31. Um die Geräte zu ermitteln, klicken Sie auf **Geräte ermitteln**.

ANMERKUNG: Standardmäßig wird Ihr OpenManage Enterprise-Konto nach drei fehlgeschlagenen Anmeldeversuchen gesperrt. Sie können sich erst anmelden, nachdem die Kontosperre abgelaufen ist. Die Dauer der Kontosperre beträgt standardmäßig 900 Sekunden. Zum Ändern dieser Sperrdauer siehe Einstellen der Sicherheitseigenschaften für die Anmeldung auf Seite 167.

OpenManage Enterprise mithilfe der textbasierten Benutzeroberfläche konfigurieren

Die textbasierte Benutzeroberfläche (TUI) bietet Ihnen eine Textschnittstelle zum Ändern des Administratorkennworts, zum Anzeigen des Appliance-Status und der Netzwerkkonfiguration, zum Konfigurieren von Netzwerkparametern, zur Aktivierung des Service-Debug-Antrags, zum Auswählen des primären Netzwerks und zur Konfiguration der Appliance für die automatische Ermittlung der Server in Ihrem Netzwerk.

Wenn Sie das System zum ersten Mal über die TUI starten, werden Sie aufgefordert, die Endbenutzer-Lizenzvereinbarung (EULA) zu akzeptieren. Ändern Sie als Nächstes das Administratorkennwort und konfigurieren Sie die Netzwerkparameter für die Appliance und laden Sie die Web-Konsole in einem unterstützten Browser, um zu beginnen. Nur Benutzer mit OpenManage-Administrator-Berechtigungen können OpenManage Enterprise konfigurieren.

Verwenden Sie auf der TUI-Oberfläche die Pfeiltasten oder drücken Sie die **Tab**-Taste, um die nächste Option zu wählen, und **Umschalt + Tab**, um die vorhergehende Option zu wählen. Drücken Sie die **Eingabetaste**, um eine Option auszuwählen. Mit der **Leertaste** wechseln Sie den Status von einem Kontrollkästchen.

ANMERKUNG:

- Um IPv6 zu konfigurieren, stellen Sie sicher, dass es bereits durch vCenter Server konfiguriert ist.
- Standardmäßig wird die zuletzt ermittelte IP eines Geräts von OpenManage Enterprise zum Ausführen aller Vorgänge verwendet. Damit eine IP-Änderung wirksam wird, muss das Gerät neu ermittelt werden.

Sie können nun OpenManage Enterprise über die TUI konfigurieren. Auf dem TUI-Bildschirm stehen die folgenden Optionen zur Verfügung:

Tabelle 7. Optionen der textbasierten Benutzeroberfläche

Optionen	Beschreibungen
Ändern des Administratorkennworts	Geben Sie auf dem Bildschirm **Administratorkennwort ändern** das neue Kennwort ein und bestätigen Sie es. Beim ersten Mal müssen Sie das Kennwort mithilfe des TUI Bildschirms ändern.
Anzeigen des aktuellen Appliancestatus	Wählen Sie **Aktuellen Appliancestatus anzeigen** aus, um die URL und den Status der Appliance anzuzeigen. Sie können auch den Status der Aufgabenausführung, Ereignisverarbeitung, Tomcat, Datenbank und Überwachungsservices anzeigen.
Anzeigen der aktuellen Netzwerkkonfiguration	Wählen Sie **Aktuelle Netzwerkkonfiguration anzeigen**, um die IP-Konfigurationsdetails anzuzeigen. Das Menü **Netzwerkadapter auswählen** führt alle verfügbaren Netzwerkadapter auf. Durch Klicken auf einen Netzwerkadapter werden die aktuellen Einstellungen angezeigt.
Festlegen des Appliance-Hostnamen	Wählen Sie **Appliance-Hostnamen festlegen** aus, um den Hostnamen der Appliance auf dem DNS-Server zu konfigurieren. Dieses Feld unterstützt die folgenden gültigen Zeichen für Hostnamen: alphanumerisch (a-z, A-Z, 0-9), Punkte (.) und Bindestriche (-). **ANMERKUNG:** Die Verwendung von Punkten kennzeichnet Domänennamen. Wenn die DNS-Informationen der Appliance statisch konfiguriert sind, anstatt Domänendetails von DHCP zu erhalten, müssen Sie den Hostnamen unter Verwendung des vollständig qualifizierten Domänennamens (FQDN) konfigurieren, damit die Domänen-Suchinformationen ausgefüllt werden können.
Einstellen der Netzwerkbetriebsparameter	Wählen Sie **Netzwerkparameter festlegen**, um die Netzwerkadapter neu zu konfigurieren. Das Menü **Netzwerkadapter auswählen** führt alle verfügbaren Netzwerkadapter auf. Wählen Sie einen Netzwerkadapter aus, konfigurieren Sie seine Netzwerkparameter neu und wählen Sie **Anwenden** aus, um die Änderungen an der entsprechenden Schnittstelle zu speichern. Standardmäßig ist nur IPv4 auf der primären Netzwerkschnittstelle mit einer privaten statischen IP-Adresse in der Appliance aktiviert. Wenn jedoch eine neue Netzwerkschnittstelle hinzugefügt wird, werden sowohl IPv4 als auch IPv6 aktiviert, um Multihoming zu ermöglichen. Wenn die OpenManage Enterprise Appliance die IPv6-Adresse nicht ermitteln kann, überprüfen Sie, ob die Umgebung so konfiguriert ist, dass die Routerankündigung das verwaltete Bit (M) eingeschaltet hat. Network Manager von aktuellen Linux-Distributionen verursacht einen Link-Fehler, wenn dieses Bit

Tabelle 7. Optionen der textbasierten Benutzeroberfläche (fortgesetzt)

Optionen	Beschreibungen
	eingeschaltet, aber DHCPv6 nicht verfügbar ist. Stellen Sie sicher, dass DHCPv6 im Netzwerk aktiviert ist oder deaktivieren Sie die Managed-Markierung für die Router-Ankündigung. **ANMERKUNG:** • Die DNS-Konfiguration ist nur auf der primären Netzwerkschnittstelle verfügbar. Wenn die DNS-Auflösung auf dieser Schnittstelle erwünscht ist, müssen alle Hostnamen durch den DNS-Server auflösbar sein, der auf der primären Schnittstelle konfiguriert ist.
Primäre Netzwerkschnittstelle auswählen	Mit der Option **Primäre Netzwerkschnittstelle auswählen** können Sie ein primäres Netzwerk festlegen. Bei der Auswahl der primären Schnittstelle hat die ausgewählte Schnittstelle im Hinblick auf Routing Vorrang und die Schnittstelle wird als Standardroute verwendet. Diese Schnittstelle hat im Falle von Mehrdeutigkeit beim Routing Priorität. Die primäre Schnittstelle ist zudem als „öffentliche“ Schnittstelle vorgesehen, die ein Unternehmensnetzwerk/ eine Internetverbindung ermöglicht. Es werden verschiedene Firewallregeln auf die primäre Schnittstelle angewendet, die eine strengere Zugriffskontrolle ermöglichen, wie z. B. die Zugriffsbeschränkung nach IP-Bereich. **ANMERKUNG:** Multihoming ist aktiviert und der Zugriff auf die Appliance ist über zwei Netzwerke möglich. Beachten Sie, dass die primäre Schnittstelle von der Appliance für die gesamte externe Kommunikation und bei der Nutzung von Proxy-Einstellungen verwendet wird. Weitere Informationen zu Multihoming auf OpenManage finden Sie im technischen Whitepaper *Remote-Skriptausführung mit Dell EMC OpenManage Enterprise* auf der Support-Website.
Konfigurieren von statischen Routen	Wählen Sie **Statische Routen konfigurieren** aus, wenn für die Netzwerke eine statische Route konfiguriert werden muss, um ein bestimmtes Subnetz über die IPv4- und IPv6-Netzwerke zu erreichen. **ANMERKUNG:** Es werden maximal 20 statische Routen pro Schnittstelle unterstützt.
Konfigurieren von Server-initiierter Ermittlung	Wählen Sie **Server-initiierte Ermittlung konfigurieren** aus, um der Appliance zu erlauben, die erforderlichen Datensätze automatisch bei dem derzeit konfigurierten DNS-Server zu registrieren. **ANMERKUNG:** • Stellen Sie sicher, dass die Appliance bei DNS registriert ist und die Datensätze dynamisch aktualisieren kann. • Die Zielsysteme müssen so konfiguriert werden, dass Registrierungsdetails von DNS angefordert werden. • Stellen Sie zum Ändern des DNS-Domänennamens sicher, dass die dynamische DNS-Registrierung auf dem DNS-Server aktiviert ist. Außerdem muss die Appliance auf dem DNS-Server registriert werden, wählen Sie die Option **nicht sichere und sichere** unter "Dynamische Aktualisierungen".
Konfigurieren der Appliance-Datenträgergröße	Wählen Sie **Appliance-Datenträgergröße konfigurieren** aus, um die Verfügbarkeit von Festplattenspeicherplatz oder neuen

Tabelle 7. Optionen der textbasierten Benutzeroberfläche (fortgesetzt)

Optionen	Beschreibungen
	Festplatten zu suchen, und weisen Sie den zusätzlichen Speicherplatz oder die Festplatte(n) für die Appliance bei Bedarf zu. **ANMERKUNG:** ● Es wird dringend empfohlen, einen VM-Snapshot der Konsole als Backup zu erstellen, bevor Sie Änderungen an der Festplattenkonfiguration vornehmen. ● Nach dem Hinzufügen von Speicherplatz wird das Löschen oder Reduzieren von erweitertem Speicherplatz nicht unterstützt. Um eine neu hinzugefügte Festplatte zu entfernen oder um die Vergrößerung einer vorhandenen Festplatte umzukehren, müssen Sie den vorherigen VM-Snapshot wiederherstellen. ● Wenn der erste Scan keinen nicht zugewiesenen Speicherplatz erkennt, weisen Sie der Konsole auf dem Hypervisor zusätzlichen Speicherplatz oder Festplatten zu und suchen Sie erneut. ● Das Scannen und die Zuweisung von Speicherplatz ist auf maximal vier Festplatten beschränkt.
Aktivieren des Kundendienst-Debug (FSD)-Modus	Wählen Sie **Field Service Debug (FSD)-Modus aktivieren** für Konsolen-Debugging. Weitere Informationen finden Sie unter Kundendienst-Debugging-Workflow auf Seite 184.
Dienste neu starten	Wählen Sie **Services neu starten** mit den folgenden Optionen aus, um die Services und Netzwerke neu zu starten: ● **Alle Services neu starten** ● **Netzwerkbetrieb neu starten**
Debug-Protokollierung einrichten	Wählen Sie **Debug-Protokollierung einrichten** mithilfe der folgenden Optionen aus: ● **Aktivieren Sie Alle Debug-Protokolle,** ○ um die Debug-Protokollierung der Anwendung, die Überwachungsaufgaben, Ereignisse und den Task-Ausführungsverlauf zu erfassen. ● **Deaktivieren Sie Alle Debug-Protokolle,** ○ um die Debug-Protokollierung zu deaktivieren. ● **Konfigurieren Sie Debug-Protokollierung,** ○ Aktivieren Sie die Debug-Protokollierung für Appliance- und Plug-in-Services selektiv. ○ Verwenden Sie das Menü **Optionen** , um alle Services auszuwählen, jede Auswahl aufzuheben oder den Wiederherstellungsstatus zu löschen, bevor Sie Änderungen vornehmen. ● **SCP-Aufbewahrung aktivieren**: zum Erfassen der .XML-Vorlagedateien. ● **SCP-Aufbewahrung deaktivieren**: zum Deaktivieren der SCP-Aufbewahrung. Klicken Sie zum Herunterladen der Debug-Protokolle in OpenManage Enterprise auf **Überwachen** > **Auditprotokolle** > **Exportieren** > **Konsolenprotokolle exportieren**.
Tastatureinstellungen ändern	Wählen Sie **Tastatur-Layout ändern**, um das Tastaturlayout bei Bedarf zu ändern.
Neustart der Appliance	Wählen Sie **Appliance neu starten**, um die Appliance neu zu starten.

Tabelle 7. Optionen der textbasierten Benutzeroberfläche (fortgesetzt)

Optionen	Beschreibungen
	ANMERKUNG: Nach dem Ausführen eines Befehls zum Neustarten der Services zeigt der TUI möglicherweise die folgende Meldung an:`NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439].` Das Problem mit dem Soft-Hängenbleiben tritt wahrscheinlich als Ergebnis des überladenen Hypervisors auf. In derartigen Situationen wird empfohlen, mindestens 16 GB RAM und eine CPU-Leistung von 8000 MHz für die OpenManage Enterprise Appliance zu reservieren. Bei Anzeige dieser Meldung wird auch empfohlen, die OpenManage Enterprise Appliance neu zu starten.

OpenManage Enterprise konfigurieren

Wenn Sie sich zum ersten Mal bei OpenManage Enterprise anmelden, wird die Seite **Willkommen bei OpenManage Enterprise** angezeigt, auf der Sie die Uhrzeit (entweder manuell oder mithilfe der NTP-Zeitsynchronisierung) und die Proxy-Konfigurationen einstellen können.

1. Um die Uhrzeit manuell zu konfigurieren, führen Sie im Abschnitt **Zeitkonfiguration** folgende Schritte aus:
   - Verwenden Sie das Drop-Down-Menü für die **Zeitzone**, um eine geeignete Zeitzone auszuwählen.
   - Geben Sie im Feld **Datum** ein Datum ein oder wählen Sie es aus.
   - Geben Sie im Feld **Uhrzeit** die Uhrzeit ein.
   - Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.
2. Wenn Sie den NTP-Server zur Zeitsynchronisation verwenden möchten, führen Sie im Abschnitt **Zeitkonfiguration** folgende Schritte aus:

   ANMERKUNG: Wenn die NTP-Servereinstellungen aktualisiert werden, werden die derzeit angemeldeten Benutzer automatisch von ihren OpenManage Enterprise-Sitzungen abgemeldet.

   - Aktivieren Sie das Kontrollkästchen **NTP verwenden**.
   - Geben Sie die IP-Adresse oder den Hostnamen in **Primäre NTP-Serveradresse** und **Sekundäre NTP-Serveradresse** (optional) für die Zeitsynchronisierung ein.
3. Wenn Sie einen Proxy-Server für die externe Kommunikation einrichten möchten, gehen Sie im Abschnitt "Proxy-Konfiguration" wie folgt vor:
   - Aktivieren Sie das Kontrollkästchen **HTTP-Proxy-Einstellungen aktivieren**.
   - Geben Sie die **Proxy-Adresse** ein.
   - Geben Sie die **Portnummer** für den Proxy-Server ein.
   - Wenn der Proxy-Server einen Berechtigungsnachweis für die Anmeldung erfordert, aktivieren Sie das Kontrollkästchen **Proxy-Authentifizierung aktivieren** und geben Sie den Benutzernamen und das Kennwort ein.
   - Aktivieren Sie das Kontrollkästchen **Zertifikat-Validierung ignorieren**, wenn der konfigurierte Proxy den SSL-Datenverkehr abfängt und kein vertrauenswürdiges Drittanbieterzertifikat verwendet. Mit dieser Option werden die integrierten Zertifikat-Prüfungen ignoriert, die für den Service und die Katalogsynchronisierung verwendet werden.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

ANMERKUNG: Weitere Informationen zu unterstützten Browsern finden Sie unter *OpenManage Enterprise-Supportmatrix* auf der Support-Website.

Empfohlene Skalierbarkeit und Leistungseinstellungen für eine optimale Nutzung von OpenManage Enterprise

In der folgenden Tabelle ist eine Liste der Leistungsparameter der in OpenManage Enterprise unterstützten Funktionen aufgeführt. Zur Sicherstellung einer optimalen Performance von OpenManage Enterprise empfiehlt Dell EMC, die Aufgaben in der angegebenen Häufigkeit auf der für die Aufgabe empfohlenen maximalen Anzahl von Geräten auszuführen.

Tabelle 8. Skalierbarkeit und Leistungsaspekte von OpenManage Enterprise

Tasks	Empfohlene Häufigkeit für die Ausführung der Aufgaben	Wurden Aufgaben vordefiniert?	Maximale Anzahl der Geräte, die pro Aufgabe empfohlen werden.
Ermittlung	Einmal täglich für eine Umgebung mit häufigen Netzwerkänderungen.	Nein	10.000/Aufgabe
Bestandsaufnahme	OpenManage Enterprise bietet eine vordefinierte Aufgabe, die die Bestandsaufnahme einmal täglich aktualisiert.	Ja. Sie können diese Funktion deaktivieren.	Von OpenManage Enterprise überwachte Geräte.
Gewährleistung	OpenManage Enterprise bietet eine vordefinierte Aufgabe, die die Gewährleistung einmal täglich aktualisiert.	Ja. Sie können diese Funktion deaktivieren.	Von OpenManage Enterprise überwachte Geräte.
Funktionszustandsabfrage	Stündlich	Ja. Sie können die Häufigkeit ändern.	Nicht anwendbar
Firmware-/Treiberaktualisierung	Bedarfsbasiert		150/Aufgabe
Konfigurationsbestandsaufnahme	Bedarfsbasiert		1500/Baseline

Unterstützte Protokolle und Schnittstellen in OpenManage Enterprise

Unterstützte Protokolle und Ports auf Verwaltungsstationen

Tabelle 9. Von OpenManage Enterprise unterstützte Protokolle und Ports auf Verwaltungsstationen

Portnummer	Protokoll	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Quelle	Richtung	Ziel	Verwendung
22	SSH	TCP	256-Bit	Verwaltungsstation	Eingang	OpenManage Enterprise Anwendung	• Nur für eingehende Kommunikation erforderlich, wenn FSD verwendet wird. Der OpenManage Enterprise-Administrator darf nur bei Interaktionen mit einem Dell EMC Support-Mitarbeiter aktiviert werden.

Tabelle 9. Von OpenManage Enterprise unterstützte Protokolle und Ports auf Verwaltungsstationen (fortgesetzt)

Portnummer	Protokoll	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Quelle	Richtung	Ziel	Verwendung
25	SMTP	TCP	Keine	OpenManage Enterprise Anwendung	Ausgang	Verwaltungsstation	• Zum Empfang von E-Mail-Warnungen von OpenManage Enterprise.
53	DNS	UDP/TCP	Keine	OpenManage Enterprise Anwendung	Ausgang	Verwaltungsstation	• Für DNS-Abfragen.
68 / 546 (IPv6)	DHCP	UDP/TCP	Keine	OpenManage Enterprise Anwendung	Ausgang	Verwaltungsstation	• Netzwerkkonfiguration.
80*	HTTP	TCP	Keine	Verwaltungsstation	Eingang	OpenManage Enterprise Anwendung	• Die Web-GUI Landingpage. Dadurch wird ein Nutzer zu HTTPS (Port 443) umgeleitet.
123	NTP	TCP	Keine	OpenManage Enterprise Anwendung	Ausgang	NTP-Server	• Zeitsynchronisierung (falls aktiviert).
137, 138, 139, 445	CIFS	UDP/TCP	Keine	iDRAC/CMC	Eingang	OpenManage Enterprise Anwendung	• Zum Hochladen oder Herunterladen von Gerätebereitstellungsvorlagen. • Zum Hochladen von TSR- und Diagnoseprotokollen. • Zum Herunterladen von Firmware/ Treiber-DUPs und Ausführen des FSD-Prozesses. • Start auf Netzwerk-ISO
				OpenManage Enterprise Anwendung	Ausgang	CIFS-Freigabe	• So importieren Sie Firmware/ Treiber-Kataloge von der CIFS-Freigabe:
111, 2049 (Standard)	NFS	UDP/TCP	Keine	OpenManage Enterprise Anwendung	Ausgang	Externe NFS-Freigabe	• Zum Herunterladen von Katalog- und DUPS von der NFS-Freigabe für Firmware-Aktualisierungen. • Für manuelles Konsolen-Upgrade von einer Netzwerkfreigabe.
162*	SNMP	UDP	Keine	Verwaltungsstation	Ein/Aus	OpenManage Enterprise Anwendung	• Ereignisempfang über SNMP. Die Richtung ist nur

Tabelle 9. Von OpenManage Enterprise unterstützte Protokolle und Ports auf Verwaltungsstationen (fortgesetzt)

Portnummer	Protokoll	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Quelle	Richtung	Ziel	Verwendung
							„Ausgehend“, wenn die Trap-Weiterleitungsrichtlinie verwendet wird.
443 (Standardeinstellung)	HTTPS	TCP	128 Bit SSL	Verwaltungsstation	Ein/Aus	OpenManage Enterprise Anwendung	• Web-GUI. • Zum Herunterladen von Updates und Gewährleistungsinformationen von Dell.com. Die 256-Bit-Verschlüsselung ist zulässig, wenn per HTTPS über die Web-GUI mit OpenManage Enterprise kommuniziert wird. • Server-initiierte Ermittlung.
514	Syslog	TCP	Keine	OpenManage Enterprise Anwendung	Ausgang	Syslog-Server	• Zum Senden von Warn- und Auditprotokollinformationen an den Syslog-Server.
3269	LDAPS	TCP	Keine	OpenManage Enterprise Anwendung	Ausgang	Verwaltungsstation	• AD-/LDAP-Anmeldung für den globalen Katalog.
636	LDAPS	TCP	Keine	OpenManage Enterprise Anwendung	Ausgang	Verwaltungsstation	• AD-/LDAP-Anmeldung für Domain Controller.

* Port kann bis zu 499 konfiguriert werden, ausschließlich der Portnummern, die bereits zugewiesen wurden.

Unterstützte Protokolle und Schnittstellen auf verwalteten Knoten

Tabelle 10. Von OpenManage Enterprise unterstützte Protokolle und Ports auf den verwalteten Knoten

Portnummer	Protokoll	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Quelle	Richtung	Ziel	Verwendung
22	SSH	TCP	256-Bit	OpenManage Enterprise Anwendung	Ausgang	Verwalteter Knoten	• Für die Linux OS, Windows und Hyper-V-Ermittlung.
161	SNMP	UDP	Keine	OpenManage Enterprise Anwendung	Ausgang	Verwalteter Knoten	• Für SNMP-Abfragen.
162*	SNMP	UDP	Keine	OpenManage Enterprise Anwendung	Ein/Aus	Verwalteter Knoten	• Senden und Empfangen von SNMP-Traps
443	Proprietär /WS-	TCP	256-Bit	OpenManage Enterprise Anwendung	Ausgang	Verwalteter Knoten	• Ermittlung und Bestandsaufnahme von iDRAC7 und neueren Versionen.

Tabelle 10. Von OpenManage Enterprise unterstützte Protokolle und Ports auf den verwalteten Knoten (fortgesetzt)

Portnummer	Protokoll	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Quelle	Richtung	Ziel	Verwendung
	Man/ Redfish						• Für die CMC-Verwaltung.
623	IPMI/ RMCP	UDP	Keine	OpenManage Enterprise Anwendung	Ausgang	Verwalteter Knoten	• IPMI-Zugang über LAN.
69	TFTP	UDP	Keine	CMC	Eingang	Verwaltungsstation	• Zur Aktualisierung der CMC-Firmware.

* Port kann bis zu 499 konfiguriert werden, ausschließlich der Portnummern, die bereits zugewiesen wurden.

ANMERKUNG: In einer IPv6-Umgebung müssen Sie IPv6 in der OpenManage Enterprise Appliance aktivieren und IPv4 deaktivieren, um sicherzustellen, dass alle Funktionen wie erwartet funktionieren.

Links zu Anwendungsfällen für unterstützte Protokolle und Schnittstellen in OpenManage Enterprise

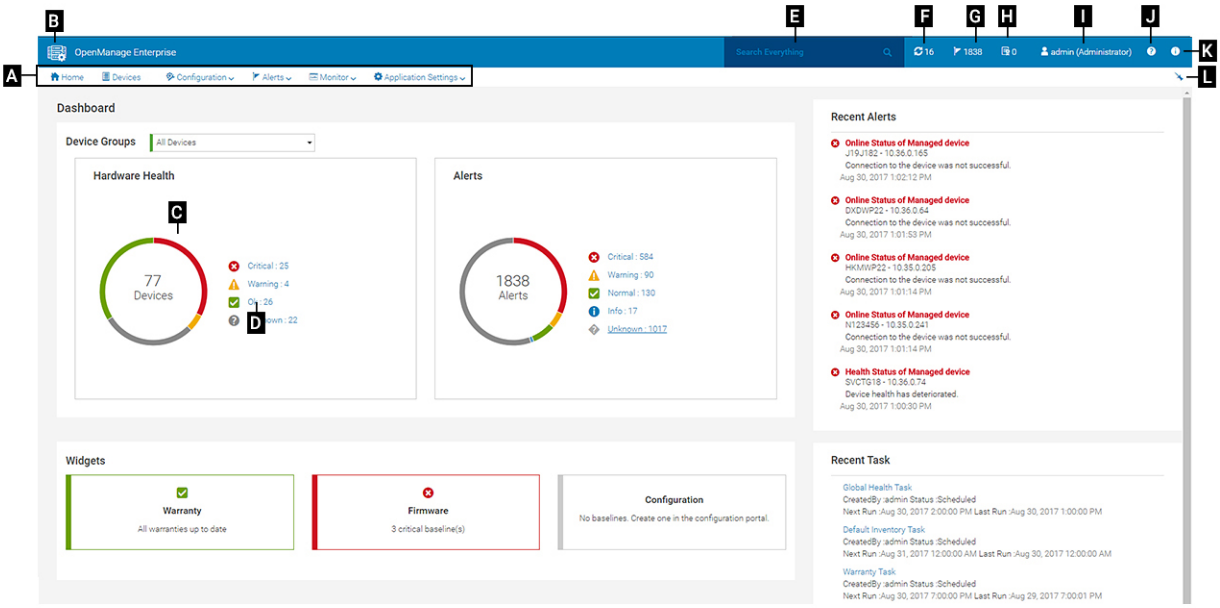
Tabelle 11. Links zu Anwendungsfällen für unterstützte Protokolle und Schnittstellen in OpenManage Enterprise

Anwendungsfall	URL
Aktualisieren der OpenManage Enterprise Anwendung	https://downloads.dell.com/openmanage_enterprise/
Zugriff auf Gerätegewährleistung	https://apigtwb2c.us.dell.com/PROD/sbil/eapi/v5/asset-entitlements
Kataloge aktualisieren	https://downloads.dell.com/catalog/
Übertragen Sie neue Warnungsbenachrichtigungen mithilfe der OpenManage Mobile-App.	https://openmanagecloud.dell.com

5

Übersicht über die grafische Benutzeroberfläche von OpenManage Enterprise

In der OpenManage Enterprise-GUI können Sie Menüoptionen, Links, Schaltflächen, Fensterbereiche, Dialogfelder, Listen, Registerkarten, Filterfelder und Seiten verwenden, um zwischen den Seiten zu navigieren und Gerätemanagementaufgaben abzuschließen. Funktionen, wie z. B. die Geräteliste, Ringdiagramme, Auditprotokolle, OpenManage Enterprise-Einstellungen, Systemwarnungen und Firmware-/Treiber-Update, werden an mehr als einer Stelle angezeigt. Es wird empfohlen, dass Sie sich mit den GUI-Elementen für eine schnelle und effektive Nutzung von OpenManage Enterprise für die Verwaltung Ihrer Geräte im Rechenzentrum vertraut machen.



- A – Das **OpenManage Enterprise**-Menü auf allen Seiten von OpenManage Enterprise enthält Links zu Funktionen, die es Administratoren ermöglichen, das Dashboard anzuzeigen (**Home**), Geräte zu verwalten (**Geräte**), Firmware-/Treiber-Baselines, Vorlagen und Konfigurations-Compliance-Baselines zu verwalten (**Konfiguration**), Warnmeldungen zu erstellen und zu speichern (**Warnungen**) und dann Jobs auszuführen, Bestandsdaten zu finden und zu erfassen und Berichte zu generieren (**Überwachen**). Sie können auch verschiedene Eigenschaften von OpenManage Enterprise anpassen (**Anwendungseinstellungen**). Klicken Sie auf das Stecknadel-Symbol in der oberen rechten Ecke, um die Menüelemente zu fixieren, sodass sie auf allen OpenManage Enterprise-Seiten erscheinen. Um die Fixierung aufzuheben, klicken Sie erneut auf das Stecknadel-Symbol.
- B – Das Dashboard-Symbol. Klicken Sie auf das Symbol, um die Dashboard-Seite von einer beliebigen Seite in OpenManage Enterprise zu öffnen. Alternativ dazu klicken Sie auf **Home**. Siehe Dashboard.
- C – Das Ringdiagramm stellt Ihnen einen Snapshot des Zustands aller von OpenManage Enterprise überwachten Geräte bereit. Ermöglicht Ihnen die schnell auf Geräte in einem kritischen Zustand zu reagieren. Jede Farbe auf dem Diagramm steht für eine Gerätegruppe in einem bestimmten Zustand. Klicken Sie auf die jeweiligen Farbbänder, um die entsprechenden Geräte in der Geräteliste anzuzeigen. Klicken Sie auf den Gerätenamen oder die IP-Adresse, die Seite der Geräteeigenschaften anzuzeigen. Informationen dazu finden Sie unter Anzeigen und Konfigurieren einzelner Geräte auf Seite 68.
- D – Die Symbole zur Anzeige des Gerätezustands. Informationen dazu finden Sie unter Gerätefunktionsstatus auf Seite 40.
- E – Geben Sie in das Feld **Alles suchen** irgendetwas ein, das von OpenManage Enterprise überwacht und angezeigt wird, um die Ergebnisse, wie z. B. Geräte-IP, Jobname, Gruppenname, Firmware-Baseline und Gewährleistungsdaten, für alle Geräte in Ihrem von der bereichsbezogenen Zugriffskontrolle (SBAC) angegebenen Bereich anzuzeigen. Sie können Daten, die durch die Verwendung der Funktion „Alles suchen" abgerufen wurden, nicht sortieren oder exportieren. Auf den einzelnen Seiten oder in Dialogfeldern können Sie Kriterien eingeben oder aus dem Abschnitt **Filter erweitern** auswählen, um die Suchergebnisse zu verfeinern.

  - **Die folgenden Operatoren werden nicht unterstützt: +, - und ".**

- F – Anzahl der OpenManage Enterprise-Jobs, die sich derzeit in der Warteschlange befinden. Jobs im Zusammenhang mit Erkennung, Bestandsaufnahme, Gewährleistung, Firmware- und/oder Treiber-Aktualisierung und so weiter. Klicken Sie zum Anzeigen des Status von Jobs in den Kategorien Zustand, Bestand und Bericht auf die Seite mit Job-Details. Um alle Ereignisse anzuzeigen, klicken Sie auf **Alle Jobs**. Informationen dazu finden Sie unter Verwenden von Jobs zur Gerätesteuerung auf Seite 130. Klicken Sie auf "Aktualisieren".
- G – Die Anzahl der im Warnmeldungsprotokoll generierten Ereignisse. Außerdem variiert die Anzahl der Warnungen in diesem Abschnitt je nach Ihren Einstellungen, ob unbestätigte Warnungen angezeigt werden sollen oder nicht. Standardmäßig werden nur unbestätigte Warnungen angezeigt. Informationen zum Ein- oder Ausblenden der bestätigten Benachrichtigungen finden Sie unter Anpassen der Warnungsanzeige auf Seite 167. Löschen der Warnmeldungen verringert den Zählwert. Weitere Informationen über Symbole für die Anzeige des Schweregrads finden Sie unter Gerätefunktionsstatus auf Seite 40. Klicken Sie auf ein Schweregrad-Symbol, um alle Ereignisse in dieser Schweregrad-Kategorie auf der Seite mit Warnungen anzeigen. Um alle Ereignisse anzuzeigen, klicken Sie auf **Alle Ereignisse**. Siehe Verwalten von Gerätewarnungen.
- H: Gesamtanzahl der Geräteservices in den Statuszuständen "Kritisch" (abgelaufen) und "Warnung" (bald ablaufend). Siehe Verwalten der Gerätegewährleistung.
- I–Name des Benutzers, der aktuell angemeldet ist. Positionieren Sie den Mauszeiger über den Nutzernamen, um die Rollen, die dem Benutzer zugewiesen sind, anzuzeigen. Weitere Informationen zu rollenbasierten Benutzern finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16. Klicken Sie zum Abmelden und melden Sie sich dann wieder als anderer Benutzer an.
- J–Derzeit wird die kontextabhängige Hilfe-Datei nur für die Seite angezeigt, auf der Sie sich befinden und nicht für die Home-Portalseiten. Klicken Sie auf diese Option, um die aufgabenbasierten Anweisungen zur effektiven Verwendung von Links, Schaltflächen, Dialogfeldern, Assistenten und Seiten in OpenManage Enterprise anzuzeigen.
- K – Klicken Sie zur Anzeige der aktuell auf dem System installierten Version von OpenManage Enterprise. Klicken Sie auf **Lizenzen**, um die Nachricht zu lesen. Klicken Sie auf die entsprechenden Links, um Open-Source-Dateien oder andere Open-Source-Lizenzen in Verbindung mit OpenManage Enterprise anzuzeigen und herunterzuladen.
- L – Klicken Sie auf das Symbol, um Menüelemente zu fixieren oder die Fixierung aufzuheben. Wenn sie nicht fixiert sind, erweitern Sie zum Fixieren der Menüoptionen das Menü **OpenManage Enterprise** und klicken auf das Stecknadel-Symbol.

Daten über in einer Tabelle aufgeführte Elemente können alle angezeigt und insgesamt oder basierend auf den ausgewählten Elementen exportiert werden. Informationen dazu finden Sie unter Alle oder ausgewählte Daten exportieren auf Seite 68. Bei der Anzeige in blauem Text können fundierte Informationen zu Elementen in einer Tabelle angezeigt und aktualisiert werden, die entweder im gleichen Fenster oder auf einer separaten Seite geöffnet werden. Tabulierte Daten können über die Funktion **Erweiterte Filter** gefiltert werden. Die Filter variieren je nach Inhalt, den Sie anzeigen. Geben Sie Daten in die folgenden Felder ein oder wählen Sie diese aus: Unvollständiger Text oder unvollständige Zahlen ergeben nicht die erwartete Ausgabe. Daten, die den Filterkriterien entsprechen, werden in der Liste angezeigt. Um die Filter zu entfernen, klicken Sie auf **Alle Filter löschen**.

Um die Daten zu sortieren, klicken Sie auf eine Spaltenüberschrift. Sie können Daten, die durch die Verwendung der Funktion „Alles suchen“ abgerufen wurden, nicht sortieren oder exportieren.

Symbole werden verwendet, um die wichtigsten Elemente, Dashboard, Status des Gerätezustands, Warnmeldungskategorie, Firmware- und Treiber-Compliance-Status, Verbindungsstatus, Stromstatus und andere zu identifizieren. Klicken Sie auf die Schaltfläche „Vorwärts“ oder „Rückwärts“ des Browsers zum Navigieren zwischen Seiten auf OpenManage Enterprise. Weitere Informationen zu unterstützten Browsern finden Sie auf der*Dell EMC OpenManage Enterprise-Supportmatrix* auf der Support-Website.

Gegebenenfalls ist die Seite aufgeteilt in linke, Arbeits- und rechte Fensterbereiche zur Vereinfachung der Aufgaben des Gerätemanagements. Gegebenenfalls werden Online-Anweisungen und Quickinfos angezeigt, wenn der Zeiger über ein GUI-Element gehalten wird.

Vorschau über ein Gerät, einen Job, eine Bestandsaufnahme, eine Firmware-/Treiber-Baseline, eine Managementanwendung, eine virtuelle Konsole usw. wird im rechten Fensterbereich angezeigt. Wählen Sie ein Element im Arbeitsbereich und klicken Sie auf **Details anzeigen** im rechten Fensterbereich, um fundierte Informationen über den Eintrag anzuzeigen.

Bei einer Anmeldung werden alle Seiten automatisch aktualisiert. Nach der Bereitstellung der Appliance werden Sie, wenn eine aktualisierte Version von OpenManage Enterprise verfügbar ist, während der nachfolgenden Anmeldung sofort zum Aktualisieren der Version durch Klicken auf **Aktualisieren** benachrichtigt. Benutzer mit allen OpenManage Enterprise-Berechtigungen (Administrator, Geräte-Manager und Betrachter) können die Nachricht anzeigen, aber nur ein Administrator kann die Version aktualisieren. Ein Administrator kann sich später daran erinnern lassen oder die Nachricht ablehnen Weitere Informationen zum Update der OpenManage Enterprise-Version finden Sie unter Überprüfen und Aktualisieren der Version von OpenManage Enterprise und der verfügbaren Plug-ins auf Seite 170.

Für alle jobbasierten Maßnahmen durch OpenManage Enterprise wird, wenn ein Job erstellt oder zur Ausführung gestartet wird, in der rechten unteren Ecke die entsprechende Meldung angezeigt. Informationen zum Job können auf der Seite **Job-Details** angezeigt werden. Informationen dazu finden Sie unter Anzeigen von Joblisten auf Seite 130.

6

OpenManage Enterprise Startportal

Durch Klicken auf **OpenManage Enterprise** > **Home** wird die Startseite von OpenManage Enterprise angezeigt. Auf der Startseite:

- Rufen Sie das Dashboard auf, um einen Live Snapshot über die Funktionszustände der Geräte zu erhalten, und ergreifen Sie dann Maßnahmen, wo erforderlich. Siehe Dashboard.
- Zeigen Sie Warnungen der Kategorien „Kritisch“ und „Warnung“ an, und beheben Sie die entsprechenden Probleme. Siehe Verwalten von Gerätewarnungen.
- Im Abschnitt „Widgets“ werden die Rollup-Gewährleistung, die Firmware-/Treiber-Compliance und der Compliance-Status aller Geräte aufgelistet. Weitere Informationen über die Funktionen unter Widgets finden Sie unter Überwachen Sie Geräte mit dem OpenManage Enterprise-Dashboard auf Seite 38. Im rechten Fensterbereich werden die letzten Warnmeldungen und Aufgaben von OpenManage Enterprise erstellt. Zum Anzeigen weiterer Informationen zu einer Warnung oder Aufgabe anzuzeigen, klicken Sie auf den Warnungs- oder Aufgabentitel. Siehe Überwachen und Verwalten von Gerätewarnungen auf Seite 118 und Verwenden von Jobs zur Gerätesteuerung auf Seite 130.
- Wenn eine aktualisierte Version von OpenManage Enterprise verfügbar ist, werden Sie sofort darauf hingewiesen, wenn ein Update verfügbar ist. Zum Aktualisieren klicken Sie auf **Aktualisieren**. Weitere Informationen zum Update der OpenManage Enterprise-Version finden Sie unter Überprüfen und Aktualisieren der Version von OpenManage Enterprise und der verfügbaren Plug-ins auf Seite 170.
- Im Abschnitt **Letzte Warnungen** sind die zuletzt von durch OpenManage Enterprise überwachte Geräte erzeugten Warnungen aufgeführt. Klicken Sie auf den Warnungstitel, um ausführliche Informationen zur Warnung anzuzeigen. Siehe Verwalten von Gerätewarnungen.
- Im Abschnitt **Letzte Aufgaben** werden die zuletzt erstellten und ausgeführten Tasks aufgeführt. Klicken Sie auf den Task-Titel, um ausführliche Informationen zum Job anzuzeigen. Informationen dazu finden Sie unter Anzeigen von Joblisten auf Seite 130.

ANMERKUNG: Wenn Sie als Geräte-Manager angemeldet sind, zeigt das Startseite-Portal Informationen in Verbindung mit dem Gerät/der Gerätegruppe an, die der DM besitzt. Außerdem werden in der Dropdown-Liste „Gerätegruppen“ nur die Gerätegruppen aufgeführt, auf die der Geräte-Manager über betrieblichen Zugriff verfügt. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Themen:

Überwachen Sie Geräte mit dem OpenManage Enterprise-Dashboard

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Abgesehen von der erstmaligen Anmeldung ist das Dashboard die erste Seite, die Ihnen nach jeder nachfolgenden Anmeldung bei OpenManage Enterprise angezeigt wird.

Zum Öffnen der Seite „Dashboard“ von einer beliebigen Seite von OpenManage Enterprise aus klicken Sie auf das Dashboard-Symbol in der oberen linken Ecke. Alternativ dazu klicken Sie auf **Home**.

Anhand von Echtzeitüberwachungsdaten zeigt das Dashboard den Gerätefunktionszustand, Firmware-/Treiber-Compliance, Gewährleistung, Warnungen und andere Aspekte der Geräte und Gerätegruppen in Ihrer Rechenzentrumsumgebung an.

Alle verfügbaren Konsolen-Updates werden auch auf dem Dashboard angezeigt. Sie können sofort ein Upgrade der OpenManage Enterprise-Version durchführen oder OpenManage Enterprise so konfigurieren, dass es Sie zu einem späteren Zeitpunkt daran erinnert.

Standardmäßig wird beim erstmaligen Starten der Anwendung die Seite „Dashboard“ leer angezeigt. Fügen Sie Geräte zu OpenManage Enterprise hinzu, damit sie überwacht und auf dem Dashboard angezeigt werden können. Informationen zum Hinzufügen von Geräten finden Sie unter Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41 und Geräte in Gruppen organisieren auf Seite 55.

- Verwalten der Geräte-Firmware und -Treiber auf Seite 77
- Verwalten von Gerätewarnungen
- Ermitteln von Geräten
- Erstellen von Berichten
- Verwalten von OpenManage Enterprise-Geräteeinstellungen auf Seite 148

ANMERKUNG: Wenn Sie eine Gerätegruppe in der Dropdown-Liste **Gerätegruppen** auswählen, werden alle auf dem Dashboard angezeigten Daten nur für die ausgewählte Gerätegruppe angezeigt.

Standardmäßig zeigt der Abschnitt **Hardware-Funktionszustand** ein Ringdiagramm an, in dem der aktuelle Zustand aller von OpenManage Enterprise überwachten Geräten angezeigt wird. Klicken Sie auf die Abschnitte des Ringdiagramms, um Informationen über die Geräte zusammen mit den entsprechenden Funktionszuständen anzuzeigen.

Ein Ringdiagramm im Abschnitt **Warnungen** gibt einen Überblick über die von Geräten empfangenen Warnungen in den ausgewählten Gerätegruppen. Informationen dazu finden Sie unter Überwachen und Verwalten von Gerätewarnungen auf Seite 118. Die Gesamtzahl der Warnungen im Ringdiagramm variiert je nach Einstellung, ob unbestätigte Warnungen angezeigt werden sollen oder nicht. Standardmäßig werden nur unbestätigte Warnungen angezeigt. Informationen dazu finden Sie unter Anpassen der Warnungsanzeige auf Seite 167. Zur Anzeige von Warnungen unter jeder Kategorie klicken Sie auf die entsprechenden Farbbänder. Im Dialogfeld **Warnungen** werden im „Kritischen Bereich" die Warnungen in einem kritischen Zustand aufgeführt. Zur Anzeige aller generierten Warnungen klicken Sie auf **Alle**. In der Spalte **QUELLENNAME** wird das Gerät angezeigt, das die Warnung generiert hat. Klicken Sie auf den Namen, um die Gerätedetails anzuzeigen und zu konfigurieren. Informationen dazu finden Sie unter Anzeigen und Konfigurieren einzelner Geräte auf Seite 68.

Weitere Informationen über das Ringdiagramm finden Sie unter Ringdiagramm auf Seite 40 und Gerätefunktionsstatus auf Seite 40. Um die Zusammenfassung von Geräten in einer anderen von OpenManage Enterprise überwachten Gerätegruppe anzuzeigen, treffen Sie eine Auswahl im Drop-Down-Menü **Gerätegruppen**. Zum Anzeigen der Liste der Geräte, die zu einem Funktionszustand gehören, können Sie entweder auf das Farbband der entsprechenden Funktionszustands-Kategorie oder auf das betreffende Funktionszustands-Symbol neben einem Ringdiagramm klicken.

ANMERKUNG: Klicken Sie in der Geräteliste auf den Gerätenamen oder die IP-Adresse, um Device-Konfigurationsdaten anzuzeigen, und bearbeiten Sie dann die Device-Konfiguration. Informationen dazu finden Sie unter Anzeigen und Konfigurieren einzelner Geräte auf Seite 68.

Der Widgets-Abschnitt liefert einen Überblick über die wichtigsten Funktionen von OpenManage Enterprise. Zum Anzeigen eines Überblicks unter jeder Kategorie klicken Sie auf den Widget-Titel.

- **Gewährleistung**: Zeigt die Anzahl der Geräte an, deren Garantie bald abläuft. Dies beruht auf den **Gewährleistungseinstellungen**. Wenn sich der Benutzer für die Benachrichtigung über den Ablauf der Gewährleistung entscheidet, wird die Anzahl der Geräte angezeigt, deren Gewährleistung abgelaufen ist. Andernfalls wird die Anzahl der in Kürze ablaufenden oder die Anzahl der aktiven Gewährleistungen angezeigt. Klicken Sie auf das Dialogfeld **Gewährleistung**, um weitere Informationen anzuzeigen. Informationen zum Verwalten der Gerätegewährleistung finden Sie unter Verwalten der Gerätegewährleistung auf Seite 138. Pausieren Sie den Mauszeiger über dem Abschnitt **Gewährleistung**, um die Definitionen über die in dem Abschnitt verwendeten Symbole zu lesen.
- **Firmware/Treiber**: zeigt den Status der Firmware-/Treiber-Compliance der Geräte-Baselines an, die auf OpenManage Enterprise erstellt wurden. Die Firmware-/Treiber-Baselines „Kritisch" und „Warnung" werden in diesem Abschnitt aufgeführt, falls sie verfügbar sind.
  - Weitere Informationen über das Integritätsstatus-Rollup finden Sie im technischen Whitepaper *VERWALTEN DES INTEGRITÄTSSTATUS-ROLLUP DURCH VERWENDUNG VON IDRAC AUF DELL EMC POWEREDGE SERVERN DER 14. GENRATION UND SPÄTER* im Dell TechCenter.
  - Klicken Sie auf das Dialogfeld **Firmware-/Treiber-Compliance**, um weitere Informationen anzuzeigen.
  - Weitere Informationen zum Aktualisieren von Firmware, Erstellen von Firmwarekatalogen, Erstellen einer Firmware-Baseline und Erstellen von Baseline-Compliance-Berichten finden Sie unter Verwalten der Geräte-Firmware und -Treiber auf Seite 77.
- **Konfiguration**: Zeigt den Rollup-Status der in OpenManage Enterprise erstellten Konfigurations-Compliance-Baselines an. Die Konfigurations-Baselines Kritisch und Warnung werden aufgelistet, falls sie verfügbar sind. Informationen dazu finden Sie unter Verwalten von Compliance-Vorlagen auf Seite 111.
- **Ressourcenauslastung**: zeigt die CPU- und die Arbeitsspeicherauslastung durch die Appliance an. Die folgenden farbcodierten Prüfungen werden verwendet, um die verschiedenen Phasen der Auslastung anzuzeigen:
  - Grün: eine Auslastung von weniger als 80 % der Ressource
  - Gelb: mehr als 80 %, aber weniger als 95 % Auslastung der Ressource
  - Rot: eine Auslastung von mehr als 95 % der Ressource

  ANMERKUNG: Die gesamte Ressourcenauslastung, die als farbcodierter vertikaler Balken links im Widget dargestellt wird, ist der Worst-Case-Rollup einer beliebigen Ressource.

Ringdiagramm

In verschiedenen Bereichen von OpenManage Enterprise können Sie ein Ringdiagramm anzeigen. Die Ausgabe, die vom der Ringdiagramm angezeigt wird, basiert auf den Elementen, die Sie in einer Tabelle wählen. Ein Ringdiagramm weist auf mehrere Status in OpenManage Enterprise hin:

- Integritätsstatus der Geräte: Angezeigt auf der Dashboard-Seite. Die Farben im Ringdiagramm teilen den Ring proportional, um den Zustand der von OpenManage Enterprise überwachten Geräte anzugeben. Jeder Gerätestatus wird durch ein farbiges Symbol gekennzeichnet. Informationen dazu finden Sie unter Gerätefunktionsstatus auf Seite 40. Wenn das Ringdiagramm den Integritätsstatus der 279 Geräte in der Gruppe anzeigt, wobei 131=kritisch, 50=Warnung und 95=ok lauten, wird der Kreis durch die Verwendung von Farbbändern gebildet, die proportional diese Werte repräsentieren.

ANMERKUNG: Das Ringdiagramm eines einzelnen Geräts wird durch einen dicken Kreis mit nur einer Farbe gebildet, die den Gerätestatus angibt. Für ein Gerät im Status „Warnung" wird ein gelber Kreis angezeigt.

- Der Warnstatus von Geräten: Zeigt alle Warnungen an, die für die durch OpenManage Enterprise überwachten Geräte erzeugt wurden. Informationen dazu finden Sie unter Überwachen und Verwalten von Gerätewarnungen auf Seite 118.

  ANMERKUNG: Die Gesamtzahl der Warnungen im Ringdiagramm variiert je nach Einstellung, ob unbestätigte Warnungen angezeigt werden sollen oder nicht. Standardmäßig werden nur unbestätigte Warnungen angezeigt. Informationen dazu finden Sie unter Anpassen der Warnungsanzeige auf Seite 167.
- Zur Übereinstimmung der Firmware-Version eines Geräts mit der Version im Katalog: Siehe Verwalten der Geräte-Firmware und -Treiber auf Seite 77.
- Zur Baseline der Konfigurationsübereinstimmung für Geräte und Gerätegruppen: Siehe Verwalten der Device-Konfigurations-Compliance auf Seite 110.

ANMERKUNG: Die Konformitätsstufe des ausgewählten Geräts wird durch ein Ringdiagramm angegeben. Wenn mehr als ein Gerät einer Baseline zugeordnet ist, wird der Status des Geräts mit der geringsten Konformitätsstufe in Bezug auf die Baseline als die Konformitätsstufe dieser Baseline angegeben. Beispiel: Wenn viele Geräte mit einer Firmware-Baseline verknüpft sind und die Konformitätsstufe nur weniger Geräte „Fehlerfrei" oder „Zurückstufen" ist, die Übereinstimmung eines Geräts in der Gruppe jedoch „Aktualisieren" ist Die Konformitätsstufe der Firmware-Baseline wird als „Upgrade" angegeben. Der Rollup-Status entspricht dem Status des Geräts mit hohem Schweregrad. Weitere Informationen über das Integritätsstatus-Rollup finden Sie im technischen Whitepaper *VERWALTEN DES INTEGRITÄTSSTATUS-ROLLUP DURCH VERWENDUNG VON IDRAC AUF DELL EMC POWEREDGE SERVERN DER 14. GENRATION UND SPÄTER* im Dell TechCenter.

ANMERKUNG: Das Ringdiagramm eines einzelnen Geräts wird durch einen dicken Kreis mit nur einer Farbe gebildet, die die Firmware-Konformitätsstufe des Geräts angibt. Zum Beispiel wird für ein Gerät mit kritischem Zustand ein roter Kreis angezeigt, der angibt, dass die Firmware des Geräts aktualisiert werden muss.

Gerätefunktionsstatus

Tabelle 12. Geräte-Funktionszustände in OpenManage Enterprise

Funktionsstatus	Definition
Kritisch	Weist darauf hin, dass bei einem wichtigen Aspekt des Geräts oder der Umgebung ein Fehler aufgetreten ist.
Warnung	Das Gerät wird in Kürze ausfallen. Zeigt an, dass einige Aspekte des Geräts oder der Umgebung nicht normal funktionieren. Erfordert sofortige Aufmerksamkeit.
OK	Das Gerät ist voll funktionsfähig.
Unbekannt	Der Gerätestatus ist unbekannt.

ANMERKUNG: Die auf dem Dashboard angezeigten Daten hängen von den Berechtigungen ab, die Ihnen bei der Verwendung von OpenManage Enterprise zur Verfügung stehen. Weitere Informationen zu den Nutzern finden Sie unter Verwalten von Nutzern.

7

Ermitteln von Geräten für die Überwachung oder Verwaltung

Indem Sie das Menü **OpenManage Enterprise** > **Überwachen** > **Ermittlung** auswählen, können Sie die Geräte in Ihrer Rechenzentrumsumgebung ermitteln, um diese zu verwalten, ihre Nutzbarkeit zu verbessern und die Ressourcenverfügbarkeit für Ihre geschäftskritischen Abläufe zu verbessern. Auf der Seite **Ermittlung** werden die Anzahl der in der Task ermittelten Geräte und Informationen zum Status des Ermittlungsjobs für dieses Gerät angezeigt. Folgende Jobstatus lauten: In Warteschlange, Abgeschlossen und Gestoppt. Im rechten Fensterbereich werden Informationen über die Task wie z. B. die mögliche Gesamtanzahl der Geräte, ermittelte Geräte mit Gerätetypen und jeweiliger Anzahl, der nächster Ausführungszeitpunkt sofern geplant und die zuletzt ermittelte Zeit angezeigt. Unter **Details anzeigen** im rechten Fensterbereich werden einzelne Jobdetails der Geräteermittlung angezeigt.

ANMERKUNG:
- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Um die Ermittlung mit Domänenanmeldeinformationen zu unterstützen, verwendet OpenManage Enterprise Version (3.2 und höher) das OpenSSH-Protokoll anstelle des WSMAN-Protokolls, das in den vorherigen Versionen verwendet wurde. Daher müssen alle vor der Aktualisierung des Geräts ermittelten Windows- und Hyper-V-Geräte gelöscht und mithilfe ihrer OpenSSH-Anmeldedaten wieder erkannt werden. Weitere Informationen zum Aktivieren von OpenSSH auf Windows und Hyper-V finden Sie in der Microsoft-Dokumentation.
- Auf den Seiten **Ermittlungs- und Bestandsaufnahme-Zeitpläne** wird der Status eines geplanten Jobs als **In Warteschlange** in der Spalte **Status** angezeigt. Jedoch wird derselbe Status als **Geplant** auf der Seite **Jobs** angezeigt.
- Standardmäßig wird die zuletzt ermittelte IP eines Geräts von OpenManage Enterprise zum Ausführen aller Vorgänge verwendet. Damit eine IP-Änderung wirksam wird, muss das Gerät neu ermittelt werden.
- Bei Geräten von Drittanbietern werden möglicherweise doppelte Einträge angezeigt, wenn sie mit mehreren Protokollen ermittelt werden. Diese Duplizierung kann korrigiert werden, indem man die Einträge löscht und das/die Gerät(e) nur unter Verwendung des IPMI-Protokolls erneut ermittelt.

Durch Verwendung der Ermittlungsfunktion können Sie:
- Geräte in der globalen Ausschlussliste anzeigen, hinzufügen und aus ihr entfernen. Informationen dazu finden Sie unter Globaler Ausschluss von Bereichen auf Seite 49.
- Die Geräteerkennungsjobs erstellen, ausführen, löschen und anhalten.

Zugehörige Tasks

Geräteermittlungsjob löschen auf Seite 54
Jobdetails der Geräteermittlung anzeigen auf Seite 47
Geräteermittlungsjob stoppen auf Seite 48
Geräteermittlungsjob ausführen auf Seite 48
Ermittlungsmodus für die Erstellung eines Server-Ermittlungsjobs festlegen auf Seite 50
Erstellen eines benutzerdefinierten Geräteerkennungs-Job-Protokolls für Server – Zusätzliche Einstellungen für Ermittlungsprotokolle auf Seite 50
Ermittlungsmodus für die Erstellung eines Dell Storage-Ermittlungsjobs festlegen auf Seite 52
Benutzerdefiniertes Geräteermittlungsjobprotokoll für SNMP-Geräte erstellen auf Seite 53
Ermittlungsmodus für die Erstellung eines MEHRFACHEN Protokoll-Ermittlungsjobs festlegen auf Seite 54
Geräteermittlungsjob bearbeiten auf Seite 48

Themen:

- Protokoll-Supportmatrix für die Ermittlung von Geräten
- Jobdetails der Geräteermittlung anzeigen
- Geräteermittlungsjob bearbeiten
- Geräteermittlungsjob ausführen
- Geräteermittlungsjob stoppen
- Mehrere Geräte durch das Importieren aus der .csv-Datei festlegen
- Globaler Ausschluss von Bereichen
- Ermittlungsmodus für die Erstellung eines Server-Ermittlungsjobs festlegen
- Erstellen eines benutzerdefinierten Geräteerkennungs-Job-Protokolls für Server – Zusätzliche Einstellungen für Ermittlungsprotokolle
- Ermittlungsmodus für die Erstellung eines Gehäuse-Ermittlungsjobs festlegen
- Erstellen eines benutzerdefinierten Protokolls zum Geräteermittlungs-Job für Gehäuse – Zusätzliche Einstellungen für Ermittlungsprotokolle
- Ermittlungsmodus für die Erstellung eines Dell Storage-Ermittlungsjobs festlegen
- Ermittlungsmodus für die Erstellung eines Netzwerk-Switch-Ermittlungsjobs festlegen
- Erstellen eines benutzerdefinierten Geräteermittlungsjobprotokolls für HTTPS-Speichergeräte – Zusätzliche Einstellungen für Ermittlungsprotokolle
- Benutzerdefiniertes Geräteermittlungsjobprotokoll für SNMP-Geräte erstellen
- Ermittlungsmodus für die Erstellung eines MEHRFACHEN Protokoll-Ermittlungsjobs festlegen
- Geräteermittlungsjob löschen

Automatisches Ermitteln von Servern mithilfe der Server-initiierten Ermittlungsfunktion

OpenManage Enterprise ermöglicht die automatische Ermittlung von Servern mit iDRAC-Firmware-Version 4.00.00.00 oder höher. Die Appliance kann so konfiguriert werden, dass diese Server die Konsole automatisch suchen, indem sie die DNS abfragen und ihre Ermittlung initiieren.

Für eine Server-initiierte Ermittlung müssen die folgenden Voraussetzungen erfüllt sein:

- Diese Funktion gilt nur für Server mit iDRAC-Firmware-Version 4.00.00.00 oder höher.
- Die Server müssen sich in derselben Domäne oder Subdomäne wie OpenManage Enterprise befinden.
- OpenManage Enterprise muss beim DNS registriert sein, um die Konfigurationsinformationen mithilfe von TUI der DNS hinzuzufügen. Es wird empfohlen, dass der DNS automatische Aktualisierungen von OpenManage Enterprise zulässt.
- Alte Aufzeichnungen der Appliance-Konsole auf dem DNS, falls vorhanden, sollten bereinigt werden, um mehrere Ankündigungen von den Servern zu vermeiden.

ANMERKUNG: Die bereichsbasierte Zugriffskontrolle (SBAC) wirkt sich nicht auf die Geräteauflistungen auf der Seite **Überwachen** > **Server-initiierte Ermittlung** aus und die Geräte-Manager können auf dieser Seite Geräte sehen, die über ihren Bereich hinausgehen.

Die folgenden Schritte werden bei der automatischen Ermittlung von Servern in OpenManage Enterprise befolgt:

1. Fügen Sie die Konfigurationsinformationen OpenManage Enterprise auf der DNS mithilfe einer der folgenden Methoden hinzu:
   - TUI – aktivieren Sie mithilfe der TUI-Schnittstelle die Option **Server-initiierte Ermittlung konfigurieren**. Weitere Informationen finden Sie unter OpenManage Enterprise mithilfe der textbasierten Benutzeroberfläche konfigurieren auf Seite 27.
   - Manuell: Fügen Sie die folgenden vier Datensätze zu Ihrem DNS-Server im Netzwerk hinzu, für das die Schnittstelle auf der Appliance konfiguriert ist. Stellen Sie sicher, dass alle `<domain>` oder `<subdomain.domain>`-Instanzen durch die entsprechende DNS-Domain und den System-Hostnamen ersetzt werden.
     - `<OME hostname>.<domain> 3600 A <OME IP address>`
     - `_dcimprovsrv._tcp.<domain> 3600 PTR ptr.dcimprovsrv._tcp.<domain>`
     - `ptr.dcimprovsrv._tcp.<domain> 3600 TXT URI=/api/DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence`
     - `ptr.dcimprovsrv._tcp.<domain> 3600 SRV 0 0 443 <hostname>.<domain>`

     Um die Datensätze mit `nsupdate` in Linux zu erstellen, verwenden Sie die folgenden Befehle:
     - Erstellen eines Hostnamen-Datensatzes

       ```
       >update add omehost.example.com 3600 A XX.XX.XX.XX
       ```

- Hinzufügen von Datensätzen für die serverinitiierte Ermittlung

```
>update add _dcimprovsrv._tcp.example.com 3600 PTR ptr.dcimprovsrv._
tcp.example.com.

>update add ptr.dcimprovsrv._tcp.example.com 3600 TXT URI=/api/DiscoveryConfigService/
Actions/DiscoveryConfigService.SignalNodePresence

>update add ptr.dcimprovsrv._tcp.example.com 3600 SRV 0 0 443 omehost.example.com.
```

Um die Datensätze mit `dnscmd` auf einem Windows-DNS-Server zu erstellen, verwenden Sie die folgenden Befehle:

- Erstellen eines Hostnamen-Datensatzes

```
>dnscmd <DnsServer> /RecordAdd example.com omehost A XX.XX.XX.XX
```

- Hinzufügen von Datensätzen für die serverinitiierte Ermittlung

```
>dnscmd <DnsServer> /RecordAdd example.com _dcimprovsrv._tcp PTR
ptr.dcimprovsrv._tcp.example.com

>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp TXT URI=/api/
DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence

>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp SRV 0 0 443
omehost.example.com
```

2. Standardmäßig ist die Ermittlungs-Genehmigungs-Richtlinie in der Appliance auf Automatic eingestellt und die Server, die Kontakt mit der Konsole herstellen, werden automatisch erkannt. Informationen zum Ändern der Einstellungen finden Sie unter Verwalten der Konsolen-Voreinstellungen auf Seite 165.
3. Nachdem die Appliance wie in den vorherigen Schritten beschrieben konfiguriert wurde, können die Server den Kontakt mit OpenManage Enterprise initiieren, indem sie den DNS abfragen. Die Appliance verifiziert die Server, nachdem sichergestellt wurde, dass das Client-Zertifikat der Server von der Dell-CA signiert ist.

   ANMERKUNG: Wenn Änderungen in der Server-IP-Adresse oder im SSL-Zertifikat vorhanden sind, initiiert der Server den Kontakt mit OpenManage Enterprise.
4. Die Seite **Überwachen** > **Server-initiierte Ermittlung** listet die Server auf, die Kontakt mit der Konsole herstellen. Außerdem werden die Server aufgelistet, deren Anmeldeinformationen in der Konsole hinzugefügt wurden, die aber noch keine Kontaktperson initiiert haben. Die folgenden Status der Server basierend auf den zuvor genannten Bedingungen werden angezeigt:
   - Angekündigt – der Server initiiert den Kontakt mit der Konsole, die Anmeldeinformationen des Servers werden jedoch nicht zur Konsole hinzugefügt.
   - Anmeldeinformationen hinzugefügt – die Anmeldeinformationen des Servers werden in der Konsole hinzugefügt, der Server hat jedoch keinen Kontakt mit der Konsole aufgenommen.
   - Bereit zur Ermittlung – die Anmeldeinformationen des Servers werden hinzugefügt und der Server hat Kontakt initiiert.

     ANMERKUNG: Die Appliance löst alle 10 Minuten einen Ermittlungs-Job aus, um alle Server im Status „Ready to discover" zu ermitteln. Wenn die Ermittlungs-Genehmigungs-Richtlinie in der Appliance jedoch als „manuell" festgelegt ist, sollte der Benutzer den Ermittlungs-Job für jeden Server manuell auslösen. Weitere Informationen finden Sie unter Verwalten der Konsolen-Voreinstellungen auf Seite 165
   - Job zur Ermittlung übermittelt – dieser Status zeigt an, dass der Ermittlungs-Job entweder automatisch oder manuell für den Server initiiert wird.
   - Ermittelt – der Server wird erkannt und auf der Seite „Alle Geräte" aufgeführt.

Die folgenden Aufgaben können auf der Seite **Überwachen** > **Server-initiierte Erkennung** durchgeführt werden:

1. **Importieren**– zum Importieren der Serveranmeldedaten:
   a. Klicken Sie auf **Importieren**.
   b. Klicken Sie im Assistenten „Aus Datei importieren" auf **Service-Tag-Datei hochladen**, um zur CSV-Datei zu navigieren und sie auszuwählen.

      Um ein Beispiel für eine CSV Datei der Serveranmeldeinformationen anzuzeigen, klicken Sie auf **Beispiel-CSV-Datei herunterladen**.
   c. Klicken Sie auf **Fertigstellen**.
2. **Erkennen**– zur manuellen Ermittlung der Server im Status „Ready to discover":

a. Wählen Sie die Server aus, die auf der Seite Server-initiierte Ermittlung aufgelistet sind und sich im Status „Ready to discover“ befinden.
b. Klicken Sie auf **Ermitteln**.

Ein Ermittlungs-Job wird ausgelöst, um die Server zu ermitteln und nach der Ermittlung werden diese Server auf der Seite „Alle Geräte“ aufgeführt.

3. **Löschen**– zum Löschen der Server, die auf der Seite „Server-initiierte Ermittlung“ aufgeführt sind:
   a. Wählen Sie die Server auf der Seite Server-initiierte Ermittlungen aus, die bereits erkannt und auf der Seite alle Geräte aufgeführt sind.
   b. Klicken Sie auf **Löschen**.

   Die Server werden von der Seite Server-initiierte Ermittlung gelöscht.

   ANMERKUNG: Einträge, die den ermittelten Servern entsprechen, werden nach 30 Tagen automatisch gelöscht.
4. **Exportieren**– zum Exportieren der Serveranmeldeinformationen im HTML-, CSV- oder PDF-Format:
   a. Wählen Sie einen oder mehrere Server auf der Seite „Server-initiierte Ermittlung“ aus.
   b. Klicken Sie auf **Exportieren**.
   c. Wählen Sie im Dialogfeld Export-Assistent eines der folgenden Ausgabeformate aus: HTML, CSV oder PDF.
   d. Klicken Sie auf **Fertigstellen**. Ein Job wird erstellt und die Daten werden zum ausgewählten Speicherort exportiert.

Geräteermittlungsjob erstellen

In den folgenden Schritten wird beschrieben, wie Sie einen Geräteermittlungs-Job in OpenManage Enterprise initiieren, um die Geräte in Ihrem Rechenzentrum mithilfe des Erstellungsassistenten für Ermittlungs-Jobs zu ermitteln.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Sie können einen der folgenden Schritte ausführen, um den Job zum Erstellen von Ermittlungen zu initiieren:
   - Klicken Sie auf **Überwachen** > **Ermittlung** > **Erstellen**.
   - Alternativ können Sie auf der Seite „Alle Geräte“ (**OpenManage Enterprise** > **Geräte**) auf das Dropdown-Menü **Ermittlung** und dann auf **Geräte ermitteln** klicken.
2. Im Dialogfeld **Ermittlungsjob erstellen** wird ein Standardname für den Job angegeben. Um diesen zu ändern, geben Sie einen anderen Ermittlungsjobnamen ein.
   Standardmäßig ermöglicht Ihnen das Dialogfeld, die Eigenschaften ähnlicher Geräts festzulegen.
   - Klicken Sie auf **Hinzufügen**, um weitere Geräte oder Bereiche zum aktuellen Ermittlungsjob hinzuzufügen. Eine weitere Reihe der folgenden Felder wird angezeigt, in welchen Sie die Geräteeigenschaften festlegen können: Typ, IP-Adresse/Hostname/Bereich und Einstellungen.

     WARNUNG: Es können maximal 8.000-Geräte von OpenManage Enterprise verwaltet werden. Geben Sie keine großen Netzwerke mit mehr Geräten als die maximale Anzahl der von OpenManage Enterprise unterstützten Geräte an. Dies kann dazu führen, dass das System plötzlich nicht mehr reagiert.

     ANMERKUNG: Wenn Sie eine große Anzahl von Geräten erkennen, vermeiden Sie das Erstellen mehrerer Ermittlungsjobs unter Verwendung der einzelnen IP-Adressen und verwenden Sie stattdessen den IP-Bereich der Geräte.
   - Ermitteln von Geräten durch Importieren von Bereichen aus der .csv-Datei: Informationen dazu finden Sie unter Mehrere Geräte durch das Importieren aus der .csv-Datei festlegen auf Seite 48.
   - Informationen zum Ausschließen bestimmter Geräte, zum Ausnehmen von Geräten von einem Ausschluss oder zum Anzeigen der Liste der Geräte, die von der Ermittlung ausgeschlossen sind, finden Sie unter Globales Ausschließen von Geräten aus den Erkennungsergebnissen.
3. Wählen Sie im Drop-down-Menü **Gerätetyp** folgende entsprechende Ermittlungsoption aus.
   - Wählen Sie für einen Server **SERVER**. Siehe Festlegen des Ermittlungsmodus für die Erstellung eines Server-Ermittlungsjobs.
   - Wählen Sie für ein Gehäuse **GEHÄUSE**. Siehe Festlegen des Ermittlungsmodus für die Erstellung eines Gehäuse-Ermittlungsjobs.
   - Wählen Sie für Dell EMC Speichergerät oder einen Netzwerkswitch **DELL STORAGE** oder **NETZWERKSWITCH**. Siehe Festlegen des Ermittlungsmodus zum Erstellen eines Speicher-, Dell Speicher- und Netzwerkswitch-Ermittlungsjobs.
   - Wählen Sie zur Ermittlung von Geräten mithilfe mehrerer Protokolle **MEHRERE**. Informationen dazu finden Sie unter Ermittlungsmodus für die Erstellung eines MEHRFACHEN Protokoll-Ermittlungsjobs festlegen auf Seite 54.
4. Geben Sie im Feld **IP/Hostname/Bereich** die IP-Adresse, den Hostnamen oder den IP-Adressbereich ein, die/der ermittelt oder eingeschlossen werden soll. Weitere Informationen zu den Daten, die Sie in dieses Feld eingeben können, erhalten Sie durch auf das **i**-Symbol.

ANMERKUNG:

- Die Bereichsgröße ist auf 16.385 (0x4001) begrenzt.
- Auch die Formate IPv6 und IPv6-CIDR werden unterstützt.

5. Geben Sie im Abschnitt **Einstellungen** den Nutzernamen und das Kennwort des Protokolls ein, das für die Ermittlung der Bereiche verwendet wird.
6. Klicken Sie auf **Zusätzliche Einstellungen**, um ein anderes Protokoll auszuwählen und die Einstellungen zu ändern.
7. Führen Sie den Job im Abschnitt **Ermittlungsjob planen** sofort aus oder planen Sie ihn für einen späteren Zeitpunkt. Informationen dazu finden Sie unter Felddefinitionen für die Jobplanung auf Seite 182.
8. Aktivieren Sie **Trap-Empfang von ermittelten iDRAC-Servern und dem MX7000-Gerät aktivieren**, damit OpenManage Enterprise die eingehenden Traps von den ermittelten Servern und dem MX7000-Gerät empfangen kann.

   ANMERKUNG: Wenn Sie diese Einstellung aktivieren, werden Warnmeldungen auf dem iDRAC (falls deaktiviert) aktiviert und ein Warnmeldungsziel für die IP-Adresse des OpenManage Enterprise-Servers festgelegt. Wenn bestimmte Warnmeldungen aktiviert werden müssen, müssen Sie diese auf dem iDRAC konfigurieren, indem Sie die entsprechenden Warnmeldungsfiler und SNMP-Traps aktivieren. Weitere Informationen finden Sie im iDRAC-Benutzerhandbuch.

9. Wählen Sie **Communitystring für Trap-Ziel aus Anwendungseinstellungen festlegen**. Diese Option ist nur für die ermittelten iDRAC-Server und MX7000-Gehäuse verfügbar.
10. Aktivieren Sie das Kontrollkästchen **Nach Abschluss per E-Mail versenden** und geben Sie die E-Mail-Adresse ein, an die eine Benachrichtigung über den Status des Ermittlungsjobs gesendet werden soll. Wenn die E-Mail-Adresse nicht konfiguriert ist, wird der Link **Zu den SMTP-Einstellungen gehen** angezeigt. Klicken Sie auf den Link und konfigurieren Sie die SMTP-Einstellungen. Informationen dazu finden Sie unter SMTP-, SNMP- und Syslog-Warnungen konfigurieren auf Seite 124. Wenn Sie diese Option wählen, aber SMTP nicht konfigurieren, wird die Schaltfläche **Fertigstellen** nicht angezeigt, um mit dem Auftrag fortfahren zu können.
11. Klicken Sie auf **Fertigstellen**. Die Schaltfläche „Fertigstellen" wird nicht angezeigt, wenn die Felder falsch oder unvollständig ausgefüllt sind.
    Ein Geräteerkennungsauftrag wird erstellt und wird ausgeführt. Der Status wird auf der Seite „Jobdetails" angezeigt.

Während der Geräteermittlung wird das für den Ermittlungsbereich angegebene Nutzerkonto mit allen verfügbaren Berechtigungen verifiziert, die auf einem Remotegerät aktiviert sind. Ist die Nutzerauthentifizierung positiv, wird das Gerät automatisch eingebunden oder kann später mit anderen Nutzerzugangsdaten eingebunden werden. Informationen dazu finden Sie unter Onboarding von Geräten auf Seite 45.

ANMERKUNG: Während der CMC-Ermittlung werden auch die Server sowie IOM- und Speichermodule (mit IP und SNMP als Communitystring auf „öffentlich" konfiguriert), die sich auf der CMC befinden, ermittelt und eingebunden. Wenn Sie den Trap-Empfang während der CMC-Ermittlung aktivieren, wird OpenManage Enterprise als Trap-Ziel auf allen Servern, aber nicht auf dem Gehäuse festgelegt.

ANMERKUNG: Während der CMC-Ermittlung werden FN I/O-Aggregatoren im PMUX-Modus (programmierbarer MUX) nicht ermittelt.

Onboarding von Geräten

Über das Onboarding können Server verwaltet anstatt nur überwacht werden.

- Wenn während der Ermittlung Anmeldeinformationen auf Administratorebene bereitgestellt werden, sind die Server eingegliedert (der Gerätestatus wird in der Ansicht „Alle Geräte" als „verwaltet" angezeigt).
- Wenn während der Ermittlung Anmeldeinformationen mit niedrigeren Berechtigungen bereitgestellt werden, sind die Server nicht eingegliedert (der Gerätestatus wird in der Ansicht „Alle Geräte" als „überwacht" angezeigt).
- Wenn die Konsole auch als ein Trap-Empfänger auf den Servern eingerichtet ist, dann wird deren Onboarding-Status immer als „Verwaltet mit Warnmeldungen" angezeigt.
- **Fehler**: Zeigt ein Problem mit dem Onboarding des Geräts an.
- **Proxy**: Nur für MX7000-Gehäuse. Gibt an, dass das Gerät über ein MX7000-Gehäuse und nicht direkt erkannt wird.

Wenn Sie Geräte mit einem anderen Nutzerkonto als dem für die Ermittlung angegebenen Konto eingliedern möchten, oder eine erneute Eingliederung wegen eines Fehlers bei der Eingliederung während der Ermittlung versuchen, machen Sie Folgendes:

ANMERKUNG:

- Alle Geräte, die mit diesem Assistenten eingegliedert wurden, bleiben über dieses Nutzerkonto eingegliedert und werden nicht durch das Ermittlungs-Nutzerkonto bei zukünftigen Ermittlungen gegen diese Geräte ausgetauscht.

- Wenn das SNMP-Trap-Ziel für die bereits ermittelten Geräte in iDRAC „manuell" als OpenManage Enterprise festgelegt ist, werden die Warnungen vom Gerät empfangen und verarbeitet. Allerdings bleibt der verwaltete Zustand des Geräts auf der Seite „Alle Geräte" identisch mit dem anfänglich ermittelten Status „Überwacht", „Verwaltet" oder „Verwaltet mit Warnmeldungen".
- Auf der Seite „Alle Geräte" wird der **Verwaltungsstatus** aller integrierten Gehäuse als „Verwaltet" angezeigt, unabhängig davon, welche Nutzerrollen-Zugangsdaten für das Gehäuse zum Zeitpunkt des Onboardings verwendet wurden. Wenn das Gehäuse mit den Zugangsdaten eines „schreibgeschützten" Nutzers integriert wurde, kann es während der Aktualisierungsaktivitäten auf dem Gehäuse zu einem Fehler kommen. Daher wird empfohlen, ein Gehäuse mit den Zugangsdaten eines Gehäuseadministrators zu verwenden, um alle Aktivitäten durchzuführen.
- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Klicken Sie im Menü **OpenManage Enterprise** unter **Geräte** auf **Alle Geräte**.
   Ein Ringdiagramm gibt den Status der Geräte im Arbeitsbereich an. Weitere Informationen finden Sie im Ringdiagramm. Die folgende Tabelle listet die Eigenschaften der ausgewählten Geräte zusammen mit deren folgendem Onboarding-Status auf:
   - **Fehler**: Gerät kann nicht eingegliedert werden. Versuchen Sie es durch die Anmeldung über die empfohlenen Berechtigungen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
   - **Verwaltet**: Gerät ist erfolgreich eingegliedert und kann durch die OpenManage Enterprise-Konsole verwaltet werden.
   - **Überwacht**: Gerät verfügt über keine Verwaltungsoption (z. B. diejenige, die unter Verwendung von SNMP ermittelt wurde).
   - **Verwaltet mit Warnmeldungen**: Gerät ist erfolgreich eingegliedert und die OpenManage Enterprise-Konsole hat Ihre IP-Adresse während der Ermittlung erfolgreich beim Gerät als Trap-Ziel registriert.
2. Aktivieren Sie im Arbeitsbereich ein Kontrollkästchen entsprechend des/der Geräts/e und klicken Sie auf **Weitere Maßnahmen** > **Onboarding**.

   Stellen Sie sicher, dass Sie aus der Seite „Alle Geräte" nur die Gerätetypen wählen, die für das Onboarding unterstützt werden. Um nach passenden Geräten in der Tabelle zu suchen, klicken Sie auf **Erweiterte Filter** und wählen im Filterfeld den Onboardingstatus aus oder geben ihn ein.

   ANMERKUNG: Alle Komponenten, die erkannt werden, werden nicht für das Onboarding unterstützt und nur iDRAC und CMC werden unterstützt. Stellen Sie sicher, dass Sie die Option zum Onboarding für diesen Gerätetyp auswählen.
3. Geben Sie im Dialogfeld **Onboarding** die folgenden WS-Man-Anmeldeinformationen ein: Nutzername und Kennwort.
4. Im Abschnitt **Verbindungseinstellungen**:
   a. Geben Sie im Feld **Wiederholungen** die Anzahl der Wiederholungsversuche ein, die zum Erkennen eines Servers unternommen werden müssen.
   b. Geben Sie im Feld **Timeout** die Zeit ein, nach der die Ausführung eines Jobs gestoppt werden muss.

      ANMERKUNG: Wenn der für das Timeout eingegebene Wert größer als die Ablaufzeit der aktuellen Sitzung ist, werden Sie von OpenManage Enterprise automatisch abgemeldet. Wenn sich der Wert jedoch innerhalb des Ablaufzeitfensters der aktuellen Sitzung befindet, wird die Sitzung fortgesetzt und eine Abmeldung findet nicht statt.
   c. Geben Sie im Feld **Port** die Portnummer ein, die der Job für die Ermittlung verwenden muss.
   d. Optionales Feld. Wählen Sie **Prüfung des allgemeinen Namens (CN) aktivieren**.
   e. Optionales Feld. Wählen Sie **Überprüfung der Zertifizierungsstelle (CN) aktivieren** und gehen Sie zur Zertifikatsdatei.
5. Klicken Sie auf **Fertigstellen**.

   ANMERKUNG: Das Kontrollkästchen **Trap-Empfang von ermitteltem Server aktivieren** ist nur für Server wirksam, die mithilfe ihrer iDRAC-Schnittstelle ermittelt wurden. Die Auswahl ist für andere Server unwirksam (wie z. B. die Geräte, die mithilfe von der BS-Erkennung ermittelt wurden).

Protokoll-Supportmatrix für die Ermittlung von Geräten

Die folgende Tabelle enthält Informationen über die unterstützten Protokolle für das Erkennen von Geräten.

ANMERKUNG: Die Funktionalität der unterstützten Protokolle zum Erkennen, Überwachen und Verwalten der PowerEdge YX1X-Server mit iDRAC6 ist begrenzt. Weitere Informationen finden Sie unter Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.

Tabelle 13. Protokoll Supportmatrix für Ermittlung

Gerät/ Betriebssystem	Protokolle						
	Web Services-Management (WS-MAN)	**Redfish**	**Simple Network Management Protocol (SNMP)**	**Secure Shell (SSH)**	**Intelligente Plattform-Verwaltungsschnittstelle**	**ESXi (VMWare)**	**HTTPS**
iDRAC6 und höher	**Unterstützt**	**Unterstützt** Nur für iDRAC9 Version 4.40.10.00 und höher **Nicht unterstützt**	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
PowerEdge C *	**Unterstützt**	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
PowerEdge-Gehäuse (CMC)	**Unterstützt**	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
PowerEdge MX7000-Gehäuse	Nicht unterstützt	**Unterstützt**	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Speichergeräte	Nicht unterstützt	Nicht unterstützt	**Unterstützt**	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Ethernet-Switches	Nicht unterstützt	Nicht unterstützt	**Unterstützt**	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
ESXi	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	**Unterstützt**	Nicht unterstützt
Linux	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	**Unterstützt**	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	**Unterstützt**	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Hyper-V	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	**Unterstützt**	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Nicht-Dell Server	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	**Unterstützt**	Nicht unterstützt	Nicht unterstützt
PowerVault ME	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	**Unterstützt**	Nicht unterstützt	**Unterstützt**

Jobdetails der Geräteermittlung anzeigen

1. Klicken Sie auf **Überwachen** > **Ermittlung**.
2. Aktivieren Sie die Zeile des entsprechenden Ermittlungsjobnamens und klicken Sie dann auf **Details anzeigen** im rechten Fensterbereich.
   Auf der Seite **Jobdetails** werden die entsprechenden Ermittlungs-Jobinformationen angezeigt.
3. Weitere Informationen zum Verwalten von Jobs finden Sie unter Verwenden von Jobs zur Gerätesteuerung auf Seite 130.

Zugehörige Informationen

Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41

Geräteermittlungsjob bearbeiten

Sie können jeweils nur einen Geräteermittlungsjob bearbeiten.

1. Aktivieren Sie das Kontrollkästchen neben dem zu bearbeitenden Ermittlungsjob und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Dialogfeld **Ermittlungsjob erstellen** die Eigenschaften.
   Weitere Informationen zu den auszuführenden Tasks in diesem Dialogfeld finden Sie im Abschnitt Erstellen von Geräteermittlungsjobs.

Zugehörige Informationen

Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41

Geräteermittlungsjob ausführen

ANMERKUNG: Sie können einen bereits laufenden Job nicht erneut ausführen.

So führen Sie einen Geräteermittlungsjob aus:

1. Aktivieren Sie in der Liste der vorhandenen Geräteermittlungsjobs das entsprechende Kontrollkästchen des Jobs, den Sie jetzt ausführen möchten.
2. Klicken Sie auf **Ausführen**.
   Der Job wird unmittelbar gestartet und eine Meldung wird in der rechten unteren Bildschirmecke angezeigt.

Zugehörige Informationen

Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41

Geräteermittlungsjob stoppen

Sie können den Job nur stoppen, wenn er ausgeführt wird. Abgeschlossene oder fehlgeschlagene Ermittlungsjobs können nicht gestoppt werden. So stoppen Sie einen Job:

1. Aktivieren Sie in der Liste der vorhandenen Ermittlungsjobs das entsprechende Kontrollkästchen des Jobs, den Sie stoppen möchten.

   ANMERKUNG: Mehrere Jobs können nicht gleichzeitig angehalten werden.

2. Klicken Sie auf **Stopp**.
   Der Job wird gestoppt und eine Meldung wird in der rechten unteren Bildschirmecke angezeigt.

Zugehörige Informationen

Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41

Mehrere Geräte durch das Importieren aus der .csv-Datei festlegen

1. Im Dialogfeld **Ermittlungsjob erstellen** wird **Ermittlungsjobname** mit einem Ermittlungsjobnamen befüllt. Um diesen zu ändern, geben Sie einen anderen Ermittlungsjobnamen ein.
2. Klicken Sie auf **Importieren**.

   ANMERKUNG: Laden Sie ggf. die Beispiel-.csv-Datei herunter.

3. Klicken Sie im Dialogfeld **Importieren** auf **Importieren**, navigieren Sie zur .csv-Datei, die eine Liste gültiger Bereiche enthält, und klicken Sie dann auf **OK**.

   ANMERKUNG: Es wird eine Fehlermeldung angezeigt, wenn die .csv-Datei ungültige Bereiche enthält, und doppelte Bereiche werden während des Importvorgangs ausgeschlossen.

Globaler Ausschluss von Bereichen

Mithilfe des Assistenten für den globalen Ausschluss von Bereichen können Sie die Adresse(n) oder den Bereich der Geräte eingeben, die von OpenManage Enterprise-Überwachungs- und Managementaktivitäten ausgeschlossen werden sollen. Die folgenden Schritte beschreiben, wie Sie den Gerätebereich ausschließen können:

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

ANMERKUNG: Gegenwärtig können Sie ein Gerät nicht durch die Verwendung von dessen Host-Namen ausschließen, sondern nur über seine IP-Adresse oder FQDN.

1. Führen Sie einen der folgenden Schritte aus, um den Assistenten für den globalen Ausschluss von Bereichen zu aktivieren:
   - Klicken Sie auf der Seite „Alle Geräte" (**OpenManage Enterprise** > **Geräte**) im Dropdown-Menü **Ermittlung** auf **Ausschlussbereiche bearbeiten**.
   - Klicken Sie unter **Überwachen** > **Ermittlung** auf die **Globale Ausschlussliste** in der oberen rechten Ecke.
2. Im Dialogfeld **Globales Ausschließen von Bereichen**:
   a. Geben Sie im Feld **Beschreibung des Ausschlussbereichs** die Informationen über den Bereich ein, der ausgeschlossen wird.
   b. Geben Sie im Feld **Ausschlussbereiche eingeben** die Adresse(n) oder einen Adressbereich der auszuschließenden Geräte ein. In das Feld können bis zu 1000 Adresseinträge auf einmal eingegeben werden – getrennt durch einen Zeilenumbruch. Das heißt, dass jeder Ausschlussbereich in unterschiedliche Zeilen im Feld eingegeben werden muss.
   Der Bereich, der ausgeschlossen werden kann, entspricht den unterstützten Bereiche, die während der Ermittlung eines Geräts gelten. Informationen dazu finden Sie unter Geräteermittlungsjob erstellen auf Seite 44.

   ANMERKUNG:
   - Die Bereichsgröße ist auf 16.385 (0x4001) begrenzt.
   - Auch die Formate IPv6 und IPv6-CIDR werden unterstützt.
3. Klicken Sie auf **Hinzufügen**.
4. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**.
   Die IP-Adresse oder der Bereich wird global ausgeschlossen und dann in der Liste der ausgeschlossenen Bereiche angezeigt. Diese Geräte werden global ausgeschlossen, was impliziert, dass sie an keinen Aktivitäten beteiligt sind, die in OpenManage Enterprise durchgeführt werden.

   ANMERKUNG: Das Gerät, das global ausgeschlossen wird, wird auf der Seite **Job-Details** eindeutig als „Global ausgeschlossen" identifiziert.

   So entfernen Sie ein Gerät aus der globalen Ausschlussliste:
   a. Aktivieren Sie das Kontrollkästchen und klicken Sie auf **Aus Ausschluss entfernen**.
   b. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**. Das Gerät wird aus der globalen Ausschlussliste entfernt. Ein Gerät, das aus der globalen Ausschlussliste entfernt wurde, wird nicht automatisch durch OpenManage Enterprise überwacht. Sie müssen das Gerät ermitteln, damit OpenManage Enterprise mit der Überwachung beginnt.

ANMERKUNG:
- Wenn Geräte, die in der Konsole bereits bekannt sind (d. h. bereits von der Konsole ermittelt wurden) zur globalen Ausschlussliste hinzugefügt werden, wird/werden das Gerät/die Geräte von OpenManage Enterprise entfernt.
- Die neu in die globale Ausschlussliste aufgenommenen Geräte werden bis zum nächsten Ermittlungszyklus weiterhin im Raster „Alle Geräte" angezeigt. Um die Durchführung von Aufgaben auf solchen Geräten zu vermeiden, wird dringend empfohlen, dass der Benutzer diese manuell von der Seite „Alle Geräte" ausschließt, indem er das entsprechende Kontrollkästchen für das/die Gerät(e) aktiviert und anschließend auf **Ausschließen** klickt.
- Geräte auf der globalen Ausschlussliste werden von allen Aufgaben auf der Konsole ausgeschlossen. Wenn sich die IP eines Geräts auf der globalen Ausschlussliste befindet und eine Ermittlungsaufgabe erstellt wird, deren Ermittlungsbereich die IP umfasst, wird das Gerät nicht ermittelt. Auf der Konsole wird jedoch keine Fehlermeldung angezeigt, wenn die Ermittlungsaufgabe erstellt wird. Wenn Sie der Ansicht sind, dass ein Gerät ermittelt werden sollte und dies nicht der Fall ist, überprüfen Sie in der globalen Ausschlussliste, ob das Gerät dort aufgelistet ist.

.

Ermittlungsmodus für die Erstellung eines Server-Ermittlungsjobs festlegen

1. Wählen Sie im Drop-Down-Menü **Gerätetyp** die Option **SERVER** aus.
2. Wenn Sie dazu aufgefordert werden, wählen Sie Folgendes:
   - **Dell iDRAC**: Zur Ermittlung mittels iDRAC.
   - **Host-BS**: Zur Ermittlung mittels eines VMware ESXi-, Microsoft Windows Hyper-V-, Windows- oder Linux-Betriebssystems.
   - **Nicht Dell Server (via OOB)**: Zur Ermittlung von Drittanbieter-Servern mithilfe von IPMI.
3. Auf **OK**.klicken.
   Basierend auf Ihrer Auswahl ändern sich die Felder unter **Einstellungen**.
4. Geben Sie im Feld **IP/Hostname/Bereich** die IP-Adresse, den Hostnamen oder den IP-Bereich ein, die/der dem Protokoll zugewiesen ist.
5. Geben Sie unter **Einstellungen** den Benutzernamen und das Kennwort für den zu ermittelnden Server ein.
6. Informationen zum Anpassen von Erkennungsprotokollen durch Klicken auf **Zusätzliche Einstellungen** finden Sie unter Erstellen einer benutzerdefinierten Geräteerkennungs-Job-Vorlage für Server.
7. Planen des Ermittlungsjobs. Informationen dazu finden Sie unter Felddefinitionen für die Jobplanung auf Seite 182.
8. Klicken Sie auf **Fertigstellen**.
   Einen Suchauftrag wird erstellt und in der Liste der Suchaufträge angezeigt.

Zugehörige Informationen

Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41

Erstellen eines benutzerdefinierten Geräteerkennungs-Job-Protokolls für Server – Zusätzliche Einstellungen für Ermittlungsprotokolle

Geben Sie im Dialogfeld **Zusätzliche Einstellungen** Details für das entsprechende Protokoll ein, mit dem Sie den/die Server ermitteln möchten:

ANMERKUNG: Die entsprechenden Protokolle werden basierend auf ihren anfänglichen Eingaben automatisch ausgewählt.

1. Zu **Ermitteln mittels WS-Man/Redfish (iDRAC, Server und/oder Gehäuse)**
   a. Geben Sie im Abschnitt „Zugangsdaten" den **Nutzernamen** und das **Kennwort** ein.
   b. Im Abschnitt **Verbindungseinstellungen**:
      - Geben Sie im Feld **Wiederholungen** die Anzahl der Wiederholungsversuche ein, die zum Erkennen eines Servers unternommen werden müssen.
      - Geben Sie im Feld **Timeout** die Zeit ein, nach der die Ausführung eines Jobs gestoppt werden muss.
      - Nehmen Sie eine Eingabe im Feld **Port** vor, um die Portnummer zu bearbeiten. Standardmäßig wird 443 für die Verbindung mit dem Gerät verwendet. Unterstützte Portnummern finden Sie unter Unterstützte Protokolle und Schnittstellen in OpenManage Enterprise auf Seite 32
      - Aktivieren Sie das Kontrollkästchen **Allgemeinen Namen (CN) aktivieren**, wenn der allgemeine Name des Geräts mit dem Hostnamen für den Zugriff auf OpenManage Enterprise identisch ist.
      - Aktivieren Sie bei Bedarf das Kontrollkästchen **Zertifizierungsstelle (CA) aktivieren**.
2. Zu **Ermitteln über IPMI (nicht Dell über OOB)**
   a. Geben Sie im Abschnitt „Zugangsdaten" den **Nutzernamen** und das **Kennwort** ein.
   b. Im Abschnitt **Verbindungseinstellungen**:
      - Geben Sie im Feld **Wiederholungen** die Anzahl der Wiederholungsversuche ein, die zum Erkennen eines Servers unternommen werden müssen.
      - Geben Sie im Feld **Timeout** die Zeit ein, nach der die Ausführung eines Jobs gestoppt werden muss.
      - Geben Sie im Feld **KgKey** einen entsprechenden Wert ein.
3. Zu **Ermitteln über SSH (Linux, Windows, Hyper-V)**

ANMERKUNG: Nur OpenSSH auf Windows und Hyper-V wird unterstützt. Cygwin SSH wird nicht unterstützt.

a. Geben Sie im Abschnitt „Zugangsdaten“ den **Nutzernamen** und das **Kennwort** ein.
b. Im Abschnitt **Verbindungseinstellungen**:
    - Geben Sie im Feld **Wiederholungen** die Anzahl der Wiederholungsversuche ein, die zum Erkennen eines Servers unternommen werden müssen.
    - Geben Sie im Feld **Timeout** die Zeit ein, nach der die Ausführung eines Jobs gestoppt werden muss.
    - Nehmen Sie eine Eingabe im Feld **Port** vor, um die Portnummer zu bearbeiten. Standardmäßig wird 22 für die Verbindung mit dem Gerät verwendet. Unterstützte Portnummern finden Sie unter Unterstützte Protokolle und Schnittstellen in OpenManage Enterprise auf Seite 32
    - Aktivieren Sie das Kontrollkästchen **Bekannten Host-Schlüssel verifizieren**, um den Host anhand bekannter Hostschlüssel zu validieren.

      ANMERKUNG: Bekannte Host-Schlüssel werden über den Dienst */DeviceService/HostKeys Rest-API* hinzugefügt. Weitere Informationen zum Verwalten von Host-Schlüsseln finden Sie im *OpenManage Enterprise RESTful API-Handbuch*.
    - Aktivieren Sie das Kontrollkästchen **SUDO-Option verwenden**, wenn sudo-Konten bevorzugt werden.

      ANMERKUNG: Damit sudo-Konten funktionieren, muss die Serverdatei `/etc/sudoer` für die Verwendung von NOPASSWD konfiguriert werden.

4. Zu **Ermitteln über ESXi (VMware)**
    a. Geben Sie im Abschnitt „Zugangsdaten“ den **Nutzernamen** und das **Kennwort** ein.
    b. Im Abschnitt **Verbindungseinstellungen**:
        - Geben Sie im Feld **Wiederholungen** die Anzahl der Wiederholungsversuche ein, die zum Erkennen eines Servers unternommen werden müssen.
        - Geben Sie im Feld **Timeout** die Zeit ein, nach der die Ausführung eines Jobs gestoppt werden muss.
        - Nehmen Sie eine Eingabe im Feld **Port** vor, um die Portnummer zu bearbeiten. Standardmäßig wird 443 für die Verbindung mit dem Gerät verwendet. Unterstützte Portnummern finden Sie unter Unterstützte Protokolle und Schnittstellen in OpenManage Enterprise auf Seite 32
        - Aktivieren Sie das Kontrollkästchen **Allgemeinen Namen (CN) aktivieren**, wenn der allgemeine Name des Geräts mit dem Hostnamen für den Zugriff auf OpenManage Enterprise identisch ist.
        - Aktivieren Sie bei Bedarf das Kontrollkästchen **Zertifizierungsstelle (CA) aktivieren**.

Zugehörige Informationen

Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41

Ermittlungsmodus für die Erstellung eines Gehäuse-Ermittlungsjobs festlegen

1. Wählen Sie im Drop-Down-Menü **Gerätetyp** die Option **GEHÄUSE** aus.
   Basierend auf Ihrer Auswahl ändern sich die Felder unter **Einstellungen**.
2. Geben Sie in **IP/Hostnamen/Bereich** die IP-Adresse, den Hostnamen oder den IP-Bereich ein.
3. Geben Sie unter **Einstellungen** den Benutzernamen und das Kennwort für den zu ermittelnden Server ein.
4. Geben Sie den Typ der Community ein.
5. Um eine benutzerdefinierte Ermittlungsvorlage zu erstellen, klicken Sie auf **Zusätzliche Einstellungen**. Siehe Erstellen eines benutzerdefinierten Protokolls zum Geräteermittlungs-Job für Gehäuse – Zusätzliche Einstellungen für Ermittlungsprotokolle auf Seite 52.

ANMERKUNG: Derzeit wird für jedes M1000e-Gehäuse, das ermittelt wurde, in CMC 5.1 x und früheren Versionen das Datum in der Spalte „TIMESTAMP“ unter „Hardware-Protokolle“ als Jan 12 2013 angezeigt. Für alle Versionen des CMC VRTX- und FX2-Gehäuses wird jedoch das korrekte Datum angezeigt.

ANMERKUNG: Wenn ein Server in einem Gehäuse separat ermittelt wird, werden die Steckplatzinformationen über den Server nicht im Abschnitt **Gehäuseinformationen** angezeigt. Bei einer Ermittlung über ein Gehäuse werden die Steckplatzinformationen jedoch angezeigt. Zum Beispiel: ein MX740c-Server in einem MX7000-Gehäuse.

Erstellen eines benutzerdefinierten Protokolls zum Geräteermittlungs-Job für Gehäuse – Zusätzliche Einstellungen für Ermittlungsprotokolle

Im Dialogfeld **Weitere Einstellungen**:

1. Wählen Sie **Ermitteln mittels WS-Man/Redfish (iDRAC, Server und/oder Gehäuse)**.

   ANMERKUNG: Für Gehäuse ist das Kontrollkästchen **Ermitteln unter Verwendung von WS-Man/Redfish** standardmäßig aktiviert. Dies bedeutet, dass das Gehäuse mit einem dieser beiden Protokolle ermittelt werden kann. Die M1000e-, CMC VRTX- und FX2-Gehäuse unterstützen die WS-Man-Befehle. Das MX7000-Gehäuse unterstützt das Redfish-Protokoll.

2. Geben Sie den Nutzernamen und das Kennwort des zu erkennenden Gehäuses ein.
3. Im Abschnitt **Verbindungseinstellungen**:
   a. Geben Sie im Feld **Wiederholungen** die Anzahl der Wiederholungsversuche ein, die zum Erkennen eines Servers unternommen werden müssen.
   b. Geben Sie im Feld **Timeout** die Zeit ein, nach der die Ausführung eines Jobs gestoppt werden muss.
   c. Nehmen Sie eine Eingabe im Feld **Port** vor, um die Portnummer zu bearbeiten. Standardmäßig wird 443 für die Verbindung mit dem Gerät verwendet. Unterstützte Portnummern finden Sie unter Unterstützte Protokolle und Schnittstellen in OpenManage Enterprise auf Seite 32.
   d. Aktivieren Sie das Kontrollkästchen **Überprüfung von allgemeinem Namen (CN) aktivieren**, wenn der allgemeine Name des Geräts mit dem Hostnamen für den Zugriff auf OpenManage Enterprise identisch ist.
   e. Aktivieren Sie das Kontrollkästchen **Überprüfung der Zertifizierungsstelle (CA) aktivieren**.
4. Zur Ermittlung der I/O-Module aktivieren Sie das Kontrollkästchen **I/O-Module mit Gehäuse ermitteln**.

   ANMERKUNG: Gilt nur für die Gehäuse CMC VRTX, M1000e und FX2 (Modelle FN2210S, FN410T und FN410S). Für die MX7000-Gehäuse werden die I/O-Module automatisch ermittelt.

   ANMERKUNG: Nur I/O-Module mit den Modi Standalone, PMUX (Programmable MUX) und VLT (Virtual Link Trunking) werden erkannt. Die Modi Full-Switch und Stacked werden nicht erkannt.

   a. Wählen Sie **Gehäuse-Anmeldeinformationen verwenden**, wenn die Nutzerzugangsdaten des M I/O-Aggregators die gleichen sind wie die des Gehäuses.
   b. Wählen Sie **Andere Anmeldeinformationen verwenden**, wenn der sich die Nutzerzugangsdaten des M I/O-Aggregators von den Anmeldeinformationen des Gehäuses unterscheiden und gehen Sie wie folgt vor:
      - Geben Sie **Nutzernamen** und **Kennwort** ein.
      - Ändern Sie gegebenenfalls die Standardwerte für **Wiederholungen**, **Timeout** und **Port**.
      - Wählen Sie **Bekannten Host-Schlüssel überprüfen**, um den Host anhand bekannter Host-Schüssel zu überprüfen.

        ANMERKUNG: Bekannte Host-Schlüssel werden über den Dienst */DeviceService/HostKeys Rest-API* hinzugefügt. Weitere Informationen zum Verwalten von Host-Schlüsseln finden Sie im *OpenManage Enterprise RESTful API-Handbuch*.
      - Wählen Sie bei Bedarf **SUDO-Option verwenden**.
5. Klicken Sie auf **Fertigstellen**.
6. Schließen Sie die Aufgaben in Geräteermittlungsjob erstellen auf Seite 44 ab.

Ermittlungsmodus für die Erstellung eines Dell Storage-Ermittlungsjobs festlegen

1. Wählen Sie im Drop-Down-Menü **Gerätetyp** die Option **DELL STORAGE** aus.
2. Wenn Sie dazu aufgefordert werden, wählen Sie Folgendes:
   - PowerVault ME: Ermitteln der Speichergeräte mithilfe des HTTPS-Protokolls wie beim PowerVault ME.
   - Sonstiges: Ermitteln von Speichergeräten, die das SNMP-Protokoll verwenden.

   Basierend auf Ihrer Auswahl ändern sich die Felder unter **Einstellungen**.
3. Geben Sie in **IP/Hostnamen/Bereich** die IP-Adresse, den Hostnamen oder den IP-Bereich ein.

4. Geben Sie unter **Einstellungen** je nach Ihrer ersten Auswahl den **Benutzernamen** und das **Kennwort** für Storage HTTPS ein oder geben Sie die **SNMP-Version** und den **Communitytyp** des zu ermittelnden Geräts ein.
5. Klicken Sie auf **Zusätzliche Einstellungen** zum Anpassen des entsprechenden Ermittlungsprotokolls. Siehe Erstellen einer benutzerdefinierten Geräteermittlungsjobvorlage für SNMP-Geräte oder siehe Erstellen eines benutzerdefinierten Geräteermittlungsjobprotokolls für HTTPS-Speichergeräte – Zusätzliche Einstellungen für Ermittlungsprotokolle auf Seite 53.
6. Schließen Sie die Aufgaben in Geräteermittlungsjob erstellen auf Seite 44 ab.

Zugehörige Informationen

Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41

Ermittlungsmodus für die Erstellung eines Netzwerk-Switch-Ermittlungsjobs festlegen

1. Wählen Sie im Drop-Down-Menü **Gerätetyp** die Option **NETZWERK-SWITCH** aus.
2. Geben Sie in **IP/Hostnamen/Bereich** die IP-Adresse, den Hostnamen oder den IP-Bereich ein.
3. Unter **Einstellungen** geben Sie die **SNMP-Version** und den **Communitytyp** des zu erkennenden Geräts ein.
4. Klicken Sie auf **Zusätzliche Einstellungen** zum Anpassen des entsprechenden Ermittlungsprotokolls. Siehe Erstellen einer benutzerdefinierten Geräteermittlungsjobvorlage für SNMP-Geräte
5. Schließen Sie die Aufgaben in Geräteermittlungsjob erstellen auf Seite 44 ab.

Erstellen eines benutzerdefinierten Geräteermittlungsjobprotokolls für HTTPS-Speichergeräte – Zusätzliche Einstellungen für Ermittlungsprotokolle

Im Dialogfeld **Weitere Einstellungen**:

1. Geben Sie den Benutzernamen und das Kennwort des zu erkennenden PowerVault ME ein.
2. Im Abschnitt **Verbindungseinstellungen**:
   a. Geben Sie im Feld **Wiederholungen** die Anzahl der Wiederholungsversuche ein, die zum Erkennen eines Servers unternommen werden müssen.
   b. Geben Sie im Feld **Zeitüberschreitung** die Zeit ein, nach der die Ausführung eines Jobs gestoppt werden muss.
   c. Nehmen Sie eine Eingabe im Feld **Port** vor, um die Portnummer zu bearbeiten. Standardmäßig wird 443 für die Verbindung mit dem Gerät verwendet. Unterstützte Portnummern finden Sie unter Unterstützte Protokolle und Schnittstellen in OpenManage Enterprise auf Seite 32.
   d. Aktivieren Sie das Kontrollkästchen **Überprüfung von allgemeinem Namen (CN) aktivieren**, wenn der allgemeine Name des Geräts mit dem Hostnamen für den Zugriff auf OpenManage Enterprise identisch ist.
   e. Aktivieren Sie das Kontrollkästchen **Überprüfung der Zertifizierungsstelle (CN) aktivieren**.
3. Klicken Sie auf **Fertigstellen**.
4. Schließen Sie die Aufgaben in Geräteermittlungsjob erstellen auf Seite 44 ab.

Benutzerdefiniertes Geräteermittlungsjobprotokoll für SNMP-Geräte erstellen

Das Kontrollkästchen **Ermitteln mittels SNMP** ist standardmäßig aktiviert, damit Sie die Speicher-, Netzwerk-, oder andere SNMP-Geräte erkennen können.

ANMERKUNG: Nur E/A-Module mit den Modi Standalone, PMUX (Programmable MUX) und VLT (Virtual Link Trunking) werden erkannt. Die Modi Full-Switch und Stacked werden nicht erkannt.

1. Wählen Sie unter **Anmeldeinformationen** die SNMP-Version aus und geben Sie dann den Community-Typ ein.
2. Im Abschnitt **Verbindungseinstellungen**:
   a. Geben Sie im Feld **Wiederholungen** die Anzahl der Wiederholungsversuche ein, die zum Erkennen eines Servers unternommen werden müssen.
   b. Geben Sie im Feld **Zeitüberschreitung** die Zeit ein, nach der die Ausführung eines Jobs gestoppt werden muss.
   c. Geben Sie im Feld **Port** die Portnummer ein, die der Job für die Ermittlung verwenden muss.

   ANMERKUNG: Die Einstellungen in den Feldern **Wiederholungen** und **Zeitüberschreitung** haben derzeit keine funktionellen Auswirkungen auf die Ermittlungsjobs für SNMP-Geräte. Daher können diese Einstellungen ignoriert werden.
3. Klicken Sie auf **Fertigstellen**.
4. Schließen Sie die Aufgaben in Geräteermittlungsjob erstellen auf Seite 44 ab.

Zugehörige Informationen

Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41

Ermittlungsmodus für die Erstellung eines MEHRFACHEN Protokoll-Ermittlungsjobs festlegen

1. Wählen Sie im Drop-down-Menü **Typ** die Option **MEHRFACH**, um Geräte mit mehreren Protokollen zu erkennen.
2. Geben Sie in **IP/Hostnamen/Bereich** die IP-Adresse, den Hostnamen oder den IP-Bereich ein.
3. Um eine benutzerdefinierte Ermittlungsvorlage zu erstellen, klicken Sie auf **Zusätzliche Einstellungen**. Siehe Erstellen eines benutzerdefinierten Geräteerkennungs-Job-Protokolls für Server – Zusätzliche Einstellungen für Ermittlungsprotokolle auf Seite 50.

Zugehörige Informationen

Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41

Geräteermittlungsjob löschen

ANMERKUNG: Ein Gerät kann auch dann gelöscht werden, wenn Tasks auf ihm ausgeführt werden. Eine auf einem Gerät initiierte Task schlägt fehl, wenn das Gerät vor der Fertigstellung gelöscht wird.

So löschen Sie einen Geräteermittlungsjob:

1. Aktivieren Sie das entsprechende Kontrollkästchen des Ermittlungsjobs, den Sie löschen möchten, und klicken Sie auf **Löschen**.
2. Klicken Sie bei der Frage, ob der Job gelöscht werden soll, auf **JA**.
   Die Ermittlungsjobs werden gelöscht, und es wird eine Meldung in der rechten unteren Ecke des Bildschirms angezeigt.

ANMERKUNG: Wenn Sie einen Ermittlungsjob löschen, werden die mit dem Job verbundenen Geräte nicht gelöscht. Wenn Sie die im Rahmen einer Ermittlungsaufgabe ermittelten Geräte aus der Konsole entfernen möchten, löschen Sie diese von der Seite **Alle Geräte**.

ANMERKUNG: Ein Geräteermittlungsjob kann nicht von der Seite „Jobs“ gelöscht werden .

Zugehörige Informationen

Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41

8

Geräte und Gerätegruppen verwalten

Durch Klicken auf **OpenManage Enterprise** > **Geräte** können Sie die in OpenManage Enterprise ermittelten Geräte und Gerätegruppen anzeigen und verwalten. Wenn Sie als Geräte-Manager angemeldet sind, sind nur die Gerätegruppen und die zugehörigen Strukturen, die sich in Ihrem Bereich befinden, für die Anzeige und Verwaltung verfügbar.

Im linken Fenster werden die Gerätegruppen wie folgt angezeigt:

- Alle Geräte: die Stammgruppe der obersten Ebene, die alle Gruppen enthält.
- Systemgruppen: von OpenManage Enterprise bei der Lieferung erstellte Standardgruppen.
- Benutzerdefinierte Gruppen: von Nutzern, z. B. Administratoren und Geräte-Managern, erstellte Gruppen. Sie können „Abfragegruppen“ oder „statische“ Gruppen unter benutzerdefinierten Gruppen erstellen.
- Plug-in-Gruppen: von Plug-ins erstellte Gruppen.

Sie können untergeordnete Gruppen im Rahmen dieser übergeordneten Gruppen erstellen. Weitere Informationen finden Sie unter Gerätegruppen.

Im oberen Bereich des Arbeitsbereichs zeigen Ringdiagramme den Funktionszustand und Warnmeldungen aller Geräte standardmäßig an. Wenn jedoch eine Gruppe im linken Fensterbereich ausgewählt ist, zeigen diese Ringdiagramme den Funktionszustand und Warnmeldungen der ausgewählten Gruppe an. Wenn ein Plug-in installiert ist, zeigt ein drittes Ringdiagramm möglicherweise die Daten des installierten Plug-ins an. Weitere Informationen über das Ringdiagramm finden Sie unter Ringdiagramm.

Die Tabelle nach dem Ringdiagramm listet die Geräte auf und zeigt deren Funktionszustand, Stromzustand, Namen, IP-Adresse und Kennung an. Standardmäßig werden alle Geräte aufgelistet, aber wenn eine Gruppe im linken Bereich ausgewählt ist, werden nur die Geräte dieser Gruppe angezeigt. Weitere Informationen über die Geräteliste finden Sie unter Geräteliste.

Mit den **erweiterten Filtern** können die in der Geräteliste angezeigten Geräte basierend auf Ihrem Funktionszustand, Stromzustand, Verbindungsstatus, Namen, IP-Adresse, Kennung, Gerätetyp, verwaltetem Zustand usw. weiter eingegrenzt werden.

Wenn Sie ein Gerät aus der Liste auswählen, wird im rechten Fensterbereich die Vorschau über die ausgewählten Geräte angezeigt. Wenn mehrere Geräte ausgewählt wurden, wird die Vorschau über das zuletzt ausgewählte Gerät angezeigt. Unter **Schnelle Aktionen** sind die Verwaltungslinks aufgelistet, die mit dem jeweiligen Gerät korrelieren. Zum Löschen der Auswahl klicken Sie auf **Auswahl löschen**.

ANMERKUNG:

- Nach der Aktualisierung von OpenManage Enterprise auf die neueste Version wird die Geräteliste nach dem erneuten Ausführen der Ermittlungsjobs aktualisiert.
- Sie können maximal 25 Geräte pro Seite auswählen. Navigieren Sie anschließend zu den Seiten, um mehr Geräte auszuwählen und Aufgaben durchzuführen.
- Einige der gerätebezogenen Aufgaben, die Sie auf der Seite „Alle Geräte“ durchführen können, z. B. Firmwareupdates, Aktualisieren der Bestandsaufnahme, Aktualisieren des Status, Serversteuerungsaktionen, können auch auf der Seite **Gerätedetails** durchgeführt werden.

Themen:

Geräte in Gruppen organisieren

In einem Rechenzentrum können Sie für ein effektives und schnelles Gerätemanagement Folgendes durchführen:

- Gruppieren Sie die Geräte. Sie können beispielsweise Geräte basierend auf Funktionen, Betriebssystemen, Benutzerprofilen, Standort oder ausgeführten Aufträgen gruppieren und dann Abfragen zur Verwaltung von Geräten ausführen.
- Filtern Sie die Geräte-bezogenen Daten beim Verwalten von Geräten, bei Firmware-Aktualisierung, beim Ermitteln von Geräten und Verwalten von Warnungsrichtlinien und Berichten.

- Sie können die Eigenschaften eines Geräts in einer Gruppe verwalten. Informationen dazu finden Sie unter Anzeigen und Konfigurieren einzelner Geräte auf Seite 68.

OpenManage Enterprise bietet einen integrierten Bericht, um einen Überblick über die von OpenManage Enterprise überwachten Geräte zu erhalten. Klicken Sie auf **OpenManage Enterprise** > **Monitor** > **Berichte** > **Geräteübersichtsbericht**. Klicken Sie auf **Ausführen**. Informationen dazu finden Sie unter Berichte ausführen auf Seite 141.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Um Dashboard-Daten zu ausgewählten Geräten oder Gruppen anzuzeigen, treffen Sie eine Auswahl aus dem Dropdown-Menü **Gerätegruppen**.

ANMERKUNG: Der Funktionsstatus eines Gerätes oder einer Gruppe wird durch entsprechende Symbole angezeigt. Der Funktionszustand einer Gruppe ist der Funktionszustand eines Geräts in einer Gruppe, die den kritischsten Zustand aufweist. Beispielsweise ist, unter vielen Geräten in einer Gruppe, wenn der Funktionszustand eines Servers eine Warnung aufweist, der Funktionszustand der Gruppe auch eine „Warnung“. Der Rollup-Status entspricht dem Status des Geräts mit hohem Schweregrad. Weitere Informationen über das Integritätsstatus-Rollup finden Sie im technischen Whitepaper *VERWALTEN DES INTEGRITÄTSSTATUS-ROLLUP DURCH VERWENDUNG VON IDRAC AUF DELL EMC POWEREDGE SERVERN DER 14. GENRATION UND SPÄTER* im Dell TechCenter.

Gruppen können eine übergeordnete und untergeordnete Gruppe vorweisen. Eine Gruppe kann seine übergeordnete Gruppe nicht als eigene untergeordnete Gruppe vorweisen. Standardmäßig enthält OpenManage Enterprise im Lieferumfang folgende integrierte Gruppen.

Systemgruppen: Von OpenManage Enterprise erstellte Standardgruppen. Sie können eine Systemgruppe nicht bearbeiten oder löschen, aber Sie können diese basierend auf Benutzerberechtigungen anzeigen. Beispiele für Systemgruppen:

- **HCI Appliances**: hyperkonvergente Geräte, wie z.B. VxRAIL- und Dell EMC XC-Geräte
- **Hypervisor-Systeme**: Hyper-V-Server und VMware ESXi-Server
- **Modulare Systeme**: Power Edge-Gehäuse, PowerEdge FX2, PowerEdge 1000e-Gehäuse, PowerEdge MX7000-Gehäuse und PowerEdge VRTX-Gehäuse

  ANMERKUNG: Bei einem MX7000-Gehäuse kann es sich um ein Haupt-, ein Standby- oder ein Mitgliedsgehäuse handeln. Wenn ein MX7000-Gehäuse ein Hauptgehäuse ist und ein Mitgliedsgehäuse besitzt, wird letzteres unter Verwendung der IP seines Hauptgehäuses ermittelt. Ein MX7000-Gehäuse wird mithilfe einer der folgenden Syntax identifiziert:

  - **MCM-Gruppe**: Zeigt die Multi-Chassis-Management(MCM)-Gruppe mit mehreren Gehäusen an, die durch folgende Syntax identifiziert werden: `Group_<MCM group name>_<Lead_Chassis_Svctag>`. Hierbei ist:
    - `<MCM group name>`: Name der MCM-Gruppe
    - `<Lead_Chassis_Svctag>`: Die Service-Tag-Nummer des Hauptgehäuses. Das Gehäuse, die Schlitten und die Netzwerk-EAMs bilden diese Gruppe.
  - **Standalone-Gehäusegruppe**: Wird durch die Syntax `<Chassis_Svctag>` identifiziert. Das Gehäuse, die Schlitten und die Netzwerk-EAMs bilden diese Gruppe.
- **Netzwerkgeräte**: Dell Force10 Networking-Switches und Fibre-Channel-Switches
- **Server**: Dell iDRAC Server, Linux-Server, Nicht-Dell Server, OEM-Server und Windows-Server.
- **Speichergeräte**: Dell Compellent-Speicherarrays, PowerVault MD-Speicherarrays und PowerVault ME-Speicherarrays
- **Ermittlungsgruppen**: Gruppen, die dem Bereich einer Ermittlungsaufgabe zugeordnet werden. Können nicht bearbeitet oder gelöscht werden, da die Gruppe vom Ermittlungsjob gesteuert wird, wo die Bedingung einschließen/ausschließen angewendet wird. Informationen dazu finden Sie unter Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41.

ANMERKUNG: Um alle Untergruppen einer Gruppe zu erweitern, klicken Sie mit der rechten Maustaste auf die Gruppe, und klicken Sie dann auf **Alle erweitern**.

Benutzerdefinierte Gruppen: von Administratoren für spezifische Anforderungen erstellt. Zum Beispiel Server, die E- Mail-Dienste hosten, werden zusammen gruppiert. Benutzer können je nach Benutzerberechtigungen und Gruppentypen anzeigen, bearbeiten und löschen.

- **Statische Gruppen**: Manuell vom Benutzer durch Hinzufügen bestimmte Geräte zu einer Gruppe erstellt. Diese Gruppen ändern sich nur, wenn ein Benutzer die Geräte in der Gruppe oder eine untergeordnete Gruppe manuell ändert. Die Elemente in der Gruppe bleiben statisch, bis die übergeordnete Gruppe bearbeitet oder das untergeordnete Gerät gelöscht wird.
- **Abfragegruppe**: Gruppen, die dynamisch anhand von benutzerdefinierten Kriterien definiert sind. Geräte in der Gruppe ändern sich basierend auf dem Ergebnis der Geräte, die durch die Verwendung von Kriterien ermittelt werden. Zum Beispiel wird eine Abfrage ausgeführt, um Server zu erkennen, die der Finanzabteilung zugewiesen wurden. Jedoch verfügen die Abfragegruppen über eine flache Struktur ohne jegliche Hierarchie.

ANMERKUNG: Statische und Abfragegruppen:

- Können nicht mehr als einen übergeordnete Gruppe aufweisen. Eine Gruppe kann nicht als eine untergeordnete Gruppe unter der übergeordneten Gruppe hinzugefügt werden.
- Wenn Änderungen an einer statischen Gruppe (Geräte werden hinzugefügt oder gelöscht) oder an einer Abfragegruppe (wenn eine Abfrage aktualisiert wird) vorgenommen werden, wird die Firmware-/Treiber-Compliance der Geräte, die diesen Gruppen zugeordnet sind, nicht automatisch aktualisiert. Es wird empfohlen, dass der Benutzer in solchen Fällen eine Firmware- und/oder Treiber-Compliance für die neu hinzugefügten/gelöschten Geräte initiiert.

ANMERKUNG: Das Erstellen einer größeren Anzahl von benutzerdefinierten (Abfrage-) Gruppen in der Gerätegruppe-Hierarchie wirkt sich auf die Gesamtleistung von OpenManage Enterprise aus. Für eine optimierte Performance erfasst OpenManage Enterprise den Rollup-Funktionszustand jeweils nach 10 Sekunden, weshalb sich eine höhere Anzahl an dynamischen Gruppen auf diese Leistung auswirkt.

Auf der Seite **Alle Geräte** im linken Fensterbereich können Sie untergeordneten Gruppen unter den übergeordneten statischen und Abfrage-Gruppen erstellen. Siehe Erstellen einer statischen Gerätegruppe auf Seite 58 und Abfrage-Gerätegruppe erstellen auf Seite 58.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

So löschen Sie die untergeordnete Gruppe einer statischen oder Abfragegruppe:

1. Klicken Sie mit der rechten Maustaste auf die statische oder Abfragegruppe und klicken Sie dann auf **Löschen**.
2. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**. Die Gruppe wird gelöscht und die Liste unter der Gruppe wird aktualisiert.

Plug-in-Gruppen: Plug-in-Gruppen werden erstellt, wenn Plug-ins wie Services, Power Manager Plug-in installiert sind. Wenn Plug-ins installiert sind, haben sie ihre eigenen Systemgruppen und einige Plug-ins, z. B. das Power Manager-Plug-in, können benutzerdefinierte Gruppen unter ihnen erstellen.

Zugehörige Tasks

Geräte aus OpenManage Enterprise löschen auf Seite 64
Aktualisieren der Geräte-Bestandsliste eines einzelnen Geräts auf Seite 73
Funktionszustand der Geräte einer Gerätegruppe aktualisieren auf Seite 66

Benutzerdefinierte Gruppe erstellen (statisch oder Abfrage)

Auf der Seite **OpenManage Enterprise** > **Geräte** („Alle Geräte") können Sie statische Gruppen oder Abfragegruppen mithilfe des Erstellungsassistenten für benutzerdefinierte Gruppen erstellen.

Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

1. Führen Sie einen der folgenden Schritte aus, um den Erstellungsassistenten für benutzerdefinierte Gruppen zu aktivieren:
   - Klicken Sie im linken Fensterbereich von **OpenManage Enterprise** > **Geräte** auf BENUTZERDEFINIERTE GRUPPEN, klicken Sie mit der rechten Maustaste oder klicken Sie auf das Menü mit den vertikalen drei Punkten und klicken Sie auf **Benutzerdefinierte Gruppe erstellen**.
   - Klicken Sie auf der Seite „Alle Geräte" im Dropdown-Menü **Gruppenaktionen** auf **Benutzerdefinierte Gruppe erstellen**.
2. Wählen Sie im Erstellungsassistenten für benutzerdefinierte Gruppe eine der folgenden benutzerdefinierten Gruppen aus:
   a. **Statische Gruppe**.
   b. **Abfragegruppe**
3. Klicken Sie auf **Erstellen**.
   Je nach Ihrer Auswahl (statisch oder Abfrage) wird entweder der Erstellungsassistent für statische Gruppen oder der Erstellungsassistent für Abfragegruppen aktiviert.

Sobald eine Gruppe (statisch oder Abfrage) erstellt wird, wird sie unter BENUTZERDEFINIERTE GRUPPE, Statische oder Abfragegruppen aufgeführt.

Erstellen einer statischen Gerätegruppe

Auf der Seite „Alle Geräte" (**OpenManage Enterprise** > **Geräte**) können Sie statische Gruppen mithilfe des Erstellungsassistenten für statische Gruppen erstellen. Die Geräte in einer statischen Gruppe bleiben statisch, bis die Geräte in der Gruppe hinzugefügt oder gelöscht werden.

Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Führen Sie einen der folgenden Schritte aus, um den Erstellungsassistenten für statische Gruppen zu aktivieren:
   - Klicken Sie entweder unter BENUTZERDEFINIERTE GRUPPEN, **Statische Gruppen** mit der rechten Maustaste oder klicken Sie auf das Menü mit den drei vertikalen Punkten und klicken Sie dann auf **Neue statische Gruppe erstellen**.
   - Klicken Sie auf **Gruppenaktionen** > **Benutzerdefinierte Gruppe erstellen** > **Statische Gruppe**.
2. Geben Sie im Dialogfeld des **Erstellungsassistenten für statische Gruppen** einen Namen und eine Beschreibung (optional) für die Gruppe ein und wählen Sie dann eine übergeordnete Gruppe aus, unter der die neue statische Gruppe erstellt werden soll.

   ANMERKUNG: Die statischen oder dynamischen Gruppennamen und die der Serverkonfiguration zugehörigen Namen in OpenManage Enterprise müssen eindeutig sein (unabhängig von Groß-/Kleinschreibung). Beispiel: *NAME1* und *Name1* können nicht gleichzeitig verwendet werden.

3. Klicken Sie auf **Weiter**.
4. Wählen Sie im Dialogfeld „Gruppenmitglied-Auswahl" die Geräte aus, die in der statischen Gruppe enthalten sein sollen.
5. Klicken Sie auf **Fertigstellen**.

Die statische Gruppe wird erstellt und unter der übergeordneten Gruppe im linken Fensterbereich gelistet. Die untergeordneten Gruppen werden unter der übergeordneten Gruppe eingerückt dargestellt.

Abfrage-Gerätegruppe erstellen

Abfragegruppen sind dynamische Gruppen, deren Geräte durch Abgleich einiger benutzerdefinierter Kriterien definiert werden. Geräte in der Gruppe ändern sich basierend auf dem Ergebnis der Geräte, die durch die Verwendung der Abfragekriterien ermittelt werden. Auf der Seite „Alle Geräte" (**OpenManage Enterprise** > **Geräte**) können Sie Abfragegruppen mithilfe des Erstellungsassistenten für Abfragegruppen erstellen.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Führen Sie einen der folgenden Schritte aus, um den Erstellungsassistenten für Abfragegruppen zu aktivieren:
   - Klicken Sie unter „Benutzerdefinierte Gruppen" entweder mit der rechten Maustaste auf **Abfragegruppen** oder klicken Sie auf das Menü mit den vertikalen drei Punkten neben den Abfragegruppen und klicken Sie dann auf **Neue Abfragegruppe erstellen**.
   - Klicken Sie auf **Gruppenaktionen** > **Benutzerdefinierte Gruppe erstellen** > **Abfragegruppe**.
2. Geben Sie im Dialogfeld **Assistent für das Erstellen einer Abfragegruppe** einen **Namen** und eine **Beschreibung** (optional) für die Gruppe ein.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie im Dialogfeld **Abfragekriterien-Auswahl** aus dem Dropdown-Menü **Vorhandene Abfrage zum Kopieren auswählen** eine Abfrage und dann die anderen Filterkriterien aus. Informationen dazu finden Sie unter Abfragekriterien auswählen auf Seite 58.
5. Klicken Sie auf **Fertigstellen**.
   Die Abfragegruppe wird erstellt und im Bereich „Abfragegruppen" im linken Fensterbereich gelistet.

Abfragekriterien auswählen

Definieren Sie Filter während des Erstellens von Abfragekriterien für:

- Erstellen benutzerdefinierter Berichte. Informationen dazu finden Sie unter Erstellen von Berichten auf Seite 143.
- Erstellen von abfragebasierten Gerätegruppen unter den BENUTZERDEFINIERTEN GRUPPEN. Informationen dazu finden Sie unter Abfrage-Gerätegruppe erstellen auf Seite 58.

Definieren Sie die Abfrage-Kriterien durch die Verwendung von zwei Optionen:

- **Wählen Sie vorhandene Abfrage zum Kopieren**: Standardmäßig bietet OpenManage Enterprise eine Liste integrierter Abfrage-Vorlagen, die Sie kopieren und Ihre eigenen Abfragekriterien aufbrauen können. Bei der Definition einer Abfrage können maximal 6

Kriterien (Filter) verwendet werden. Zum Hinzufügen von Filtern müssen Sie eine Option aus dem Drop-Down-Menü **Typ auswählen** wählen.

- **Typ auswählen**: Erstellen Sie ein Abfragekriterium von Grund auf, indem Sie Attribute aus diesem Drop-Down-Menü verwenden. Optionen im Menü hängen von den durch OpenManage Enterprise überwachten Geräten ab. Wenn ein Abfragetyp ausgewählt ist, werden nur entsprechende Operatoren, wie z. B. =, >, < und null angezeigt, basierend auf dem Abfragetyp. Diese Methode wird empfohlen für die Definition von Abfragekriterien bei der Erstellung von benutzerspezifischen Berichten.

  ANMERKUNG: Bei der Bewertung einer Abfrage mit mehreren Bedingungen ist die Reihenfolge der Auswertung die gleiche wie bei SQL. Zur Angabe einer bestimmten Reihenfolge für die Beurteilung der Bedingungen fügen Sie bei der Definition einer Abfrage Klammern hinzu bzw. entfernen diese.

ANMERKUNG: Bei Auswahl werden die Filterkriterien einer vorhandenen Abfrage nur virtuell kopiert, um ein neues Abfragekriterium zu erstellen. Die standardmäßigen Filterkriterien im Zusammenhang mit vorhandenen Abfragekriterien werden nicht geändert. Die Definition (Filter) von integrierten Abfragekriterien wird als Startpunkt für den Aufbau eines benutzerdefinierten Abfragekriteriums verwendet. Beispiel:

1. *Abfrage1* ist ein integriertes Abfragekriterium mit dem folgenden vordefinierten Filter: `Task Enabled=Yes`.
2. Kopieren Sie die Filter-Eigenschaften von *Abfrage1*, erstellen Sie *Abfrage2* und passen Sie die Abfragekriterien durch Hinzufügen eines weiteren Filters an: `Task Enabled=Yes` UND `(Task Type=Discovery)`.
3. Später öffnen Sie *Abfrage1*. Das Filterkriterium bleibt weiterhin `Task Enabled=Yes`.

1. Im Dialogfeld **Abfragekriterien-Auswahl** wählen Sie aus dem Drop-Down-Menü je nachdem, ob Sie ein Abfragekriterium für Abfrage-Gruppen oder für die Berichterstellung erstellen möchten.
2. Hinzufügen oder Entfernen eines Filters durch Klicken auf das Plus- oder Papierkorb-Symbol.
3. Klicken Sie auf **Fertigstellen**.
   Ein Abfragekriterium wird in der Liste der vorhandenen Abfragen erstellt und gespeichert. Ein Überwachungsprotokoll-Eintrag wird gemacht und in der Überwachungsprotokoll-Liste angezeigt. Informationen dazu finden Sie unter Überwachen von Auditprotokollen auf Seite 127.

Zugehörige Informationen

Verwalten der Device-Konfigurations-Compliance auf Seite 110
Konfigurations-Compliance-Baseline bearbeiten auf Seite 114
Konfigurations-Compliance-Baseline entfernen auf Seite 116

Statische Gruppe bearbeiten

Auf der Seite „Alle Geräte“ (**OpenManage Enterprise** > **Geräte**) können die vorhandenen statischen Gruppen umbenannt, neu positioniert und die Geräte in der statischen Gruppe mithilfe des Assistenten zum Bearbeiten von statischen Gruppen hinzugefügt oder gelöscht werden.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Klicken Sie mit der rechten Maustaste auf die statische Gruppe oder klicken Sie auf das Menü mit den drei vertikalen Punkten neben der statischen Gruppe und klicken Sie dann auf **Bearbeiten**, um den Assistenten zum Bearbeiten von statischen Gruppen zu aktivieren.
2. Im Assistenten zum Bearbeiten von statischen Gruppen können Sie den Namen, die Beschreibung und die übergeordnete Gruppe bearbeiten.
3. Klicken Sie auf **Weiter**.
4. Im Bildschirm Gruppenmitglied-Auswahl können Sie die Geräte aktivieren oder deaktivieren, um Sie in die statische Gruppe einzuschließen oder aus ihr auszuschließen.
5. Klicken Sie auf **Fertigstellen**.

Die an der statischen Gruppe vorgenommenen Änderungen werden implementiert.

Bearbeiten einer Abfragegruppe

Auf der Seite „Alle Geräte“ (**OpenManage Enterprise** > **Alle Geräte**) kann die vorhandene Abfragegruppe umbenannt, neu positioniert werden und die Abfragekriterien können basierend darauf, welche Geräte in der Abfragegruppe enthalten sind, mit dem Assistenten zum Bearbeiten von Abfragegruppe bearbeitet werden.

Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Klicken Sie unter BENUTZERDEFINIERTE GRUPPEN mit der rechten Maustaste auf die Abfragegruppe oder klicken Sie auf das Menü mit den drei vertikalen Punkten neben der Abfragegruppe und klicken Sie dann auf **Bearbeiten**.
2. Nehmen Sie im Assistenten zum Bearbeiten von Abfragegruppen nach Bedarf Änderungen am Namen und an der Beschreibung vor.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie im Dialogfeld „Abfragekriterien-Auswahl“ wählen Sie aus dem Dropdown-Menü **Vorhandene Abfrage zum Kopieren auswählen** eine Abfrage und dann die anderen Filterkriterien aus.
5. Klicken Sie auf **Fertigstellen**.

Die an der Abfragegruppe vorgenommenen Änderungen werden implementiert.

Statische oder Abfragegruppe umbenennen

So benennen Sie eine statische oder Abfragegruppe auf der Seite „Alle Geräte“ (**OpenManage Enterprise** > **Geräte**) um:

1. Klicken Sie unter **BENUTZERDEFINIERTE GRUPPEN** mit der rechten Maustaste auf die statische oder Abfragegruppe oder klicken Sie auf das Menü mit den drei Punkten neben der Gruppe, die Sie umbenennen möchten, und klicken Sie dann auf **Umbenennen**. Oder wählen Sie eine Gruppe aus und klicken Sie dann auf **Gruppenaktionen** > **Gruppe umbenennen**.
2. Geben Sie im Dialogfeld **Gruppe umbenennen** einen neuen Namen für die Gruppe ein.
3. Klicken Sie auf **Fertigstellen**.
   Der aktualisierte Name wird im linken Bereich aufgeführt.

Statische oder Abfragegerätegruppe löschen

Auf der Seite „Alle Geräte“ (**OpenManage Enterprise** > **Geräte**) können Sie eine vorhandene statische oder Abfragegruppe wie folgt löschen:

Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

ANMERKUNG: Dieses Verfahren gilt nur für das Löschen einer statischen oder Abfragegruppe. Die Geräte in der Gruppe werden jedoch nicht von der Seite „Alle Geräte“ gelöscht. Informationen zum Entfernen von Geräten aus OpenManage Enterprise erhalten Sie unter Geräte aus OpenManage Enterprise löschen auf Seite 64.

1. Klicken Sie unter **BENUTZERDEFINIERTE GRUPPEN** mit der rechten Maustaste auf die statische oder Abfragegruppe oder klicken Sie auf das Menü mit den vertikalen drei Punkten neben der Gruppe und klicken Sie dann auf **Löschen**. Oder wählen Sie die Gruppe aus, die Sie löschen möchten, und klicken Sie dann im Dropdown-Menü **Gruppenaktionen** auf **Gruppe löschen**.
2. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**.

Das Gerät wird aus BENUTZERDEFINIERTE GRUPPEN gelöscht.

Statische oder Abfragegruppe klonen

Die vorhandenen statischen oder Abfragegruppen können geklont und zu den BENUTZERDEFINIERTEN GRUPPEN hinzugefügt werden.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

1. Klicken Sie mit der rechten Maustaste auf die statische oder Abfragegruppe oder klicken Sie auf das Menü mit den vertikalen drei Punkten neben der statischen oder der Abfragegruppe und klicken Sie dann auf **Klonen**.

2. Geben Sie im Dialogfeld **Gruppe klonen** einen Namen und eine Beschreibung für die Gruppe ein. Wählen Sie zusätzlich für statische Gruppen eine übergeordnete Gruppe aus, unter der die geklonte statische Gruppe erstellt werden soll.
3. Klicken Sie auf **Fertigstellen**.
   Die geklonte Gruppe wird erstellt und unter der übergeordneten Gruppe im linken Fensterbereich gelistet.

Geräte zu einer neuen Gruppe hinzufügen

Sie können eine neue Gruppe erstellen und Ihr Geräte aus der Gerätelistentabelle auf der Seite „Alle Geräte“ hinzufügen.

Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Klicken Sie im **OpenManage Enterprise**-Menü auf **Geräte**.
   Es wird die Seite „Geräte“ angezeigt.
2. Aktivieren Sie in der Geräteliste das Kontrollkästchen der entsprechenden Geräte und klicken Sie dann auf **Gruppenaktionen** > **Zu neuer Gruppe hinzufügen**.
   a. Im Dialogfeld des **Erstellungsassistenten für statische Gruppen** geben Sie den **Namen** und die **Beschreibung** (optional) der Gruppe ein und wählen Sie dann eine **Übergeordnete Gruppe** aus, unter der die neue untergeordnete Gruppe erstellt werden soll. Weitere Informationen über Gruppen finden Sie unter Gerätegruppen.
   b. Um weitere Geräte zur Gruppe hinzuzufügen, klicken Sie auf **Weiter**. Andernfalls fahren Sie mit Schritt 3 fort.
3. Wählen Sie im Dialogfeld **Gruppenmitglied-Auswahl** mehrere Geräte aus der Liste **Geräte hinzufügen** aus.
   Nach Auswahl der Geräte auf der Registerkarte **Alle Geräte** werden die ausgewählten Geräte unter **Alle ausgewählten Geräte** aufgelistet.
4. Klicken Sie auf **Fertigstellen**.
   Eine neue Gruppe wird erstellt, und die Geräte werden zur ausgewählten Gruppe hinzugefügt.

   ANMERKUNG: Zum Erstellen von Gruppen oder zum Hinzufügen von Geräten zu einer Gruppe müssen Sie die Beziehungen der über- und untergeordneten Gruppen einhalten. Siehe Gerätegruppen.

Geräte zu einer vorhandenen Gruppe hinzufügen

Sie können Geräte einer vorhandenen Gruppe aus der Gerätelistentabelle auf der Seite „Alle Geräte“ hinzufügen.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Klicken Sie im **OpenManage Enterprise**-Menü auf **Geräte**.
   Es wird die Seite „Geräte“ angezeigt.
2. Aktivieren Sie in der Geräteliste das Kontrollkästchen der entsprechenden Geräte und klicken Sie dann auf **Gruppenaktionen** > **Zu vorhandener Gruppe hinzufügen**.
3. Geben Sie im Dialogfeld **Ausgewählte Geräte zu vorhandener Gruppe hinzufügen** einen Wert ein oder wählen Sie Daten aus.
   Weitere Informationen über Gruppen finden Sie unter Gerätegruppen.
4. Klicken Sie auf **Fertigstellen**.
   Die Geräte werden dann zu der ausgewählten bereits bestehenden Gruppe hinzugefügt.

   ANMERKUNG: Zum Erstellen von Gruppen oder zum Hinzufügen von Geräten zu einer Gruppe müssen Sie die Beziehungen der über- und untergeordneten Gruppen einhalten. Siehe Gerätegruppen.

Aktualisieren des Funktionszustands für Gruppen

In den folgenden Schritten wird beschrieben, wie Sie den Funktionszustand und den Onlinestatus einer ausgewählten Gruppe aktualisieren können.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

- Für die In-Band-Geräte, die unter Verwendung des ESXi- und Linux-Betriebssystems ermittelt werden, wird der Integritätsstatus ( ) als unbekannt ( ) angezeigt.

1. Navigieren Sie zu der Seite „Alle Geräte“ durch Klicken auf **OpenManage Enterprise** > **Geräte**.
2. Wählen Sie im linken Bereich die Gruppe aus, für die Sie den Funktionszustand aktualisieren möchten.
   Nach der Auswahl der Gruppe werden in der Geräteliste die Geräte der ausgewählten Gruppe aufgelistet.
3. Klicken Sie auf das Dropdown-Menü **Funktionszustand aktualisieren** und dann auf **Funktionszustand für Gruppe aktualisieren**.
   Der Funktionszustandsassistent wird angezeigt.
4. Im Funktionszustandassistenten wird unter **Jobname** der von der Appliance generierte Jobname für den Task zum Aktualisieren des Funktionszustands angezeigt. Bei Bedarf können Sie den Jobnamen ändern.
5. Das Dropdown-Menü **Gruppe auswählen** zeigt die Gruppe an, die Sie ausgewählt haben.
6. Wählen Sie aus der Dropdown-Liste eine der folgenden Optionen aus:
   a. **Jetzt ausführen**: zur sofortigen Ausführung der Aktualisierung des Funktionszustands für die ausgewählte Gruppe.
   b. **Später ausführen**: Sie können diese Option auswählen und dann den gewünschten Tag und die Uhrzeit auswählen, wann der Job zum Aktualisieren des Funktionszustands in der Gruppe ausgeführt wird.
   c. **Nach Zeitplan ausführen**: Wählen Sie diese Option aus, wählen Sie dann die Option „Täglich“ oder „Wöchentlich“ aus und wählen Sie dann eine Zeit aus, wenn Sie den Funktionszustand der Gruppe täglich oder wöchentlich zu einem bestimmten Zeitpunkt aktualisieren möchten.

Ein Job zum Aktualisieren des Funktionszustands und des Online-Status der Gruppe wird erstellt. Sie können die Auftragsdetails auf der Seite „Jobs“ (**OpenManage Enterprise** > **Überwachen** > **Jobs**) anzeigen.

Geräteliste

Die Liste der Geräte zeigt die Geräteeigenschaften an, wie z. B. IP-Adresse und Service-Tag-Nummer. Sie können maximal 25 Geräte pro Seite auswählen. Navigieren Sie anschließend zu den Seiten, um mehr Geräte auszuwählen und Aufgaben durchzuführen. Weitere Informationen zu den Vorgängen, die Sie auf der Seite „Alle Geräte“ durchführen können, finden Sie unter Seite „Alle Geräte“ – Geräteliste Vorgänge auf Seite 63.

ANMERKUNG: Standardmäßig zeigt die Geräteliste beim Aufstellen des ringförmigen Diagramms alle berücksichtigten Geräte an. Zum Anzeigen einer Liste der zugehörigen Geräte, die zu einem bestimmten Funktionszustand gehören, klicken Sie auf das entsprechende Farbband im ringförmigen Diagramm oder klicken Sie auf das Funktionszustands-Symbol. Geräte, die nur zu der ausgewählten Kategorie gehören, werden aufgelistet.

- **Funktionszustand** zeigt den betriebsfähigen Zustand des Geräts an. Die Funktionszustände (Normal, Kritisch und Warnung) werden anhand der Farbsymbole identifiziert. Siehe Gerätefunktionsstatus auf Seite 40
- **Stromzustand** zeigt an, ob das Gerät ein- oder ausgeschaltet ist.
- **Verbindungsstatus** zeigt den Verbindungsstatus der ermittelten Geräte zu OpenManage Enterprise an als: verbunden, getrennt oder getrennt (Authentifizierungsfehler).
- **Name** zeigt den Gerätenamen an.
- **IP-Adresse** gibt die IP-Adresse des auf dem Gerät installierten iDRAC an.
- **Kennung** zeigt die Service-Tag-Nummer des Geräts an.
- **Modell** zeigt die Modellnummer an.
- **Typ** zeigt den Gerätetyp an – Server, Gehäuse, Dell Storage und Netzwerkswitch.
- **Gehäusename** zeigt den Namen des Gehäuses an.
- **Steckplatzname** zeigt den Steckplatznamen für die Gehäusegeräte an.
- Die Spalte **Verwaltungsstatus** zeigt an, ob das Gerät überwacht oder gemanagt wird oder ein Proxy ist. Informationen dazu finden Sie unter Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41.

Zum Filtern der Daten in der Tabelle klicken Sie auf **Erweiterte Filter** oder auf das Filtersymbol. Um Daten als HTML-, CSV- oder PDF-Datei zu exportieren, klicken Sie auf das Export-Symbol oben rechts in der Ecke.

ANMERKUNG: Klicken Sie in der Geräteliste auf den Gerätenamen oder die IP-Adresse, um Device-Konfigurationsdaten anzuzeigen, und bearbeiten Sie dann die Device-Konfiguration. Informationen dazu finden Sie unter Anzeigen und Konfigurieren einzelner Geräte auf Seite 68.

ANMERKUNG: Der Fensterbereich zeigt das ringförmige Diagramm der ausgewählten Gerätegruppe an. Anhand des ringförmigen Diagramms können Sie die Liste der Geräte anzeigen, die zu den jeweiligen Funktionszuständen in dieser Gruppe gehören. Zum Anzeigen der Geräte mit einem anderen Funktionszustand klicken Sie auf das entsprechende Farbband im ringförmigen Diagramm.

Die Daten in der angegebenen Tabelle ändern sich. Weitere Informationen zur Verwendung des ringförmigen Diagramms finden Sie unter Ringförmiges Diagramm.

Seite „Alle Geräte“ – Geräteliste Vorgänge

Auf der Seite „Alle Geräte“ (**OpenManage Enterprise** > **Geräte**) können Sie in der Geräteliste verschiedene Geräteaktionen durchführen.

Die Aktionsschaltflächen sind kontextbezogen auf die Gruppenauswahl in der Struktur auf der linken Seite und auch auf die im Raster ausgewählten Geräte. Wenn die Aktion also gruppenbezogen ist, z. B. Gruppenaktionen wie „Bestandsaufnahme auf Gruppe ausführen“ und „Funktionszustand für Gruppe aktualisieren“, wird standardmäßig die ausgewählte Gruppe angezeigt. Alle Geräteaktionen werden standardmäßig auf die ausgewählten Geräte angewendet. Einige Aktionen, wie z. B. die Ermittlung, sind jedoch immer ohne Auswahl anwendbar. Außerdem hängt die Art der verfügbaren Aktionen pro Gerät vom ausgewählten Gerätetyp ab.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

- In der Dropdown-Liste **Gruppenaktionen** können Sie Folgendes tun:
  - Erstellen von benutzerdefinierten Gerätegruppen. Informationen dazu finden Sie unter Benutzerdefinierte Gruppe erstellen (statisch oder Abfrage) auf Seite 57.
  - Erstellen statischer Gerätegruppen. Informationen dazu finden Sie unter Erstellen einer statischen Gerätegruppe auf Seite 58.
  - Erstellen von Abfragegruppen. Siehe Abfrage-Gerätegruppe erstellen auf Seite 58
  - Bearbeiten von statischen oder Abfragegruppen. Siehe Statische Gruppe bearbeiten auf Seite 59 und Bearbeiten einer Abfragegruppe auf Seite 60.
  - Klonen von Gruppen. Informationen dazu finden Sie unter Statische oder Abfragegruppe klonen auf Seite 60.
  - Umbenennen von Gruppen. Informationen dazu finden Sie unter Statische oder Abfragegruppe umbenennen auf Seite 60.
  - Löschen von Gruppen. Informationen dazu finden Sie unter Statische oder Abfragegerätegruppe löschen auf Seite 60.
  - Hinzufügen von Geräten zu einer neuen Gruppe. Informationen dazu finden Sie unter Geräte zu einer neuen Gruppe hinzufügen auf Seite 61.
  - Hinzufügen von Geräten zu einer vorhandenen Gruppe. Informationen dazu finden Sie unter Geräte zu einer vorhandenen Gruppe hinzufügen auf Seite 61.
- In der Dropdown-Liste **Ermittlung** können Sie Folgendes tun:
  - Ermitteln und Integrieren von Geräten. Siehe Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41 und Onboarding von Geräten auf Seite 45.
  - Ausschließen von Geräten. Informationen dazu finden Sie unter Geräte aus OpenManage Enterprise ausschließen auf Seite 64.
  - Bearbeiten von Ausschlussbereichen. Informationen dazu finden Sie unter Globaler Ausschluss von Bereichen auf Seite 49.
- In der Dropdown-Liste **Bestandsaufnahme** können Sie Folgendes tun:
  - Ausführen einer Bestandsaufnahme für eine Gerätegruppe. Siehe Erstellen und Ausführen eines Bestandsaufnahme-Jobs.
  - Ausführen von Aktionen auf Geräten. Informationen dazu finden Sie unter Bestandsaufnahme auf Geräten ausführen auf Seite 65.
- In der Dropdown-Liste **Funktionszustand aktualisieren** können Sie Folgendes tun:
  - Aktualisieren des Funktionszustands für Gruppen. Informationen dazu finden Sie unter Aktualisieren des Funktionszustands für Gruppen auf Seite 61.
  - Aktualisieren des Funktionszustands für Geräte. Informationen dazu finden Sie unter Funktionszustand für Geräte aktualisieren auf Seite 66.
- Im Dropdown-Menü **Weitere Aktionen** können Sie Folgendes tun:
  - Einschalten der LED. Informationen dazu finden Sie unter Job zum Schalten von Geräte-LEDs erstellen auf Seite 134.
  - Ausschalten der LED. Informationen dazu finden Sie unter Job zum Schalten von Geräte-LEDs erstellen auf Seite 134.
  - Einschalten von Geräten. Informationen dazu finden Sie unter Job zur Stromverwaltung der Geräte erstellen auf Seite 135.
  - Ausschalten von Geräten. Informationen dazu finden Sie unter Job zur Stromverwaltung der Geräte erstellen auf Seite 135.
  - Ordentliches Herunterfahren von Geräten. Informationen dazu finden Sie unter Job zur Stromverwaltung der Geräte erstellen auf Seite 135.
  - Aus- und wieder Einschalten des Systems (Hardwareneustart). Informationen dazu finden Sie unter Job zur Stromverwaltung der Geräte erstellen auf Seite 135.
  - Systemzurücksetzung (Warmstart). Informationen dazu finden Sie unter Job zur Stromverwaltung der Geräte erstellen auf Seite 135.
  - Durchführen des IPMI CLI-Remotebefehls auf einem Gerät. Informationen dazu finden Sie unter Remote-RACADM- und IPMI-Befehle auf einzelnen Geräten ausführen auf Seite 72.

- Durchführen des RACADM CLI-Remotebefehls auf einem Gerät. Informationen dazu finden Sie unter Remote-RACADM- und IPMI-Befehle auf einzelnen Geräten ausführen auf Seite 72.
- Löschen von Geräten aus OpenManage Enterprise. Informationen dazu finden Sie unter Geräte aus OpenManage Enterprise löschen auf Seite 64.
- Exportieren von Daten auf allen Geräten. Siehe Alle oder ausgewählte Daten exportieren auf Seite 68
- Exportieren von Daten auf den ausgewählten Geräten. Siehe Alle oder ausgewählte Daten exportieren auf Seite 68

Geräte aus OpenManage Enterprise löschen

Die folgenden Schritte beschreiben, wie Sie die ermittelten Geräte in OpenManage Enterprise löschen und offboarden.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Ein Gerät, dem ein Profil zugeordnet ist, kann nicht gelöscht werden, es sei denn, die Zuordnung des Profils zu diesem Gerät wird aufgehoben. Weitere Informationen finden Sie unter Aufheben der Zuweisung von Profilen auf Seite 108.
- Ein Gerät kann auch dann gelöscht werden, wenn Tasks auf ihm ausgeführt werden. Auf einem Gerät initiierte Aufgaben schlagen fehl, wenn das Gerät vor deren Abschluss gelöscht wird.

So löschen Sie die ermittelten Geräte:

1. Navigieren Sie zu der Seite „Alle Geräte“ durch Klicken auf **OpenManage Enterprise** > **Geräte**.
2. Aktivieren Sie in der Geräteliste die Kontrollkästchen der entsprechenden Geräte, die Sie löschen möchten.
3. Klicken Sie auf das Dropdown-Menü **Weitere Aktionen** und dann auf **Nutzer löschen**.
4. Klicken Sie in der Eingabeaufforderung, die angibt, dass die Geräte aus OpenManage Enterprise gelöscht und offboardet werden , auf **Ja**.

Die ausgewählten Geräte werden vollständig aus OpenManage Enterprise entfernt. Nach dem Löschen des Geräts werden alle Onboarding-Informationen, die dem gelöschten Gerät entsprechen, entfernt. Die Nutzer-Anmeldeinformationen werden automatisch gelöscht, wenn sie nicht mit anderen Geräten geteilt werden. Wenn OpenManage Enterprise als Trap-Ziel auf dem gelöschten Gerät festgelegt wurde, müssen Sie die IP-Adresse der OpenManage Enterprise-Konsole als Trap-Ziel vom Gerät entfernen.

Zugehörige Informationen

Geräte in Gruppen organisieren auf Seite 55

Geräte aus OpenManage Enterprise ausschließen

Geräte werden in OpenManage Enterprise für die effiziente Handhabung von wiederholten Aufgaben wie Firmwareupdates, Konfigurationsaktualisierungen, Bestandsaufnahmeerstellung und Warnungsüberwachung ermittelt und gruppiert. Sie können allerdings auch die Geräte aus allen OpenManage Enterprise-Ermittlungs-, Überwachungs- und Verwaltungsaktivitäten ausschließen. In den folgenden Schritten wird beschrieben, wie Sie die bereits ermittelten Geräte aus OpenManage Enterprise ausschließen.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Navigieren Sie zu der Seite „Alle Geräte“ durch Klicken auf **OpenManage Enterprise** > **Geräte**.
2. Wählen Sie im linken Fensterbereich die Systemgruppe oder benutzerdefinierte Gruppe, deren Gerät ausgeschlossen werden soll.
3. Aktivieren Sie in der Geräteliste das Kontrollkästchen der entsprechenden Geräte und klicken Sie dann im Dropdown-Menü **Ermittlung** auf **Geräte ausschließen**.
4. Klicken Sie in der Eingabeaufforderung, die angibt, dass die Geräte vollständig entfernt und der globalen Ausschlussliste hinzugefügt werden, auf **JA**.

Die Geräte werden ausgeschlossen, der globalen Ausschlussliste hinzugefügt und nicht mehr von OpenManage Enterprise überwacht.

ANMERKUNG: Um das Gerät aus der globalen Ausschlussliste zu entfernen und seine Überwachung durch OpenManage Enterprise wiederherzustellen, müssen Sie die Geräte aus dem globalen Ausschlussbereich entfernen und dann auf „Erneut ermitteln“ klicken.

Bestandsaufnahme auf Geräten ausführen

In den folgenden Schritten wird beschrieben, wie Sie die Bestandserfassung für die ermittelten Geräte initiieren können.

Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

1. Navigieren Sie zu der Seite „Alle Geräte" durch Klicken auf **OpenManage Enterprise** > **Geräte**.
2. Aktivieren Sie in der Geräteliste das Kontrollkästchen der entsprechenden Geräte.
3. Klicken Sie im Dropdown-Menü **Bestandsaufnahme** auf **Bestandsaufnahme auf Geräten ausführen**.

Ein Bestandsaufnahme-Job wird für die Bestandserfassung der ausgewählten Geräte erstellt. Sie können den Status des Jobs auf der Seite „Bestandsaufnahme" (**OpenManage Enterprise** > **Überwachen** > **Bestandsaufnahme**) anzeigen.

Aktualisieren der Geräte-Firmware und -Treiber mithilfe von Baselines

Sie können die Firmware und/oder Treiberversion der Geräte auf der Seite „Alle Geräte" oder auf der Seite „Firmware/Treiber-Compliance" aktualisieren (siehe So aktualisieren Sie eine Firmware und/oder Treiber mithilfe des Baseline-Compliance-Berichts: auf Seite 84). Die Aktualisierung über die Seite „Alle Geräte" wird bei der Aktualisierung der Firmware und/des Treibers für ein einzelnes Gerät empfohlen.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Treiberaktualisierungen gelten nur für Geräte, die mit 64-Bit-Windows Versionen verknüpft sind.
- Treiberaktualisierungen auf den Geräten können nicht zurückgesetzt werden.
- Wenn das Firmwareupdate mit der Option „**Stufe für nächsten Server-Neustart**" durchgeführt wird, müssen die Bestandsaufnahme und die Baselineprüfung manuell ausgeführt werden, nachdem das Paket auf dem Remote-Gerät installiert wurde.
- Wenn das Gerät keine Baseline zugeordnet ist, ist das Drop-Down-Menü **Baseline** nicht vorausgefüllt. Um ein Gerät einer Baseline zuzuordnen, siehe Erstellen der Firmware-Baseline.
- Wenn Sie mehrere Geräte auswählen, werden nur die Geräte im Zusammenhang mit dem ausgewählten Basisplan in der Tabelle aufgeführt.

1. Wählen Sie auf der Seite „Alle Geräte" **die Geräteliste** aus und klicken Sie auf **Weitere Aktionen** > **Aktualisieren**.

   ANMERKUNG: Wenn Sie Geräte ausgewählt haben, stellen Sie sicher, dass diese mit einer oder mehreren Firmware-Baselines verknüpft sind. Ansonsten werden die Geräte im Compliance-Bericht nicht angezeigt und können daher nicht aktualisiert werden.

2. Im Dialogfeld **Gerät aktualisieren**:
   a. Wählen Sie auf dem Bildschirm **Aktualisierungsquelle auswählen** eine der folgenden Optionen aus:
      - Wählen Sie aus dem Drop-Down-Menü **Baseline** die Baseline aus. Es wird eine Liste der Geräte angezeigt, die der ausgewählten Firmware-Baseline zugeordnet sind. Die Compliance-Stufe für jedes Gerät wird in der Spalte „Compliance" angezeigt. Basierend auf der Compliance-Stufe können Sie die Firmware- und/oder Treiber-Version aktualisieren. Weitere Informationen über die Feldbeschreibungen auf dieser Seite finden Sie unter Anzeigen des Compliance-Berichts der Geräte-Firmware.
        i. Aktivieren Sie die Kontrollkästchen der Geräte, die aktualisiert werden müssen.
        ii. Klicken Sie auf **Weiter**.
      - Sie können die Firmware und/oder Treiber auch mithilfe eines individuellen Aktualisierungspakets aktualisieren. Klicken Sie auf **Individuelles Paket** und führen Sie die Anweisungen auf dem Bildschirm aus. Klicken Sie auf **Weiter**.

   b. Im Abschnitt **Zeitplan**:

- Klicken Sie unter „**Aktualisierung planen**" auf **Weitere Informationen**, um die wichtigen Informationen anzuzeigen, und wählen Sie eine der folgenden Optionen aus:
  a. **Jetzt aktualisieren**: Wendet die Firmware-/Treiber-Updates sofort an.
  b. **Später planen**: Wählen Sie diese Option, um ein Datum und die Uhrzeit für die Aktualisierung der Firmware- oder Treiber-Version anzugeben. Dieser Modus wird empfohlen, wenn Sie Ihre aktuellen Tasks nicht stören möchten.
- Wählen Sie unter **Serveroptionen** eine der folgenden Neustart-Optionen aus:

a. Um den Server unmittelbar nach der Aktualisierung der Firmware/Treiber neu zu starten, wählen Sie **Sofortiger Neustart des Servers** aus und wählen Sie im Drop-Down-Menü eine der folgenden Optionen aus:
   i. **Ordentlicher Neustart ohne erzwungenes Herunterfahren**
   ii. **Ordentlicher Neustart mit erzwungenem Herunterfahren**
   iii. **PowerCycle** für einen harten Reset des Geräts.
b. Wählen Sie **Stufe für nächsten Serverneustart** aus, um die Firmware-/Treiber-Aktualisierung auszulösen, wenn der nächste Neustart des Servers erfolgt. Wenn diese Option ausgewählt ist, müssen die Bestandsaufnahme- und die Baselineprüfung manuell ausgeführt werden, nachdem das Paket auf dem Remote-Gerät installiert wurde.

3. Klicken Sie auf **Fertigstellen**.

Ein Firmware-/Treiber-Aktualisierungsjob wird erstellt und in der Jobliste aufgeführt. Informationen dazu finden Sie unter Verwenden von Jobs zur Gerätesteuerung auf Seite 130.

Funktionszustand der Geräte einer Gerätegruppe aktualisieren

Standardmäßig wird der Funktionszustand aller Geräte und Gerätegruppen automatisch von der Appliance stündlich aktualisiert. Sie können jedoch jederzeit den Funktionszustand von Geräten und/oder Gerätegruppen aktualisieren. In den folgenden Schritten wird beschrieben, wie der Funktionszustand und der Onlinestatus für die ausgewählte Gerätegruppe auf der Seite „Alle Geräte" aktualisiert werden.

1. Wählen Sie im linken Fensterbereich die Gruppe, zu der das Gerät gehört.
   Die der Gruppe zugeordneten Geräte werden aufgelistet.
2. Aktivieren Sie das Kontrollkästchen der entsprechenden Geräte und klicken Sie dann auf **Status aktualisieren**.
   Ein Job wird erstellt, in der Liste „Jobs" aufgeführt und durch **Neu** in der Spalte „JOBSTATUS" gekennzeichnet.

Der neueste Status der ausgewählten Geräte wird erfasst und auf dem Dashboard und in anderen relevanten Abschnitten von OpenManage Enterprise angezeigt. Hier erfahren Sie, wie Sie eine Gerätebestandsliste herunterladen Einzelnen Gerätebestand exportieren auf Seite 67.

Zugehörige Informationen

Geräte in Gruppen organisieren auf Seite 55

Funktionszustand für Geräte aktualisieren

Standardmäßig wird der Funktionszustand aller Geräte und Gerätegruppen automatisch von der Appliance stündlich aktualisiert. Sie können jedoch jederzeit den Funktionszustand von Geräten und/oder Gerätegruppen aktualisieren. In den folgenden Schritten wird beschrieben, wie der Funktionszustand und der Onlinestatus für die ausgewählten Geräte auf der Seite „Alle Geräte" aktualisiert werden.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Für die In-Band-Geräte, die unter Verwendung des ESXi- und Linux-Betriebssystems ermittelt werden, wird der Integritätsstatus ( ) als unbekannt ( ) angezeigt.

1. Navigieren Sie zu der Seite „Alle Geräte" durch Klicken auf **OpenManage Enterprise** > **Geräte**.
2. Wählen Sie aus der Geräteliste die Geräte aus, für die Sie den aus Funktionszustand aktualisieren möchten.
3. Klicken Sie auf das Dropdown-Menü **Funktionszustand aktualisieren** und dann auf **Funktionszustand für Geräte aktualisieren**.

Für die ausgewählten Geräte wird eine Funktionszustands-Aufgabe initiiert. Sie können den Status der Funktionszustands-Aufgabe auf der Seite „Jobs" (**OpenManage** > **Überwachen** > **Jobs**) anzeigen.

Rollback der Firmware-Version eines einzelnen Geräts durchführen

Sie können auf einem Gerät ein Rollback der Firmware-Version durchführen, wenn diese höher ist als die Firmware-Version der ihm zugeordneten Baseline. Diese Funktion steht nur dann zur Verfügung, wenn Sie Eigenschaften für ein einzelnes Gerät anzeigen und konfigurieren. Informationen dazu finden Sie unter Anzeigen und Konfigurieren einzelner Geräte auf Seite 68. Sie können ein Upgrade oder Rollback der Firmware-Version eines einzelnen Geräts durchführen. Sie können ein Rollback der Firmware-Version von jeweils nur einem Gerät durchführen.

ANMERKUNG:

- Ein Rollback ist nur auf Firmware anwendbar. Gerätetreiber können nach der Aktualisierung nicht auf eine vorherige Version zurückgesetzt werden.
- Das Rollback gilt nur für Geräte, die von der OME-Konsole aus aktualisiert werden (gilt sowohl für das Baseline-Update als auch für ein einzelnes DUP-Update).
- Wenn einer der installierten iDRACs nicht im Zustand „Bereit" ist, kann ein Firmware-Aktualisierungs-Job Fehler anzeigen, obwohl die Firmware erfolgreich angewendet wird. Überprüfen Sie den iDRAC, der nicht im Zustand „Bereit" ist und dann drücken Sie F1, um beim Hochfahren des Servers fortzufahren.

Die Firmware anderer Geräte, die über die iDRAC GUI aktualisiert wurden, ist hier nicht aufgeführt und kann nicht aktualisiert werden. Weitere Informationen über das Erstellen einer Baseline finden Sie unter Erstellen einer Firmware-/Treiber-Baseline auf Seite 81.

1. Wählen Sie dann im linken Fensterbereich die Gruppe aus und klicken Sie anschließend auf den Gerätenamen in der Liste.
2. Klicken Sie auf der Seite **<Gerätename>** auf **Firmware/Treiber**.
3. Wählen Sie aus dem Drop-Down-Menü **Baseline** die Baseline aus, der das Gerät angehört.
   Alle Geräte, die mit der ausgewählten Baseline verbunden sind, werden aufgelistet. Weitere Informationen zur Feldbeschreibung in der Tabelle finden Sie unter Anzeigen des Baseline-Compliance-Berichts auf Seite 83.
4. Aktivieren Sie das Kontrollkästchen für das Gerät, dessen Firmware-Version zurückgesetzt werden muss, was durch angezeigt wird..
5. Klicken Sie auf **Firmware zurücksetzen**.
6. Im Dialogfeld **Firmware zurücksetzen** werden die folgenden Informationen angezeigt:
   - **KOMPONENTENNAME**: Komponente auf dem Gerät, dessen Firmware-Version höher als die Baseline-Version ist.
   - **AKTUELLE** VERSION: Aktuelle Version der Komponente.
   - **ROLLBACK-VERSION**: Empfohlene Firmware-Version, auf welche die Komponente zurückgestuft werden kann.
   - **ROLLBACK-QUELLE**: Klicken Sie auf **Durchsuchen**, um eine Quelle auszuwählen, von welcher die Firmware-Version heruntergeladen werden kann.
7. Klicken Sie auf **Fertigstellen**. Die Firmware-Version wird zurückgesetzt.

   ANMERKUNG: Derzeit verfolgt die Rollback-Funktion nur die Versionsnummer, aus der die Firmware zurückgesetzt wird, zurück. Rollback zieht nicht in Betracht, welche Firmwareversion installiert wurde, indem die Rollback-Funktion verwendet wurde (durch Zurücksetzung der Version).

Einzelnen Gerätebestand exportieren

Sie können Bestandsdaten von jeweils nur einem Gerät und ausschließlich in das .csv-Format exportieren

1. Wählen Sie im linken Fensterbereich die Gerätegruppe aus. Eine Liste der Geräte in der Gruppe wird unter Geräteliste angezeigt.
   Ein Ringdiagramm gibt den Gerätestatus im Arbeitsbereich an. Siehe Ringdiagramm. Eine Tabelle listet die Eigenschaften der ausgewählten Geräte auf. Siehe Geräteliste.
2. Aktivieren Sie in der Geräteliste das Kontrollkästchen für das entsprechende Gerät bzw. die Geräte und klicken Sie dann auf **Bestand exportieren**.
3. Im Dialogfeld **Speichern unter** an einem bekannten Speicherort speichern.

   ANMERKUNG: Beim Export in das .csv-Format werden einige in der grafischen Benutzeroberfläche (GUI) angezeigten Daten nicht mit einer beschreibenden Variable aufgelistet (Datenverlust beim Export).

Durchführen weiterer Aktionen für Gehäuse und Server

Über das Drop-Down-Menü **Weitere Aktionen** können Sie die folgenden Aktionen auf der Seite „Alle Geräte" ausführen. Wählen Sie das Gerät bzw. die Geräte aus und klicken Sie auf eine der folgenden Optionen:

- **LED einschalten**: Schaltet die LED des Geräts zur Identifizierung des Geräts in einer Gruppe von Geräten in einem Rechenzentrum ein.
- **LED ausschalten**: Schaltet die LED des Geräts aus.
- **Einschalten**: Schaltet das Gerät bzw. die Geräte ein.
- **Ausschalten**: Schaltet das Gerät bzw. die Geräte aus.
- **Ordentliches Herunterfahren**: Klicken Sie zum Herunterfahren des Zielsystems.
- **System aus- und einschalten (Kaltstart)**: Klicken Sie, um das System aus- und wieder einzuschalten.

- **System zurücksetzen (Softwareneustart)**: Klicken Sie zum Herunterfahren und Neustarten des Betriebssystems durch erzwungenes Ausschalten des Zielsystems.
- **Proxy**: Wird nur für MX7000-Gehäuse angezeigt. Gibt an, dass das Gerät im Falle von Multi-Chassis-Management (MCM) über ein MX7000-Hauptgehäuse erkannt wird.
- **IPMI-CLI**: Klicken Sie, um einen IPMI-Befehl auszuführen. Informationen dazu finden Sie unter Remote-Befehlsjob für die Geräteverwaltung erstellen auf Seite 135.
- **RACADM-CLI**: Klicken Sie, um einen RACADM-Befehl auszuführen. Informationen dazu finden Sie unter Remote-Befehlsjob für die Geräteverwaltung erstellen auf Seite 135.
- **Firmware aktualisieren**: Siehe Aktualisieren der Geräte-Firmware und -Treiber mithilfe von Baselines auf Seite 65.
- **Onboarding**: Siehe Onboarding von Geräten auf Seite 45.
- **Alle exportieren und ausgewählte exportieren**: Siehe Alle oder ausgewählte Daten exportieren auf Seite 68.

Hardware-Informationen für das MX7000-Gehäuse

- **Gehäusenetzteile**: Informationen über die Netzteile (PSUs), die in den Schlitten und anderen Komponenten verwendet werden.
- **Gehäusesteckplätze**: Informationen über die verfügbaren Steckplätze im Gehäuse und gegebenenfalls in den Steckplätzen installierte Komponenten.
- **Gehäuse-Controller**: Der Chassis Management Controller (CMC) und seine Version.
- **Lüfter**: Informationen über die im Gehäuse verwendeten Lüfter und ihr Betriebsstatus.
- **Temperatur**: Temperaturstatus und die Schwellenwerte des Gehäuses.
- **FRU:** Komponenten oder vor Ort austauschbare Einheiten (FRUs), die im Gehäuse installiert werden können.

Alle oder ausgewählte Daten exportieren

Sie können Daten exportieren:

- Über die Geräte, die Sie in einer Gerätegruppe anzeigen, und für die Sie strategische und statistische Analysen durchführen.
- Über maximal 1000 Geräte.
- Im Zusammenhang mit Systemwarnungen, Berichten, Auditprotokollen Gerätegruppenbestand, Geräteliste, Gewährleistungsinformationen, OpenManage Enterprise Services usw.
- In die folgenden Formate: HTML, CSV und PDF.

ANMERKUNG:

- Vermeiden Sie den PDF-Export von „Wide“-Tabellen mit Spalten mit langen Zeichenfolgen oder zu vielen Spalten. Aufgrund einer Beschränkung in der PDFMaker-Bibliothek wird der rechts außen liegende Abschnitt dieser exportierten Daten abgeschnitten.
- Ain einzelner Gerätebestand kann nur in das .csv-Format exportiert werden. Siehe Einzelnen Gerätebestand exportieren auf Seite 67
- Nur im Falle von Berichten können Sie nur ausgewählte Berichte zugleich und nicht alle Berichte exportieren. Informationen dazu finden Sie unter Exportieren ausgewählter Berichte auf Seite 144.

.

1. Um Daten zu exportieren, wählen Sie **Alle exportieren** oder **Ausgewählte exportieren**.
   Ein Job wird erstellt und die Daten werden zum ausgewählten Speicherort exportiert.
2. Laden Sie die Data herunter und führen Sie strategische und statistische Analysen durch, falls erforderlich.
   Basierend auf Ihrer Auswahl wurden die Daten geöffnet oder erfolgreich gespeichert.
   ANMERKUNG: Wenn Sie Daten in das .CSV-Format exportieren, müssen Sie über Anmeldeinformationen auf Administratorebene verfügen, um die Datei zu öffnen.

Anzeigen und Konfigurieren einzelner Geräte

ANMERKUNG: Klicken Sie in der Geräteliste auf den Gerätenamen oder die IP-Adresse, um Device-Konfigurationsdaten anzuzeigen, und bearbeiten Sie dann die Device-Konfiguration, wie in diesem Abschnitt beschrieben.

Durch Klicken auf **OpenManage Enterprise** > **Geräte** > **Auswahl eines Geräts in der Geräteliste** > **Details anzeigen** können Sie:

- Anzeigen von Informationen über den Funktions- und Stromzustand, die Geräte-IP und die Service-Tag-Nummer.
- Allgemeine Informationen über das Gerät anzeigen und Gerätesteuerung sowie Schritte zum Troubleshooting ausführen.

- Geräteinformationen anzeigen, wie RAID, Netzteil, Betriebssystem, NIC, Speicher, Prozessoren und das Speichergehäuse. OpenManage Enterprise bietet einen integrierten Bericht, um einen Überblick über NIC, BIOS, das physische und das virtuelle Laufwerk, die auf den von OpenManage Enterprise überwachten Geräten verwendet werden, zu erhalten. Klicken Sie auf **OpenManage Enterprise** > **Überwachen** > **Berichte**.
- Die Firmware-Versionen von Komponenten in einem Gerät aktualisieren oder zurücksetzen, die mit einer Firmware Baseline verbunden sind. Informationen dazu finden Sie unter Verwalten der Geräte-Firmware und -Treiber auf Seite 77.

  ANMERKUNG: Das Aktualisieren eines Geräts unter Verwendung des individuellen Paket-Workflows unterstützt nur auf ausführbaren Dateien (.exe) basierende Dell Update Packages. Beim Aktualisieren eines FX2-CMC muss das ausführbare DUP über einen der Schlitten im Gehäuse installiert werden.
- Die Warnungen im Zusammenhang mit einem Gerät bestätigen, exportieren, löschen oder ignorieren. Siehe Verwalten von Gerätewarnungen.
- Zeigen Sie die Protokolldaten für ein Gerät an und exportieren Sie sie. Informationen dazu finden Sie unter Verwalten einzelner Geräte-Hardwareprotokolle auf Seite 71.
- Zeigen Sie Konfigurations-Bestandsaufnahme für das Gerät für die Zwecke der Konfigurations-Compliance und verwalten Sie es. Ein Compliance-Abgleich wird eingeleitet, wenn die Konfigurations-Bestandsaufnahme gegen die Geräte ausgeführt wird.
- Zeigen Sie die Compliance-Stufe eines Geräts gegen die Konfigurations-Compliance-Baseline an, die ihm zugeordnet ist. Informationen dazu finden Sie unter Verwalten der Device-Konfigurations-Compliance auf Seite 110.

Geräteübersicht

- Auf der Seite **<Gerätename>** unter **Übersicht**, wird der Funktions- und Stromversorgungszustand sowie die Service-Tag-Nummer des Geräts angezeigt. Klicken Sie auf die IP-Adresse, um die iDRAC-Anmeldeseite zu öffnen. Siehe *iDRAC Benutzerhandbuch* auf der Support-Website von Dell.
  - **Informationen**: Zeigt Geräteinformationen wie Service-Tag-Nummer, DIMM-Steckplätze, iDRAC-DNS-Name, Prozessoren, Gehäuse, Betriebssystem und Name des Rechenzentrums an. Mehrere mit dem Gerät korrelierte Verwaltungs-IP-Adressen sind aufgelistet und können angeklickt werden, um die jeweilige Schnittstelle zu aktivieren.
  - **Aktuelle Warnungen**: Die letzten erzeugten Warnungen für das Gerät.
  - **Kürzlich durchgeführte Aktivitäten**: Eine Liste der zuletzt auf dem Gerät ausgeführten Jobs. Klicken Sie auf **Alle anzeigen**, um alle Jobs aufzurufen. Informationen dazu finden Sie unter Verwenden von Jobs zur Gerätesteuerung auf Seite 130.
  - **Remote-Konsole**: Klicken Sie auf **iDRAC starten** zum Starten der iDRAC-Anwendung. Klicken Sie auf **Virtuelle Konsole starten** zum Starten der virtuellen Konsole. Klicken Sie auf das Symbol **Vorschau aktualisieren**, um die Seite **Übersicht** zu aktualisieren.
  - **Server Subsystem**: Zeigt den Funktionszustand von anderen Komponenten des Geräts an, z. B. von Netzteil, Lüfter, CPU und Akku.

    ANMERKUNG: Die Zeit für die Erfassung von Subsystemdaten der Sensorkomponenten, die mithilfe IPMI ermittelt wurden, hängt von der Netzwerkverbindung, dem Zielserver und der Ziel-Firmware ab. Wenn während der Erfassung der Sensordaten Timeouts auftreten, starten Sie den Zielserver neu.
  - Der Abschnitt **Zuletzt aktualisiert** zeigt an, wann der Bestandsstatus des Geräts zuletzt aktualisiert wurde. Klicken Sie auf die Schaltfläche **Aktualisieren**, um den Status zu aktualisieren. Ein Bestandsaufnahme-Job wird gestartet wird und der Status wird auf der Seite aktualisiert.
- Durch die Verwendung von **Stromregelung** können Sie ein Gerät einschalten, ausschalten, aus- und einschalten und ordnungsgemäß herunterfahren.
- Durch die Verwendung von **Troubleshooting** können Sie:
  - Führen Sie den Diagnosebericht aus und laden Sie ihn herunter. Informationen dazu finden Sie unter Diagnoseberichte ausführen und herunterladen auf Seite 70.
  - iDRAC zurücksetzen.
  - Extrahieren Sie den Services-(SupportAssist-)Bericht und laden Sie ihn herunter. Informationen dazu finden Sie unter Extrahieren und Herunterladen des Services-(SupportAssist-)Berichts auf Seite 71.
- Den Gerätestatus aktualisieren.
- Den Gerätebestand anzeigen.
- Den gefundenen Gerätebestand können Sie durch Klicken auf **Bestandsaufnahme aktualisieren** exportieren. Informationen dazu finden Sie unter Alle oder ausgewählte Daten exportieren auf Seite 68.
- Führen Sie einen Remote-RACADM- und IPMI-Befehl auf dem Gerät aus. Informationen dazu finden Sie unter Remote-RACADM- und IPMI-Befehle auf einzelnen Geräten ausführen auf Seite 72.

OpenManage Enterprise liefert einen integrierten Bericht, damit Sie einen Überblick über die von OpenManage Enterprise überwachten Geräte erhalten. Klicken Sie auf **OpenManage Enterprise** > **Monitor** > **Berichte** > **Geräteübersichtsbericht**. Klicken Sie auf **Ausführen**. Informationen dazu finden Sie unter Berichte ausführen auf Seite 141.

Gerätehardwareinformationen

OpenManage Enterprise bietet einen integrierten Bericht über die Komponenten und deren Compliance mit der Firmware-Compliance-Baseline. Klicken Sie auf **OpenManage Enterprise** > **Überwachen** > **Berichte** > **Firmware-Compliance pro Komponentenbericht**. Klicken Sie auf **Ausführen**. Informationen dazu finden Sie unter Berichte ausführen auf Seite 141.

- **Gerätekarteninformationen** – Informationen über die im Gerät verwendeten Karten.
- **Installierte Software** – Liste der Firmware und Software, die auf den verschiedenen Komponenten im Gerät installiert sind.
- **Prozessor –** Prozessorinformationen wie Sockets, Familie, Geschwindigkeit, Kerne und Modell.
- **RAID-Controller-Informationen** — auf den Speichergeräten verwendete PERC- und RAID-Controller. Der Rollup-Status entspricht dem Status der RAID mit hohem Schweregrad. Weitere Informationen über Integritätsstatus-Rollup, finden Sie im Whitepaper *VERWALTEN DES INTEGRITÄTSSTATUS-ROLLUP DURCH VERWENDUNG VON IDRAC AUF DELL EMC POWEREDGE SERVERN DER 14. GENRATION UND SPÄTER* im Dell TechCenter.
- **NIC-Informationen** – Informationen über im Gerät verwendeten NICs.
- **Speicherinformation** — Daten zu auf Gerät verwendeten DIMMs.
- **Array-Festplatte**: Informationen zu den Laufwerken, die auf dem Gerät installiert sind. OpenManage Enterprise bietet einen integrierten Bericht über die HDDs oder virtuellen Laufwerke, die auf den von OpenManage Enterprise überwachten Geräten verfügbar sind. Klicken Sie auf **OpenManage Enterprise** > **Überwachen** > **Berichte** > **Bericht physisches Laufwerk**. Klicken Sie auf **Ausführen**. Informationen dazu finden Sie unter Berichte ausführen auf Seite 141.
- **Speicher-Controller**: Speicher-Controller, der auf dem Gerät installiert ist. Klicken Sie zum Anzeigen einzelner Controller Daten auf das Plussymbol.
- **Netzteilinformationen**: Informationen zu den Netzteileinheiten, die auf dem Gerät installiert sind.
- **Betriebssystem** — Auf dem Gerät installiertes BS.
- **Lizenzen** – Funktionsstatus der verschiedenen auf dem Gerät installierten Lizenzen.
- **Speichergehäuse** — Speichergehäusestatus und EMM-Version.
- **Virtual Flash** – Liste der virtuellen Flash-Laufwerke und deren technische Daten.
- **FRU –** Liste der vor Ort austauschbaren Einheiten, die nur von Servicetechnikern verarbeitet und repariert werden können OpenManage Enterprise bietet einen integrierten Bericht über die vor Ort austauschbaren Einheiten (Field Replaceable Units (FRUs)), die auf den von OpenManage Enterprise überwachten Geräten installiert sind. Klicken Sie auf **OpenManage Enterprise** > **Überwachen** > **Berichte** > **Bericht über vor Ort austauschbare Einheiten**. Klicken Sie auf **Ausführen**. Informationen dazu finden Sie unter Berichte ausführen auf Seite 141.
- **Gerätemanagementinformationen –** Informationen zur IP-Adresse von iDRAC (nur im Falle eines Servergeräts installiert).
- **Gast-Informationen** – Zeigt die Gastgeräte, die von OpenManage Enterprise überwacht werden. UUID ist der Universally Unique Identifier des Geräts. Die Spalte **Gast-Zustand** zeigt den Betriebsstatus des Gastgeräts.

Diagnoseberichte ausführen und herunterladen

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Siehe .Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

ANMERKUNG: Sie müssen KMUv1 in den **KMU Einstellungen** aktivieren, bevor Sie mit Firmware-Aufgaben beginnen, die Kommunikation mit einem beliebigen Gehäuse oder PowerEdge YX2X- und YX3X-Servern mit iDRAC-Version 2.50.50.50 und früheren Versionen erfordern. Weitere Informationen erhalten Sie unter Verwalten der Konsolen-Voreinstellungen auf Seite 165 und Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.

1. Wählen Sie auf der Seite **<Device name>** aus dem Dropdown-Menü **Fehlerbehebung** die Option **Diagnose ausführen** aus.
2. Wählen Sie im Dialogfeld **RemoteDiagnostic-Typ** aus dem Drop-Down-Menü **Remotediagnose-Typ** eine der folgenden Optionen aus, um einen Bericht zu generieren.
   - **Express**: So schnell wie möglich.
   - **Erweitert**: Mit Sollgeschwindigkeit.
   - **Langzeit**: Langsam.

   ANMERKUNG: Siehe technisches Whitepaper *Remotely Running Automated Diagnostics Using WS-Man and RACADM Commands* (Remote-Ausführung automatischer Diagnosen mithilfe von WS-Man- und RACADM-Befehlen) unter https://en.community.dell.com/techcenter/extras/m/white_papers/20438187.
3. Wählen Sie zum sofortigen Generieren des Diagnoseberichts **Jetzt ausführen** aus.
4. Klicken Sie auf **OK**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**.

WARNUNG: Das Ausführen eines Diagnoseberichts führt automatisch zu einem Neustart des Servers.

Es wird ein Job erstellt und auf der Seite **Jobs** angezeigt. Um Informationen zum Job anzuzeigen, klicken Sie im rechten Fensterbereich auf **Details anzeigen**. Informationen dazu finden Sie unter Anzeigen von Joblisten auf Seite 130. Der Job-Status wird auch im Abschnitt **Kürzlich durchgeführte Aktivitäten** angezeigt. Nachdem der Job erfolgreich ausgeführt wurde, wird der Status des Jobs als **Diagnose abgeschlossen** angezeigt, und der **Download**-Link wird im Abschnitt **Kürzlich durchgeführte Aktivitäten** angezeigt.

5. Um den Bericht herunterzuladen, klicken Sie auf den **Download**-Link und laden die Diagnoseberichtdatei <*Servicetag-jobid*.TXT herunter.
   - Andernfalls klicken Sie auf **Fehlerbehebung** > **Diagnosebericht herunterladen** und laden Sie dann die Datei herunter.
6. Klicken Sie im Dialogfeld **Remote-Diagnosedateien herunterladen** auf den Link zur .TXT-Datei, und laden Sie dann den Bericht herunter.
7. Klicken Sie auf **OK**.

Extrahieren und Herunterladen des Services-(SupportAssist-)Berichts

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Siehe Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

ANMERKUNG: Sie müssen KMUv1 in den **KMU Einstellungen** aktivieren, bevor Sie mit Firmware-Aufgaben beginnen, die Kommunikation mit einem beliebigen Gehäuse oder PowerEdge YX2X- und YX3X-Servern mit iDRAC-Version 2.50.50.50 und früheren Versionen erfordern. Weitere Informationen erhalten Sie unter Verwalten der Konsolen-Voreinstellungen auf Seite 165 und Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.

1. Wählen Sie auf der Seite **<Device name>** aus dem Dropdown-Menü **Fehlerbehebung** die Option **SupportAssist-Bericht extrahieren** aus.
2. Führen Sie im Dialogfeld **SupportAssist-Bericht extrahieren** folgende Schritte aus:
   a. Geben Sie den Dateinamen ein, unter dem der SupportAssist-Bericht gespeichert werden soll.
   b. Aktivieren Sie die Kontrollkästchen, die den Protokolltypen entsprechen, deren SupportAssist-Bericht extrahiert werden soll.
3. Klicken Sie auf **OK**.
   Es wird ein Job erstellt und auf der Seite **Jobs** angezeigt. Um Informationen zum Job anzuzeigen, klicken Sie im rechten Fensterbereich auf **Details anzeigen**. Informationen dazu finden Sie unter Anzeigen von Joblisten auf Seite 130. Der Job-Status wird auch im Abschnitt **Kürzlich durchgeführte Aktivitäten** angezeigt. Nachdem der Job erfolgreich ausgeführt wurde, wird der Status des Jobs als **Diagnose abgeschlossen** angezeigt, und der **Download**-Link wird im Abschnitt **Kürzlich durchgeführte Aktivitäten** angezeigt.
4. Um den Bericht herunterzuladen, klicken Sie auf den **Download**-Link, und laden Sie dann die SupportAssist Berichtsdatei <*Service-Tag -Nummer*> .<*Zeit*>.TXT herunter.
   - Andernfalls klicken Sie auf **Fehlerbehebung** > **SupportAssist-Bericht herunterladen**.
5. Klicken Sie im Dialogfeld **SupportAssist Dateien herunterladen** auf den .TXT-Datei-Link, und laden Sie dann den Bericht herunter. Jeder Link steht für den von Ihnen ausgewählten Protokolltyp.
6. Klicken Sie auf **OK**.

Verwalten einzelner Geräte-Hardwareprotokolle

ANMERKUNG: Die Hardwareprotokolle sind für YX4X-Server, MX7000-Gehäuse und -Schlitten verfügbar. Weitere Informationen finden Sie unter Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.

- Klicken Sie auf der Seite **<Gerätename>** auf **Hardwareprotokolle**. Es werden alle für das Gerät erzeugten Ereignis- und Fehlermeldungen aufgelistet. Informationen zu Feldbeschreibungen finden Sie unter Überwachen von Auditprotokollen auf Seite 127.
- Für ein Gehäuse werden Echtzeitdaten über die Hardwareprotokolle vom Gehäuse abgerufen.
- Um einen Kommentar hinzuzufügen, klicken Sie auf **Kommentar hinzufügen**.
- Geben Sie den Kommentar im Dialogfeld ein und klicken Sie dann auf **Speichern**. Der Kommentar wird gespeichert und durch ein Symbol in der Spalte **KOMMENTAR** gekennzeichnet.

- Um ausgewählte Protokolldaten in eine CSV-Datei zu exportieren, aktivieren Sie die entsprechenden Kontrollkästchen, und klicken Sie dann auf **Exportieren** > **Ausgewählte exportieren**.
- Klicken Sie zum Exportieren aller Protokolle einer Seite auf **Exportieren** > **Aktuelle Seite exportieren**.

Remote-RACADM- und IPMI-Befehle auf einzelnen Geräten ausführen

RACADM- und IPMI-Befehle können von der Seite „Gerätename“ an den iDRAC eines Geräts gesendet werden, um das entsprechende Gerät remote zu verwalten.

ANMERKUNG:

- Die RACADM-CLI erlaubt nur einen Befehl gleichzeitig.
- Die Verwendung der folgenden Sonderzeichen als RACADM- und IPMI-CLI-Parameter wird nicht unterstützt: **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, * und **'**.

1. Aktivieren Sie das Kontrollkästchen des entsprechenden Geräts und klicken Sie dann auf **Details anzeigen**.
2. Klicken Sie auf der Seite **<Gerätename>** auf **Remote-Befehlszeile** und wählen Sie dann **RACADM CLI** oder **IPMI CLI**.

   ANMERKUNG: Die Registerkarte „RACADM-CLI“ wird für die folgenden Server nicht angezeigt, weil die entsprechende Aufgabe im Gerätpaket nicht verfügbar ist: MX740c, MX840c und MX5016S.

3. Geben Sie im Dialogfeld **Remote-Befehl senden** den Befehl ein. Bis zu 100 Befehle können eingegeben werden, wobei jeder Befehl in einer neuen Zeile stehen muss. Aktivieren Sie das Kontrollkästchen **Ergebnisse nach dem Senden öffnen**, um die Ergebnisse im gleichen Dialogfeld anzuzeigen.

   ANMERKUNG: Geben Sie einen IPMI-Befehl mit der folgenden Syntax ein: `-I lanplus <command>`. Um den Befehl zu beenden, geben Sie „Exit“ ein.

4. Klicken Sie auf **Senden**.
   Ein Job wird erstellt und im Dialogfeld angezeigt. Der Job wird auch in den Jobdetails angezeigt. Informationen dazu finden Sie unter Anzeigen von Joblisten auf Seite 130.
5. Klicken Sie auf **Fertigstellen**.
   Im Abschnitt **Letzte Warnungen** wird der Fertigstellungs-Status des Jobs angezeigt.

Management-Anwendung iDRAC eines Geräts starten

1. Aktivieren Sie das Kontrollkästchen für das jeweilige Gerät.
   Status, Name, Typ, IP und Service-Tag-Nummer des Geräts werden angezeigt.
2. Klicken Sie im rechten Fensterbereich auf **Management-Anwendung starten**.
   Die iDRAC-Anmeldeseite wird angezeigt. Melden Sie sich mit iDRAC-Anmeldeinformationen an.

   Weitere Informationen zur Verwendung von iDRAC finden Sie unter Dell.com/idracmanuals.

   ANMERKUNG: Sie können die Verwaltungsanwendung auch durch Klicken auf die IP-Adresse in der Geräteliste starten. Informationen dazu finden Sie unter Geräteliste auf Seite 62.

Virtuelle Konsole starten

Der Link zur **virtuellen Konsole** kann mit der iDRAC Enterprise-Lizenz von YX4X Servern aufgerufen werden. Auf YX2X- und YX3X-Servern funktioniert der Link ab Version 2.52.52.52 von iDRAC Enterprise. Wird der Link angeklickt, wenn der aktuelle Plugin-Typ für die virtuelle Konsole Active X ist, werden Sie in einer Meldung zum Aktualisieren der Konsole auf HTML 5 aufgefordert, um die Benutzererfahrung zu verbessern. Weitere Informationen erhalten Sie unter Erstellen eines Jobs zum Ändern des Plugin-Typs der virtuellen Konsole auf Seite 136 und Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.

1. Aktivieren Sie das Kontrollkästchen für das jeweilige Gerät.
   Status, Name, Typ, IP und Service-Tag-Nummer des Geräts werden angezeigt.
2. Klicken Sie im rechten Fensterbereich auf **Virtuelle Konsole starten**.
   Die Seite der Remote-Konsole auf dem Server wird angezeigt.

Aktualisieren der Geräte-Bestandsliste eines einzelnen Geräts

Standardmäßig wird der Bestand der Software- und Hardwarekomponenten in Geräte oder Gerätegruppen alle 24 Stunden automatisch erfasst (z. B. jeden Tag um 12:00 Uhr). Um jedoch jederzeit den Bestandsbericht eines Geräts zu erfassen:

1. Aktivieren Sie das Kontrollkästchen des entsprechenden Geräts auf der Seite „Alle Geräte“ (**OpenManage Enterprise** > **Geräte**) und klicken Sie im rechten Fensterbereich auf **Details anzeigen** . Die Übersichtsseite für das Gerät wird angezeigt.
2. Klicken Sie auf **Bestandsaufnahme aktualisieren**, um einen Bestandsaufnahme-Job zu starten.
   Der Status des Bestandsaufnahme-Jobs kann auf der Seite „Bestand“ (**OpenManage Enterprise** > **Überwachen** > **Bestand**) angezeigt werden. Wählen Sie den Bestandsaufnahme-Job aus und klicken Sie auf **Details anzeigen**, um den erfassten Bestand des ausgewählten Geräts anzuzeigen. Weitere Informationen zum Anzeigen der aktualisierten Bestandsdaten finden Sie unter Anzeigen und Konfigurieren einzelner Geräte auf Seite 68. Hier erfahren Sie, wie Sie eine Gerätebestandsliste herunterladen Einzelnen Gerätebestand exportieren auf Seite 67.

Zugehörige Informationen

Geräte in Gruppen organisieren auf Seite 55

9

Verwalten von Geräteinventar

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Indem Sie auf das Menü **OpenManage Enterprise** > **Überwachen** > **Bestandsaufnahme** auswählen, können Sie einen Gerätebestandsbericht generieren, um Ihr Rechenzentrum besser zu verwalten, die Wartung zu reduzieren, den Mindestbestand aufrecht zu erhalten und die Betriebskosten zu senken. Durch die Verwendung der Funktion „Bestandsaufnahme-Zeitplan" in OpenManage Enterprise können Sie Jobs geplant zu einer vordefinierten Zeit ausführen und dann Berichte erstellen. Sie können Bestandsaufnahme-Jobs auf PowerEdge Servern, Netzwerkgeräten, PowerEdge Gehäusen, Equal Logic-Arrays, Compellent-Arrays und PowerVault-Geräten ab der 12. Generation planen.

Auf dieser Seite können Sie Bestandsaufnahme-Zeitpläne erstellen, bearbeiten, ausführen, stoppen oder löschen. Es wird eine Liste der vorhandenen Bestandsaufnahme-Zeitpläne angezeigt.

- **NAME**: Der Name des Bestandsaufnahme-Zeitplans.
- **ZEITPLAN**: Gibt an, ob der Job jetzt oder später ausgeführt werden soll.
- **LETZTE AUSFÜHRUNG**: Gibt die Zeit der letzten Ausführung des Jobs an.
- **STATUS**: Gibt an, ob der Job ausgeführt wird, abgeschlossen oder fehlgeschlagen ist.

ANMERKUNG: Auf den Seiten **Ermittlung** und **Bestandsaufnahme-Zeitpläne** wird der Status eines geplanten Jobs durch **In Warteschlange** in der Spalte **STATUS** definiert. Jedoch wird derselbe Status als **Geplant** auf der Seite **Jobs** angezeigt.

Um eine Vorschau einer Jobinformation zu erstellen, klicken Sie auf die Zeile des Jobs. Im rechten Fensterbereich werden die Job-Daten und die Zielgruppen im Zusammenhang mit der Bestandsaufnahme-Task angezeigt. Um Informationen über den Job anzuzeigen, klicken Sie auf **Details anzeigen**. Auf der Seite **Jobdetails** werden weitere Informationen angezeigt. Informationen dazu finden Sie unter Einzelne Jobinformationen anzeigen auf Seite 134.

Zugehörige Tasks

Sofortiges Ausführen eines Bestandsaufnahme-Jobs auf Seite 75

Stoppen eines Bestandsaufnahme-Jobs auf Seite 75

Löschen eines Bestandsaufnahme-Jobs auf Seite 76

Erstellen eines Bestandsaufnahme-Jobs auf Seite 74

Themen:

Erstellen eines Bestandsaufnahme-Jobs

In den folgenden Schritten wird beschrieben, wie Sie die Bestandserfassung für die ermittelten Gruppen initiieren können.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Die Bestandsaufnahme auf Gehäuse-Speicherschlitten wird in OpenManage Enterprise nicht unterstützt, wenn sie über die Gehäusegeräteverwaltung verwaltet werden.

1. Führen Sie einen der folgenden Schritte aus, um den Bestandsaufnahmeassistenten zu initiieren:
   a. Wählen Sie auf der Seite „Alle Geräte“ (**OpenManage Enterprise** > **Geräte**) eine Gruppe im linken Bereich aus und klicken Sie im Dropdown-Menü **Bestandsaufnahme** auf **Bestandsaufnahme auf Gruppe ausführen**.
   b. Klicken Sie auf der Seite „Bestandsaufnahme“ (**OpenManage Enterprise** > **Monitor** > **Bestandsaufnahme**) auf **Erstellen**.
2. Im Dialogfeld **Bestandsaufnahme** wird ein Standard-Bestandsaufnahme-Jobnamen unter **Bestandsaufnahme-Jobnamen** eingetragen. Um diesen zu ändern, geben Sie einen Bestandsaufnahme-Jobnamen ein.
3. Wählen Sie im Drop-Down-Menü **Gruppen auswählen** die Geräte aus, für die die Bestandsaufnahme ausgeführt werden muss.

   Wenn Sie den Bestandsaufnahme-Job von der Seite „Alle Geräte“ aus initiiert haben, nachdem Sie eine Gruppe ausgewählt haben, wird „Gruppen auswählen“ vorab mit dem ausgewählten Gruppennamen ausgefüllt. Weitere Informationen zu Gerätegruppen finden Sie unter Geräte in Gruppen organisieren auf Seite 55.
4. Führen Sie den Job im Abschnitt **Zeitplanung** sofort aus oder planen Sie ihn für einen späteren Zeitpunkt.

   Informationen dazu finden Sie unter Felddefinitionen für die Jobplanung auf Seite 182.
5. Sie können die folgenden **zusätzlichen Optionen** auswählen, während Sie den Bestandsaufnahme-Job ausführen:
   - Aktivieren Sie das Kontrollkästchen **Konfigurationsbestand erfassen**, um eine Bestandsaufnahme der Konfigurations-Compliance-Baseline zu erzeugen.
   - Aktivieren Sie das Kontrollkästchen **Treiber-Bestandsaufnahme erfassen**, um Treiber-Bestandsaufnahme-Informationen vom Windows-Server zu sammeln. Außerdem können Sie die Bestandsaufnahme und die Dell System-Aktualisierung auf dem Windows-Server installieren, wenn diese Komponenten auf dem Server nicht verfügbar sind.

   ANMERKUNG:
   - Die Bestandsaufnahme der Treiber-Erfassung gilt nur für Geräte, die als Windows 64 Bit-Server ermittelt wurden.
   - Die Bestandserfassung von Windows-basierten Geräten wird nur unter Verwendung von OpenSSH unterstützt. Andere SSH-Implementierungen auf Windows, wie die CygWin-SSH, werden nicht unterstützt.

   Weitere Informationen zu Compliance-Baselines der Konfiguration finden Sie unter Verwalten der Device-Konfigurations-Compliance auf Seite 110.
6. Klicken Sie auf **Fertigstellen**.
7. Der Job wird erstellt und in der Liste aufgeführt.
   Ein Bestandsaufnahme-Job wird erstellt und wird in der Liste der Bestandsaufnahme-Jobs angezeigt. Die Spalte **ZEITPLAN** gibt an, ob der Job eingeplant oder nicht eingeplant ist. Informationen dazu finden Sie unter Sofortiges Ausführen eines Bestandsaufnahme-Jobs auf Seite 75.

Zugehörige Informationen

Verwalten von Geräteinventar auf Seite 74

Sofortiges Ausführen eines Bestandsaufnahme-Jobs

ANMERKUNG: Sie können einen bereits laufenden Job nicht erneut ausführen.

1. Aktivieren Sie in der Liste der vorhandenen Jobs des Bestandsaufnahme-Zeitplans das entsprechende Kontrollkästchen des Bestandsaufnahmejobs, den Sie sofort ausführen möchten.
2. Klicken Sie auf **Jetzt ausführen**.

   Der Job wird unmittelbar gestartet und eine Meldung wird in der rechten unteren Bildschirmecke angezeigt.

Zugehörige Informationen

Verwalten von Geräteinventar auf Seite 74

Stoppen eines Bestandsaufnahme-Jobs

Sie können den Job nur stoppen, wenn er ausgeführt wird. Abgeschlossene oder fehlgeschlagene Bestandsaufnahme-Jobs können nicht gestoppt werden. So stoppen Sie einen Job:

1. Aktivieren Sie in der Liste der vorhandenen Jobs des Bestandsaufnahme-Zeitplans das entsprechende Kontrollkästchen des Jobs des Bestandsaufnahme-Zeitplans, den Sie stoppen möchten.
2. Klicken Sie auf **Stopp**.

Der Job wird gestoppt und eine Meldung wird in der rechten unteren Bildschirmecke angezeigt.

Zugehörige Informationen

Verwalten von Geräteinventar auf Seite 74

Löschen eines Bestandsaufnahme-Jobs

ANMERKUNG: Sie können keinen Auftrag löschen, wenn er ausgeführt wird.

1. Aktivieren Sie in der Liste der vorhandenen Jobs des Bestandsaufnahme-Zeitplans das entsprechende Kontrollkästchen des Jobs der Bestandsaufnahme, den Sie löschen möchten.
2. Klicken Sie auf **Löschen**.
   Der Job wird gelöscht und eine Meldung wird in der rechten unteren Bildschirmecke angezeigt.

Zugehörige Informationen

Verwalten von Geräteinventar auf Seite 74

Bearbeiten eines Jobs des Bestandsaufnahmezeitplans

1. Klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Dialogfeld **Bestandsaufnahmezeitplan** den Bestandsaufnahme-Jobnamen unter **Bestandsaufnahme-Jobname**.
   Informationen dazu finden Sie unter Erstellen eines Bestandsaufnahme-Jobs auf Seite 74.
   Der Zeitplan für die Bestandsaufnahme wird aktualisiert und in der Tabelle angezeigt.

10

Verwalten der Geräte-Firmware und -Treiber

Auf der Seite **OpenManage Enterprise** > **Konfiguration** > **Firmware-/Treiber-Compliance** können Sie die Firmware aller „gemanagten“ Geräte verwalten. Sie können auch die Treiber der 64-Bit-Windows-basierten Geräte aktualisieren.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Die Geräte-Firmware- oder -Treiber-Version, wenn Sie älter als die Baseline-Version ist, wird nicht automatisch aktualisiert und der Nutzer muss die Aktualisierung initiieren.
- Es wird empfohlen, die Geräte-Firmware und -Treiber während Wartungsfenstern zu aktualisieren, um zu verhindern, dass die Geräte oder die Umgebung während der Geschäftszeiten offline gehen.
- Zur Verwaltung der Firmware und/oder Treiber eines Geräts sollte der Onboarding-Status des Systems entweder „Verwaltet“ oder „Verwaltet mit Warnmeldungen“ sein. Siehe . Onboarding von Geräten auf Seite 45
- Derzeit enthält der Katalog Treiber nur für 64-Bit-Windows-basierte Geräte.

Durch Verwendung der Firmware-/Treiber-Funktion können Sie:

- Verwenden Sie einen Firmware- und Treiberkatalog von Dell.com entweder direkt oder nach dem Speichern auf einem Netzwerkpfad. Siehe Hinzufügen eines Katalogs unter Verwendung von Dell.com auf Seite 78 oder Erstellen eines Firmwarekatalogs mithilfe eines lokalen Netzwerks.
- Erstellen Sie eine Firmware- und Treiber-Baseline unter Verwendung der verfügbaren Kataloge. Diese Baselines dienen als Benchmarks zum Vergleich der Firmware- und Treiberversion auf den Geräten mit der Version im Katalog. Siehe Erstellen der Firmware-Baseline.
- Führen Sie einen Compliance-Bericht aus, um zu überprüfen, ob die der Firmware- und Treiber-Baseline zugeordneten Geräte den Baseline-Versionen entsprechen. Siehe Überprüfen der Firmware-Compliance. Die Spalte **COMPLIANCE** zeigt Folgendes an:
  - **OK** – – wenn die Version der Firmware und/oder Treiber des/der Zielgerät(e) mit der Baseline übereinstimmt.
  - **Aktualisierung**: wenn das/die Zielgerät/e eine oder mehrere Versionen aufweist, die älter als die Firmware- oder Treiber-Baseline sind. Siehe Aktualisieren der Firmware-Version des Geräts.
  - **Kritisch** – wenn das Gerät nicht mit der Baseline konform ist und anzeigt, dass es sich um eine kritische Aktualisierung handelt, und die Firmware und Treiber der Geräte aktualisiert werden müssen, um die ordnungsgemäße Funktion sicherzustellen.
  - **Warnung** – wenn die Geräte-Firmware und/oder -Treiber nicht mit der Baseline übereinstimmen und die Geräte-Firmware aktualisiert werden kann, um die Funktionalität zu verbessern.
  - **Downgrade** – wenn die Geräte-Firmware und/oder -Treiber über der Baseline-Version liegen.
  - Exportieren Sie den Compliance-Bericht für statistische und Analysezwecke.
  - Aktualisieren Sie die Geräte-Firmware und/oder -Treiber mithilfe der Baseline. Informationen dazu finden Sie unter Aktualisieren der Geräte-Firmware und -Treiber mithilfe von Baselines auf Seite 65.

ANMERKUNG:

- Wenn eine Firmware/Treiber-Baseline mit vielen Geräten auf Compliance geprüft wird, wird die Warnmeldung CDEV9000 auf der Seite Warnmeldungen nur für ein zufälliges nicht konformes Gerät von dieser Baseline protokolliert.
- Der Firmware-oder Treiber-Compliance-Status von Netzwerkswitches, modularen EAAs und Dell Speichergeräten wird als **Unbekannt** angezeigt, da diese nicht über den Dell Katalog aktualisierbar sind. Es wird empfohlen, für diese Geräte einzelne Firmware- oder Treiber-Updates über das jeweilige Update-Paket durchzuführen. Um einzelne Firmware- oder Treiber-Updates durchzuführen, wählen Sie ein Gerät auf der Seite „Alle Geräte“ aus und klicken Sie auf **Details anzeigen** > **Firmware/Treiber** und wählen Sie die jeweilige Paketoption aus. Weitere Informationen über die Liste der nicht unterstützten Geräte finden Sie unter Firmware/Treiber-Compliance-Baseline-Berichte: Geräte mit dem Konformitätsstatus „Unbekannt“ auf Seite 186.

Sie können die Firmware-Version eines Geräts auch auf folgenden Seiten aktualisieren:

- Seite „Alle Geräte“. Siehe Aktualisieren der Firmware-Version des Geräts.

- Seite „Gerätedetails“ Klicken Sie in der Geräteliste auf den Gerätenamen oder die IP-Adresse, um Device-Konfigurationsdaten anzuzeigen, und bearbeiten Sie dann die Device-Konfiguration. Informationen dazu finden Sie unter Anzeigen und Konfigurieren einzelner Geräte auf Seite 68.

  ANMERKUNG: Das Aktualisieren eines Geräts unter Verwendung des individuellen Paket-Workflows unterstützt nur auf ausführbaren Dateien (.exe) basierende Dell Update Packages. Beim Aktualisieren eines FX2-CMC muss das ausführbare DUP über einen der Schlitten im Gehäuse installiert werden.

  Die Zusammenfassung aller Baselines wird im Arbeitsbereich angezeigt, und die Compliance einer ausgewählten Baseline wird im rechten Fensterbereich anhand eines Ringdiagramms angezeigt. Ein Ringdiagramm und die Liste der Elemente in der Baseline ändert sich entsprechend der Baseline, die Sie aus der Baseline-Liste auswählen. Siehe Ringdiagramm.

Themen:

Firmware- und Treiber-Kataloge verwalten

Kataloge sind Firmware- und Treiber-Bündel basierend auf Gerätetypen. Alle verfügbaren Kataloge (Update-Pakete) werden validiert und auf Dell.com veröffentlicht. Sie können den Katalog direkt aus dem Online-Repository verwenden oder auf eine Netzwerkfreigabe herunterladen.

Mithilfe dieser Kataloge können Sie Firmware-/Treiber-Baselines für die ermittelten Geräte erstellen und deren Compliance überprüfen. Dies verringert den zusätzlichen Aufwand für Administratoren und Device-Manager und reduziert außerdem die Gesamtzeit für den Update-Vorgang und die Wartung.

Administratornutzer können alle Kataloge in OpenManage Enterprise anzeigen und auf sie zugreifen. Geräte-Manager können hingegen nur Kataloge anzeigen und verwalten, die sie erstellt haben und besitzen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Informationen zu Felddefinitionen auf der Seite „Katalog-Verwaltung“ finden Sie unter Felddefinitionen Katalogverwaltung auf Seite 186. Diese Katalogquellen können Sie derzeit abrufen:

ANMERKUNG:

- Die Verwaltung des Firmware-Katalogs über Dell.com oder einen lokalen Netzwerkpfad ist auf den Enterprise Server-Katalog beschränkt.
- Kataloge, deren Basisspeicherort auf „Downloads.dell.com“ verweist, können ohne die Dell Update Packages (DUPs) verwendet werden, während der Katalog in OpenManage Enterprise Version 3.5 von einer Netzwerkfreigabe importiert wird. Während der Aktualisierung der Firmware werden die DUPs direkt von https://downloads.dell.com heruntergeladen.

- **Neueste Komponenten-Versionen auf Dell.com**: Listet die neuesten Firmware- und Treiber-Versionen (64-Bit-Windows) von Geräten auf. Beispiel: iDRAC, BIOS, PSU und HDDs, die umfassend getestet und freigegeben und auf Dell.com veröffentlicht wurden. Siehe Erstellen eines Firmwarekatalogs unter Verwendung von Dell.com.
- **Netzwerkpfad**: Speicherort, an dem Firmware- und Treiber-Kataloge von Dell Repository Manager (DRM) heruntergeladen und auf einer Netzwerkfreigabe gespeichert werden. Siehe Erstellen eines Firmwarekatalogs mithilfe eines lokalen Netzwerks.

Hinzufügen eines Katalogs unter Verwendung von Dell.com

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Benutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

ANMERKUNG: Sie müssen SMBv1 in den **SMB Einstellungen** aktivieren, bevor Sie mit Firmware-Aufgaben beginnen, die Kommunikation mit einem beliebigen Gehäuse oder PowerEdge YX2X- und YX3X-Servern mit iDRAC-Version 2.50.50.50 und früheren Versionen erfordern. Weitere Informationen erhalten Sie unter Verwalten der Konsolen-Voreinstellungen auf Seite 165 und Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.

1. Klicken Sie auf der Seite **Katalogverwaltung** auf **Hinzufügen**.

2. Im Dialogfeld **Aktualisierungskatalog hinzufügen**:
   a. Geben Sie in das Feld **Name** einen Firmware-Katalognamen ein.
   b. Für die **Katalogquelle** wählen Sie die Option **Neueste Komponenten-Versionen auf Dell.com**.
   c. Wählen Sie im Dialogfeld **Katalog aktualisieren** entweder **Manuell** oder **Automatisch**.
   d. Wenn **Automatisch** im Dialogfeld **Katalog aktualisieren** ausgewählt ist, muss für **Aktualisierungshäufigkeit** entweder **Täglich** oder **Wöchentlich** gewählt werden, gefolgt von der Zeit im 12-Stunden-Format mit AM/PM.
   e. Klicken Sie auf **Fertigstellen**.

      Die Schaltfläche **Fertigstellen** wird erst angezeigt, nachdem Sie alle Felder im Dialogfeld ausgefüllt haben.

      Ein neuer Firmwarekatalog wird erstellt und in der Katalogtabelle auf der Seite **Katalogverwaltung** aufgeführt.
3. Für die Rückkehr auf die Seite **Firmware-/Treiber-Compliance** klicken Sie auf **Zurück zu Firmware-/Treiber-Compliance**.

Hinzufügen eines Katalogs zum lokalen Netzwerk

Katalog, der die Firmware und Treiber (64-Bit-Windows) enthält, kann unter Verwendung des Dell Repository Managers (DRM) heruntergeladen und auf einer Netzwerkfreigabe gespeichert werden.

1. Klicken Sie auf der Seite **Katalogverwaltung** auf **Hinzufügen**.
2. Im Dialogfeld **Aktualisierungskatalog hinzufügen**:
   a. Geben Sie in das Feld **Name** einen Katalognamen ein.
   b. Für die Katalogquelle wählen Sie die Option **Netzwerkpfad**.
      Das Dropdown-Menü **Freigabetyp** wird angezeigt.
   c. Wählen Sie eine der folgenden Optionen:

      ANMERKUNG: Sie müssen KMUv1 in den **KMU Einstellungen** aktivieren, bevor Sie mit Firmware-Aufgaben beginnen, die Kommunikation mit einem beliebigen Gehäuse oder PowerEdge YX2X- und YX3X-Servern mit iDRAC-Version 2.50.50.50 und früheren Versionen erfordern. Weitere Informationen erhalten Sie unter Verwalten der Konsolen-Voreinstellungen auf Seite 165 und Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.

      - NFS
        i. Geben Sie in das Feld **Freigabeadresse** die IP-Adresse des Systems ein, auf dem der Firmwarekatalog auf dem Netzwerk gespeichert ist.
        ii. Geben Sie in das Feld **Katalogdateipfad** den vollständigen Dateipfad des Katalogdatei-Speicherorts ein. Beispielpfad: *nfsshare\catalog.xml*
      - CIFS
        i. Geben Sie in das Feld **Freigabeadresse** die IP-Adresse des Systems ein, auf dem der Firmwarekatalog auf dem Netzwerk gespeichert ist.
        ii. Geben Sie in das Feld **Katalogdateipfad** den vollständigen Dateipfad des Katalogdatei-Speicherorts ein. Beispielpfad: *Firmware\m630sa\catalog.xml*
        iii. Geben Sie in das Feld **Domäne** den Domänennamen des Geräts ein.
        iv. Geben Sie in das Feld **Nutzername** den Nutzernamen des Geräts ein, auf dem der Katalog gespeichert ist.
        v. Geben Sie in das Feld **Kennwort** das Kennwort des Geräts für Zugriff auf die Freigabe ein. Geben Sie den Nutzernamen und das Kennwort des freigegebenen Ordners ein, in dem die Datei catalog.xml gespeichert ist.
      - HTTP
        i. Geben Sie in das Feld **Freigabeadresse** die IP-Adresse des Systems ein, auf dem der Firmwarekatalog auf dem Netzwerk gespeichert ist.
        ii. Geben Sie in das Feld **Katalogdateipfad** den vollständigen Dateipfad des Katalogdatei-Speicherorts ein. Beispielpfad: *compute/catalog.xml*
      - HTTPS
        i. Geben Sie in das Feld **Freigabeadresse** die IP-Adresse des Systems ein, auf dem der Firmwarekatalog auf dem Netzwerk gespeichert ist.
        ii. Geben Sie in das Feld **Katalogdateipfad** den vollständigen Dateipfad des Katalogdatei-Speicherorts ein. Beispielpfad: *compute/catalog.xml*
        iii. Geben Sie in das Feld **Nutzername** den Nutzernamen des Geräts ein, auf dem der Katalog gespeichert ist.
        iv. Geben Sie in das Feld **Kennwort** das Kennwort des Geräts ein, auf dem der Katalog gespeichert ist.
        v. Aktivieren Sie das Kontrollkästchen **Zertifikatprüfung**.

           Die Authentizität des Geräts, auf dem die Katalogdatei gespeichert ist, wird validiert, und ein Sicherheitszertifikat wird erzeugt und im Dialogfeld **Zertifikatsinformationen** angezeigt.

    d. Nach Eingabe von **Freigabe-Adresse** und **Katalogdateipfad** wird der Link **Jetzt testen** angezeigt. Zur Validierung einer Verbindung zum Katalog klicken Sie auf **Jetzt testen**. Wenn die Verbindung zum Katalog hergestellt ist, wird die Meldung *Verbindung erfolgreich* angezeigt. Wenn die Verbindung zur Freigabe-Adresse oder zum Katalogdateipfad nicht hergestellt wird, wird die Fehlermeldung *Verbindung zum Pfad fehlgeschlagen* angezeigt. Dies ist ein optionaler Schritt.
    e. Wählen Sie im Dialogfeld **Katalog aktualisieren** entweder **Manuell** oder **Automatisch**.
    Wenn für **Katalog aktualisieren** die Option **Automatisch** ausgewählt ist, wählen Sie entweder **Täglich** oder **Wöchentlich** als Aktualisierungshäufigkeit und geben Sie die Uhrzeit im 12-Std.-Format ein.
3. Klicken Sie auf **Fertigstellen**. Die Schaltfläche **Fertigstellen** wird erst angezeigt, nachdem Sie alle Felder im Dialogfeld ausgefüllt haben.
   Ein neuer Firmwarekatalog wird erstellt und in der Katalogtabelle auf der Seite **Katalogverwaltung** aufgeführt.
4. Für die Rückkehr auf die Seite **Firmware-/Treiber-Compliance** klicken Sie auf **Zurück zu Firmware-/Treiber-Compliance**.

Zugehörige Tasks

Löschen eines Katalogs auf Seite 81

SSL-Zertifikatinformationen

Die Katalogdateien für Firmware- und Treiber-Aktualisierungen können von der Dell Support-Website, Dell EMC Repository Manager (Repository Manager), oder einer Website innerhalb Ihres Unternehmensnetzwerks heruntergeladen werden.

Wenn Sie beschließen, die Katalogdatei von der Internetseite innerhalb Ihres Unternehmensnetzwerks herunterzuladen, können Sie das SSL-Zertifikat annehmen oder ablehnen. Sie können Einzelheiten des SSL-Zertifikats im Fenster **Zertifikatsinformationen** anzeigen. Die Informationen umfassen die Gültigkeitsdauer, die ausstellende Zertifizierungsstelle sowie den Namen der Entität, für die das Zertifikat ausgegeben wird.

ANMERKUNG: Das Fenster **Zertifikatsinformationen** wird nur dann angezeigt, wenn Sie den Katalog mit dem Assistenten **Baseline erstellen** erstellen.

Maßnahmen

Akzeptieren	Akzeptiert das SSL-Zertifikat und gewährt Ihnen den Zugriff auf die Webseite.
Abbrechen	Schließt die Fenster **Zertifikatsinformationen** ohne Annahme des SSL-Zertifikats.

Katalog aktualisieren

Die vorhandenen Firmware- und Treiber Kataloge können von der Website Dell.com (Basisadresse) aktualisiert werden.

Gehen Sie zum Aktualisieren eines Katalogs wie folgt vor:

1. Wählen Sie auf der Katalogverwaltungsseite einen Katalog aus.
2. Klicken Sie auf die Schaltfläche **Nach Aktualisierung suchen** im rechten Fensterbereich der Seite **Katalogverwaltung**.
3. Klicken Sie auf **JA**.
   Der ausgewählte Katalog wird, wenn es sich um einen Online-Katalog handelt, durch die aktuellste auf der Website Dell.com gepflegte Version ersetzt. Für Kataloge im lokalen Netzwerk werden jegliche aktuelle Firmware und Treiber, die an der Basisadresse verfügbar sind, bei der Berechnung der Baseline-Compliance berücksichtigt.

Bearbeiten eines Katalogs

1. Wählen Sie auf der Seite **Katalogverwaltung** einen Katalog aus.
   Die Details des Katalogs werden im rechten Fensterbereich **<Katalogname>** angezeigt.
2. Klicken Sie im rechten Fensterbereich auf **Bearbeiten**.
3. Bearbeiten Sie im Assistenten **Updatekatalog bearbeiten** die Eigenschaften.

   Der Eigenschaften, die Sie nicht bearbeiten können, sind ausgegraut. Felddefinitionen finden Sie unter Hinzufügen eines Katalogs unter Verwendung von Dell.com auf Seite 78 und Hinzufügen eines Katalogs zum lokalen Netzwerk auf Seite 79.
4. Nach Eingabe von **Freigabe-Adresse** und **Katalogdateipfad** wird der Link **Jetzt testen** angezeigt. Zur Validierung einer Verbindung zum Katalog klicken Sie auf **Jetzt testen**. Wenn die Verbindung zum Katalog hergestellt ist, wird die Meldung `Connection`

`Successful` angezeigt. Wenn die Verbindung zur Freigabe-Adresse oder zum Katalogdateipfad nicht hergestellt wird, wird die Fehlermeldung `Connection to path failed` angezeigt. Dies ist ein optionaler Schritt.

5. Wählen Sie im Dialogfeld **Katalog aktualisieren** entweder **Manuell** oder **Automatisch**.
   Wenn für **Katalog aktualisieren** die Option **Automatisch** ausgewählt ist, wählen Sie entweder **Täglich** oder **Wöchentlich** als Aktualisierungshäufigkeit und geben Sie die Uhrzeit im 12-Std.-Format ein.
6. Klicken Sie auf **Fertigstellen**.
   Ein Job wird erstellt und sofort ausgeführt. Der Jobstatus wird in der Spalte **REPOSITORY-STANDORT** der Seite **Katalogverwaltung** angezeigt.

Löschen eines Katalogs

1. Aktivieren Sie auf der Seite **Katalogverwaltung** das Kontrollkästchen des entsprechenden Katalogs und klicken Sie dann auf **Löschen**.
   Die Kataloge werden aus der Liste gelöscht.
2. Für die Rückkehr auf die Seite **Firmware-/Treiber-Compliance** klicken Sie auf **Zurück zu Firmware-/Treiber-Compliance**.

   ANMERKUNG: Kataloge können nicht gelöscht werden, wenn sie mit einer Baseline verknüpft sind.

Zugehörige Informationen

Hinzufügen eines Katalogs zum lokalen Netzwerk auf Seite 79

Erstellen einer Firmware-/Treiber-Baseline

Eine Baseline ist eine Gruppe von Geräten oder Gerätegruppen, die einem Firmware-/Treiberkatalog zugeordnet sind. Eine Baseline wird erstellt, um die Compliance-Bewertung der Firmware und Treiber für die Geräte in dieser Baseline anhand der im Katalog angegebenen Versionen zu bewerten. So erstellen Sie eine Baseline:

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Der Geräte-Manager kann nur die Firmware-/Treiber-Baselines anzeigen und verwalten, die der entsprechende Geräte-Manager erstellt hat und besitzt. Außerdem werden bei der Erstellung von Baselines die Zielgruppen oder Geräte (fähig zum Firmwareupdate), die nur im Umfang des Geräte-Managers sind, angezeigt.
- Nach dem Upgrade auf Version 3.5 werden alle Firmware-/Treiber-Baselines, die von Geräte-Managern von einer der vorherigen OpenManage Enterprise-Versionen erstellt wurden, nur dem Administrator zugewiesen. Die Geräte-Manager müssen daher die Firmware-/Treiber-Baselines aus früheren Versionen nach dem Upgrade neu erstellen.
- Ein nicht konformes Gerät mit einer Firmware- und/oder Treiber-Version, die älter als die Katalogversion ist, wird nicht automatisch aktualisiert. Sie müssen die Firmware-Version aktualisieren. Es wird empfohlen, die Geräte-Firmware während Wartungsfenstern zu aktualisieren, um zu verhindern, dass die Geräte oder die Umgebung während der Geschäftszeiten offline gehen.

1. Klicken Sie unter **Firmware** auf **Baseline erstellen**.
2. Im Dialogfeld **Aktualisierungs-Baseline erstellen**:
   a. Im Abschnitt **Baseline-Informationen**:
      i. Wählen Sie im Drop-Down-Menü **Katalog** einen Katalog aus.
      ii. Um einen Katalog hinzuzufügen, klicken Sie auf **Hinzufügen**. Siehe Verwalten von Firmwarekatalogen.
      iii. Geben Sie im Feld **Baselinename** einen Namen für die Baseline und die Beschreibung ein.
      iv. Klicken Sie auf **Weiter**.
   b. Im Abschnitt **Ziel**:
      - So wählen Sie Zielgeräte:
        i. Wählen Sie **Geräte auswählen** und klicken Sie auf die Schaltfläche **Geräte auswählen**.
        ii. Im Dialogfeld **Geräte auswählen** werden alle von OpenManage Enterprise überwachten Geräte, EAMs und Geräte unter statischer oder Abfragegruppe in entsprechenden Gruppen angezeigt.

    iii. Klicken Sie im linken Fensterbereich auf den Kategorienamen. Geräte in dieser Kategorie werden im Arbeitsbereich angezeigt.
    iv. Aktivieren Sie das Kontrollkästchen für das jeweilige Gerät. Die ausgewählten Geräte werden unter der Registerkarte **Ausgewählte Geräte** angezeigt.
- So wählen Sie die Zielgerätgruppe(n):
    i. Wählen Sie **Gruppe auswählen**, und klicken Sie auf die Schaltfläche **Gruppe auswählen**.
    ii. Im Dialogfeld **Gruppe auswählen** werden alle von OpenManage Enterprise überwachten Geräte, EAMs und Geräte unter statischer oder Abfragegruppe in entsprechenden Kategorien angezeigt.
    iii. Klicken Sie im linken Fensterbereich auf den Kategorienamen. Geräte in dieser Kategorie werden im Arbeitsbereich angezeigt.
    iv. Aktivieren Sie das Kontrollkästchen neben der (den) entsprechenden Gruppe(n). Die ausgewählten Gruppen werden auf der Registerkarte **Ausgewählte Gruppen** angezeigt.

3. Klicken Sie auf **Fertigstellen**.
   Eine Meldung wird angezeigt, dass ein Job zum Erstellen der Baseline erstellt wird.

   Im der Baseline-Tabelle werden Daten zu Gerät und Baseline angezeigt. Feld-Definitionen finden Sie unter Feld-Definitionen Firmware-Baseline auf Seite 182.

Löschen von Konfigurations-Compliance-Baselines

Sie können die Konfigurations-Compliance-Baselines auf der Seite **Konfiguration** > **Konformitäts-Compliance** löschen und die Geräte von den zugehörigen Baselines trennen.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Siehe Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

So löschen Sie die Konfigurations-Compliance-Baselines:

1. Wählen Sie die Baseline(s) aus den Baselines, die auf der Konfigurations-Compliance-Seite aufgeführt sind.
2. Klicken Sie auf **Löschen** und klicken Sie in der Bestätigungsaufforderung auf **Ja**.

Die gelöschten Konfigurations-Baselines werden von der Konfigurations-Compliance-Seite entfernt.

Baseline bearbeiten

Die Baselines auf der Seite **Konfigurationen** > **Firmware-/Treiber-Compliance** können wie folgt bearbeitet werden:

1. Wählen Sie eine Baseline aus und klicken Sie dann im rechten Fensterbereich auf **Bearbeiten**.
2. Ändern Sie die Daten gemäß der Beschreibung in Erstellen der Firmware-Baseline.
   Die aktualisierten Informationen werden in der Grundlinienliste angezeigt.
3. Für die Rückkehr auf die Seite **Firmware-/Treiber-Compliance** klicken Sie auf **Zurück zu Firmware-/Treiber-Compliance**.

Überprüfen von Geräte-Firmware- und -Treiber-Compliance

Auf der Seite **Konfiguration** > **Firmware-/Treiber-Compliance** können Sie die Compliance der Firmware und Treiber von Baseline-Geräten mit dem zugehörigen Katalog überprüfen, den Bericht anzeigen und die Firmware und Treiber von nicht konformen Geräten aktualisieren.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Die Firmware und Treiber (64-Bit-Windows) für die nicht konformen Geräte in der Baseline werden nicht automatisch aktualisiert und müssen vom Benutzer aktualisiert werden. Es wird empfohlen, die Geräte-Firmware und -Treiber während Wartungsfenstern zu aktualisieren, um zu verhindern, dass die Geräte oder die Umgebung während der Geschäftszeiten offline gehen.

- Um die Inventarinformationen zu erfassen, müssen der Inventory Collector und die Dell System-Aktualisierung auf dem Windows Server verfügbar sein. Wenn diese Komponenten auf dem Server nicht zur Verfügung stehen, initiieren Sie einen Bestandsaufnahme-Job und wählen Sie **Treiber-Bestandsaufnahme sammeln** aus. Der Ermittlungs-Job erfasst auch Treiber-Bestandsinformationen, aber nur der Bestandsaufnahme-Job installiert die erforderlichen Komponenten auf dem Server. Zum Erfassen der Treiber-Bestandsaufnahme-Informationen erstellen oder bearbeiten Sie einen Bestandsaufnahme-Job und aktivieren Sie das Kontrollkästchen **Treiber-Bestandsaufnahme sammeln**. Weitere Informationen finden Sie unter Erstellen eines Bestandsaufnahme-Jobs auf Seite 74 und Bearbeiten eines Jobs des Bestandsaufnahmezeitplans auf Seite 76.

1. Aktivieren Sie das Kontrollkästchen der entsprechenden Baseline und klicken Sie auf **Compliance prüfen**.
   Der Baseline-Compliance-Job wird ausgeführt.

   ANMERKUNG: Wenn die Geräte nicht einem Katalog zugeordnet sind, wird die Compliance nicht überprüft. Ein Job wird nur für Geräte erstellt, die zugeordnet und in der Geräte-Compliance-Tabelle aufgeführt sind. Um ein Gerät einem Katalog zuzuordnen, siehe Erstellen der Firmware-Baseline.

   In der Baseline-Tabelle werden Daten zu Gerät und Baseline angezeigt. Feld-Definitionen finden Sie unter Feld-Definitionen Firmware-Baseline auf Seite 182.
2. Um den Compliance-Bericht und das Up- oder Downgrade der Firmware- und Treiber-Version von Geräten anzuzeigen, klicken Sie im rechten Fensterbereich auf **Bericht anzeigen**.

   Siehe Anzeigen des Compliance-Berichts der Geräte-Firmware.

   ANMERKUNG: Rollback wird für Treiber nicht unterstützt.

Anzeigen des Baseline-Compliance-Berichts

Auf der Seite **Konfiguration** > **Firmware/Treiber-Compliance** wird der Compliance-Status der Baselines angezeigt. Ein Ringdiagramm enthält eine Zusammenfassung der Compliance der Baselines mit ihren jeweiligen Katalogen. Wenn mehr als ein Gerät einer Baseline zugeordnet ist, wird der Status des Geräts mit der geringsten Compliance in Bezug auf die Baseline als die Compliance dieser Baseline angegeben. Beispiel: Die Compliance einer Baseline mit nur einem Gerät mit der Compliance „kritisch" wird als „kritisch" angezeigt, selbst wenn die meisten Geräte konform sind.

Sie können jedoch die Firmware- und Treiber-Compliance der einzelnen Geräte anzeigen, die einer Firmware-Baseline für ein Up- oder Downgrade der Firmware- oder Treiber-Version auf dem Gerät zugeordnet sind. So zeigen Sie den Baseline-Compliance-Bericht an:

- Aktivieren Sie das Kontrollkästchen der entsprechenden Baseline und klicken Sie dann im rechten Fensterbereich auf **Bericht anzeigen**.

  Auf der Seite **Compliance-Bericht** wird die Liste der Geräte angezeigt, die der Baseline und deren Compliance-Stufe zugeordnet ist. Standardmäßig werden Geräte mit dem Zustand **Kritisch** und **Warnung** angezeigt.

  ANMERKUNG: Wenn jedes Gerät über einen eigenen Status verfügt, wird der höchste Schweregrad als Status der Gruppe angenommen. Weitere Informationen über Integritätsstatus-Rollup, finden Sie im Whitepaper *VERWALTEN DES INTEGRITÄTSSTATUS-ROLLUP DURCH VERWENDUNG VON IDRAC AUF DELL EMC POWEREDGE SERVERN DER 14. GENRATION UND SPÄTER* im Dell TechCenter.
- **Compliance**: Zeigt die Compliance-Stufe eines Geräts zur Baseline an. Weitere Informationen über Symbole, die für Firmware/Treiber-Compliance-Stufen des Geräts verwendet werden, finden Sie unter Verwalten der Geräte-Firmware und -Treiber auf Seite 77.
- **TYP**: Typ des Geräts, für den der Compliance-Bericht erstellt wird.
- **GERÄTENAME/KOMPONENTEN**: Standardmäßig wird die Service-Tag-Nummer des Geräts angezeigt.
  1. Um die Sie Informationen über die Komponenten im Gerät anzuzeigen, klicken Sie auf das Symbol **>**.

     Es wird eine Liste der Komponenten und deren Compliance zum Katalog angezeigt.

     ANMERKUNG: Für alle Geräte (außer bei MX7000 Gehäusen), die vollständig in Übereinstimmung mit der Firmware-Baseline sind, wird das **>**-Symbol nicht angezeigt.
  2. Aktivieren Sie die Kontrollkästchen der entsprechenden Geräte, deren Firmware-Compliance-Status „kritisch" ist und aktualisiert werden muss.
  3. Klicken Sie auf **Übereinstimmend machen**. Siehe Update the device firmware version by using the baseline compliance report (Aktualisieren Sie die Geräte-Firmware-Version mit Hilfe des Berichts über die Einhaltung der Baseline).
- **SERVICE-TAG-NUMMER**: Klicken Sie auf diese Option, um die vollständigen Informationen über das Gerät auf der Seite **<Gerätename>** anzuzeigen. Weitere Informationen zu den Aktionen, die Sie auf der Seite abschließen können, finden Sie unter Anzeigen und Konfigurieren einzelner Geräte auf Seite 68.

- **NEUSTART ERF**: Gibt an, ob das Gerät nach der Aktualisierung der Firmware neu gestartet werden muss.
- **Information** : Das Symbol zu jeder Gerätekomponente ist mit der Seite der Support-Website verlinkt, auf der die Firmware/der Treiber aktualisiert werden kann. Klicken Sie auf diese Option, um die entsprechende Treiberdetails-Seite der Support-Website zu öffnen.
- **AKTUELLE VERSION**: Zeigt die aktuelle Firmware-Version des Geräts an.
- **BASELINE-VERSION**: Zeigt die entsprechende Firmware- und Treiberversion des Geräts an, die im zugehörigen Katalog verfügbar ist.
- Um einen Compliance-Bericht in eine Excel-Datei zu exportieren, aktivieren Sie die Kontrollkästchen des entsprechenden Geräts und wählen Sie dann **Exportieren**.
- Für die Rückkehr auf die Seite **Firmware** klicken Sie auf **Zurück zu Firmware**.
- Zur Sortierung von Daten basierend auf einer Spalte klicken Sie auf den Spaltentitel.
- Um nach einem Gerät in der Tabelle zu suchen, klicken Sie auf **Erweiterte Filter** und ändern Sie die Daten durch Auswählen oder Eingeben in die Filterfelder. Siehe „Erweiterte Filter" in Übersicht über die grafische Benutzeroberfläche von OpenManage Enterprise auf Seite 36.

So aktualisieren Sie eine Firmware und/oder Treiber mithilfe des Baseline-Compliance-Berichts:

Wenn nach dem Ausführen eines Firmware- oder Treiber-Compliance-Berichts auf dem Gerät eine frühere Firmwareversion oder Treiberversionen als die im Katalog angezeigt wird, wird auf der Seite „Compliance-Bericht" der Firmware-Status oder Treiber-Status des Geräts als „Aktualisieren" angezeigt (oder).

Die Firmware- und Treiber-Version der zugehörigen Baseline-Geräte wird nicht automatisch aktualisiert, daher muss der Nutzer die Aktualisierung initiieren. Es wird empfohlen, die Geräte-Firmware und/oder -Treiber während Wartungsfenstern zu aktualisieren, um zu verhindern, dass die Geräte oder die Umgebung während der Geschäftszeiten offline gehen.

Geräte-Manager können die Firmware/Treiber-Aktualisierung nur auf Geräten durchführen, die in ihrem Umfang enthalten sind.

ANMERKUNG: Bestandsaufnahme und Firmware-Update auf Gehäuse-Speicherschlitten werden in OpenManage Enterprise nicht unterstützt, wenn sie über die Gehäusegeräteverwaltung verwaltet werden.

Voraussetzungen:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Sie müssen eine eingehende Firewall-Regel erstellen, um die Kommunikation mit Port 22 zu ermöglichen.
- Wenn HTTP- und HTTPS-Freigaben mithilfe der Proxy-Einstellungen konfiguriert wurden, stellen Sie sicher, dass diese lokalen URLs in der Proxy-Ausnahmeliste enthalten sind, bevor Sie Aktualisierungsaufgaben starten.
- Auf dem Zielcomputer kann zu einem bestimmten Zeitpunkt nur eine Aktualisierungsaufgabe initiiert werden.

ANMERKUNG:

- Die Funktion „iDRAC zurücksetzen" wird nicht für die Geräte unter einem MCM-Gehäuse unterstützt, die sich in einem „proxied"-integrierten Zustand befinden, und nur für die Aktualisierung der Treiber der Geräte. Weitere Informationen zu Onboarding-Zuständen finden Sie unter Onboarding von Geräten auf Seite 45.
- Der Firmware-oder Treiber-Compliance-Status von Netzwerkswitches, modularen EAAs und Dell Speichergeräten wird als unbekannt angezeigt, da diese nicht über den Dell Katalog aktualisierbar sind. Es wird empfohlen, für diese Geräte einzelne Firmware- oder Treiber-Updates über das jeweilige Update-Paket durchzuführen. Um einzelne Firmware- oder Treiber-Updates durchzuführen, wählen Sie ein Gerät auf der Seite „Alle Geräte" aus und klicken Sie auf **Details anzeigen** > **Firmware/Treiber** und wählen Sie die jeweilige Paketoption aus. Weitere Informationen über die Liste der nicht unterstützten Geräte finden Sie unter Firmware/Treiber-Compliance-Baseline-Berichte: Geräte mit dem Konformitätsstatus „Unbekannt" auf Seite 186

Wenn die MCM-Gruppe (Multi-Chassis Management) über OpenManage Enterprise-Modular-Versionen unter 1.30.00 verwaltet wird, müssen Sie vor der Aktualisierung der Firmware und/oder Treiber von MX7000-Gehäuse und -Schlitten Folgendes berücksichtigen:

- Gehäuse- und Schlitten-Firmwareupdates müssen separat durchgeführt werden.
- Das Lead-Gehäuse muss im letzten Schritt nach der Aktualisierung aller Mitglieds-Gehäuse separat aktualisiert werden.
- Die Firmware kann nur für bis zu 9 Mitglieds-Gehäuse gleichzeitig aktualisiert werden.

- Das Firmwareupdate wird auf maximal 43 Schlitten gleichzeitig unterstützt, unabhängig vom Onboarding-Zustand (verwaltet oder „Proxy“).

Diese Funktion ist nur auf Geräten verfügbar, die als 64-Bit-Windows-Server ermittelt wurden. Führen Sie die folgenden Schritte aus, bevor Sie die Treiber aktualisieren:

- Beachten Sie, dass das Rollback der Treiber-Updates nicht unterstützt wird.
- In-Band-Treiber-Updates werden nur auf Windows mit OpenSSH unterstützt. Treiber-Updates auf Drittanbieter-SSH, die auf Windows gehostet werden, z. B. CygwinSSH, werden nicht unterstützt.
- Um die Inventarinformationen zu erfassen, müssen der Inventory Collector und die Dell System-Aktualisierung auf dem Windows Server verfügbar sein. Wenn diese Komponenten auf dem Server nicht zur Verfügung stehen, initiieren Sie einen Bestandsaufnahme-Job und wählen Sie **Treiber-Bestandsaufnahme sammeln** aus. Der Ermittlungs-Job erfasst auch Treiber-Bestandsinformationen, aber nur der Bestandsaufnahme-Job installiert die erforderlichen Komponenten auf dem Server. Zum Erfassen der Treiber-Bestandsaufnahme-Informationen erstellen oder bearbeiten Sie einen Bestandsaufnahme-Job und aktivieren Sie das Kontrollkästchen **Treiber-Bestandsaufnahme sammeln**. Weitere Informationen finden Sie unter Erstellen eines Bestandsaufnahme-Jobs auf Seite 74 und Bearbeiten eines Jobs des Bestandsaufnahmezeitplans auf Seite 76.

So aktualisieren Sie eine Geräte-Firmware oder einen Geräte-Treiber mithilfe des Baseline-Compliance-Berichts:

1. Aktivieren Sie auf der Seite **Konfiguration** > **Firmware-/Treiber-Compliance** das Kontrollkästchen für die entsprechende Baseline, mit der das Gerät verbunden ist, und klicken Sie dann auf **Bericht anzeigen** im rechten Fensterbereich.

   Auf der Seite **Compliance-Bericht** wird die Liste der Geräte angezeigt, die der Baseline und deren Compliance-Stufe zugeordnet ist. Informationen zu Feldbeschreibungen finden Sie unter Anzeigen des Baseline-Compliance-Berichts auf Seite 83.
2. Aktivieren Sie das Kontrollkästchen für das Gerät, dessen Firmware oder Treiber aktualisiert werden muss. Sie können mehr als ein Gerät mit ähnlichen Eigenschaften auswählen.
3. Klicken Sie auf **Übereinstimmend machen**.
4. Im Dialogfeld **Geräte übereinstimmend machen** können Sie Folgendes anzeigen:
   - Klicken Sie unter „**Aktualisierung planen**“ auf **Weitere Informationen**, um die wichtigen Informationen anzuzeigen, und wählen Sie eine der folgenden Optionen aus:
     a. **Jetzt aktualisieren**: Wendet die Firmware-/Treiber-Updates sofort an.
     b. **Später planen**: Wählen Sie diese Option, um ein Datum und die Uhrzeit für die Aktualisierung der Firmware- und/oder Treiber-Version anzugeben. Dieser Modus wird empfohlen, wenn Sie Ihre aktuellen Tasks nicht stören möchten.
   - Wählen Sie unter **Serveroptionen** eine der folgenden Neustart-Optionen aus:
     a. Um den Server unmittelbar nach der Aktualisierung der Firmware/Treiber neu zu starten, wählen Sie **Sofortiger Neustart des Servers** aus und wählen Sie im Drop-Down-Menü eine der folgenden Optionen aus:
        i. **Ordentlicher Neustart ohne erzwungenes Herunterfahren**
        ii. **Ordentlicher Neustart mit erzwungenem Herunterfahren**
        iii. **PowerCycle** für einen harten Reset des Geräts.
     b. Wählen Sie **Stufe für nächsten Serverneustart** aus, um die Firmware-/Treiber-Aktualisierung auszulösen, wenn der nächste Neustart des Servers erfolgt.

        ANMERKUNG: Wenn die Firmware-/Treiber-Aktualisierungs-Jobs mit der Option „Stufe für nächsten Serverneustart“ erstellt werden, müssen die Bestandsaufnahme und die Baseline-Prüfung manuell ausgeführt werden, nachdem das Paket auf dem Remote-Gerät installiert wurde.
   - **Jobs-Warteschlange löschen:** Wählen Sie diese Option aus, um alle Jobs (geplant, abgeschlossen und fehlgeschlagen) auf dem Zielgerät zu löschen, bevor der Update-Job gestartet wird.

     ANMERKUNG: Diese Funktion wird nicht für die Aktualisierung der Treiber unterstützt.
   - **iDRAC zurücksetzen:** Wählen Sie diese Option, um einen Neustart des iDRAC zu initiieren, bevor der Update-Job gestartet wird.

     ANMERKUNG: Diese Funktion wird nicht für die Aktualisierung der Treiber unterstützt.
5. Klicken Sie auf **Aktualisieren**.

Es wird ein Firmware-/Treiber-Aktualisierungs-Job erstellt, um die Firmware und/oder den Treiber des Geräts zu aktualisieren. Sie können den Status des Jobs auf der Seite **Überwachen** > **Jobs** anzeigen.

11

Verwalten von Gerätebereitstellungsvorlagen

Die Gerätebereitstellungsvorlage in OpenManage Enterprise ermöglicht es Ihnen, die Konfigurationseigenschaften, wie z. B. BIOS, Systemstart, Netzwerkeigenschaften usw. von Servern und Gehäusen einzustellen.

Die Bereitstellungsvorlage ist eine Zusammenfassung der Systemkonfigurationseinstellungen, die als Attribute bezeichnet werden. Die Bereitstellungsvorlage ermöglicht es, dass mehrere Server oder Gehäuse schnell und automatisch ohne das Risiko menschlicher Fehler konfiguriert werden.

Vorlagen ermöglichen Ihnen die Optimierung von Rechenzentrumsressourcen und reduzieren die Zykluszeit beim Erstellen von Klonen und bei Bereitstellungen. Außerdem optimieren Vorlagen Ihre geschäftskritischen Vorgänge in einer konvergenten Infrastruktur, die softwarebasierte Infrastrukturen verwendet.

Sie können entweder die vordefinierten Bereitstellungsvorlagen verwenden oder die Bereitstellungsvorlagen aus einem Referenzgerät oder einer vorhandenen Vorlagendatei importieren. Klicken Sie zum Anzeigen der Liste der vorhandenen Vorlagen im OpenManage Enterprise-Menü auf **Konfiguration** > **Vorlagen**.

Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Ein Geräte-Manager kann Aufgaben für die Standardvorlagen und nur die benutzerdefinierten Vorlagen anzeigen und ausführen, die im Besitz dieses Geräte-Managers sind.

Themen:

So erstellen Sie eine Bereitstellungsvorlage aus einem Referenz-Gerät

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

ANMERKUNG: Sie müssen KMUv1 in den **KMU Einstellungen** aktivieren, bevor Sie mit Aufgaben beginnen, die Kommunikation mit einem beliebigen Gehäuse oder PowerEdge YX2X- und YX3X-Servern mit iDRAC-Version 2.50.50.50 und früheren Versionen erfordern. Siehe Verwalten der Konsolen-Voreinstellungen auf Seite 165 und Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.

Sie können eine Bereitstellungsvorlage mit einem Verweisgerät oder durch Importieren aus einer vorhandenen Bereitstellungsvorlage erstellen oder bearbeiten. Erstellen mithilfe eines Referenzgeräts:

1. Klicken Sie im Menü **OpenManage Enterprise** auf **Konfigurationen** > **Vorlagen** > **Vorlage erstellen** und wählen Sie dann **Von Referenzgerät**.
2. Führen Sie im Dialogfeld **Vorlage erstellen** folgende Schritte aus:
   a. Geben Sie im Abschnitt **Vorlageninformationen** einen Namen für die Bereitstellungsvorlage sowie eine Beschreibung für die Vorlage ein.
   b. Wählen Sie den Bereitstellungsvorlagentyp aus:
      - **Referenzserver klonen**: Ermöglicht das Cloning der Konfiguration eines vorhandenen Servers.
      - **Referenzgehäuse klonen**: Ermöglicht das Cloning der Konfiguration eines vorhandenen Gehäuses.
      - **Referenz-EAA klonen**: Ermöglicht das Cloning der Konfiguration eines vorhandenen M E/A-Aggregators.

        ANMERKUNG: Attribute in der EAA-Vorlage sind nicht veränderbar. Nur **Name** und **Beschreibung** einer EAA-Vorlage können bearbeitet werden.
   c. Klicken Sie auf **Weiter**.
   d. Klicken Sie im Abschnitt **Referenzgerät** auf **Gerät auswählen**, um das Gerät auszuwählen, dessen Konfigurationseigenschaften für das Erstellen der neuen Bereitstellungsvorlage verwendet werden müssen. Weitere Informationen zum Auswählen von Geräten finden Sie unter Auswählen von Zielgeräten und Gerätegruppen.

      ANMERKUNG: Sie können nur ein Gerät als Referenzgerät auswählen.

      ANMERKUNG: Nur EAA-Vorlagen, die zum Zeitpunkt der Gehäuseermittlung extrahiert wurden, stehen zum Cloning zur Verfügung. Siehe . Erstellen eines benutzerdefinierten Geräteerkennungs-Job-Protokolls für Server – Zusätzliche Einstellungen für Ermittlungsprotokolle auf Seite 50
   e. Aktivieren Sie im Abschnitt **Konfigurationselemente** die Kontrollkästchen neben den Geräteelementen, die geklont werden müssen. Bei der Erstellung einer Bereitstellungsvorlage mithilfe eines Servers als Gerät können Sie auswählen, die Servereigenschaften zu klonen, z. B. iDRAC, BIOS, Lifecycle Controller und Ereignisfilter. Standardmäßig werden alle Elemente ausgewählt.
   f. Klicken Sie auf **Fertigstellen**.
      Nach der erfolgreichen Erstellung wird der Job in der Liste angezeigt. Ein Erstellungsjob für eine Bereitstellungsvorlage wird gestartet und der Status wird in der Spalte **Status** angezeigt.

      Die Job-Informationen werden ebenfalls auf der Seite **Überwachen** > **Jobs** angezeigt. Um weitere Informationen zu einem Job anzuzeigen, wählen Sie einen Job aus und klicken Sie im Arbeitsbereich auf **Details anzeigen**. Auf der Seite **Job-Details** werden die Ausführungsdetails des Jobs angezeigt. Klicken Sie im Fensterbereich **Ergebnisse** auf **Details anzeigen**, um detaillierte Informationen von der Aufgabendurchführung anzusehen.

Bereitstellungsvorlage durch Importieren einer Vorlagendatei erstellen

ANMERKUNG: Sie müssen KMUv1 in den **KMU Einstellungen** aktivieren, bevor Sie mit Aufgaben beginnen, die Kommunikation mit einem beliebigen Gehäuse oder PowerEdge YX2X- und YX3X-Servern mit iDRAC-Version 2.50.50.50 und früheren Versionen erfordern. Weitere Informationen erhalten Sie unter Verwalten der Konsolen-Voreinstellungen auf Seite 165 und Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.

1. Klicken Sie im Menü **OpenManage Enterprise** auf **Konfiguration** > **Vorlagen** > **Vorlage erstellen**, und wählen Sie dann **Von Datei importieren**.
2. Führen Sie im Dialogfeld **Vorlage importieren** folgende Schritte aus:
   a. Geben Sie einen Namen für die neue Bereitstellungsvorlage ein.
   b. Klicken Sie auf **Eine Datei auswählen** und wählen Sie dann eine Vorlagendatei aus.
   c. Wählen Sie **Server**, **Gehäuse** oder **IOA**, um den Vorlagentyp anzugeben.
3. Klicken Sie auf **Fertigstellen**.
   Die Eigenschaften einer vorhandenen Vorlagendatei werden importiert und eine neue Bereitstellungsvorlage wird erstellt.

- Um weitere Informationen zu einer Bereitstellungsvorlage anzuzeigen, aktivieren Sie das Kontrollkästchen und klicken Sie dann im rechten Fensterbereich auf **Details anzeigen**. Auf der Seite **Vorlagendetails** können Sie eine Bereitstellungsvorlage bereitstellen oder bearbeiten. Siehe Bereitstellen von Gerätebereitstellungsvorlagen auf Seite 91 und So erstellen Sie eine Bereitstellungsvorlage aus einem Referenz-Gerät auf Seite 86.

- So bearbeiten Sie eine Bereitstellungsvorlage:
  1. Aktivieren Sie das entsprechende Kontrollkästchen und klicken Sie dann auf **Bearbeiten**.
  2. Bearbeiten Sie im Dialogfeld **Vorlage bearbeiten** den Namen der Bereitstellungsvorlage und klicken Sie dann auf **Fertig stellen**. Aktualisierte Informationen werden in der Liste der Bereitstellungsvorlagen angezeigt.

Bereitstellungsvorlageninformationen anzeigen

Eine Liste der vordefinierten, vom Nutzer erstellten oder geklonten Gerätebereitstellungsvorlage wird angezeigt unter **Konfiguration** > **Vorlagen**.

1. Aktivieren Sie in der Liste der Bereitstellungsvorlagen das Kontrollkästchen des entsprechenden Geräts.
2. Klicken Sie im Arbeitsbereich auf **Details anzeigen**.
   Auf der Seite **Vorlagendetails** werden Bereitstellungsvorlagenname und -beschreibung, das Referenzgerät, von dem die Bereitstellungsvorlage erstellt wurde, sowie das Datum der letzten Aktualisierung der OpenManage Enterprise Benutzerinformationen angezeigt.
3. Klicken Sie im Bereich **Konfigurationsdetails** mit der rechten Maustaste auf ein Element, um alle untergeordneten Elemente zu erweitern bzw. verkleinern und alle Attribute anzuzeigen, die für die Erstellung der Bereitstellungsvorlage benötigt werden. Sie können auch einzelne untergeordneten Elemente erweitern, die zu einem übergeordneten Element gehören. Wenn Sie zum Beispiel auswählen, dass iDRAC- und BIOS-Elemente für das Cloning auf dem Zielgerät verwendet werden müssen, werden nur die Attribute im Zusammenhang mit diesen Elementen angezeigt.

Bearbeiten einer Serverbereitstellungsvorlage

Integrierte Bereitstellungsvorlagen können nicht bearbeitet werden. Nur nutzerdefinierte Bereitstellungsvorlagen, die als „Nutzerdefiniert" gekennzeichnet sind, können bearbeitet werden. Sie können die Attribute der Bereitstellungsvorlage bearbeiten, unabhängig davon, ob Sie sie über eine Referenzvorlagendatei oder ein Referenzgerät angelegt haben. Wenn Sie eine Vorlage bearbeiten, werden durch Auswahl bzw. Deaktivierung von Attributen die in der Vorlage gespeicherten Attribute nicht geändert und alle Attribute sind weiterhin Teil der Vorlage, wenn diese exportiert wird. Dies wirkt sich auf die bereitgestellten Daten aus.

1. Markieren Sie auf der Seite **Konfiguration** > **Vorlagen** das entsprechende Kontrollkästchen, und klicken Sie dann auf **Bearbeiten**.
2. Führen Sie im Dialogfeld **Vorlage bearbeiten** folgende Schritte aus:
   a. Bearbeiten Sie im Abschnitt **Vorlageninformationen** den Namen und die Beschreibung der Bereitstellungsvorlage. Ein Vorlagentyp kann nicht bearbeitet werden.
   b. Klicken Sie auf **Weiter**.
   c. Auf der Seite **Komponenten bearbeiten** werden die folgenden Attribute der Bereitstellungsvorlage angezeigt:
      - Die **Geführte Ansicht**: Diese Ansicht von Attributen zeigt nur häufige Attribute an, gruppiert nach Funktion. Es werden Attribute aus den folgenden Kategorien angezeigt:
        i. Wählen Sie im Abschnitt **BIOS-Einstellungen** eine der folgenden Optionen aus:
           - **Manuell**: Ermöglicht es Ihnen, die folgenden BIOS-Eigenschaften manuell zu definieren:
             - **Systemprofil**: Wählen Sie im Dropdownmenü die Art der Leistungsoptimierung, die im Systemprofil erreicht werden soll.
             - **Nutzerzugängliche USB-Ports**: Wählen Sie im Dropdownmenü die Ports aus, auf die der Nutzer zugreifen kann.
             - Standardmäßig sind die Verwendung des logischen Prozessors und die In-Band-Verwaltung aktiviert.
           - **Optimieren auf Basis der Auslastung**: Wählen Sie im Dropdownmenü „Arbeitsauslastungsprofil auswählen" die Art der Arbeitsauslastungs-Leistungsoptimierung aus, die Sie für das Profil erreichen möchten.
        ii. Klicken Sie auf **Start** und definieren Sie den Startmodus:
           - Wenn Sie die Option „BIOS" als den Startmodus festgelegt haben, gehen Sie wie folgt vor:
             - Um die lokale Startreihenfolge erneut zu versuchen, wählen Sie das Kontrollkästchen **Aktiviert** aus.
             - Ziehen Sie die Elemente, um die Startreihenfolge und Reihenfolge der Festplatten festzulegen.
           - Wenn Sie „UEFI" als den Startmodus festgelegt haben, ziehen Sie die Elemente, um die UEFI-Startreihenfolge festzulegen. Aktivieren Sie bei Bedarf das Kontrollkästchen, um die Schlüsselsequenz zu aktivieren.
        iii. Klicken Sie auf **Netzwerk**. Alle Netzwerke, die mit der Bereitstellungsvorlage verknüpft sind, werden unter **Netzwerkschnittstellen** angezeigt.
           - Um einen optionalen Identitäts-Pool mit der Bereitstellungsvorlage zu verknüpfen, wählen Sie eine Option aus dem Drop-down-Menü **Identitäts-Pool**. Die mit dem ausgewählten Identitäts-Pool verknüpften Netzwerke werden

angezeigt. Wenn die Bereitstellungsvorlage in der Ansicht „Erweitert“ bearbeitet wird, ist die Auswahl des Identitäts-Pools für diese Bereitstellungsvorlage deaktiviert.

- Zum Anzeigen der Netzwerkeigenschaften erweitern Sie das Netzwerk.
- Um die Eigenschaften zu bearbeiten, klicken Sie auf das entsprechende Stiftsymbol.
  - Wählen Sie das Protokoll aus, das für den Startvorgang verwendet werden soll. Wählen Sie diese Option nur aus, wenn das Protokoll von Ihrem Netzwerk unterstützt wird.
  - Wählen Sie das nicht markierte und markierte Netzwerk aus, das mit dem Netzwerk verknüpft werden soll.
  - Die Partition sowie die maximale und minimale Bandbreite werden aus der zuvor erstellten Bereitstellungsvorlage (Profil) angezeigt.
- Klicken Sie auf **Fertigstellen**. Die Netzwerkeinstellungen der Bereitstellungsvorlage werden gespeichert.

- Die **Erweiterte Ansicht**: Diese Ansicht listet alle Bereitstellungsvorlagenattribute auf, die geändert werden können (einschließlich derjenigen, die in der Geführten Ansicht angezeigt werden). In dieser Ansicht können Sie nicht nur Attributwerte angeben (wie in der Geführten Ansicht), sondern auch, ob ein Attribut bei der Bereitstellung der Bereitstellungsvorlage auf einem Zielgerät eingebunden wird.

  Attribute werden zur Anzeige nach Funktion gruppiert. Herstellerspezifische Attribute sind unter „Andere Attribute“ zusammengefasst. Für jedes einzelne Attribut wird vor dem Namen ein Kontrollkästchen angezeigt. Das Kontrollkästchen gibt an, ob das Attribut eingebunden wird, wenn die Bereitstellungsvorlage auf einem Zielgerät bereitgestellt wird. Wenn Sie die Einstellung ändern, ob ein bestimmtes Attribut bereitgestellt wird oder nicht, kann es aufgrund von Attributabhängigkeiten zu unerwarteten Ergebnissen auf dem Zielgerät kommen oder die Bereitstellung kann fehlschlagen. Für jede Gruppe wird links neben dem Namen ein Kontrollkästchen angezeigt. Jedes Symbol in den Gruppen-Kontrollkästchen weist einen der folgenden drei Werte auf:

  i. Aktiviert: zeigt an, dass alle Attribute in der Gruppe für die Bereitstellung ausgewählt wurden.
  ii. Bindestrich: zeigt an, dass einige (aber nicht alle) Attribute für die Bereitstellung ausgewählt wurden.
  iii. Leer: zeigt an, dass keines der Attribute in der Gruppe für die Bereitstellung ausgewählt wurde.

  ANMERKUNG:

  - Die Verwendung dieser Option erfordert Sorgfalt und gute Kenntnisse über Attribute und Attributabhängigkeiten, um ihr Verhalten zu bestimmen, denn verschiedene Attribute hängen von dem Wert in einem anderen Attribut ab.
  - Sie können auf die Gruppensymbole klicken, um die Bereitstellungseinstellung für alle Attribute in der Gruppe umzuschalten.
  - Die Attribute mit sicheren Informationen, wie z. B. Passwörter, werden ausgeblendet und beim ersten Laden als „leer“ angezeigt und die Änderungen an diesen sicheren Attributwerten sind maskiert.
  - Der zugeordnete Identitäts-Pool einer Bereitstellungsvorlage kann nicht geändert werden, wenn ihr bereits ein Profil zugeordnet ist.

3. Klicken Sie auf **Weiter**.
   Im Abschnitt **Zusammenfassung** werden die Attribute angezeigt, die Sie unter Verwendung des geführten und erweiterten Modus bearbeitet haben.
4. Dieser Abschnitt ist schreibgeschützt. Überprüfen Sie die Einstellungen und klicken Sie auf **Fertig stellen**.
   Die aktualisierten Vorlagenattribute werden in der Bereitstellungsvorlage gespeichert.

Bearbeiten einer Gehäusebereitstellungsvorlagen

Das Bearbeiten von Gehäusebereitstellungsvorlagen ist mit OpenManage Enterprise möglich. Wenn Sie eine Vorlage bearbeiten, werden durch Auswahl bzw. Deaktivierung von Attributen die in der Vorlage gespeicherten Attribute nicht geändert und alle Attribute sind weiterhin Teil der Vorlage, wenn diese exportiert wird. Dies wirkt sich auf die bereitgestellten Daten aus.

ANMERKUNG:

- Zum Bearbeiten von Gehäusebereitstellungsvorlagen müssen Sie über die Berechtigungen eines Administrators oder eines Geräte-Managers verfügen. Weitere Informationen finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Nutzerkennwörter können nicht für das MX7000-Gehäuse und die CMC-(Chassis Management Controller-)Bereitstellungsvorlagen festgelegt werden.

So bearbeiten Sie eine Gerätebereitstellungsvorlage:

1. Wählen Sie **OpenManage Enterprise** > **Konfiguration** > **Vorlagen**, um eine Liste der Bereitstellungsvorlagen zu erhalten.
2. Aktivieren Sie das Kontrollkästchen der erforderlichen Gehäusevorlage und klicken Sie auf **Bearbeiten**. Stellen Sie sicher, dass die Bereitstellungsvorlage als "Nutzerdefiniert" gekennzeichnet ist.

3. Bearbeiten Sie **Vorlagenname** und **Beschreibung** im Abschnitt **Vorlageninformationen**. Den **Vorlagentyp** können Sie nicht bearbeiten.
4. Klicken Sie auf **Weiter**.
5. Im Abschnitt **Komponenten bearbeiten** unter **Erweiterte Ansicht** können Sie Attribute zum Einbeziehen oder Ausschließen für die Bereitstellungsvorlage auswählen oder abwählen.
6. Klicken Sie auf **Weiter**.
7. Sie können die Änderungen an den Attributen unter **Zusammenfassung** überprüfen. Ein Kreis erscheint neben den geänderten Attributen.
8. Klicken Sie auf **Fertigstellen**, um die Änderungen an der Gehäusebereitstellungsvorlage zu speichern.

Bearbeiten einer EAA-Bereitstellungsvorlage

Attribute in der EAA-Bereitstellungsvorlage sind nicht veränderbar. Nur **Name** und **Beschreibung** einer EAA-Bereitstellungsvorlage können bearbeitet werden.

ANMERKUNG:

IOA-Vorlagenattribute dürfen nicht außerhalb der Appliance bearbeitet werden, da die Vorlage bei der Bereitstellung als korrupte Datei angesehen wird.

Bearbeiten der Netzwerkeigenschaften einer Bereitstellungsvorlage

Auf der Seite **Konfigurationen** > **Vorlagen** können Sie die Netzwerkkonfiguration für die Bereitstellungsvorlagen bearbeiten, die die entsprechenden NIC-Attribute enthält.

Nachdem Sie eine Bereitstellungsvorlage ausgewählt haben, klicken Sie auf **Netzwerk bearbeiten**, um den Assistenten Netzwerk bearbeiten zu aktivieren, und gehen Sie folgendermaßen vor:

ANMERKUNG: VLAN-Einstellungen auf „Proxy"-MX7000-Schlitten innerhalb des Geltungsbereichs sind für einen Gerätemanager zulässig, auch wenn das MX7000-Chassis außerhalb des Geltungsbereichs liegt.

1. Klicken Sie auf **IO-Poolzuweisung** und wählen Sie in der Liste **Identitäts-Pool** einen Identitäts-Pool für die Bereitstellungsvorlage aus. Klicken Sie auf **Weiter**.
2. Bearbeiten Sie im Abschnitt **Bandbreite** die **Minimale Bandbreite (%)** und die **Maximale Bandbreite (%)** der zugehörigen NICs und klicken Sie auf **Weiter**.

   ANMERKUNG: Bandbreiteneinstellungen gelten nur für partitionierte NICs.

3. Im Abschnitt **VLANs** (gilt nur für modulare Systeme):
   a. Wählen Sie eine geeignete **NIC Teaming**-Option aus.
   b. Aktivieren Sie das Kontrollkästchen **VLAN-Einstellungen sofort übertragen**, um die geänderten VLAN-Einstellungen auf den zugeordneten modularen Systemservern sofort zu übertragen, ohne dass ein Neustart des Servers erforderlich ist. Klicken Sie auf **Details anzeigen**, um die betroffenen Geräte anzuzeigen.

      ANMERKUNG:

      - **VLAN-Einstellungen sofort übertragen** wird nur dann durchgeführt, wenn die Bereitstellungsvorlage bereits bereitgestellt wurde.
      - Bevor Sie die VLAN-Einstellungen verteilen, stellen Sie sicher, dass die Netzwerkprofile für die modularen Systemserver in der Fabric bereits erstellt wurden.
      - Wenn das Kontrollkästchen **VLAN-Einstellungen sofort übertragen** aktiviert ist, wird ein Job mit dem Namen **VLAN Propagation** erstellt, um die Änderungen zu übernehmen. Der Status des Jobs kann auf der Seite **Überwachen** > **Jobs** geprüft werden.

   c. Aktivieren Sie das Kontrollkästchen **Strenge Prüfung verwenden**, um die VLANs mit ähnlichen Merkmalen abzugleichen. Wenn diese Option nicht ausgewählt ist, werden nur VLAN-Name und QoS für die Zuordnung verwendet.

      ANMERKUNG: Diese Option gilt nur für modulare Systemschlitten.

    d. Nehmen Sie nach Bedarf Änderungen an den Attributen **Nicht markiertes Netzwerk** und **Markiertes Netzwerk** der zugehörigen NICs vor.
4. Klicken Sie auf **Fertig stellen**, um die Änderungen zu übernehmen.

Bereitstellen von Gerätebereitstellungsvorlagen

Sie können eine Bereitstellungsvorlage bereitstellen, die eine Reihe von Konfigurationsattributen für bestimmte Geräte enthält. Durch die Bereitstellung einer Gerätebereitstellungsvorlage auf den Geräten wird sichergestellt, dass die Geräte einheitlich konfiguriert werden.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Wenn ein Geräte-Manager Vorlagen bereitstellt, werden nur die Zielgruppe(n) und die Geräte, die sich im Bereich des Geräte-Managers befinden und für die Bereitstellung geeignet sind, angezeigt.

Bevor Sie eine Gerätebereitstellungsvorlage bereitstellen, stellen Sie Folgendes sicher:

- Sie haben entweder eine Gerätebereitstellungsvorlage erstellt oder eine Musterbereitstellungsvorlage geklont. Informationen dazu finden Sie unter So erstellen Sie eine Bereitstellungsvorlage aus einem Referenz-Gerät auf Seite 86.
- Die Zielgeräte erfüllen die unter Mindestsystemanforderungen für die Bereitstellung von OpenManage Enterprise auf Seite 21 angegebenen Anforderungen.
- Die OpenManage Enterprise Advanced Lizenz ist auf allen Zielgeräten installiert.

VORSICHT: Stellen Sie sicher, dass nur geeignete Geräte für die Bereitstellung ausgewählt sind. Nach der Bereitstellung einer Bereitstellungsvorlage auf einem Neuzuweisungs- und Bare-Metal-Gerät ist es unter Umständen nicht möglich, das Gerät auf die ursprüngliche Konfiguration zurückzusetzen.

ANMERKUNG: Während der Bereitstellung einer MX7000-Gehäusevorlage:

- Das Zielgerät kann nur das MX7000-Hauptgehäuse sein.
- Wenn ein MX7000-Gehäuse aus der Gruppe entfernt wird, muss es in OpenManage Enterprise neu ermittelt werden.
- Die Nutzer auf dem MX7000-Gehäuse werden durch die in der Vorlage konfigurierten Nutzer ersetzt.
- Importierte Active Directory-Einstellungen werden durch die Werte im Gehäuseprofil ersetzt.

1. Markieren Sie in der Liste der Bereitstellungsvorlagen auf der Seite **Konfiguration** > **Vorlagen** das entsprechende Kontrollkästchen der Bereitstellungsvorlage, das Sie bereitstellen möchten, und klicken Sie dann auf **Vorlage bereitstellen**.
2. Im Dialogfeld **Vorlage bereitstellen: <Vorlagenname>** unter **Ziel**:
    a. Klicken Sie auf **Auswählen**, und wählen Sie dann ein Gerät/Geräte im Dialogfeld **Job-Ziel** aus. Siehe Auswählen von Zielgeräten und Zielgerätegruppen.
    b. Während der Bereitstellung der Gerätebereitstellungsvorlage wird aufgrund der Änderungen der Konfiguration möglicherweise ein Neustart des Servers erzwungen. Wenn Sie nicht möchten, dass der Server neu gestartet wird, wählen Sie die Option **Kein Neustart des Host-BS erzwingen**.
    Ein ordentlicher Neustart des Servers wird versucht, wenn die Option **Kein Neustart des Host-BS erzwingen** ausgewählt ist. Wenn der Neustart fehlschlägt, müssen Sie die Vorlagenbereitstellung erneut durchführen.
    c. Aktivieren Sie das Kontrollkästchen **Strenge Prüfung verwenden**, um die VLANs mit ähnlichen Merkmalen abzugleichen. Wenn diese Option nicht ausgewählt ist, werden nur VLAN-Name und QoS für die Zuordnung verwendet.

    ANMERKUNG: Diese Option wird nur dann angezeigt, wenn die ausgewählten Zielgeräte modulare Systemschlitten sind.

    d. Klicken Sie auf **Weiter**.
3. Wenn es sich bei dem Zielgerät um einen Server handelt im Abschnitt **Start auf Netzwerk-ISO**:
    a. Markieren Sie das Kontrollkästchen **Start auf Netzwerk-ISO**.
    b. Wählen Sie entweder **CIFS** oder **NFS** als Freigabetyp aus und geben Sie dann in die Felder wie „ISO-Image-Dateipfad“ und „Freigabespeicherort“ Informationen zum Speicherort der ISO-Image-Datei ein. Verwenden Sie die Tooltips, damit Sie die richtige Syntax eingeben.
    c. Wählen Sie die **Zeit zum Anhängen der ISO**-Drop-Down-Menü-Optionen, um die Anzahl der Stunden festzulegen, die die Netzwerk-ISO-Datei den Zielgeräten zugewiesen bleibt. Standardmäßig wird dieser Wert auf vier Stunden festgelegt.
    d. Klicken Sie auf **Weiter**.
4. Im Abschnitt **iDRAC-Verwaltungs-IP** ändern Sie ggf. die IP-Einstellungen des Zielgeräts und klicken Sie auf **Weiter**.

ANMERKUNG:

- Die Bereitstellung der Vorlage schlägt fehl, wenn DHCP-Einstellungen während der Vorlagenbereitstellung auf einem Zielgerät zugewiesen werden, das ursprünglich mit einer statischen IP-Adresse ermittelt wurde.
- Wenn die IP-Einstellung nicht auf dem ermittelten MX7000-Schlitten konfiguriert ist, wir der Vorgang „Start auf Netzwerk-ISO“ nicht während der Vorlagenbereitstellung ausgeführt.

5. Im Abschnitt **Zielattribute** können die nicht virtuellen Identitätsattribute, die für jedes der ausgewählten Zielgeräte spezifisch sind, wie z.B. die Standort-Attribute und die IP-Adresse, vor der Bereitstellung der Bereitstellungsvorlage geändert werden. Wenn die Vorlage bereitgestellt wird, werden diese geänderten Zielattribute nur auf den spezifischen Geräten implementiert. So ändern Sie die gerätespezifischen, nicht virtuellen Identitätsattribute:
   a. Wählen Sie ein Zielgerät aus der Liste aus, in der die zuvor ausgewählten Zielgeräte angezeigt werden.
   b. Erweitern Sie die Attributkategorien und aktivieren oder deaktivieren Sie dann die Attribute, die während der Vorlagenbereitstellung auf dem Zielgerät eingeschlossen oder ausgeschlossen werden müssen.
   c. Klicken Sie auf **Weiter**.
6. Im Abschnitt **Virtuelle Identitäten** klicken Sie auf **Identitäten reservieren**.
   Die zugewiesenen virtuellen Identitäten der NIC-Karten des ausgewählten Zielgeräts werden angezeigt. Um alle zugewiesenen Identitäten des Identitätspools des ausgewählten Zielgeräts anzuzeigen, klicken Sie auf **Alle NIC-Details anzeigen**.

   ANMERKUNG: Wenn bereits Identitäten außerhalb der Appliance zugewiesen sind, nutzt eine neue Bereitstellung diese Identitäten nur dann, wenn Sie gelöscht werden. Weitere Informationen finden Sie unter Identitäts-Pools auf Seite 96
7. Führen Sie im Abschnitt **Zeitplan** den Job sofort aus oder planen Sie ihn für einen späteren Zeitpunkt. Informationen dazu finden Sie unter Felddefinitionen für die Jobplanung auf Seite 182.
8. Klicken Sie auf **Fertigstellen**. Überprüfen Sie die Warnmeldung und klicken Sie auf **JA**.
   Es wird ein Device-Konfigurationsjob erstellt. Informationen dazu finden Sie unter Verwenden von Jobs zur Gerätesteuerung auf Seite 130.

Bereitstellen von EAA-Bereitstellungsvorlagen

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Bevor Sie eine EAA-Bereitstellungsvorlage bereitstellen, stellen Sie Folgendes sicher:

- Sie haben eine IOA-Bereitstellungsvorlage für die Bereitstellung erstellt. Informationen dazu finden Sie unter So erstellen Sie eine Bereitstellungsvorlage aus einem Referenz-Gerät auf Seite 86.
- Die Zielgeräte erfüllen die unter Mindestsystemanforderungen für die Bereitstellung von OpenManage Enterprise auf Seite 21 angegebenen Anforderungen.
- Die Firmware-Version des Zielgerätes entspricht der Version der IOA-Bereitstellungsvorlage.
- Nur die folgenden vorlagenübergreifenden Bereitstellungen werden unterstützt:

Tabelle 14. Unterstützte vorlagenübergreifende Bereitstellungen

EAA-Bereitstellungsvorlagen-Modus	Unterstützte EAA-Vorlagenmodi des Ziels
Standalone	Standalone, PMUX
PMUX (Programmable MUX)	PMUX, Standalone
VLT	VLT

VORSICHT: Stellen Sie sicher, dass nur geeignete Geräte für die Bereitstellung ausgewählt sind. Nach der Bereitstellung einer Bereitstellungsvorlage auf einem Neuzuweisungs- und Bare-Metal-Gerät ist es unter Umständen nicht möglich, das Gerät auf die ursprüngliche Konfiguration zurückzusetzen.

1. Markieren Sie in der Liste der Bereitstellungsvorlagen auf der Seite **Konfiguration** > **Vorlagen** das entsprechende Kontrollkästchen der EAA-Vorlage, die Sie bereitstellen möchten, und klicken Sie auf **Vorlage bereitstellen**.
2. Im Dialogfeld **Vorlage bereitstellen: <Vorlagenname>** unter **Ziel**:
   a. Klicken Sie auf **Auswählen**, und wählen Sie dann ein Gerät/Geräte im Dialogfeld **Job-Ziel** aus. Siehe Auswählen von Zielgeräten und Zielgerätegruppen.
   b. Klicken Sie auf **OK**.
3. Im Dialogfeld **Hostnamen** können Sie den **Hostnamen** des EAA-Zielgeräts ändern. Klicken Sie auf **Weiter**.

4. Im Dialogfeld **Erweiterte Optionen** wählen Sie **Vorschaumodus** zum Simulieren der Bereitstellung oder **Bei Warnung fortfahren** zum Bereitstellen der Vorlage und ignorieren von auftretenden Warnungen. Klicken Sie auf **Weiter**.
5. Führen Sie im Abschnitt **Zeitplan** den Job sofort aus oder planen Sie ihn für einen späteren Zeitpunkt. Informationen dazu finden Sie unter Felddefinitionen für die Jobplanung auf Seite 182.
6. Klicken Sie auf **Fertigstellen**. Überprüfen Sie die Warnmeldung und klicken Sie auf **JA**.
   Es wird ein Device-Konfigurationsjob unter Jobs erstellt. Informationen dazu finden Sie unter Verwenden von Jobs zur Gerätesteuerung auf Seite 130.

Klonen von Bereitstellungsvorlagen

1. Klicken Sie im Menü **OpenManage Enterprise** unter **Konfiguration** auf **Vorlagen**.
   Eine Liste der verfügbaren Bereitstellungsvorlagen wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen der Vorlage, die Sie klonen möchten.
3. Klicken Sie auf **Cloning**.
4. Geben Sie den Namen der neuen Bereitstellungsvorlage ein und klicken Sie dann auf **Fertig stellen**.
   Die geklonte Bereitstellungsvorlage wird erstellt und in der Liste der Bereitstellungsvorlagen angezeigt.

Automatische Bereitstellung der Konfiguration auf noch zu ermittelndem Server oder Gehäuse

Bestehende Bereitstellungsvorlagen in OpenManage Enterprise können den Servern und Gehäusen zugewiesen werden, deren Ermittlung noch aussteht. Diese Bereitstellungsvorlagen werden automatisch auf den jeweiligen Geräten bereitgestellt, wenn sie ermittelt und integriert werden.

Sie gelangen zur Seite **Automatische Bereitstellung** durch Klicken auf **OpenManage Enterprise** > **Konfiguration** > **Automatische Bereitstellung**.

Die Ziele für die automatische Bereitstellung und ihre jeweiligen **Kennungen** (Service-Tag-Nummer oder Knoten-IDs), **Vorlagenname**, **Vorlagentyp**, **Status** und **Status für Starten in Netzwerk-ISO** (für Server) werden angezeigt.

Die Zielliste für die **automatische Bereitstellung** kann mithilfe der Felder **Erweiterte Filter** am oberen Rand der Liste angepasst werden.

Auf der rechten Seite der Seite "Automatische Bereitstellung" werden im Abschnitt **Erstellt am** und **Erstellt von** die Details des ausgewählten automatischen Bereitstellungsziels angezeigt. Wenn mehrere Elemente ausgewählt werden, werden im Abschnitt Details zum zuletzt ausgewählten Element angezeigt.

Nachdem ein Ziel für die automatische Bereitstellung erkannt wurde, wird der Eintrag auf der Seite „Automatische Bereitstellung“ automatisch gelöscht und auf die Seite „Alle Geräte“ verschoben. Außerdem wird auf der Seite „Profile“ ein Profil erstellt, das die Konfigurationseinstellungen für das Gerät enthält.

Die folgenden Aktionen können auf der Seite "Automatische Bereitstellung" ausgeführt werden:

- **Erstellen** von Vorlagen für die automatische Bereitstellung. Siehe . Automatische Bereitstellungsziele erstellen auf Seite 93
- **Löschen** nicht benötigter Vorlagen. Siehe .Automatische Bereitstellungsziele löschen auf Seite 94
- **Exportieren** der Vorlagen für die automatische Bereitstellung in verschiedene Formate. Siehe . Exportieren der Details von automatischen Bereitstellungzielen in verschiedene Formate auf Seite 95

ANMERKUNG:

- Nur Administratoren können die Aufgaben zum Erstellen, Löschen und Exportieren in den Vorlagen für die automatische Bereitstellung durchführen. Die Geräte-Manager können nur die Vorlagen für die automatische Bereitstellung „exportieren“. Weitere Informationen finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Automatische Bereitstellungsziele erstellen

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

So erstellen Sie automatische Bereitstellungsziele:

1. Klicken Sie auf **OpenManage Enterprise** > **Konfiguration** > **Automatische Bereitstellung** > **Erstellen**
   Daraufhin wird der **Vorlagenassistent für die automatische Bereitstellung** angezeigt.
2. Auf der Seite **Vorlageninformationen** wählen Sie den Bereitstellungsvorlagentyp aus (Server oder Gehäuse).
3. Wählen Sie aus dem Drop-Down-Menü **Vorlage wählen** eine passende Vorlage aus. Wenn die ausgewählte Vorlage über Identitätsattribute verfügt, die keinem virtuellen Identitätspool zugeordnet sind, wird die folgende Meldung angezeigt: *Die ausgewählte Vorlage verfügt über Identitätsattribute, wurde jedoch keinem virtuellen Identitätspool zugeordnet. Durch die Bereitstellung dieser Vorlage werden die virtuellen Netzwerkadressen auf den Zielgeräten nicht geändert.*
4. Klicken Sie auf Weiter.
   Daraufhin wird die Seite **Zielinformationen** angezeigt.
5. Auf der Seite **Zielinformationen** können Zielgeräte auf eine der folgenden Arten ausgewählt werden:
   - **Manuell eingeben**: Geben Sie die Service-Tag-Nummer oder die Knoten-ID ein, um die Zielgeräte zu identifizieren. Die Kennungen können in beliebiger Reihenfolge eingegeben werden, die Kennungen müssen jedoch durch Kommas getrennt werden. Klicken Sie auf "Überprüfen", um die Richtigkeit der Werte zu überprüfen. Es ist zwingend erforderlich, die Kennungen zu überprüfen.
   - **CSV importieren**: Klicken Sie auf **CSV importieren**, um die Ordner zu durchsuchen und die entsprechende CSV-Datei mit den Zielgerätedetails auszuwählen. Es wird eine Zusammenfassung der Anzahl der erfolgreich importierten und ungültigen Einträge angezeigt. Um eine detailliertere Übersicht über das Import-Ergebnis zu erhalten, klicken Sie auf **Details anzeigen**.

     Die Einträge in der CSV-Datei müssen das folgende Format haben: Die Kennungen müssen in der ersten Spalte aufgeführt werden, und zwar einer pro Zeile, beginnend mit der zweiten Zeile. Klicken Sie für eine Vorlage-CSV-Datei auf **Beispiel-CSV-Datei herunterladen**.
6. Klicken Sie auf **Weiter**.
7. Geben Sie auf der Seite **Zielgruppeninformationen** eine Untergruppe unter der **Gruppe "Statisch"** an, sofern verfügbar. Weitere Informationen zum Gruppieren von Geräten finden Sie unter Geräte in Gruppen organisieren auf Seite 55. Die Zielgeräte würden bei ihrer Ermittlung der angegebenen Zielgruppe zugeordnet.
8. Klicken Sie auf **Weiter**.
9. Wenn es sich bei dem Zielgerät um einen Server handelt auf der Seite **Start von Netzwerk-ISO**:
   - Markieren Sie das Kontrollkästchen **Start auf Netzwerk-ISO**.
   - Wählen Sie **CIFS** oder **NFS**.
   - Geben Sie den **ISO-Pfad** des Speicherorts an, an dem die ISO-Image-Datei gespeichert ist. Verwenden Sie die Tooltips, damit Sie die richtige Syntax eingeben.
   - Geben Sie **Freigabe-IP-Adresse**, **Arbeitsgruppe**, **Nutzername** und **Kennwort** ein.
   - Wählen Sie die **Zeit zum Anhängen der ISO**-Drop-Down-Menü-Optionen, um die Anzahl der Stunden festzulegen, die die Netzwerk-ISO-Datei den Zielgeräten zugewiesen bleibt. Standardmäßig wird dieser Wert auf vier Stunden festgelegt.
   - Klicken Sie auf **Weiter**.
10. Klicken Sie auf der Seite **Virtuelle Identitäten** auf **Identitäten reservieren**.
    Die zugewiesenen virtuellen Identitäten der NIC-Karten des ausgewählten Zielgeräts werden angezeigt. Um alle zugewiesenen Identitäten des Identitätspools des ausgewählten Zielgeräts anzuzeigen, klicken Sie auf **Alle NIC-Details anzeigen**.
11. Im Abschnitt **Zielattribute** können die nicht virtuellen Identitätsattribute, die für jedes der ausgewählten Zielgeräte spezifisch sind, wie z.B. die Standort-Attribute und die IP-Adresse, vor der Bereitstellung der Bereitstellungsvorlage geändert werden. Wenn die Vorlage bereitgestellt wird, werden diese geänderten Zielattribute nur auf den spezifischen Geräten implementiert. So ändern Sie die gerätespezifischen, nicht virtuellen Identitätsattribute:
    a. Wählen Sie ein Zielgerät aus der Liste aus, in der die zuvor ausgewählten Zielgeräte angezeigt werden.
    b. Erweitern Sie die Attributkategorien und aktivieren oder deaktivieren Sie dann die Attribute, die während der Vorlagenbereitstellung auf dem Zielgerät eingeschlossen oder ausgeschlossen werden müssen.
    c. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Fertigstellen**.
    Eine Warnmeldung wird angezeigt: Das Bereitstellen einer Vorlage kann zu Datenverlust und zum Neustart des Geräts führen. *Möchten Sie die Vorlage wirklich bereitstellen?* wird angezeigt.
13. Klicken Sie auf **Ja**.
    Ein neues automatisches Bereitstellungsziel wird erstellt und auf der Seite **Automatische Bereitstellung** aufgeführt.

Automatische Bereitstellungsziele löschen

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

ANMERKUNG: Wenn eine mit automatischen Bereitstellungszielen verknüpfte Vorlage von der Seite **OpenManage Enterprise** > **Konfiguration** > **Vorlagen** gelöscht wird, werden die zugehörigen automatischen Bereitstellungseinträge unabhängig vom aktuellen Status ebenfalls gelöscht.

So entfernen Sie die automatischen Bereitstellungsziele aus der Liste **Automatische Bereitstellung**.

1. Wechseln Sie zur Seite "Automatische Bereitstellung" und klicken Sie auf **OpenManage Enterprise** > **Konfiguration** > **Automatische Bereitstellung**.
2. Wählen Sie die Ziele für die automatische Bereitstellung aus der Liste aus.
3. Klicken Sie auf **Löschen** und klicken Sie dann zur Bestätigung auf **Ja**.
   Die automatischen Bereitstellungsziele, die zum Löschen ausgewählt werden, werden von der Seite "Automatische Bereitstellung" entfernt.

Exportieren der Details von automatischen Bereitstellungzielen in verschiedene Formate

1. Wechseln Sie zur Seite "Automatische Bereitstellung" und klicken Sie auf **OpenManage Enterprise** > **Konfiguration** > **Automatische Bereitstellung**.
2. Wählen Sie das automatische Bereitstellungsziel aus der Liste aus und klicken Sie auf **Exportieren**.
3. Wählen Sie im Dialogfeld **Alle exportieren** das Format entweder als HTML oder CSV oder als PDF aus. Klicken Sie auf **Fertigstellen**.
   Ein Job wird erstellt und die Daten der automatischen Bereitstellungziele werden im ausgewählten Format exportiert.

Übersicht über statusfreie Bereitstellung

Um eine Gerätebereitstellungsvorlage mit virtuellen Identitäts-Attributen auf Zielgeräten bereitzustellen, gehen Sie wie folgt vor:

1. **Erstellen einer Gerätevorlage** – Klicken Sie die Task **Vorlage erstellen** unter der Registerkarte **Bereitstellen** zum Erstellen einer Bereitstellungsvorlage. Sie können die Vorlage entweder aus einer Konfigurationsdatei oder einem Referenzgerät erstellen.
2. **Virtuellen I/O-Poolerstellen** – Klicken Sie auf die Task **Erstellen** unter der Registerkarte Identitäts-Pools, um einen Pool aus einem oder mehreren virtuellen Identitätstypen zu erstellen.
3. **Virtuelle Identitäten einer Gerätevorlage zuweisen** – Wählen Sie im Bereich **Vorlagen** eine Bereitstellungsvorlage aus und klicken Sie auf **Netzwerk bearbeiten**, um der Bereitstellungsvorlage einen Identitätspool zuzuweisen. Sie können auch das gekennzeichnete und nicht gekennzeichnete Netzwerk auswählen und den Ports die minimale und maximale Bandbreite zuweisen.
4. **Bereitstellungsvorlage auf den Zielgeräten bereitstellen**: Verwenden Sie die Task **Vorlage bereitstellen** unter der Registerkarte **Bereitstellen**, um die Bereitstellungsvorlage und virtuellen I/O-Identitäten auf den Zielgeräten bereitzustellen.

Identity-Pools verwalten – Statuslose Bereitstellung

Die I/O-Schnittstellen eines Servers, wie etwa NICs oder HBAs, verfügen über eindeutige Identitätsattribute, die vom Hersteller der Schnittstellen zugewiesen werden. Diese eindeutigen Identitätsattribute werden kollektiv als I/O-Identität eines Servers bezeichnet. Die I/O-Identitäten identifizieren einen Server im Netzwerk eindeutig und bestimmen zudem, wie der Server unter Verwendung eines spezifischen Protokolls mit einer Netzwerkressource kommuniziert. Unter Verwendung von OpenManage Enterprise können Sie virtuelle Identitätsattribute automatisch generieren und den I/O-Schnittstellen eines Servers zuweisen.

Server, die mithilfe einer Gerätebereitstellungsvorlage bereitgestellt werden, die virtuelle I/O-Identitäten enthält, werden als „statusfrei“ bezeichnet. Statusfreie Bereitstellungen ermöglichen Ihnen das Erstellen einer dynamischen und flexiblen Serverumgebung. Wenn Sie beispielsweise einen Server mit virtuellen I/O-Identitäten in einer Start-von-SAN-Umgebung bereitstellen, können Sie Folgendes schnell durchführen:

- Ersetzen eines fehlerhaften oder ausgefallenen Servers durch Verschieben der I/O-Identität des Servers auf einen Ersatzserver
- Bereitstellen zusätzlicher Server zur Steigerung der Rechenleistung bei hoher Arbeitslast

Über die Seite **OpenManage Enterprise** > **Konfiguration** > **Identitäts-Pools** können Sie virtuelle I/O-Pools erstellen, bearbeiten, löschen oder exportieren.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16
- Umfangsbasierte Einschränkungen gelten nicht für Identitäts-Pools, daher können alle Identitäts-Pools angezeigt und von allen Nutzertypen verwendet werden. Wenn die Identitäten jedoch von einem Geräte-Manager zugewiesen werden, können nur diese Identitäten angezeigt und von diesem Geräte-Manager verwendet werden.

Identitätspool erstellen – Pool-Informationen

Identitäts-Pools werden für vorlagenbasierte Bereitstellung auf Servern verwendet, um die Netzwerkidentität für Folgendes zu virtualisieren:

- Ethernet
- iSCSI
- Fibre-Channel Over Ethernet (FCoE)
- Fibre Channel (FC)

Sie können bis zu 5000 Identitätspools in jeder dieser Kategorien erstellen.

Der Serverbereitstellungsprozess ruft die nächste verfügbare Identität aus dem Pool ab und verwendet diese und stellt außerdem einen Server aus der Vorlagenbeschreibung zur Verfügung. Sie können dann das Profil von einem Server auf einen anderen migrieren, ohne den Zugriff auf die Netzwerk- oder Speicherressourcen in Ihrer Umgebung zu verlieren.

Sie können die Anzahl der Einträge im Pool bearbeiten. Sie können jedoch nicht die Anzahl der Einträge auf weniger als die zugewiesenen oder reservierten reduzieren. Sie können auch die Einträge löschen, die nicht zugewiesen oder reserviert sind.

ANMERKUNG: Das Bearbeiten des Identitätspool schlägt fehl, wenn der Identitätsbereich überlappt. Ein Tauschen ist nicht zulässig, wenn Sie Identitätspools für Ethernet, FCoE und iSCSI konfiguriert haben und versuchen, eine Startadresse zu bearbeiten und zu tauschen, die mit dem vorhandenen Bereich überlappt. Um die Start-MAC-Adresse zu tauschen, müssen Sie sie bereichsweise aus dem in Konflikt stehenden Bereich verschieben.

Poolname	Geben Sie den Namen für den Identitäts-Pool ein. Der Poolname darf maximal 255 Zeichen enthalten.
Beschreibung	Geben Sie eine Beschreibung für den Identitäts-Pool ein. Die maximale Länge der Beschreibung ist 255 Zeichen.

Maßnahmen

Weiter	Zeigt die Registerkarte **Ethernet** an.
Fertig stellen	Speichert die Änderungen und zeigt die Seite **Identitäts-Pools** an.
Abbrechen	Schließt das Fenster **Identitäts-Pool erstellen**, ohne die Änderungen zu speichern.

Identitäts-Pools

Ein Identitäts-Pool ist eine Sammlung aus einem oder mehreren virtuellen Identitätstypen, die für die Netzwerkkommunikation erforderlich sind. Ein Identitäts-Pool kann eine beliebige Kombination folgender virtueller Identitätstypen enthalten:

- Ethernet-Identitäten

  Die Identitäten, die durch die MAC-Adresse (Media Access Control) definiert werden. MAC-Adressen werden für die Ethernet (LAN)-Kommunikation benötigt.

- iSCSI-Identitäten

  Die Identitäten, die durch den qualifizierten iSCSI-Namen (IQN) definiert werden. IQN-Identitäten sind für die Unterstützung von Start-von-SAN unter Verwendung des iSCSI-Protokolls erforderlich.

- Fibre Channel (FC)-Identitäten

  Identitäten, die durch den Weltweiten Knotennamen (World Wide Node Name, WWNN) und den Weltweiten Schnittstellennamen (World Wide Port Name, WWPN) definiert werden. Eine WWNN-Identität wird einem Knoten (Gerät) in einem FC-Fabric zugewiesen und kann von manchen oder allen Ports eines Geräts geteilt werden. In einem FC-Fabric ist jedem Port eine WWPN-Identität zugewiesen. Diese ist für jeden Port eindeutig. WWNN- und WWPN-Identitäten sind erforderlich, um den Start-von-SAN zu unterstützen sowie für den Datenzugriff über FC- und Fibre Channel über Ethernet (FCoE)-Protokolle.

- Fibre-Channel Over Ethernet (FCoE) Identitäten

  Identitäten, die eine einzigartige virtuelle Identität für FCoE-Vorgänge bieten. Diese Identitäten sind sowohl von MAC- als auch FC-Adressen definiert (also WWNN und WWPN). WWNN- und WWPN-Identitäten sind erforderlich, um den Start-von-SAN zu unterstützen sowie für den Datenzugriff über FC- und Fibre Channel über Ethernet (FCoE)-Protokolle.

OpenManage Enterprise verwendet die Identitäts-Pools, um der für die Bereitstellung eines Servers verwendeten Gerätebereitstellungsvorlage automatisch virtuelle Identitäten zuzuweisen.

ANMERKUNG:
- Für Identitäten, die zu einem vorhandenen Identitäts-Pool gehören, aber außerhalb von OpenManage Enterprise bereitgestellt wurden, muss ein neuer Konfigurations-Bestandsaufnahme-Job initiiert werden, um sie in der Appliance als „zugewiesen" zu identifizieren und festzulegen.
- Die virtuellen Identitäten, die bereits zugewiesen sind, werden für eine neue Bereitstellung nur verwendet, wenn diese Identitäten gelöscht werden.

Identitäts-Pools erstellen

Sie können einen Identitäts-Pool erstellen, der einen oder mehrere virtuelle Identitätstypen enthält. Ein vom Administrator erstellter gemeinsamer Pool kann von allen Geräte-Managern verwendet werden. Außerdem kann der Administrator alle Identitäten sehen, die verwendet werden. Die Geräte-Manager sehen alle Identitäts-Pools und führen alle zugehörigen Vorgänge aus (gemäß RBAC). Unter „Verwendung" können Geräte-Manager jedoch nur die Identitäten anzeigen, die den Geräten in ihrem Bereich zugeordnet sind.

So erstellen Sie einen Pool mit virtuellen Identitätstypen:

1. Klicken Sie auf der Seite **Konfiguration** auf **Identitäts-Pools**.
2. Klicken Sie auf **Erstellen**.
3. Im Dialogfeld **Identitätspools erstellen** unter **Pool-Informationen**:
   a. Geben Sie einen eindeutigen Namen für den Identitäts-Pool und eine passende Beschreibung ein.
   b. Klicken Sie auf **Weiter**.
4. Im Abschnitt **Ethernet**:
   a. Aktivieren Sie das Kontrollkästchen **Virtuelle Ethernet-MAC-Adressen einschließen**, um die MAC-Adressen einzuschließen.
   b. Geben Sie eine MAC-Start-Adresse ein und geben Sie dann die Anzahl der virtuellen MAC-Identitäten an, die erstellt werden sollen.
5. Im Abschnitt **iSCSI**:
   a. Aktivieren Sie das Kontrollkästchen **iSCSI-MAC-Adressen einschließen**, um iSCSI-MAC-Adressen einzuschließen.
   b. Geben Sie die MAC- Start-Adresse ein und geben Sie dann die Anzahl der iSCSI-MAC-Adressen an, die erstellt werden sollen.
   c. Aktivieren Sie **iSCSI-Initiator konfigurieren** und geben Sie dann das IQN-Präfix ein.
   d. Aktivieren Sie **iSCSI-Initiator-IP-Pool aktivieren** und geben Sie dann die Netzwerkdetails ein.

      ANMERKUNG: Der iSCSI-Initiator-IP-Pool unterstützt keine IPv6-Adressen.
6. Im Abschnitt **FCoE**:
   a. Aktivieren Sie das Kontrollkästchen **FCoE-Identität einschließen**, um FCoE-Identitäten einzuschließen.
   b. Geben Sie die MAC- Start-Adresse ein und geben Sie dann die Anzahl der FCoE-Identitäten an, die erstellt werden sollen.

      ANMERKUNG: Die WWPN- und WWNN-Adressen werden generiert, indem den MAC-Adressen das Präfix 0x2001 bzw. 0x2000 vorangestellt wird.
7. Im Abschnitt **Fibre Channel**:
   a. Aktivieren Sie das Kontrollkästchen **FC-Identität einschließen**, um FC-Identitäten einzuschließen.
   b. Geben Sie die Postfix-Oktette (sechs Oktette) und die Anzahl der WWPN- und WWNN-Adressen ein, die erstellt werden sollen.

      ANMERKUNG: Die WWPN- und WWNN-Adressen werden generiert, indem dem bereitgestellten Postfix das Präfix 0x2001 bzw. 0x2000 vorangestellt wird.

Der Identitäts-Pool wird erstellt und unter der Registerkarte **Identitäts-Pools** aufgelistet.

Identitätspool erstellen – Fibre Channel

Sie können Fibre Channel (FC)-Adressen zum Identitäts-Pool hinzufügen. Der FC umfasst WWPN/WWNN-Adressen.

FC-Identität einschließen

Aktivieren Sie das Kontrollkästchen, um FC-Adressen zum Identitäts-Pool hinzuzufügen.

Post-Fix (6 Oktette)

Geben Sie den Post-Fix in einem der nachfolgenden Formate ein:

- `AA:BB:CC:DD:EE:FF`
- `AA-BB-CC-DD-EE-FF`
- `AABB.CCDD.EEFF`

Die Länge des Post-Fix darf maximal 50 Zeichen betragen. Diese Option wird nur angezeigt, wenn das Kontrollkästchen **FC-Identität einschließen** aktiviert ist.

Anzahl der WWPN-WWNN-Adressen

Wählen Sie die Nummer der WWPN oder WWNN Adresse aus. Die Adresse kann zwischen 1 und 5000 liegen.

Diese Option wird nur angezeigt, wenn das Kontrollkästchen **FC-Identität einschließen** aktiviert ist.

Maßnahmen

Zurück

Zeigt die Registerkarte **FCoE** an.

Fertig stellen

Speichert die Änderungen und zeigt die Seite **Konfiguration** an.

Abbrechen

Schließt das Fenster **Identitäts-Pool erstellen**, ohne die Änderungen zu speichern.

Identitätspool erstellen – iSCSI

Sie können die erforderliche Anzahl von iSCSI-MAC-Adressen auf der Registerkarte „iSCSI" konfigurieren.

ANMERKUNG: Die iSCSI-Attribute werden nur dann angewendet, wenn die DHCP-Option für den iSCSI-Initiator in der Quellvorlage deaktiviert ist.

Virtuelle iSCSI-MAC-Adressen einschließen

Aktivieren Sie das Kontrollkästchen, um die iSCSI-MAC-Adressen zum Identitäts-Pool hinzuzufügen.

Virtuelle MAC-Start-Adresse

Geben Sie die MAC-Start-Adresse des Identitäts-Pools in einem der nachfolgenden Formate ein:

- `AA:BB:CC:DD:EE:FF`
- `AA-BB-CC-DD-EE-FF`
- `AABB.CCDD.EEFF`

Die maximale Länge einer MAC-Adresse ist 50 Zeichen. Diese Option wird nur angezeigt, wenn das Kontrollkästchen **iSCSI-MAC-Adressen einschließen** aktiviert ist.

Anzahl der iSCSI-MAC-Identitäten

Geben Sie die Anzahl der iSCSI-MAC-Adressen ein. Die MAC-Adresse kann zwischen 1 und 5000 liegen. Diese Option wird nur angezeigt, wenn das Kontrollkästchen **iSCSI-MAC-Adressen einschließen** aktiviert ist.

iSCSI-Initiator konfigurieren

Aktivieren Sie dieses Kontrollkästchen, um den iSCSI-Initiator zu konfigurieren. Diese Option wird nur angezeigt, wenn das Kontrollkästchen **iSCSI-MAC-Adressen einschließen** aktiviert ist.

IQN-Präfix

Geben Sie das IQN-Präfix des iSCSI Identitäts-Pools ein. Die Länge des IQN-Präfix darf maximal 200 Zeichen betragen. Das System generiert den Pool der IQN-Adressen automatisch durch das Anhängen der generierte Nummer an das Präfix. Beispiel: `<IQN Prefix>.<number>`

Diese Option wird nur angezeigt, wenn das Kontrollkästchen **iSCSI-Initiator konfigurieren** aktiviert ist.

ANMERKUNG: Der mit Identitäts-Pools konfigurierte IQN wird auf dem Zielsystem nicht angewendet, falls der Startmodus "BIOS" ist.

> **ANMERKUNG:** Wenn der iSCSI-Initiatorname in einer separaten Zeile im Feld **Identitäts-Pools** > **Nutzung** > **iSCSI IQN** angezeigt wird, weist dies darauf hin, dass der iSCSI-IQN nur auf dieser NIC-Partition aktiviert ist.

iSCSI-Initiator-IP-Pool aktivieren Aktivieren Sie das Kontrollkästchen, um einen Pool von iSCSI-Initiator-Identitäten zu konfigurieren. Diese Option wird nur angezeigt, wenn das Kontrollkästchen **iSCSI-MAC-Adressen einschließen** aktiviert ist.

IP-Adressbereich Geben Sie den IP-Adressbereich des Identitäts-Pools in einem der nachfolgenden Formate ein:

- `A.B.C.D - W.X.Y.Z`
- `A.B.C.D/E`

Subnetzmaske Wählen Sie die Subnetzmasken-Adresse des iSCSI-Pools aus dem Drop-Down-Menü aus.

Gateway Geben Sie die Gateway-Adresse des iSCSI-Pools ein.

Primärer DNS-Server Geben Sie die IP-Adresse des primären DNS-Servers ein.

Sekundärer DNS-Server Geben Sie die IP-Adresse des sekundären DNS-Servers ein.

> **ANMERKUNG:** Die Angaben für **IP-Adressbereich**, **Gateway**, **Primärer DNS-Server** und **Sekundärer DNS-Server** müssen gültige IPv4-Adressen sein.

Maßnahmen

Zurück Zeigt die Registerkarte **Ethernet** an.

Weiter Zeigt die Registerkarte **FCoE** an.

Fertig stellen Speichert die Änderungen und zeigt die Seite **Konfiguration** an.

Abbrechen Schließt das Fenster **Identitäts-Pool erstellen**, ohne die Änderungen zu speichern.

Identitätspool erstellen – Fibre Channel over Ethernet

Sie können die erforderliche Anzahl von Fibre Channel over Ethernet (FCoE) Initialisierungsprotokoll (FIP) MAC-Adressen zum Identitäts-Pool hinzufügen. Die World Wide Port Name (WWPN)- /World Wide Node Name (WWNN)-Werte werden von diesen MAC-Adressen generiert.

FCoE-Identität einschließen Aktivieren Sie das Kontrollkästchen, um die FCoE-MAC-Adressen zum Identitäts-Pool hinzuzufügen.

FIP-MAC-Adresse Geben Sie die FCoE-Initialisierungsprotokoll (FIP)-Start-MAC-Adresse des Identitäts-Pools in einem der nachfolgenden Formate ein:

- `AA:BB:CC:DD:EE:FF`
- `AA-BB-CC-DD-EE-FF`
- `AABB.CCDD.EEFF`

Die maximale Länge einer MAC-Adresse ist 50 Zeichen. Diese Option wird nur angezeigt, wenn das Kontrollkästchen **FCoE-Identität einschließen** aktiviert ist.

Die WWPN/WWNN-Werte werden von der MAC-Adresse generiert.

Anzahl der FCoE-Identitäten Wählen Sie die erforderliche Anzahl von FCoE-Identitäten aus. Die Identitäten können zwischen 1 und 5000 liegen.

Maßnahmen

Zurück	Zeigt die Registerkarte **iSCSI** an.
Weiter	Zeigt die Registerkarte **Fibre-Channel** an.
Fertig stellen	Speichert die Änderungen und zeigt die Seite **Identitäts-Pools** an.
Abbrechen	Schließt das Fenster **Identitäts-Pool erstellen**, ohne die Änderungen zu speichern.

Identitätspool erstellen – Ethernet

Auf der Registerkarte **Ethernet** können Sie Sie die erforderliche Anzahl von MAC-Adressen zum Identitäts-Pool hinzufügen.

Virtuelle Ethernet-MAC-Adressen einschließen	Aktivieren Sie das Kontrollkästchen, um die virtuellen MAC-Adressen zum Identitäts-Pool hinzuzufügen.
Virtuelle MAC-Start-Adresse	Geben Sie die virtuelle MAC-Start-Adresse in einem der nachfolgenden Formate ein: • `AA:BB:CC:DD:EE:FF` • `AA-BB-CC-DD-EE-FF` • `AABB.CCDD.EEFF` Die maximale Länge einer MAC-Adresse ist 50 Zeichen. Diese Option wird nur angezeigt, wenn das Kontrollkästchen **Virtuelle Ethernet-MAC-Adressen einschließen** aktiviert ist.
Anzahl der virtuellen MAC-Identitäten	Wählen Sie die Anzahl der virtuellen MAC-Identitäten aus. Die Identitäten können zwischen 1 und 50 liegen. Diese Option wird nur angezeigt, wenn das Kontrollkästchen **Virtuelle Ethernet-MAC-Adressen einschließen** aktiviert ist.

Maßnahmen

Zurück	Zeigt die Registerkarte **Poolinformationen** an.
Weiter	Zeigt die Registerkarte **iSCSI** an.
Fertig stellen	Speichert die Änderungen und zeigt die Seite **Identitäts-Pools** an.
Abbrechen	Schließt das Fenster **Identitäts-Pool erstellen**, ohne die Änderungen zu speichern.

Definitionen von Identitäts-Pools anzeigen

So können Sie die Definitionen eines Identitäts-Pools bearbeiten:

1. Klicken Sie auf der Seite **Konfiguration** auf **Identitäts-Pools**.
2. Wählen Sie den Identitäts-Pool aus und klicken Sie dann auf **Zusammenfassung**.
   Die verschiedenen Identitätsdefinitionen des Identitäts-Pools werden aufgelistet.
3. Um die Nutzung dieser Identitätsdefinitionen anzuzeigen, klicken Sie auf die Registerkarte **Nutzung** und wählen die Filteroption **Anzeigen nach** aus.

Identitäts-Pools bearbeiten

Sie können einen Identitäts-Pool bearbeiten, wenn Sie beispielsweise noch nicht angegebene Bereiche hinzufügen, einen Identitätstyp hinzufügen oder Identitätstypbereiche löschen möchten.

So können Sie die Definitionen eines Identitäts-Pools bearbeiten:

1. Klicken Sie auf der Seite **Konfiguration** auf **Identitäts-Pools**.
2. Wählen Sie den Identitäts-Pool aus und klicken Sie dann auf **Bearbeiten**.

Das Dialogfeld **Identitäts-Pool bearbeiten** wird angezeigt.

3. Nehmen Sie die erforderlichen Änderungen an den Definitionen in den entsprechenden Abschnitten vor und klicken Sie dann auf **Fertig stellen**.

Der Identitäts-Pool ist jetzt geändert.

Identitäts-Pools löschen

Sie können einen Identitäts-Pool nicht löschen, wenn die Identitäten reserviert sind oder einer Bereitstellungsvorlage zugewiesen sind.

So löschen Sie einen Identitäts-Pool:

1. Klicken Sie auf der Seite **Konfiguration** auf **Identitäts-Pools**.
2. Wählen Sie den Identitäts-Pool aus und klicken Sie dann auf **Löschen**.
3. Klicken Sie auf **Ja**.

Der Identitäts-Pool wird gelöscht und die reservierten Identitäten, die mit einer oder mehreren Bereitstellungsvorlagen verknüpft sind, werden entfernt.

Netzwerke definieren

Auf der Seite „VLANs" können Sie Informationen zu den Netzwerken eingeben, die derzeit in Ihrer Umgebung konfiguriert sind, auf die die Geräte zugreifen können.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Wählen Sie **Konfiguration** > **VLANs** > **Definieren**.
2. Geben Sie im Dialogfeld **Netzwerk definieren** einen Namen und eine passende Beschreibung ein.
3. Geben Sie die VLAN-ID ein und wählen Sie dann den Netzwerktyp aus.

   Sie können nur für MX7000-Gehäuse einen Netzwerktyp wählen. Weitere Informationen zu Netzwerktypen finden Sie unter Netzwerktypen auf Seite 101.
4. Klicken Sie auf **Fertigstellen**.

Das derzeit in Ihrer Umgebung konfigurierte Netzwerk ist jetzt definiert und Ressourcen können auf das Netzwerk zugreifen.

ANMERKUNG: Bereichsbasierte Einschränkungen gelten nicht für VLANs, da es sich hierbei um gängige Ressourcenpools handelt. Sobald ein VLAN vom Administrator definiert wurde, ist es für alle Geräte-Manager zur Verwendung verfügbar.

Netzwerktypen

ANMERKUNG: Sie können nur für MX7000-Gehäuse einen Netzwerktyp wählen.

Tabelle 15. Netzwerktypen

Netzwerktypen	Beschreibung
Allgemeiner Zweck (Bronze)	Wird für Datenverkehr mit niedriger Priorität verwendet
Allgemeiner Zweck (Silber)	Wird für Datenverkehr mit Standard-Priorität verwendet
Allgemeiner Zweck (Gold)	Wird für Datenverkehr mit hoher Priorität verwendet
Allgemeiner Zweck (Platin)	Wird für Datenverkehr mit extrem hoher Priorität verwendet
Cluster-Interconnect	Wird für Cluster-Heartbeat-VLANs verwendet
Hypervisor-Verwaltung	Wird für Hypervisor-Management-Verbindungen wie z. B. das ESXi-Verwaltungs-VLAN verwendet

Tabelle 15. Netzwerktypen (fortgesetzt)

Netzwerktypen	Beschreibung
Speicher – iSCSI	Wird für iSCSI-VLANs verwendet
Speicher – FCoE	Wird für FCoE-VLANs verwendet
Speicher – Datenreplikation	Wird für VLANs mit Unterstützung für Speicherdatenreplikation wie z. B. für VMware Virtual Storage Area Network (VSAN) verwendet
VM-Migration	Wird für VLANs mit Unterstützung für vMotion und ähnliche Technologien verwendet
VMWare FT-Protokollierung	Wird für VLANs mit Unterstützung für VMware Fault Tolerance verwendet

Ein konfiguriertes Netzwerk bearbeiten und löschen

1. Navigieren Sie zur Seite „VLANs“, indem Sie auf **Konfiguration** > **VLANs**klicken.
2. Wählen Sie ein Netzwerk aus der Liste aus und klicken Sie dann im rechten Fensterbereich auf **Bearbeiten**, um den Namen, die Beschreibung, die VLAN-ID oder den Netzwerktyp zu ändern.

   ANMERKUNG: VLAN-Konfiguration auf M1000e- und FX2-Gehäusen wird in einer IPv6 Infrastruktur nicht unterstützt, da die IPv6 Adressierung nicht von M E/A-Aggregator (IOA) und FN E/A-Modulen unterstützt wird.

   ANMERKUNG: Der geänderte VLAN-Name und die geänderten VLAN-IDs nwerden ach dem Ausführen einer statuslosen Bereitstellungsaufgabe nicht auf den MX7000-Zielgeräten aktualisiert.

3. Zum Löschen des Netzwerks wählen Sie das Netzwerk aus und klicken auf **Löschen**.
4. Klicken Sie auf **Ja**.

Exportieren von VLAN-Definitionen

Die in OpenManage Enterprise verfügbaren Netzwerkdefinitionen können entweder als CSV- oder als Json-Datei heruntergeladen werden.

1. So laden Sie sie als CSV-Datei herunter:
   a. Klicken Sie auf **Konfiguration** > **VLANs** > **Exportieren** und wählen Sie **Alle als CSV exportieren** aus.
2. So laden Sie die JSON-Datei herunter:
   a. Klicken Sie auf **Konfiguration** > **VLANs** > **Exportieren** und wählen Sie **Alle als JSON exportieren** aus.

Importieren von Netzwerkdefinitionen

Die folgenden Optionen sind verfügbar, um die Netzwerkdefinitionen zu importieren:

1. **Importieren von VLAN-Definitionen aus einer Datei**

   So importieren Sie VLAN-Definitionen aus einer Datei:

   a. Klicken Sie auf **Konfiguration** > **VLANs**.
   b. Klicken Sie auf **Importieren** und wählen Sie dann **Aus Datei importieren**.
   c. Navigieren Sie zum Speicherort der Datei und wählen Sie eine vorhandene.json- oder.csv-Datei mit den VLAN-Definitionen aus, und klicken Sie auf **Öffnen**.

      ANMERKUNG:

      - Ungültige Einträge oder ungültiger Content-Typ in den Dateien sind markiert und werden nicht importiert.
      - VLAN-Definitionen in den CSV- und JSON-Dateien müssen in den folgenden Formaten eingegeben werden:

Tabelle 16. VLAN-Definitionsformat für CSV-Datei

Name	Beschreibung	VLANMin	VLANMax	Typ
VLAN1	VLAN mit Einzel-ID	1	1	1
VLAN2 (Bereich)	VLAN mit einem ID-Bereich	2	10	2

und

Tabelle 17. VLAN-Definitionsformat für JSON-Dateien

```
[{„Name":„VLAN1",„Description":„VLAN mit Einzel-ID",„VlanMinimum":1,„VlanMaximum":1,
„Type":1},

{„Name":„VLAN2" (Bereich),„Description":„VLAN mit einem ID-Bereich",„VlanMinimum":2,
„VlanMaximum":10,„Type":2}]
```

d. Klicken Sie auf **Fertigstellen**. Ein Job mit dem Namen **ImportVLANDefinitionsTask** wird erstellt, um die Netzwerke aus der ausgewählten Datei zu importieren.

2. **Importieren von VLAN-Definitionen aus einem Gehäuse**

   So importieren Sie VLAN-Definitionen aus einem vorhandenen MX7000-Gehäuse:

   ANMERKUNG: OpenManage Enterprise-Modular Version 1.2 muss bereits im MX7000 installiert sein.

   a. Klicken Sie auf **Konfiguration** > **VLANs**.
   b. Klicken Sie auf **Importieren** und wählen Sie **VLANs aus Gehäuse importieren**.
   c. Wählen Sie auf dem Bildschirm **Auftragsziel** das Gehäuse aus, von dem die VLAN-Definitionen importiert werden müssen, und klicken Sie auf **OK**. Ein Job mit dem Namen **ImportVLANDefinitionsTask** wird erstellt, um die Netzwerke aus dem ausgewählten Gehäuse zu importieren.

Aktualisieren Sie nach Abschluss des Jobs die Seite **Konfiguration** > **VLANs**, um die erfolgreich importierten VLAN-Definitionen anzuzeigen.

Zum Anzeigen der Ausführungsdetails des Jobs und zum Status der einzelnen Netzwerke, die aus dem Gehäuse importiert wurden, gehen Sie zur Seite **Jobs**, indem Sie auf **Überwachen** > **Jobs**klicken, den Job auswählen und auf **Details anzeigen**klicken.

12

Profile verwalten

Ein „Profil" ist eine bestimmte Instanz einer vorhandenen Bereitstellungsvorlage, die mit den für ein einzelnes Gerät spezifischen Attributen angepasst ist. Profile können entweder implizit während der Bereitstellung/Auto-Bereitstellung einer Vorlage oder aus den vorhandenen Vorlagen des Nutzers erstellt werden. Ein Profil besteht aus zielspezifischen Attributwerten zusammen mit den BootToISO-Optionen und iDRAC-Management-IP-Details des Zielgeräts. Es kann auch alle Netzwerkbandbreite und VLAN-Zuweisungen für Server-NIC-Ports nach Bedarf enthalten. Ein Profil ist mit der Quellvorlage verknüpft, von der es erstellt wurde.

Auf der Seite **Konfiguration** > **Profile** werden alle Profile angezeigt, die im Bereich des angemeldeten Benutzers enthalten sind. Ein Administrator kann z. B. alle Profile anzeigen und verwalten, Geräte-Manager mit eingeschränktem Bereich können jedoch nur die Profile sehen und verwenden, die sie erstellt haben und besitzen.

Folgende Einzelheiten der aufgelisteten Profile werden angezeigt:

Tabelle 18. Verwalten von Profilen – Felddefinitionen

Feldname	Beschreibung
Geändert	Ein „geändertes" Symbol für ⚠ wird angezeigt, um nach der anfänglichen Zuweisung Änderungen an den verknüpften Profil- oder Vorlagen-Attributen anzuzeigen. Wenn das geänderte Profil auf dem Gerät erneut bereitgestellt wird, wird das Symbol nicht mehr angezeigt.
Profilname	Name des Profils
Vorlagenname	Name der verknüpften Quellvorlage
Ziel	Service-Tag-Nummer oder IP-Adresse des Geräts, auf dem das Profil zugewiesen ist. Wenn das Profil keinem Gerät zugewiesen ist, ist das Ziel leer.
Target Type (Zieltyp)	Der Gerätetyp (Server oder Gehäuse), auf dem das Profil zugewiesen ist
Gehäuse	Gehäusename des Gehäuses, wenn der Zielserver als Teil eines Gehäuses erkannt wird
Profilstatus	Profilstatus wird als „Gerät zugewiesen" angezeigt, wenn das Profil zugewiesen wird, „nicht zugewiesen" für nicht zugewiesene Profile und „bereitgestellt" für die bereitgestellten Profile.
Letzter Aktionsstatus	Zeigt den Status der letzten Aktion des Profils an, z.B. fehlgeschlagen, abgebrochen, fehlgeschlagen, neu, nicht ausgeführt, pausiert, in Warteschlange, wird ausgeführt, geplant.

Erweiterte Filter können zum Anpassen der Profilliste verwendet werden.

Auf der rechten Seite werden für das ausgewählte Profil die Beschreibung, die letzte bereitgestellte Zeit, die Zeit der letzten Änderung, erstellt am und erstellt von angezeigt. Klicken Sie auf Identitäten anzeigen, um die NIC-Konfiguration und die virtuellen Identitäten anzuzeigen, die mit dem Profil markiert sind.

Je nach den verschiedenen Profil-Zuständen können die folgenden Aktionen auf der Seite **Konfiguration** > **Profile** durchgeführt werden, wie unten beschrieben:

ANMERKUNG: Erstellungs- und Löschvorgänge werden nicht als Teil der Tabelle aufgeführt.

Tabelle 19. Profil-Zustände und mögliche Vorgänge

Profilstatus	Bearbeiten	Ziel zuweisen	Zielzuweisung aufheben	Erneute Bereitstellung	Migrieren
Nicht zugewiesenes Profil	Ja	Ja	Nein	Nein	Nein

Tabelle 19. Profil-Zustände und mögliche Vorgänge (fortgesetzt)

Profilstatus	Bearbeiten	Ziel zuweisen	Zielzuweisung aufheben	Erneute Bereitstellung	Migrieren
Zugewiesen zu Gerät	Ja	Nein	Ja	Nein	Nein
Bereitgestellt	Ja	Nein	Ja	Ja	Ja

- Erstellen Sie Profile und reservieren Sie vorab virtuelle Identitäten. Siehe Profile erstellen auf Seite 105
- Profildetails anzeigen Siehe Profildetails anzeigen auf Seite 106
- Bearbeiten Sie Profilattribute und Einstellungen. Siehe Profil bearbeiten auf Seite 106
- Zuweisen eines Profils zu einem Gerät oder eines Service-Tags (über die automatische Bereitstellung) Siehe Profil zuweisen auf Seite 107
- Aufheben der Zuweisung eines Profils zu einem Gerät oder eines Service-Tags. Siehe Aufheben der Zuweisung von Profilen auf Seite 108
- Erneutes Bereitstellen von Profiländerungen am zugehörigen Zielgerät. Siehe Erneutes Bereitstellen von Profilen auf Seite 108
- Migrieren Sie das Profil von einem Ziel (Gerät oder Service-Tag) zu einem anderen.
- Profile löschen Siehe Profile löschen auf Seite 109
- Exportieren und dann herunterladen von Profildaten in HTML, CSV oder PDF. Siehe Exportieren von Profildaten als HTML, CSV oder PDF auf Seite 109

Themen:

Profile erstellen

Profile können mithilfe der vorhandenen Bereitstellungsvorlagen für die Bereitstellung auf vorhandenen Zielgeräten erstellt werden oder können für die automatische Bereitstellung auf den noch nicht ermittelten Geräten reserviert werden.

ANMERKUNG:

- Nur Nutzer mit Berechtigungen für OpenManage Enterprise Administrator oder Device Manager können die Profil-Verwaltungsaufgaben durchführen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Nach dem Upgrade von Version 3.5 oder früher werden alle Profile, die von den Geräte-Managern AD/LDAP und OIDC (PingFederate oder KeyCloak) erstellt wurden, von einer der früheren OpenManage Enterprise-Versionen nur dem Administrator zugewiesen. Die Geräte-Manager müssen daher die Profile nach dem Upgrade neu erstellen.

Erstellen durch Import aus einer vorhandenen Bereitstellungsvorlage:

1. Navigieren Sie zur Seite Profile, indem Sie auf **Konfigurationen** > **Profile** klicken.
2. Klicken Sie auf **Erstellen**, um den Assistenten zum Erstellen von Profilen zu aktivieren.
3. Wählen Sie im Bereich „Vorlage“ den **Vorlagentyp** entweder als Server oder Gehäuse aus und wählen Sie dann eine Bereitstellungsvorlage in der Drop-Down-Liste **Vorlage wählen** aus. Klicken Sie auf **Weiter**.
4. Ändern Sie auf der Seite **Details** das **Namenspräfix** und geben Sie bei Bedarf eine Beschreibung in das Feld **Beschreibung** ein. Geben Sie im Feld **Profilanzahl** die Anzahl der Profile ein. Klicken Sie auf **Weiter**.
5. Wählen Sie optional auf der Seite **Start auf Netzwerk-ISO** das Kontrollkästchen **Auf Netzwerk-ISO starten** aus und geben Sie den vollständigen ISO-Pfad und den Speicherort für die Dateifreigabe an, und wählen Sie die Option **Zeit zum Anhängen der ISO** aus, um die Anzahl der Stunden festzulegen, die die Netzwerk-ISO-Datei den Zielgeräten zugewiesen bleibt.
6. Klicken Sie auf **Fertigstellen**.

Profile werden basierend auf dem Bereitstellungsvorlagennamen und der angegebenen Anzahl erstellt. Diese Profile werden auf der Seite Profile aufgelistet.

Profildetails anzeigen

So zeigen Sie die Details eines vorhandenen Profils ohne Bearbeitung an:

1. Wählen Sie ein Profil aus der Liste der Profile auf der Seite **Konfigurationen** > **Profile** aus.
2. Klicken Sie auf **Anzeigen**, um den Assistenten „Profil anzeigen" zu aktivieren.
3. Auf der **Detail**-Seite des Assistenten werden Quellvorlage, Name, Beschreibung und Zielinformationen angezeigt.
4. Klicken Sie auf **Weiter**. Auf der Seite **Start auf Netzwerk-ISO** werden der ISO-Image-Dateipfad, der Freigabespeicherort der ISO-Image-Datei und die Zeit zum Anhängen der ISO angezeigt, wenn das Profil anfänglich mit dieser Einstellung eingestellt wurde.

Profile – Netzwerk anzeigen

So zeigen Sie die Netzwerkbandbreite und VLAN Zuweisungen für die NIC-Ports an, die einem Profil zugeordnet sind:

1. Wählen Sie auf der Seite **Konfigurations** > **profile** ein Profil aus.
2. Klicken Sie auf **Anzeigen**, um den Assistenten „Profil anzeigen" zu aktivieren.
3. Der Abschnitt **Bandbreite** zeigt die folgenden Bandbreiteneinstellungen der partitionierten NICs an: Nic Bezeichner, Schnittstelle, Partition, min. Bandbreite (%) und maximale Bandbreite (%). Klicken Sie auf **Weiter.**
4. Der Abschnitt **VLANs** zeigt die folgenden VLAN Details der Profile an: NIC Teaming, NIC Kennung, Port, Team, nicht markiertes Netzwerk und markiertes Netzwerk.
5. Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen.

Profil bearbeiten

Ein vorhandenes Profil kann auf der Seite **Konfigurationen** > **Profile** bearbeitet werden. Die Änderungen am Profil haben keine automatischen Auswirkungen auf das zugeordnete Zielsystem. Damit die Änderungen wirksam werden, muss das geänderte Profil auf dem Zielgerät erneut bereitgestellt werden.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

Um das Netzwerk umzubenennen, zu bearbeiten oder die Attribute eines vorhandenen Profils zu bearbeiten, wählen Sie das Profil auf der Seite Profile aus und klicken Sie auf **Bearbeiten**. Die folgenden Bearbeitungsoptionen können ausgewählt werden:

1. Wählen Sie **Umbenennen** und bearbeiten Sie im Assistenten Profil umbenennen den Profilnamen im Feld **Name** .
2. Wählen Sie **Profil bearbeiten** aus, um den Assistenten Profil bearbeiten zu aktivieren und Folgendes zu bearbeiten:
   a. Auf der Seite **Details** können Sie den **Namen** und die **Beschreibung**bearbeiten. Klicken Sie auf **Weiter**.
   b. Aktivieren Sie auf der Seite Start auf Netzwerk-ISO das Kontrollkästchen **starten auf Netzwerk-ISO**, um den vollständigen ISO-Pfad und den Freigabespeicherort anzugeben, und gehen Sie folgendermaßen vor:
      - Wählen Sie **Freigabetyp** als CIFS oder NFS.
      - Geben Sie in das Feld **ISO-Pfad** den vollständigen ISO-Pfad ein. Verwenden Sie die Tooltips, damit Sie die richtige Syntax eingeben.
      - Geben Sie in den Feldern **Freigabe IP-Adresse**, **Nutzername** und **Kennwort** Details ein.
      - Wählen Sie die **Zeit zum Anhängen der ISO**-Drop-Down-Menü-Optionen, um die Anzahl der Stunden festzulegen, die die Netzwerk-ISO-Datei dem Zielgerät zugewiesen bleibt. Standardmäßig wird dieser Wert auf vier Stunden festgelegt.
      - Klicken Sie auf **Weiter**.
   c. Wählen Sie auf der Seite **iDRAC-Management-IP** eine der folgenden Optionen:
      - Ändern Sie die IP-Einstellungen nicht.
      - DHCP festlegen
      - Legen Sie die statische IP-Adresse fest und geben Sie die entsprechende Verwaltungs-IP-Adresse, Subnetzmaske und Gateway-Details an.
   d. Auf der Seite **Zielattribute** können Sie die Attribute BIOS, System, NIC, iDRAC und virtuelle Identität des Profils auswählen und bearbeiten.

e. Klicken Sie auf **Fertig stellen**, um die Änderungen zu übernehmen.

Profil zuweisen

Auf der Seite **Konfiguration** > **Profile** kann ein nicht zugewiesenes Profil entweder auf einem vorhandenen Server bereitgestellt oder für die automatische Bereitstellung auf einem noch nicht ermittelten Server reserviert werden.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Die vorhandenen Attribute (sofern vorhanden) des Zielservers würden überschrieben, wenn ein Profil bereitgestellt wird.
- Nur die Geräte, die keinem Profil zugeordnet sind, stehen für die Bereitstellung oder die automatische Bereitstellung zur Verfügung.

1. So **Stellen Sie ein Profil bereit**:
   a. Wählen Sie auf der Seite **Konfiguration** > **Profile** ein nicht zugewiesenes Profil aus und klicken Sie auf **Zuweisen** > **Bereitstellen**, um den Assistenten zum Bereitstellen des Profils zu aktivieren.
   b. Die Seite **Details** zeigt die Quellvorlage, den Profilnamen und die Beschreibung an. Klicken Sie auf **Weiter**.
   c. Auf der Seite **Ziel**:
      - Klicken Sie auf **Auswählen** und wählen Sie in der Liste der Geräte ein Zielgerät aus.

        ANMERKUNG: Geräte, denen bereits ein Profil zugewiesen ist, werden ausgegraut und können in der Zielliste nicht ausgewählt werden.
      - Wenn nach der Bereitstellung ein Neustart erforderlich ist, wählen Sie das Kontrollkästchen **Host-Betriebssystem nicht zwangsweise neu starten, wenn der ordnungsgemäße Neustart fehlschlägt**.
      - Klicken Sie auf **Weiter**.
   d. (Optional) Wählen Sie auf der Seite **Start auf Netzwerk-ISO** das Kontrollkästchen **Start auf Netzwerk-ISO** aus und geben Sie die entsprechenden Details zum ISO-Pfad und Freigabespeicherort an und den Wert „Zeit zum Anhängen der ISO“ an. Klicken Sie auf **Weiter**.
   e. Wählen Sie auf der Seite **iDRAC-Management-IP** eine der folgenden Optionen aus und geben Sie weitere relevante Details an.
      - IP-Einstellungen nicht ändern
      - DHCP festlegen
      - Verwendung einer statischen IP-Adresse
   f. Auf der Seite **Zielattribute** werden die Attribute unter den Abschnitten BIOS, System, NIC und iDRAC angezeigt. Sie können die Attribute vor der Bereitstellung auswählen, die Auswahl aufheben oder diese bearbeiten.
   g. Klicken Sie auf der Seite **Virtuelle Identitäten** auf **Identitäten reservieren**. Die zugewiesenen virtuellen Identitäten der NIC-Karten des ausgewählten Zielgeräts werden angezeigt. Um alle zugewiesenen Identitäten des Identitätspools des ausgewählten Zielgeräts anzuzeigen, klicken Sie auf **Alle NIC-Details anzeigen**.
   h. Auf der Seite **Zeitplan** können Sie **Jetzt ausführen** auswählen, um das Profil sofort bereitzustellen, oder wählen Sie **Zeitplan aktivieren** aus und wählen Sie ein geeignetes Zeit-und Datumsfeld für die Profil-Bereitstellung
   i. Klicken Sie auf **Fertigstellen**.

   ANMERKUNG: Wenn bereits Identitäten außerhalb der Appliance zugewiesen sind, nutzt eine neue Bereitstellung diese Identitäten nur dann, wenn Sie gelöscht werden. Weitere Informationen finden Sie unter Identitäts-Pools auf Seite 96

2. So **Stellen Sie ein Profil automatisch bereit**:

   ANMERKUNG: Bei modularen Geräten ist die strenge Überprüfung der VLAN-Definitionen standardmäßig aktiviert.

   a. Wählen Sie auf der Seite**Konfiguration** > **Profile** ein nicht zugewiesenes Profil aus, und klicken Sie auf **Zuweisen** > **Automatisch bereitstellen**, um den Assistenten für die automatische Bereitstellung zu aktivieren.
   b. Die Seite Details zeigt die Quellvorlage, den Namen und die Beschreibung (falls vorhanden) des Profils an. Klicken Sie auf **Weiter**.
   c. Geben Sie auf der Seite **Ziel** die Service-Tag-Nummer oder Knoten-ID des noch nicht ermittelten Geräts im Feld **Kennung** ein. Klicken Sie auf **Weiter**.
   d. (Optional) Gehen Sie auf der Seite „Start auf Netzwerk-ISO“ wie folgt vor, um das Kontrollkästchen **Start auf Netzwerk-ISO** auszuwählen, um den vollständigen ISO-Pfad und den Freigabespeicherort anzugeben:
      - Wählen Sie **Freigabetyp** als CIFS oder NFS.

- Geben Sie in das Feld **ISO-Pfad** den vollständigen ISO-Pfad ein. Verwenden Sie die Tooltips, damit Sie die richtige Syntax eingeben.
- Geben Sie die Details in den Feldern **Freigabe IP-Adresse**, **Nutzername** und **Kennwort** ein.
- Wählen Sie die **Zeit zum Anhängen der ISO**-Drop-Down-Menü-Optionen, um die Anzahl der Stunden festzulegen, die die Netzwerk-ISO-Datei den Zielgeräten zugewiesen bleibt. Standardmäßig wird dieser Wert auf vier Stunden festgelegt.

e. Klicken Sie auf **Fertigstellen**.

Aufheben der Zuweisung von Profilen

Mit **Konfiguration** > **Profilen** > **Aufheben** können die bereitgestellten oder automatisch bereitgestellten Profile von ihren jeweiligen Zielen aufgehoben werden. .

So heben Sie die Zuweisung von Profilen auf:

1. Wählen Sie die Profile aus der Profilliste auf der Seite **Konfigurationen** > **Profil** aus.
2. Klicken Sie auf **Aufheben**.
3. Klicken Sie im Bestätigungsdialogfeld auf **Fertigstellen**.

Die Zuweisung der ausgewählten Profile wird aufgehoben und die Identitäten ihrer jeweiligen Ziele werden entfernt.

ANMERKUNG: Bei den bereitgestellten Zielgeräten werden die Zuweisungen der Profile auf Ihre werkseitig zugewiesenen Identitäten zurückgesetzt.

Erneutes Bereitstellen von Profilen

Damit die Attributänderungen eines bereits bereitgestellten Profils auf dem zugeordneten Zielgerät wirksam werden, muss es erneut bereitgestellt werden. Bei modularen Geräten können VLAN-Definitionen während der erneuten Bereitstellung konfiguriert werden, jedoch ist die strenge Überprüfung der VLAN-Attribute deaktiviert.

ANMERKUNG: VLAN-Attributsänderungen schlagen während der Neubereitstellung des Profils auf den MX7000-Zielschlitten fehl, wenn die VLAN-Attribute während der Vorlagenbereitstellung nicht über die Option „VLAN-Einstellungen sofort übertragen“ auf den MX7000-Schlitten bereitgestellt wurden.

So stellen Sie Profil(e) erneut bereit:

1. Wählen Sie auf der Seite **Konfiguration** > **Profile** das/die Profil(e) aus, die „bereitgestellt“ und/oder „geändert“ ( ) sind, und klicken Sie auf **Erneut bereitstellen**.
2. Wählen Sie auf der Seite „Bereitstellungsoptionen für Attribute“ des Assistenten für die erneute Bereitstellung eine der folgenden Optionen zum Bereitstellen von Attributen aus und klicken Sie auf **Weiter**:
   - **Nur geänderte Attribute**: um nur die geänderten Attribute auf dem Zielgerät erneut bereitzustellen.
   - **Alle Attribute**: um alle Attribute zusammen mit geänderten Attributen auf dem Zielgerät erneut bereitzustellen.
3. Wählen Sie auf der Seite „Zeitplan“ eine der folgenden Optionen aus:
   - **Jetzt ausführen**, um Änderungen sofort durchzuführen.
   - **Zeitplan aktivieren** und wählen Sie einen Tag und eine Uhrzeit für die Planung der erneuten Bereitstellung aus.
4. Klicken Sie auf **Fertigstellen**, um den Vorgang zu bestätigen.

Wenn ein Profil erneut bereitgestellt wird, wird ein Job zum **Erneuten Bereitstellen von** Profilen ausgeführt. Der Jobstatus kann auf der Seite **Überwachen** > **Jobs** angezeigt werden.

Migrieren eines Profils

Ein bereitgestelltes oder ein automatisch bereitgestelltes Profil kann von seinem vorhandenen Zielgerät oder einem Service-Tag zu einem anderen identischen Zielgerät oder einem anderen Service-Tag migriert werden.

Wenn eine Migration erfolgreich abgeschlossen wurde, gibt die Profil-Zielzuweisung das neue Ziel wieder. Wenn die Migration von einem Zielgerät zu einem noch nicht gesehenen Service-Tag erfolgt, wird der Status des Profils in „Zugewiesen“ geändert.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Benutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Das Migrationsprofil verschiebt die Einstellungen, die vom Profil (einschließlich der bereitgestellten virtuellen Identitäten) definiert sind, von der Quelle zum Ziel.
- Sie können die Migration eines Profils erzwingen, auch wenn das Quellgerät nicht kontaktiert werden kann. In diesem Fall muss der Benutzer sicherstellen, dass keine virtuellen Identitätskonflikte vorhanden sind.
- Die echten zielspezifischen Attribute werden im Rahmen der Migration nicht vom Quellserver zurückgefordert. Aus diesem Grund können dieselben Bestandsaufnahme-Details auf zwei Servern nach der Migration vorhanden sein.

So migrieren Sie ein Profil:

1. Wählen Sie auf der Seite **Konfiguration** > **Profile** ein Profil aus und klicken Sie auf **Migrieren**, um den Assistenten zum Migrieren eines Profils zu aktivieren.
2. Auf der Auswahlseite:
   a. Wählen Sie aus dem Drop-down-Menü **Quellprofil auswählen** das Profil aus, das Sie migrieren möchten.
   b. Klicken Sie auf **Ziel auswählen** und wählen Sie im Dialogfeld „Job-Ziel“ ein Zielgerät aus und klicken Sie auf **OK**.
   c. Aktivieren Sie bei Bedarf das Kontrollkästchen „Migration erzwingen, auch wenn das Quellgerät nicht kontaktiert werden kann“.

      ANMERKUNG: Sie müssen sicherstellen, dass keine virtuellen Identitätskonflikte vorhanden sind.

   d. Klicken Sie auf **Weiter**.
3. Wählen Sie auf der Seite „Terminplan“ eine der folgenden Optionen aus:
   a. Wählen Sie **Jetzt aktualisieren** aus, um die Profileinstellungen sofort zum Ziel zu migrieren.
   b. Wählen Sie einen **Tag** und eine **Uhrzeit** für die Planung der Migration aus.
4. Klicken Sie auf **Fertigstellen**.

Es wird ein Job erstellt, um die Profileinstellungen auf das neue Zielgerät zu migrieren. Sie können den Status des Jobs auf der Seite **Überwachen** > **Jobs** anzeigen.

Profile löschen

Die vorhandenen „nicht zugewiesenen“ Profile können von der Seite **Konfigurationen** > **Profil** gelöscht werden:

ANMERKUNG:

- Ein zugewiesenes oder bereitgestelltes Profil kann nur dann aus dem Profil-Portal gelöscht werden, wenn es nicht zugewiesen ist.
- Wenn Sie ein nicht zugewiesenes Profil löschen, dessen Identitäten reserviert waren, werden diese Identitäten in den Identitäts-Pool zurückgegeben, von dem sie stammen. Es wird empfohlen, 10 Minuten zu warten, bis diese zurückgewonnenen Identitäten für neue Reservierungen und Bereitstellungen verwendet werden.

So löschen Sie nicht zugewiesene Profile:

1. Wählen Sie auf der Seite Profile die nicht zugewiesenen Profile aus.
2. Klicken Sie auf **Löschen** und bestätigen Sie durch Klicken auf **Ja**, wenn Sie dazu aufgefordert werden.

Exportieren von Profildaten als HTML, CSV oder PDF

Zum Exportieren von Profildaten als HTML-, CSV- oder PDF-Datei.

1. Wählen Sie auf der Seite **Konfiguration** > **Profile** das/die Profil(e) aus.
2. Klicken Sie auf **Exportieren** und wählen Sie im Dialogfeld „Exportieren ausgewählt“ zwischen HTML, CSV oder PDF.
3. Klicken Sie auf **Fertigstellen**. Die Profildaten werden im ausgewählten Format heruntergeladen.

13

Verwalten der Device-Konfigurations-Compliance

Durch die Auswahl von **OpenManage Enterprise** > **Konfiguration** > **Konfigurations-Compliance** können Sie die Konfigurations-Compliance-Baselines über Verwendung der integrierten oder vom Benutzer erstellten Vorlagen erstellen. Sie können eine Compliance-Vorlage durch Verwendung einer bestehenden Bereitstellungsvorlage oder eines Referenz-Geräts oder durch Importieren aus einer Datei erstellen. Um diese Funktion zu verwenden, müssen Sie über die Lizenz auf Unternehmensebene von OpenManage Enterprise und iDRAC für Server verfügen. Für Chassis Management Controller ist keine Lizenz erforderlich. Nur Nutzer, die über bestimmte Berechtigungen verfügen, dürfen diese Funktion verwenden. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Wurde eine Konfigurations-Baseline unter Verwendung einer Bereitstellungsvorlage erstellt, wird die Zusammenfassung der Compliance-Stufe für jede Baseline in einer Tabelle aufgelistet. Jedes der Baseline zugeordnete Gerät verfügt über einen eigenen Status, der höchste Schweregrad-Status wird jedoch als Status der Baseline angenommen. Weitere Informationen über den Rollup-Funktionsstatus finden Sie im Whitepaper *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* (VERWALTEN DES ROLLUP-FUNKTIONSSTATUS MITHILFE VON IDRAC AUF DELL EMC-SERVERN DER 14. GENERATION UND NEUER) auf der Support-Seite.

ANMERKUNG: Eine Baseline mit mehreren Geräten kann manchmal dauerhaft als nicht konform angezeigt werden, da einige der Attributwerte nicht notwendigerweise für alle Ziele identisch sind. Beispiel: die Boot-Steuerungs-Attribute, z. B. iSCSI-Ziel-IQN, LUN-ID, FCoE-Ziel-WWPN usw., die nicht für alle Ziele identisch sind und eine permanente Nicht-Compliance der Baseline zur Folge haben können.

Die „Allgemeine Compliance-Zusammenfassung“ zeigt folgende Felder an:

- **COMPLIANCE**: Die Rollup-Compliance-Stufe von Geräten, die zu einer Konfigurations-Compliance-Baseline gehören. Der Gerätestatus mit der geringsten Compliance (z. B. „kritisch") wird immer als Status der ganzen Baseline angezeigt.
- **NAME**: Name der Konfigurations-Compliance-Baseline.
- **VORLAGE**: Der Name des von der Baseline verwendeten Compliance-Status.
- **ZEITPUNKT DER LETZTEN AUSFÜHRUNG**: Datum und Uhrzeit der letzten Ausführung der Compliance-Baseline.

Zur Anzeige des Konfiguration Compliance-Berichts für eine Baseline, markieren Sie das entsprechende Kontrollkästchen und klicken auf **Bericht anzeigen** im rechten Fensterbereich.

Verwenden Sie die Funktion „Abfrage-Generator", um Übereinstimmung mit der ausgewählten Baseline auf Gerätelevel zu generieren. Informationen dazu finden Sie unter Abfragekriterien auswählen auf Seite 58.

OpenManage Enterprise bietet einen integrierten Bericht zum Anzeigen der Liste der überwachten Geräten und deren Compliance mit der Konfigurations-Compliance-Baseline. Wählen Sie **OpenManage Enterprise** > **Überwachung** > **Berichte** > **Geräte nach Vorlagen-Compliance-Baseline** und klicken Sie dann auf **Ausführen**. Informationen dazu finden Sie unter Berichte ausführen auf Seite 141.

Zugehörige Tasks

Konfigurations-Compliance-Baseline erstellen auf Seite 113

Konfigurations-Compliance-Baseline bearbeiten auf Seite 114

Konfigurations-Compliance-Baseline entfernen auf Seite 116

Verwalten von Compliance-Vorlagen auf Seite 111

Abfragekriterien auswählen auf Seite 58

Themen:

Verwalten von Compliance-Vorlagen

Verwenden Sie die Compliance-Vorlage zum Erstellen von Compliance-Baselines und überprüfen Sie dann regelmäßig den Einhaltungsstatus der dieser Baseline zuzuordnenden Device-Konfiguration. Informationen dazu finden Sie unter Verwalten der Device-Konfigurations-Compliance auf Seite 110.

Sie können Compliance-Vorlagen mithilfe der Bereitstellungsvorlage oder mithilfe von Referenzgeräten durch Import aus einer Datei erstellen. Informationen dazu finden Sie unter Verwalten von Compliance-Vorlagen auf Seite 111.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Durch Auswahl von **Konfiguration** > **Konfiguration s-Compliance** > **Vorlagenverwaltung** können Sie die Liste der Compliance-Vorlagen basierend auf Ihrem bereichsbasierten Zugriff in OpenManage Enterprise anzeigen. Ein Administrator kann z. B. alle Compliance-Vorlagen anzeigen und verwalten, ein Geräte-Manager kann hingegen nur die Vorlagen anzeigen und verwalten, die von diesem Geräte-Manager erstellt wurden und in seinem Besitz sind. Auf dieser Seite:

- Können Sie Compliance-Vorlage wie folgt erstellen:
  - Verwenden von Bereitstellungsvorlagen Informationen dazu finden Sie unter Compliance-Vorlage aus Bereitstellungsvorlage erstellen auf Seite 111.
  - Verwenden von Referenzgerät. Informationen dazu finden Sie unter Compliance-Baseline aus Referenzgerät erstellen auf Seite 112.
  - Importieren aus einer Vorlagendatei. Informationen dazu finden Sie unter Compliance-Vorlage durch Importieren aus einer Datei erstellen auf Seite 112.
- Bearbeiten einer Compliance-Vorlage. Informationen dazu finden Sie unter Bearbeiten einer Compliance-Vorlage auf Seite 113.
- Cloning einer Compliance-Vorlage. Informationen dazu finden Sie unter Klonen einer Compliance-Vorlage auf Seite 112.
- Exportieren des Berichts über eine Compliance-Vorlage. Wählen Sie auf der Seite **Compliance-Vorlagen** das entsprechende Kontrollkästchen und klicken Sie auf **Exportieren**. Informationen dazu finden Sie unter Alle oder ausgewählte Daten exportieren auf Seite 68.
- Löschen einer Compliance-Vorlage. Wählen Sie auf der Seite **Compliance-Vorlagen** das entsprechende Kontrollkästchen und klicken Sie auf **Löschen**.

Die Konfigurations-Compliance ist bis auf maximal 6.000-Geräte skalierbar. Gehen Sie wie folgt vor, um eine umfassende Konfigurations-Compliance-Aktivität effizient zu managen:

- Deaktivieren Sie die standardmäßige Konfigurationsbestandsaufnahme-Aufgabe, die automatisch ausgelöst und bei Bedarf manuell ausgeführt wird.
- Erstellen Sie Compliance-Baselines mit einer geringeren Anzahl von Geräten. Zum Beispiel müssen 6.000-Geräte in vier separate Baselines mit jeweils 1.500 Geräten kategorisiert werden.
- Alle Baselines sollten nicht gleichzeitig auf Compliance geprüft werden.

ANMERKUNG: Wenn Sie eine Compliance-Vorlage bearbeiten, wird die Konfigurations-Compliance automatisch auf allen Baselines ausgelöst, denen sie zugeordnet ist. Wenn ein Anwendungsfall häufige Template-Änderungen vorsieht, wird die oben angeführte Skalierungsumgebung nicht unterstützt, und es wird empfohlen, für eine optimale Performance maximal 100 Geräte pro Baseline zuzuordnen.

Zugehörige Informationen

Verwalten der Device-Konfigurations-Compliance auf Seite 110
Konfigurations-Compliance-Baseline bearbeiten auf Seite 114
Konfigurations-Compliance-Baseline entfernen auf Seite 116
Compliance-Vorlage aus Bereitstellungsvorlage erstellen auf Seite 111
Bearbeiten einer Compliance-Vorlage auf Seite 113

Compliance-Vorlage aus Bereitstellungsvorlage erstellen

1. Klicken Sie auf **Konfiguration** > **Konfigurations-Compliance** > **Vorlagenverwaltung** > **Erstellen** > **Von Bereitstellungsvorlage**.
2. Wählen Sie im Dialogfeld **Bereitstellungsvorlage klonen** aus dem Dropdown-Menü **Vorlage** eine Bereitstellungsvorlage, die als Referenz für die neue Vorlage verwendet werden muss.
3. Geben Sie einen Namen und eine Beschreibung für die Compliance-Vorlage ein.
4. Klicken Sie auf **Fertigstellen**.
   Eine Compliance-Vorlage wird erstellt und in der Liste der Compliance-Vorlagen aufgeführt.

Zugehörige Tasks

Verwalten von Compliance-Vorlagen auf Seite 111
Klonen einer Compliance-Vorlage auf Seite 112

Compliance-Baseline aus Referenzgerät erstellen

Um die Konfigurationseigenschaften eines Geräts als Vorlage für die Erstellung einer Konfigurations-Baseline zu verwenden, muss das Gerät bereits integriert sein. Informationen dazu finden Sie unter Onboarding von Geräten auf Seite 45.

1. Klicken Sie auf **Konfiguration** > **Konfigurations-Compliance** > **Vorlagenverwaltung** > **Erstellen** > **Von Referenzgerät**.
2. Geben Sie im Dialogfeld **Compliance-Vorlage erstellen** einen Namen und eine Beschreibung für die Compliance-Vorlage ein.
3. Wählen Sie die Optionen zum Erstellen der Compliance-Vorlage durch Klonen der Eigenschaften eines Servers oder Gehäuses aus.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie im Abschnitt **Referenzgerät** das Gerät aus, das als Referenz für die Erstellung der Compliance-Vorlage verwendet werden soll. Informationen dazu finden Sie unter Zielgeräte und Zielgerätegruppen auswählen auf Seite 136.
   a. Wenn Sie einen Server als Referenz auswählen, müssen Sie auch die Server-Konfigurationseigenschaften auswählen, die geklont werden sollen.
6. Klicken Sie auf **Fertigstellen**.
   Ein Vorlagenerstellungs-Job wurde erstellt und wird ausgeführt. Die neu erstellte Compliance-Vorlage ist auf der Seite **Compliance-Vorlagen** aufgeführt.

Compliance-Vorlage durch Importieren aus einer Datei erstellen

1. Klicken Sie auf **Konfiguration** > **Konfigurations-Compliance** > **Vorlagenverwaltung** > **Erstellen** > **Aus Datei importieren**.
2. Geben Sie im Dialogfeld **Compliance-Vorlage importieren** einen Namen für die Compliance-Vorlage ein.
3. Wählen Sie entweder den Server- oder Gehäuse-Vorlagentyp und klicken Sie auf **Datei auswählen**, um zum Dateispeicherort zu gelangen und treffen Sie eine Wahl.
4. Klicken Sie auf **Fertigstellen**.
   Eine Compliance-Vorlage wird erstellt und aufgeführt.

Klonen einer Compliance-Vorlage

1. Klicken Sie auf **Konfiguration** > **Konfigurations-Compliance** > **Vorlagenverwaltung**.
2. Wählen Sie die zu klonende Konformitäts-Vorlage und klicken Sie dann auf **Klonen**.
3. Im Dialogfeld **Vorlage klonen** geben Sie den Namen der neuen Compliance-Vorlage ein.
4. Klicken Sie auf **Fertigstellen**.
   Die neue Compliance-Vorlage wird erstellt und unter **Konformitäts-Vorlagen** aufgeführt.

Zugehörige Informationen

Compliance-Vorlage aus Bereitstellungsvorlage erstellen auf Seite 111
Bearbeiten einer Compliance-Vorlage auf Seite 113

Bearbeiten einer Compliance-Vorlage

Die Compliance-Vorlagen können auf der Seite **Konfigurations-Compliance** > **Vorlagen** bearbeitet werden. Beim Bearbeiten, Auswählen oder Deaktivieren der Vorlagenattribute werden die in der Vorlage gespeicherten Attribute nicht geändert und alle Attribute sind weiterhin Teil der Vorlage, wenn diese exportiert wird. Dies wirkt sich auf die bereitgestellten Daten aus.

ANMERKUNG:

- Beim Bearbeiten einer Compliance-Vorlage, die bereits anderen Baselines zugeordnet ist, wird automatisch eine Konfigurations-Compliance für alle Geräte in allen Baselines ausgelöst, die die Vorlage verwenden.
- Das Bearbeiten einer Compliance-Vorlage, die mit mehreren Baselines mit einer großen Anzahl von Geräten verknüpft ist, kann zu einem Timeout der Sitzung führen, da die Prüfung der Konfigurations-Compliance für alle zugehörigen Geräte mehrere Minuten dauern kann. Ein Sitzungs-Timeout zeigt Probleme bei den Änderungen an der Compliance-Vorlage nicht an.
- Stellen Sie bei der Bearbeitung einer Compliance-Vorlage auf Großsystemen mit 1.000 oder einer Konfigurationsbestandsaufnahme von maximal 6.000 verwalteten Geräten sicher, dass keine anderen Konfigurationsbestands- oder Compliance-Vorgänge gleichzeitig ausgeführt werden. **Deaktivieren** Sie außerdem den standardmäßig vom System generierten Konfigurations-Bestandsaufnahme-Job auf der Seite **Überwachen** > **Jobs** (Quelle auf systemgeneriert festlegen).
- Für optimale Performance wird empfohlen, dass Sie maximal 1.500 Geräte pro Baseline zuordnen.
- Wenn ein Anwendungsfall häufige Template-Änderungen vorsieht, wird empfohlen, für eine optimale Performance maximal 100 Geräte pro Baseline zuzuordnen.

1. Markieren Sie auf der Seite **Compliance-Vorlagen** das entsprechende Kontrollkästchen und klicken Sie dann auf **Bearbeiten**.
2. Auf der Seite **Vorlagendetails** sind die Konfigurationseigenschaften für die Compliance-Vorlage aufgeführt.
3. Erweitern Sie die Eigenschaft, die Sie bearbeiten möchten, und geben Sie dann Daten ein oder wählen Sie Daten in den Feldern aus.
   a. Um die Eigenschaft zu aktivieren, markieren Sie das Kontrollkästchen, falls dieses nicht bereits aktiviert ist.
4. Klicken Sie auf **Speichern** oder **Verwerfen**, um die Änderungen zu übernehmen oder abzulehnen.
   Die Compliance-Vorlage wird bearbeitet und die aktualisierten Informationen werden gespeichert.

Zugehörige Tasks

Verwalten von Compliance-Vorlagen auf Seite 111
Klonen einer Compliance-Vorlage auf Seite 112

Konfigurations-Compliance-Baseline erstellen

Eine Konfigurations-Compliance-Baseline ist eine Liste von Geräten, die einer Compliance-Vorlage zugeordnet sind. Ein Gerät in OpenManage Enterprise kann 10 Baselines zugewiesen werden. Sie können die Compliance von maximal 250 Geräten auf einmal überprüfen. .

Zum Anzeigen der Liste der Baselines klicken Sie auf **OpenManage Enterprise** > **Konfiguration** > **Konfigurations-Compliance**.

Die Liste der verfügbaren Compliance-Baselines hängt von Ihrer Rolle und Ihren bereichsbasierten Zugriffsberechtigungen in OpenManage Enterprise ab. Ein Administrator kann z. B. alle Compliance-Baselines anzeigen und verwalten, ein Geräte-Manager kann hingegen nur die Compliance-Baselines anzeigen und verwalten, die von diesem Geräte-Manager erstellt wurden und in seinem Besitz sind. Außerdem werden die Zielgeräte, die für die Geräte-Manager verfügbar sind, durch die Geräte/Gerätegruppen eingeschränkt, die im jeweiligen Bereich enthalten sind.

Erstellen können Sie eine Konfigurations-Compliance-Baseline durch:

- Verwendung einer vorhandenen Bereitstellungsvorlage. Informationen dazu finden Sie unter Verwalten der Device-Konfigurations-Compliance auf Seite 110.
- Verwendung einer von einem unterstützten Gerät erfassten Vorlage. Informationen dazu finden Sie unter Compliance-Baseline aus Referenzgerät erstellen auf Seite 112.
- Verwendung einer von einer Datei importierten Vorlage. Informationen dazu finden Sie unter Compliance-Vorlage durch Importieren aus einer Datei erstellen auf Seite 112.

Wenn Sie eine Vorlage für die Erstellung einer Baseline auswählen, werden auch die mit den Vorlagen verbundenen Attribute ausgewählt. Sie können jedoch die Baseline-Eigenschaften bearbeiten. Informationen dazu finden Sie unter Konfigurations-Compliance-Baseline bearbeiten auf Seite 114.

VORSICHT: Wenn eine Compliance-Vorlage, die für eine Baseline verwendet wird, bereits mit einer anderen Baseline verbunden ist, werden durch die Bearbeitung der Vorlageneigenschaften auch die Baseline-Compliance-Stufen der

bereits zugeordneten Geräte geändert. Lesen Sie die angezeigten Fehler- und Ereignismeldungen und handeln Sie entsprechend. Weitere Informationen über die Fehler- und Ereignismeldungen finden Sie im *Referenzhandbuch zu Fehler- und Ereignismeldungen*, das auf der Support-Website verfügbar ist.

ANMERKUNG: Stellen Sie vor dem Erstellen einer Konfigurations-Compliance Baseline sicher, dass Sie die entsprechende Compliance-Vorlage erstellt haben.

1. Wählen Sie **Konfiguration** > **Konfigurations-Compliance** > **Baseline erstellen**.
2. Im Dialogfeld **Compliance-Baseline erstellen**:
   - Im Abschnitt **Baseline-Informationen**:
   a. Wählen Sie aus dem Drop-Down-Menü **Vorlage** eine Compliance-Vorlage aus. Weitere Informationen über Vorlagen finden Sie unter Verwalten der Device-Konfigurations-Compliance auf Seite 110.
   b. Geben Sie einen Compliance-Baseline-Namen und eine Beschreibung ein.
   c. Klicken Sie auf **Weiter**.
   - Im Abschnitt **Ziel**:
   a. Wählen Sie Geräte oder Gerätegruppen aus. Nur kompatible Geräte werden angezeigt. Informationen dazu finden Sie unter Zielgeräte und Zielgerätegruppen auswählen auf Seite 136.

      ANMERKUNG: Nur kompatible Geräte werden gelistet. Wenn Sie eine Gruppe auswählen, werden die Geräte, die nicht kompatibel mit der Compliance-Vorlage sind, oder die Geräte, die die Konfigurations-Compliance-Baseline-Funktion nicht unterstützen, exklusiv identifiziert, um Sie bei einer effektiven Auswahl zu unterstützen.

3. Klicken Sie auf **Fertigstellen**.
   Eine Compliance-Baseline wird erstellt und gelistet. Wenn der Baseline erstellt oder aktualisiert wird, wird ein Compliance-Vergleich initiiert. Der allgemeine Compliance-Grad der Baseline wird in der Spalte **COMPLIANCE** angegeben. Weitere Informationen zu den Feldern in der Liste finden Sie unter Verwalten der Device-Konfigurations-Compliance auf Seite 110.

   ANMERKUNG: Wenn eine Konfigurations-Baseline erstellt wird, wird automatisch ein Konfigurations-Bestandsaufnahme-Job erstellt und von der Appliance ausgeführt, um den Bestand der mit der Baseline verknüpften Geräte zu erfassen, für die keine Bestandsdaten verfügbar sind. Dieser neu erstellte Konfigurations-Bestandsaufnahme-Job hat denselben Namen wie die Baseline, für die die Bestandsaufnahme durchgeführt wird. Außerdem wird auf der Seite „Konfigurations-Compliance" eine Fortschrittsleiste angezeigt, die den Fortschritt des Bestandsaufnahme-Jobs neben der jeweiligen Baseline anzeigt.

Zugehörige Informationen

Verwalten der Device-Konfigurations-Compliance auf Seite 110

Konfigurations-Compliance-Baseline entfernen auf Seite 116

Konfigurations-Compliance-Baseline bearbeiten

Sie können die Geräte, den Namen und andere Eigenschaften, die einer Konfigurations-Baseline zugeordnet sind, bearbeiten. Feldbeschreibungen, die in der Liste angezeigt werden, finden Sie hier: Verwalten der Device-Konfigurations-Compliance auf Seite 110.

VORSICHT: Wenn eine Compliance-Vorlage, die für eine Baseline verwendet wird, bereits mit einer anderen Baseline verbunden ist, werden durch die Bearbeitung der Vorlageneigenschaften auch die Baseline-Compliance-Stufen der bereits zugeordneten Geräte geändert. Informationen dazu finden Sie unter Bearbeiten einer Compliance-Vorlage auf Seite 113. Lesen Sie die angezeigten Fehler- und Ereignismeldungen und handeln Sie entsprechend. Weitere Informationen über die Fehler- und Ereignismeldungen finden Sie im *Referenzhandbuch zu Fehler- und Ereignismeldungen*, das auf der Support-Website verfügbar ist.

1. Wählen Sie **Konfiguration** > **Konfigurations-Compliance**.
2. Aktivieren Sie in der Liste der Baselines der Konfigurations-Compliance das entsprechende Kontrollkästchen und klicken Sie dann auf **Bearbeiten**.
3. Im Dialogfeld **Compliance-Baseline bearbeiten** aktualisieren Sie die Informationen. Informationen dazu finden Sie unter Konfigurations-Compliance-Baseline erstellen auf Seite 113.

   ANMERKUNG: Wenn eine Konfigurations-Baseline bearbeitet wird, wird automatisch ein Konfigurations-Bestandsaufnahme-Job gestartet, um den Bestand der mit der Baseline verknüpften Geräte zu erfassen, für die keine Bestandsdaten verfügbar sind. Dieser neu erstellte Konfigurations-Bestandsaufnahme-Job hat denselben Namen wie die Baseline, für die die Bestandsaufnahme durchgeführt wird. Außerdem wird auf der Seite „Konfigurations-Compliance“ eine Fortschrittsleiste angezeigt, die den Fortschritt des Bestandsaufnahme-Jobs neben der jeweiligen Baseline anzeigt.

Zugehörige Tasks

Verwalten von Compliance-Vorlagen auf Seite 111
Abfragekriterien auswählen auf Seite 58

Zugehörige Informationen

Verwalten der Device-Konfigurations-Compliance auf Seite 110
Konfigurations-Compliance-Baseline entfernen auf Seite 116

Löschen von Konfigurations-Compliance-Baselines

Sie können die Konfigurations-Compliance-Baselines auf der Seite **Konfiguration** > **Konformitäts-Compliance** löschen und die Geräte von den zugehörigen Baselines trennen.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Siehe Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

So löschen Sie die Konfigurations-Compliance-Baselines:

1. Wählen Sie die Baseline(s) aus den Baselines, die auf der Konfigurations-Compliance-Seite aufgeführt sind.
2. Klicken Sie auf **Löschen** und klicken Sie in der Bestätigungsaufforderung auf **Ja**.

Die gelöschten Konfigurations-Baselines werden von der Konfigurations-Compliance-Seite entfernt.

Aktualisieren der Compliance der Konfigurations-Compliance-Baselines

Die Überprüfung des Compliance-Status einer Compliance-Baseline wird automatisch ausgelöst, wenn Änderungen an den Attributen der Baseline-Referenzvorlage vorgenommen werden oder wenn eine Änderung an der Konfigurations-Bestandsaufnahme von einem der Baseline-assoziierten Geräte vorliegt.

Der Compliance-Status einer Konfigurations-Compliance-Baseline ist eine Rollup-Compliance-Stufe der Geräte, die mit dieser Konfigurations-Compliance-Baseline verbunden sind. Der Gerätestatus mit der geringsten Compliance (z. B. „kritisch") wird immer als Status der ganzen Baseline angezeigt.

Die allgemeine Compliance-Zusammenfassung aller Konfigurations-Baselines wird in einem Ringdiagramm über dem Baseline-Raster dargestellt. Das Datum und die Uhrzeit der letzten Ausführung der Compliance werden unterhalb des Diagramms angezeigt.

Die Überprüfung des Compliance-Status bei großen Baselines kann einige Minuten dauern. Sie können jedoch auf **Compliance aktualisieren** klicken, um eine allgemeine Compliance-Zusammenfassung der Geräte nach Bedarf abzurufen, während die großen Baseline-Compliance-Jobs ausgeführt werden.

ANMERKUNG: Wenn die Konfigurations-Compliance den Status „Wird ausgeführt“ hat, ist es nicht zulässig, neue Jobs zu initiieren, die sich auf Baselines auswirken, z. B. die Bearbeitung einer Compliance-Vorlage oder Baseline.

Gehen Sie wie folgt vor, um eine Aktualisierung der allgemeinen Compliance-Zusammenfassung aller Baselines zu initiieren:

1. Klicken Sie auf **Konfiguration** > **Konfigurations-Compliance**, woraufhin die Seite „Konfigurations-Compliance“ angezeigt wird.
2. Klicken Sie auf **Compliance aktualisieren**.

Der Compliance-Aktualisierungs-Job (Compliance-Zusammenfassung laden) wird initiiert. Die allgemeine Compliance-Zusammenfassung wird in diesem Moment angezeigt und die Zeit der letzten Ausführung der Compliance wird aktualisiert.

Warten von nicht übereinstimmenden Geräten

Auf der Seite „Compliance-Bericht“ einer Baseline können Sie die Geräte warten, die nicht mit der zugehörigen Baseline übereinstimmen, indem Sie die Attributwerte so ändern, dass sie mit den zugehörigen Baseline-Attributen übereinstimmen.

Auf der Seite „Compliance-Bericht“ werden die folgenden Felder für die Zielgeräte angezeigt, die der Compliance-Vorlagen-Baseline zugeordnet sind:

- **COMPLIANCE**: Der Gerätestatus mit der geringsten Konformität (z. B. „kritisch") wird immer als Status des Geräts angezeigt.
- **GERÄTENAME**: Der Name des Zielgeräts, das der Baseline zugeordnet ist.
- **IP ADRESSE**: Die IP-Adresse des Zielgeräts an.
- **TYP**: Typ des zugeordneten Zielgeräts.
- **MODELL**: Modellname des Zielgeräts.
- **SERVICE-TAG**: Die Service-Tag-Nummer des Zielgeräts.
- **ZEITPUNKT DER LETZTEN AUSFÜHRUNG**: Datum und Uhrzeit der letzten Ausführung der Compliance-Baseline.

Sie können die erweiterten Filter verwenden, um nicht konforme Geräte schnell anzuzeigen. Außerdem können die Optionen „Alle auswählen“ and Sortiierung für Konfigurations-Compliance-Ergebnisse verwendet werden. Um die Filter zurückzusetzen, klicken Sie auf **Alle Filter löschen**.

Um abweichende Attribute eines nicht konformen Zielgeräts anzuzeigen, wählen Sie das Gerät aus und klicken auf **Bericht anzeigen**. In der Tabelle **Compliance-Bericht** sind die Attributnamen des entsprechenden Zielgeräts mit den erwarteten und den aktuellen Werten der Attribute aufgelistet.

So warten Sie ein oder mehrere nicht übereinstimmende Geräte:

1. Wählen Sie **Konfiguration** > **Konfigurations-Compliance**.
2. Wählen Sie aus der Liste der Baselines der Konfigurations-Compliance das entsprechende Kontrollkästchen aus und klicken Sie dann auf **Bericht anzeigen**.
3. Wählen Sie aus der Liste der nicht übereinstimmenden Geräte eines oder mehrere Geräte aus und klicken Sie dann auf **Übereinstimmend machen**.
4. Planen Sie die Konfigurationsänderungen für eine sofortige oder spätere Ausführung und klicken Sie dann auf **Fertigstellen**.

   Um die Konfigurationsänderungen nach dem nächsten Neustart des Servers anzuwenden, wählen Sie die Option **Geräte-Konfigurationsänderungen beim nächsten Neustart einplanen**.

Eine neue Bestandsaufnahme für die Device-Konfiguration wird ausgeführt und der Compliance-Status der Baseline wird auf der Seite **Compliance** aktualisiert.

Exportieren des Compliance-Baseline-Berichts

Eine vollständige oder unvollständige Liste der Geräte, die einer Compliance-Vorlagen-Baseline zugeordnet sind, kann in eine CSV-Datei exportiert werden.

Seite „Compliance-Bericht“ einer Konfigurations-Baseline

1. Klicken Sie auf **Alle exportieren**, um Details aller Geräte in der Compliance-Baseline zu exportieren. Oder:
2. Klicken Sie nach Auswahl der einzelnen Geräte im Bericht auf **Ausgewählte exportieren** .

Konfigurations-Compliance-Baseline entfernen

Sie können die Konfigurations-Kompatibilitäts-Ebene der Geräte in Verbindung mit einer Konfigurations-Baseline entfernen. Feldbeschreibungen, die in der Liste angezeigt werden, finden Sie hier: Verwalten der Device-Konfigurations-Compliance auf Seite 110.

VORSICHT: Beim Löschen einer Kompatibilitäts-Baseline oder von Geräten aus der Kompatibilitäts-Baseline passiert Folgendes:

- **Die Kompatibilitätsdaten der Baseline und/oder der Geräte werden aus den OpenManage Enterprise-Daten gelöscht.**
- **Wenn ein Gerät entfernt wird, wird dessen Konfigurationsbestand nicht mehr abgerufen und die bereits abgerufenen Informationen werden gelöscht, außer wenn der Bestand einem Inventarjob zugeordnet wurde.**

Eine Compliance-Vorlage, die als Kompatibilitäts-Baseline verwendet wird, kann nicht gelöscht werden, wenn diese einem Gerät zugeordnet ist. In diesen Fällen werden entsprechende Meldungen angezeigt. Lesen Sie die angezeigten Fehler- und Ereignismeldungen und unternehmen Sie entsprechende Maßnahmen. Weitere Informationen über die Fehler- und Ereignismeldungen finden Sie im *Referenzhandbuch zu Fehler- und Ereignismeldungen*, das auf der Support-Website verfügbar ist.

1. Klicken Sie auf **Konfiguration** > **Konfigurations-Compliance**.
2. Aktivieren Sie in der Liste der Konfigurations-Kompatibilitäts-Baselines das entsprechende Kontrollkästchen und klicken Sie dann auf **Löschen**.
3. Wenn Sie gefragt werden, ob Sie die Option löschen möchten, klicken Sie auf **JA**.

Die Kompatibilitäts-Baseline wird gelöscht und die Tabelle **Gesamte Kompatibilitätszusammenfassung** der Baselines wird aktualisiert.

Zugehörige Tasks

Konfigurations-Compliance-Baseline erstellen auf Seite 113
Abfragekriterien auswählen auf Seite 58
Verwalten von Compliance-Vorlagen auf Seite 111
Konfigurations-Compliance-Baseline bearbeiten auf Seite 114

Zugehörige Informationen

Verwalten der Device-Konfigurations-Compliance auf Seite 110

14

Überwachen und Verwalten von Gerätewarnungen

Wenn Sie **OpenManage Enterprise** > **Warnmeldungen** auswählen, können Sie Warnmeldungen anzeigen und verwalten, die von den Geräten in der Management-Systemumgebung generiert wurden. Die Seite „Warnmeldungen" wird mit folgenden Registerkarten angezeigt:

- **Warnungsprotokoll**: Sie können alle Warnungen anzeigen und verwalten, die auf den Zielgeräten generiert wurden.
- **Warnungsrichtlinien**: Sie können Warnungsrichtlinien erstellen, um Warnmeldungen zu senden, die auf Zielgeräten generiert wurden, z. B. E-Mail, Mobilgeräte, Syslog-Server usw.
- **Definitionen von Warnmeldungen**: Sie können Warnmeldungen anzeigen, die für Fehler oder zu Informationszwecken generiert wurden.

ANMERKUNG:

- Zum Verwalten und Überwachen von Gerätewarnmeldungen in OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Warnungsrichtlinien und Warnungsprotokolle unterliegen Ihrem bereichsbasierten Zugriff in OpenManage Enterprise. Ein Administrator kann z. B. alle Warnungsrichtlinien anzeigen und verwalten, ein Geräte-Manager kann hingegen nur Standard-Warnungsrichtlinien und die Richtlinien anzeigen und verwalten, die von diesem Geräte-Manager erstellt wurden und in seinem Besitz sind. Außerdem können die Geräte-Manager nur die Warnmeldungen für die Geräte anzeigen, die in ihrem Bereich enthalten sind.
- Momentan werden nur die SNMPv1- und SNMPv2-Warnungen von OpenManage Enterprise von den folgenden PowerEdge-Servern empfangen: MX840c und MX5016s.
- OpenManage Enterprise bietet einen integrierten Bericht, um die Liste der von OpenManage Enterprise überwachten Geräte und die für jedes Gerät erzeugten Alarme anzuzeigen. Klicken Sie auf **OpenManage Enterprise** > **Überwachen** > **Berichte** > **Anzahl der Warnmeldungen pro Gerätebericht**. Klicken Sie auf **Ausführen**. Siehe . Berichte ausführen auf Seite 141

Zugehörige Konzepte

Anzeigen von Warnungsprotokollen auf Seite 118

Themen:

Anzeigen von Warnungsprotokollen

Die Seite **Warnungsprotokoll** zeigt die Liste der Warnungsprotokolle für Ereignisse an, die in den Geräten stattfinden. Klicken Sie in OpenManage Enterprise auf **Warnungen** > **Warnungsprotokoll**. Die Seite **Warnungsprotokoll** wird angezeigt.

Standardmäßig werden nur unbestätigte Warnungen angezeigt. Sie können die Liste der Warnungen anpassen, entweder mit **Erweiterte Filter** links oberhalb der Warnungsliste oder durch Ändern der **Anzeigeeinstellungen für Warnmeldungen** auf der Seite **Anwendungseinstellungen**. Informationen dazu finden Sie unter Anpassen der Warnungsanzeige auf Seite 167. Sie können die Warnungsdetails wie folgt anzeigen:

- **Bestätigen**: Wenn die Warnmeldung bestätigt wurde, wird ein Häkchen unter **Bestätigen** angezeigt. Klicken Sie zwischen den eckigen Klammern unter **BESTÄTIGEN**, um eine Warnmeldung zu bestätigen oder die Bestätigung aufzuheben.
- **Zeit**: Die Zeit, zu der die Warnmeldung generiert wurde.
- **Quellname**: Betriebssystem-Hostname des Geräts, das die Warnmeldung generiert hat. Klicken Sie auf den Quellnamen, um die Eigenschaften des Geräts anzuzeigen und zu konfigurieren.

ANMERKUNG: Warnungen können nicht basierend auf der IP-Adresse (Quellname) gefiltert werden, wenn die Warnung von einem nicht erkannten Gerät erzeugt wird oder im Falle einer internen Warnung.

- **Kategorie**: Die Kategorie gibt den Typ der Warnmeldung an. Wie zum Beispiel Systemzustand und Überwachung.
- **Meldungs-ID**: Die ID der erzeugten Warnmeldung.
- **Meldung**: Die erzeugte Warnmeldung.
- Das Feld auf der rechten Seite enthält zusätzliche Informationen wie die ausführliche Beschreibung und die empfohlene Maßnahme für eine ausgewählte Warnmeldung.

ANMERKUNG: OpenManage Enterprise 3.2 ermöglicht die Verfolgung des Datenpunkts **Zuletzt aktualisiert von**. In den vorhergehenden Versionen wurde dies jedoch nicht aufgezeichnet. Beachten Sie daher, dass die Warnmeldungen der vorherigen Versionen nicht angezeigt werden, wenn das Warnungsprotokoll mit dem erweiterten Filterfeld **Benutzer** gefiltert wird.

Wählen Sie eine Warnmeldung aus, um zusätzliche Informationen wie die ausführliche Beschreibung und die empfohlene Maßnahme auf der rechten Seite der Seite „Warnungsprotokoll" anzuzeigen. Auf der Seite Warnungsprotokoll können Sie auch folgende Aufgaben ausführen:

- Warnung bestätigen
- Warnungen nicht bestätigen
- Warnungen ignorieren
- Warnungen exportieren
- Warnungen löschen
- Archivierte Warnungen

Zugehörige Informationen

Überwachen und Verwalten von Gerätewarnungen auf Seite 118

Warnungsprotokolle verwalten

Wenn Warnungsprotokolle generiert und auf der Seite **Warnungsprotokoll** angezeigt werden, können Sie diese bestätigen, ablehnen, ignorieren, exportieren, löschen und archivieren.

Warnung bestätigen

Nachdem Sie eine Warnung angezeigt und ein Verständnis ihres Inhalts erlangt haben, können Sie bestätigen, dass Sie die Warnungsmeldung gelesen haben. Das Bestätigen einer Warnung verhindert die Speicherung 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.

Zum Bestätigen einer Warnung auf der Seite **Warnungsprotokoll** aktivieren Sie das Kontrollkästchen der entsprechenden Warnmeldung und klicken Sie dann auf **Bestätigen**.

Ein Häkchen wird in der Spalte **BESTÄTIGEN** angezeigt. Nachdem eine Warnung bestätigt wurde, wird das Feld **Letzte Aktualisierung von** im Abschnitt "Warnmeldungsdetails" ausgefüllt.

Warnungen 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.

Um die Bestätigung für Warnmeldungen zurückzunehmen, aktivieren Sie das Kontrollkästchen der entsprechenden Warnmeldungen und klicken Sie dann auf **Nicht bestätigen**. Andernfalls können Sie auf das Häkchen klicken, um die Bestätigung der Warnung zurückzunehmen.

ANMERKUNG: Das Feld **Zuletzt aktualisiert von** im Abschnitt mit den Warnmeldungsdetails enthält den Nutzernamen des Benutzers, der die Warnmeldung zuletzt bestätigt hat.

Warnungen ignorieren

Durch das Ignorieren einer Warnung wird eine Warnungsrichtlinie erstellt, die aktiviert ist, und alle zukünftigen Vorkommen dieser Warnung werden verworfen. Aktivieren Sie das Kontrollkästchen der entsprechenden Warnmeldung und klicken Sie dann auf **Ignorieren**. Eine Meldung wird angezeigt, dass ein Job zum Ignorieren der ausgewählten Warnung erstellt wird. Die Gesamtzahl der Warnungen, die in der Kopfzeile von OpenManage Enterprise angezeigt werden, wird verringert.

Warnungen exportieren

Sie können Warnungsprotokolle im Format .csv auf eine Netzwerkfreigabe oder ein lokales Laufwerk Ihres Systems exportieren.

Zum Exportieren von Warnungsprotokollen 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.

Warnungen löschen

Sie können eine Warnung löschen, um dieses Vorkommen der Warnung von der Konsole zu entfernen.

Aktivieren Sie das Kontrollkästchen der entsprechenden Warnung und klicken Sie dann auf **Löschen**. Sie werden dazu aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf **Ja**, um die Warnmeldung zu löschen. Die Gesamtzahl der Warnungen, die in der Kopfzeile von OpenManage Enterprise angezeigt werden, wird verringert.

Archivierte Warnungen anzeigen

Es können maximal 50.000 Warnmeldungen in OpenManage Enterprise generiert und eingesehen werden. Wenn die Grenze von 95 % der 50.000 Warnungen (47.500) erreicht ist, erzeugt OpenManage Enterprise eine interne Meldung, die darauf hinweist, dass OpenManage Enterprise bei Erreichen der Anzahl von 50.000 Warnungen 10 % der archivierten Warnungen (5000 Warnungen) automatisch löscht. Die Tabelle zeigt die verschiedenen Szenarien zum Löschen von Warnungen an.

Tabelle 20. Dauerhaftes Löschen von Warnungen

Workflow	Beschreibung	Ergebnis
Löschaufgabe	Wird alle 30 Minuten in der Konsole ausgeführt.	Wenn die Warnungen ihre maximale Kapazität erreicht haben (d. h. 50 000), überprüfen und generieren Sie die Bereinigungsarchive.
Warnmeldung zum Löschen von Warnungen	Erzeugt eine interne Warnmeldung zum Löschen von Warnungen.	Wenn die Warnungen mehr als 95% (475 000) überschritten haben, wird eine interne Lösch-Warnung generiert, um 10% der Warnungen zu bereinigen.
Löschen von Warnungen	Warnungen werden aus dem Warnungsprotokoll gelöscht.	Wenn die Anzahl der Warnungen zu mehr als 100% überschritten wurden, werden 10% der alten Warnungen endgültig gelöscht, um wieder auf den Stand von 90% (45 000) zurückzukehren.
Gelöschte Warnungen herunterladen	Laden Sie die gelöschten Warnungen herunter.	Archive der letzten fünf gelöschten Warnungen können aus dem Archiv der Warnungen heruntergeladen werden.

Archivierte Warnungen herunterladen

Archivierte Warnungen sind die ältesten 10 % der Warnungen (5000), die endgültig gelöscht werden, wenn die Warnungen 50.000 überschreiten. Diese ältesten 5000 Warnungen werden aus der Tabelle entfernt und in einer .CSV-Datei gespeichert und anschließend archiviert. So laden Sie die Datei der archivierten Warnungen herunter:

1. Klicken Sie auf **Archivierte Warnungen**.

Im Dialogfeld **Archivierte Warnungen** werden die letzten fünf gelöschten archivierten Warnungen angezeigt. Dateigröße, Name, und Datum der Archivierung werden angegeben.

2. Aktivieren Sie das Kontrollkästchen für die entsprechende Warnungsdatei und klicken Sie auf **Fertig stellen**. Die .CSV-Datei wird an den ausgewählten Speicherort heruntergeladen.

ANMERKUNG: Zum Herunterladen archivierter Warnmeldungen müssen Sie über die erforderlichen Berechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Warnungsrichtlinien

In diesem Thema wird das Konzept der Warnungsrichtlinien erklärt und erläutert, inwiefern sie nützlich sein können. Eine Anleitung zum Erstellen, Bearbeiten, Aktivieren, Deaktivieren und Löschen von Warnungsrichtlinien finden Sie unter *Konfigurieren und Verwalten von Warnungsrichtlinien*.

Mit Warnungsrichtlinien können Sie spezielle Warnmeldungen für bestimmte Geräte oder Komponenten an ein bestimmtes Ziel konfigurieren und senden, z. B. E-Mail, Mobilgeräte, Syslog-Server usw. Warnmeldungen helfen Ihnen bei der effektiven Überwachung und Verwaltung von Geräten.

Verwenden Sie Warnungsrichtlinien, um die folgenden Funktionen auszuführen:

- Aktionen automatisch basierend auf der Eingabe einer Warnung auslösen.
- Eine Warnmeldung an eine E-Mail-Adresse senden.
- Eine Warnmeldung an ein Telefon per SMS oder Benachrichtigung senden.
- Eine Warnmeldung über einen SNMP-Trap versenden.
- Eine Warnmeldung an einen Syslog-Server senden.
- Aktionen zur Gerätestromregelung wie das Einschalten oder Ausschalten eines Geräts durchführen, wenn eine Warnmeldung einer vordefinierten Kategorie erstellt wird.
- Ein Remote-Skript ausführen.

Zum Anzeigen, Erstellen, Bearbeiten, Aktivieren, Deaktivieren und Löschen von Warnungsrichtlinien klicken Sie auf **Warnmeldungen** > **Warnungsrichtlinien**.

Zugehörige Tasks

Konfigurieren und Verwalten von Warnungsrichtlinien auf Seite 121

Konfigurieren und Verwalten von Warnungsrichtlinien

In diesem Thema erhalten Sie Anweisungen zum Erstellen, Bearbeiten, Aktivieren, Deaktivieren und Löschen von Warnungsrichtlinien.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Zugehörige Informationen

Warnungsrichtlinien auf Seite 121
Auditprotokolle an Remote-Syslog-Server weiterleiten auf Seite 123

Erstellen einer Warnungsrichtlinie

Sie können Warnungsrichtlinien erstellen und aktivieren, um Warnmeldungen an E-Mail-Adresse, Telefonnummer oder SNMP-Traps zu senden und Gerätesteuerungsmaßnahmen auszuführen, wie z. B. das Ein- oder Ausschalten eines Geräts und das ordnungsgemäße Herunterfahren, wenn eine Warnmeldung einer vordefinierten Kategorie generiert wird.

ANMERKUNG: Nach dem Upgrade auf Version 3.5 werden alle Warnungsrichtlinien, die von Geräte-Managern von einer der vorherigen OpenManage Enterprise-Versionen erstellt wurden, nur dem Administrator zugewiesen. Die Geräte-Manager müssen daher die Warnungsrichtlinien nach dem Upgrade neu erstellen, um weiterhin Warnungen zu erhalten.

Klicken Sie auf der Seite **Warnmeldungen** > **Warnungsrichtlinien** auf **Erstellen** und gehen Sie folgendermaßen vor:

1. Geben Sie den Namen sowie eine Beschreibung für die Warnungsrichtlinie ein und klicken Sie auf **Weiter**. Das Kontrollkästchen **Richtlinie aktivieren** ist standardmäßig aktiviert.
2. Wählen Sie die Warnungskategorie aus, indem Sie eine oder alle integrierten und importierten Kategorien der Drittanbieter-Management-Informationsbasis (MIB) auswählen.

   Sie können jede Kategorie erweitern, um Unterkategorien anzuzeigen und auszuwählen. Weitere Informationen über Kategorien und Unterkategorien finden Sie unter Warnungsdefinitionen auf Seite 126.
3. Wählen Sie die Geräte oder Gruppen aus, für die eine Warnmeldung erforderlich ist, und klicken Sie auf **Weiter**. Eine Warnmeldung kann angewendet werden für:
   - Ein Gerät oder Geräte.
   - Eine Gruppe oder Gruppen von Geräten.
   - Ein angegebenes nicht erkanntes Gerät durch Eingabe von IP-Adresse oder Hostname.
   - Alle nicht erkannten Geräte.

     ANMERKUNG: Die Aufgaben „Remote-Skriptausführung“ und „Strom-Maßnahme“ können nicht auf den nicht erkannten Geräten ausgeführt werden.

     ANMERKUNG: Warnungen von SNMPv1-, SNMPv2- und SNMPv3-Protokollen, die von solchen nicht erkannten (fremden) Geräten gesendet werden, werden von OpenManage Enterprise nicht erkannt.
4. (Optional) Geben Sie die Dauer an, für die die Warnungsrichtlinie gelten soll, indem Sie die erforderlichen Werte für **Datumsbereich**, **Zeitintervall** und **Tage** auswählen, und klicken Sie dann auf **Weiter**.
5. Wählen Sie den Schweregrad der Warnmeldung aus und klicken Sie auf **Weiter**.

   Um alle Schweregradkategorien auswählen, aktivieren Sie das Kontrollkästchen **Alle**.
6. Wählen Sie eine oder mehrere Warnungsmaßnahmen aus und klicken Sie auf **Weiter**. Folgende Optionen stehen zur Verfügung:
   - E-Mail – Wählen Sie „E-Mail“, um eine E-Mail an einen festgelegten Empfänger zu senden, indem Sie Informationen für jedes Feld angeben und bei Bedarf für den Betreff und die Nachricht Token verwenden. Siehe Token-Ersetzung in Remote-Skripts und Warnmeldungsrichtlinien auf Seite 184

     ANMERKUNG: E-Mails für mehrere Warnmeldungen mit derselben Kategorie, derselben Meldungs-ID und demselben Inhalt werden nur einmal alle 2 Minuten ausgelöst, um wiederholte/redundante Warnmeldungen im Posteingang zu vermeiden.
   - SNMP-Trap-Weiterleitung (Aktivieren) – Klicken Sie auf Aktivieren, um das Fenster SNMP-Konfiguration anzuzeigen. Dort können Sie die SNMP-Einstellungen für die Warnung konfigurieren. Informationen dazu finden Sie unter SMTP-, SNMP- und Syslog-Warnungen konfigurieren auf Seite 124.
   - Syslog (Aktivieren) – Klicken Sie auf Aktivieren, um das Fenster Syslog -Konfiguration anzuzeigen. Dort können Sie die Syslog -Einstellungen für die Warnung konfigurieren. Informationen dazu finden Sie unter SMTP-, SNMP- und Syslog-Warnungen konfigurieren auf Seite 124.
   - Aktivieren Sie das Kontrollkästchen Ignorieren, um die Warnmeldung zu ignorieren und die Warnungsrichtlinie nicht zu aktivieren.
   - Senden Sie eine SMS an eine angegebene Telefonnummer.
   - Stromsteuerung – Wählen Sie das Kontrollkästchen „Stromsteuerung“, um die Maßnahmen anzuzeigen, mit denen Sie ein Gerät einschalten, ausschalten, aus- und einschalten und ordnungsgemäß herunterfahren können. Um ein Betriebssystem vor der Durchführung von Stromsteuerungsmaßnahmen herunterzufahren, aktivieren Sie das Kontrollkästchen **Zuerst BS herunterfahren**.
   - Remote-Skriptausführung (Aktivieren) – Klicken Sie auf „Aktivieren“, um das Fenster „Remote-Befehl Einstellung“ anzuzeigen, in dem Sie Remote-Befehle auf Remote-Nodes hinzufügen und ausführen können. Weitere Informationen über das Hinzufügen von Remote-Befehlen finden Sie unter Befehle und Skripts ausführen auf Seite 125.

     Wählen Sie aus dem Dropdown-Menü das Skript aus, das ausgeführt wird, wenn diese Warnungsrichtlinie ausgeführt wird. Sie können die Ausführung des Remote-Befehls auch einrichten wie hier beschrieben Verwalten von OpenManage Enterprise-Geräteeinstellungen auf Seite 148.
   - Senden Sie eine Benachrichtigung an das für OpenManage Enterprise registrierte Mobiltelefon. Informationen dazu finden Sie unter OpenManage Mobile-Einstellungen auf Seite 177.
7. Überprüfen Sie die Details der erstellten Warnungsrichtlinie auf der Registerkarte „Zusammenfassung“ und klicken Sie auf **Fertigstellen**.
   Die Warnungsrichtlinie wurde erfolgreich erstellt und wird im Abschnitt **Warnungsrichtlinien** aufgeführt.

Verwalten von Warnungsrichtlinien

Nachdem Warnungsrichtlinien auf der Seite **Warnungsrichtlinien** erstellt wurden, können Sie sie bearbeiten, aktivieren, deaktivieren und löschen. OME bietet außerdem integrierte Warnungsrichtlinien, die zugehörige Aktionen auslösen, wenn die Warnmeldung empfangen wird. Sie können die integrierten Warnungsrichtlinien nicht bearbeiten oder löschen, Sie können sie jedoch aktivieren oder deaktivieren.

Um die erstellten Warnungsrichtlinien anzuzeigen, klicken Sie auf **Warnungen** > **Warnungsrichtlinien**.

Um alle Warnungsrichtlinien auszuwählen, markieren Sie das Kontrollkästchen links neben **Aktiviert**. Wählen Sie ein oder mehrere Kontrollkästchen neben der Warnungsrichtlinie aus, um die folgenden Aktionen durchzuführen:

- **Warnungsrichtlinie bearbeiten**: Wählen Sie eine Warnungsrichtlinie aus und klicken Sie auf **Bearbeiten**, um die erforderlichen Informationen im Konfigurieren und Verwalten von Warnungsrichtlinien auf Seite 121-Dialogfeld zu bearbeiten.

  ANMERKUNG: Es kann jeweils nur eine Warnungsrichtlinie bearbeitet werden.

  ANMERKUNG: Das Kontrollkästchen Zeitintervall ist für Warnungsrichtlinien auf OpenManage Enterprise-Versionen vor Version 3.3.1 standardmäßig deaktiviert. Aktivieren Sie nach dem Upgrade das Zeitintervall und aktualisieren Sie die Felder, um die Richtlinien erneut zu aktivieren.

- **Warnungsrichtlinien aktivieren**: Wählen Sie die Warnungsrichtlinie aus und klicken Sie auf **Aktivieren**. Ein Häkchen wird in der Spalte **Aktiviert** angezeigt, wenn eine Warnungsrichtlinie aktiviert ist. Die Schaltfläche **Aktivieren** einer bereits aktivierten Warnungsrichtlinie ist ausgegraut.
- **Warnungsrichtlinien deaktivieren**: Wählen Sie die Warnungsrichtlinie aus und klicken Sie auf **Deaktivieren**. Die Warnungsrichtlinie wird deaktiviert und das Häkchen in der Spalte **AKTIVIERT** wird entfernt.

  Sie können auch eine Warnungsrichtlinie beim Erstellen deaktivieren, indem Sie das Kontrollkästchen **Richtlinie aktivieren** im Abschnitt „Name und Beschreibung" deaktivieren.

- **Warnungsrichtlinien löschen**: Wählen Sie die Warnungsrichtlinie aus und klicken Sie auf **Löschen**.

  Sie können mehrere Warnungsrichtlinien gleichzeitig löschen, indem Sie die jeweiligen Kontrollkästchen aktivieren. Um alle Kontrollkästchen auszuwählen und zu löschen, aktivieren oder deaktivieren Sie das Kontrollkästchen in der Kopfzeile neben **AKTIVIERT**.

Auditprotokolle an Remote-Syslog-Server weiterleiten

Um alle Auditprotokolle von OpenManage Enterprise von Syslog-Servern aus zu überwachen, können Sie eine Warnrichtlinie erstellen. Alle Auditprotokolle, z. B. Anmeldeversuche für Benutzer, das Erstellen von Warnrichtlinien und das Ausführen verschiedener Jobs, können an Syslog-Server weitergeleitet werden.

So erstellen Sie eine Warnungsrichtlinie zum Weiterleiten von Auditprotokollen an Syslog-Server:

1. Wählen Sie **Warnungen** > **Warnungsrichtlinien** > **Erstellen**.
2. Geben Sie im Dialogfeld **Warnungsrichtlinie erstellen** im Abschnitt **Name und Beschreibung** einen Namen und eine Beschreibung der Warnungsrichtlinie ein.
   a. Das Kontrollkästchen **Richtlinie aktivieren** ist standardmäßig aktiviert, um anzugeben, dass die Warnungsrichtlinie aktiviert wird, sobald sie erstellt wurde. Deaktivieren Sie das Kontrollkästchen, um die Warnungsrichtlinie zu deaktivieren. Weitere Informationen zum Aktivieren von Warnungsrichtlinien zu einem späteren Zeitpunkt finden Sie unter Konfigurieren und Verwalten von Warnungsrichtlinien auf Seite 121.
   b. Klicken Sie auf **Weiter**.
3. Erweitern Sie im Abschnitt **Kategorie** den Eintrag **Anwendung** und wählen Sie die Kategorien und Unterkategorien der Appliance-Protokolle aus. Klicken Sie auf **Weiter**.
4. Im Bereich **Ziel** ist die Option **Geräte auswählen** standardmäßig ausgewählt. Klicken Sie auf **Geräte auswählen** und wählen Sie im linken Bereich Geräte aus. Klicken Sie auf **Weiter**.

   ANMERKUNG: Die Auswahl von Zielgeräten oder -gruppen ist bei der Weiterleitung der Auditprotokolle an den Syslog-Server nicht möglich.

5. (Optional) Die Warnungsrichtlinien sind standardmäßig immer aktiv. Wählen Sie zur Einschränkung der Aktivität im Abschnitt **Datum und Uhrzeit** das Start- und Enddatum aus und wählen Sie dann den Zeitraum.
   a. Aktivieren Sie die Kontrollkästchen der entsprechenden Tage, an denen die Warnungsrichtlinien ausgeführt werden sollen.
   b. Klicken Sie auf **Weiter**.
6. Wählen Sie im Abschnitt **Schweregrad** den Schweregrad der Warnungen aus, für die diese Richtlinie aktiviert sein muss.
   a. Um alle Schweregradkategorien auswählen, aktivieren Sie das Kontrollkästchen **Alle**.
   b. Klicken Sie auf **Weiter**.
7. Wählen Sie unter **Aktionen** den Punkt **Syslog** aus.

   Wenn Syslog-Server nicht in OpenManage Enterprise konfiguriert sind, klicken Sie auf **Aktivieren** und geben Sie die Ziel-IP-Adresse oder den Hostnamen der Syslog-Server ein. Weitere Informationen zum Konfigurieren der Syslog-Server finden Sie unter SMTP-, SNMP- und Syslog-Warnungen konfigurieren auf Seite 124.

8. Klicken Sie auf **Weiter**.

9. Im Abschnitt **Zusammenfassung** werden die Details der Warnungsrichtlinie angezeigt, die Sie definiert haben. Lesen Sie die Informationen sorgfältig durch.
10. Klicken Sie auf **Fertigstellen**.

Die Warnungsrichtlinie wurde erfolgreich erstellt und wird im Abschnitt **Warnungsrichtlinien** aufgeführt.

Zugehörige Tasks

Konfigurieren und Verwalten von Warnungsrichtlinien auf Seite 121
Überwachen von Auditprotokollen auf Seite 127

SMTP-, SNMP- und Syslog-Warnungen konfigurieren

Indem Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Warnungen** klicken, können Sie die E-Mail-Adresse (SMTP) konfigurieren, die Systemwarnungen, SNMP-Warnungs-Weiterleitungsziele und die Syslog-Weiterleitungseigenschaften empfängt. Zum Verwalten dieser Einstellungen müssen Sie über OpenManage Enterprise-Anmeldeinformationen auf Administratorebene verfügen.

So konfigurieren und authentifizieren Sie den SMTP-Server, der die E-Mail-Kommunikation zwischen Nutzern und OpenManage Enterprise verwaltet:

ANMERKUNG: OpenManage Enterprise kann keine E-Mails an einen internen SMTP-Server senden, auf dem sich ein Zertifikat befindet, das von einer internen Stammzertifizierungsstelle ausgestellt wurde.

1. Erweitern Sie **E- Mail-Konfiguration**.
2. Geben Sie die SMTP-Server-Netzwerkadresse ein, von der aus E-Mail-Nachrichten gesendet werden.
3. Um den SMTP-Server zu authentifizieren, aktivieren Sie die Kontrollkästchen **Authentifizierung aktivieren** und geben Sie den Nutzernamen und das Kennwort ein.
4. Standardmäßig ist die SMPT-Portnummer, auf den zugegriffen wird, 25. Bearbeiten Sie dies gegebenenfalls.
5. Aktivieren Sie das Kontrollkästchen **SSL verwenden**, um Ihre SMTP-Transaktion zu sichern.
6. Um zu überprüfen, ob der SMTP-Server ordnungsgemäß funktioniert, klicken Sie auf das Kontrollkästchen **Test-E-Mail senden** und geben Sie einen **E-Mail-Empfänger** ein.
7. Klicken Sie auf **Anwenden**.
8. Um die Einstellungen auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.

So konfigurieren Sie die SNMP-Warnungsweiterleitung:

1. Erweitern Sie **SNMP-Warnungs-Weiterleitungskonfiguration**.
2. Aktivieren Sie das Kontrollkästchen **AKTIVIERT**, damit die entsprechenden SNMP-Traps Warnungen im Fall von vordefinierten Ereignisse senden können.
3. Geben Sie im Feld **ZIELADRESSE** die IP-Adresse des Zielgeräts ein, das die Warnung empfangen soll.

   ANMERKUNG: Die Eingabe der Konsolen-IP ist nicht erlaubt, um eine Duplizierung von Warnmeldungen zu vermeiden.
4. Wählen Sie im Menü **SNMP-VERSION** den Typ der SNMP-Version als SNMPv1, SNMPv2 oder SNMPv3 aus und füllen Sie die folgenden Felder aus:
   a. Geben Sie im Feld COMMUNITIYSTRING den Communitystring des Geräts ein, das die Warnung empfangen soll.
   b. Bearbeiten Sie bei Bedarf die PORTNUMMER. Die standardmäßige Portnummer für SNMP-Traps=162. Informationen dazu finden Sie unter Unterstützte Protokolle und Schnittstellen in OpenManage Enterprise auf Seite 32.
   c. Wenn SNMPv3 ausgewählt ist, geben Sie die folgenden zusätzlichen Details ein:
      i. NUTZERNAME: Geben Sie einen Nutzernamen ein.
      ii. AUTHENTIFIZIERUNGSTYP: Wählen Sie in der Dropdown-Liste SHA, MD_5 oder „Keine“ aus.
      iii. AUTHENTIFIZIERUNGS-PASSPHRASE: Geben Sie eine Authentifizierungs-Passphrase mit mindestens acht Zeichen an.
      iv. DATENSCHUTZTYP: Wählen Sie in der Dropdown-Liste DES, AES_128 oder „Keine“ aus.
      v. DATENSCHUTZ-PASSPHRASE: Geben Sie eine Datenschutz-Passphrase an, die mindestens acht Zeichen enthält.
5. Um eine SNMP-Meldung zu testen, klicken Sie auf die Schaltfläche **Senden** des entsprechenden Traps.
6. Klicken Sie auf **Anwenden**. Um die Einstellungen auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.

So aktualisieren Sie die Syslog-Weiterleitungskonfiguration:

1. Erweitern Sie **Syslog-Weiterleitungskonfiguration**.
2. Aktivieren Sie das Kontrollkästchen, um die Syslog-Funktion auf dem entsprechenden Server in der Spalte **SERVER** zu aktivieren.
3. Geben Sie im Feld **ZIELADRESSE/HOSTNAME** die IP-Adresse des Geräts ein, das die Syslog-Meldungen empfangen soll.
4. Die standardmäßige Portnummer mittels UPD=514. Bearbeiten Sie dies bei Bedarf durch Eingabe in das Feld oder Auswahl aus dem Feld. Informationen dazu finden Sie unter Unterstützte Protokolle und Schnittstellen in OpenManage Enterprise auf Seite 32.
5. Klicken Sie auf **Anwenden**.
6. Um die Einstellungen auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.

Befehle und Skripts ausführen

Bei Erhalt eines SNMP-Traps können Sie auf OpenManage Enterprise ein Skript ausführen. Dadurch wird eine Richtlinie eingerichtet, die ein Ticket auf Ihrem Drittanbieter-Ticketing-System für die Warnungsverwaltung öffnet. Sie können nur bis zu **vier** Remote-Befehle erstellen und speichern.

ANMERKUNG: Die Verwendung der folgenden Sonderzeichen als RACADM- und IPMI-CLI-Parameter wird nicht unterstützt: **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, * und **'**.

1. Klicken Sie auf **Anwendungseinstellungen** > **Skriptausführung**.
2. Gehen Sie im Abschnitt **Remote-Befehl – Einstellung** wie folgt vor:
   a. Zum Hinzufügen eines Remote-Befehls klicken Sie auf **Erstellen**.
   b. Geben Sie den in das Feld **Befehlsname** den Befehlsnamen ein.
   c. Wählen Sie einen der folgenden Befehlstypen aus:
      i. Skript
      ii. RACADM
      iii. IPMI Tool
   d. Wenn Sie **Skript** auswählen, gehen Sie wie folgt vor:
      i. Geben Sie in das Feld **IP-Adresse** die IP-Adresse ein.
      ii. Wählen Sie die Authentifizierungsmethode: **Kennwort** oder **SSH-Schlüssel**.
      iii. Geben Sie **Benutzername** und **Kennwort** oder **SSH-Schlüssel** ein.
      iv. Im Feld **Befehl** geben Sie die Befehle ein.
         - Bis zu 100 Befehle können eingegeben werden, wobei jeder Befehl in einer neuen Zeile sein muss.
         - Token-Ersetzung in Scripts ist möglich. Siehe . Token-Ersetzung in Remote-Skripts und Warnmeldungsrichtlinien auf Seite 184
      v. Klicken Sie auf **Fertigstellen**.
   e. Wenn Sie **RACADM** auswählen, gehen Sie wie folgt vor:
      i. Geben Sie den in das Feld **Befehlsname** den Befehlsnamen ein.
      ii. Im Feld **Befehl** geben Sie die Befehle ein. Bis zu 100 Befehle können eingegeben werden, wobei jeder Befehl in einer neuen Zeile sein muss.
      iii. Klicken Sie auf **Fertigstellen**.
   f. Wenn Sie **IPMI Tool** auswählen, gehen Sie wie folgt vor:
      i. Geben Sie den in das Feld **Befehlsname** den Befehlsnamen ein.
      ii. Im Feld **Befehl** geben Sie die Befehle ein. Bis zu 100 Befehle können eingegeben werden, wobei jeder Befehl in einer neuen Zeile sein muss.
      iii. Klicken Sie auf **Fertigstellen**.
3. Zum Bearbeiten der Einstellung eines Remote-Befehls wählen Sie den Befehl aus und klicken dann auf **Bearbeiten**.
4. Zum Löschen der Einstellung eines Remote-Befehls wählen Sie den Befehl aus und klicken dann auf **Löschen**.

Automatische Aktualisierung des MX7000-Gehäuses bei Einschub und Entfernung von Schlitten

OpenManage Enterprise kann fast sofort das Hinzufügen oder Entfernen von Schlitten reflektieren, nachdem ein eigenständiges oder ein Lead MX7000-Gehäuse erkannt oder integriert wurde.

Wenn ein eigenständiges oder ein Lead-MX7000-Gehäuse ermittelt oder mit OpenManage Enterprise (Version 3.4 oder höher) integriert wird, wird gleichzeitig eine Warnungsrichtlinie auf dem MX7000-Gehäuse erstellt. Weitere Informationen zum Ermitteln und eingliedern von Geräten in OpenManage Enterprise finden Sie unter Geräteermittlungsjob erstellen auf Seite 44 und Onboarding von Geräten auf Seite 45.

Die automatisch erstellte Warnungsrichtlinie auf der MX7000-OpenManage Enterprise-Modular-Appliance löst einen Job zum Aktualisieren der Gehäuse-Bestandsaufnahme mit dem Namen **Refresh Inventory of Chassis** in OpenManage Enterprise jedes Mal aus, wenn ein Schlitten eingesetzt, entfernt oder im MX7000-Gehäuse ausgetauscht wird.

Nach Abschluss des Gehäuse-Bestandsaufnahme-Aktualisierungs-Jobs werden die Schlitten-bezogenen Änderungen an den MX7000 auf der Seite „Alle Geräte“ angezeigt.

Die folgenden Voraussetzungen müssen erfüllt sein, wenn das MX7000-Gehäuse für eine erfolgreiche Erstellung der automatischen Warnungsrichtlinie integriert wird:

- OpenManage Enterprise-Modular Version 1.2 muss bereits im MX7000 installiert sein.
- MX7000-Gehäuse sollten mit den Optionen **„Trap-Empfang von ermittelten iDRAC-Servern und MX7000-Gehäuse aktivieren“** und **„Community-Zeichenfolge für Trap-Ziel von Anwendungseinstellungen festlegen“** integriert werden.
- Die IP-Adresse des OpenManage Enterprise-Geräts sollte als eines der vier verfügbaren Warnungsziele im neu integrierten MX7000 erfolgreich registriert werden. Wenn alle Warnungsziele im MX7000 bereits zum Zeitpunkt der Onboarding-Konfiguration konfiguriert sind, schlägt die automatische Erstellung der Warnungsrichtlinie fehl.

ANMERKUNG:

- Die Warnungsrichtlinie auf MX7000 ist nur spezifisch für die Schlitten und gilt nicht für die anderen Komponenten des Gehäuses, wie z.B. die IOMs.
- Die MX7000-Warnungseinstellungen können in OpenManage Enterprise so festgelegt werden, dass entweder alle Warnmeldungen oder nur die Gehäuse-Kategorie-Warnmeldungen vom MX7000-Gehäuse empfangen werden. Weitere Informationen finden Sie unter Verwalten der Konsolen-Voreinstellungen auf Seite 165.
- Zwischen der tatsächlichen Maßnahme auf den Schlitten und der Auslösung der Aktualisierung des Gehäusebestands auf OpenManage Enterprise ist eine gewisse Verzögerung zu erwarten.
- Die automatisch erstellte Warnungsrichtlinie wird gelöscht, wenn das MX7000-Gehäuse aus dem Gerätebestand von OpenManage Enterprise gelöscht wird.
- Auf der Seite „Alle Geräte“ wird der **Verwaltete Status** für ein erfolgreich eingegliedertes MX7000-Gehäuse mit automatischer Warnmeldungs-Weiterleitungs-Richtlinie als „Managed with Alerts“ aufgelistet. Weitere Informationen zur Integration finden Sie unter Onboarding von Geräten auf Seite 45

Warnungsdefinitionen

Indem Sie auf das Menü **OpenManage Enterprise** > **Warnmeldungen** > **Definitionen von Warnmeldungen** klicken, können Sie Warnmeldungen anzeigen, die für Fehler oder zu Informationszwecken generiert werden. Diese Meldungen:

- Werden Ereignis- und Fehlermeldungen genannt.
- Werden auf der grafischen Benutzeroberfläche (GUI) und der Befehlszeilenschnittstelle (CLI) für RACADM und WS-Man angezeigt.
- Werden zu Informationszwecken nur in Protokolldateien gespeichert.
- Werden nummeriert und klar definiert, damit Sie Korrektur- und Präventionsmaßnahmen effektiv implementieren können.

Eine Fehler- und Ereignismeldung enthält:

- **MELDUNGS-ID**: Meldungen werden anhand der von Komponenten wie BIOS, Stromquelle (PSU), Speicher (STR), Protokolldaten (Protokoll) und Gehäusemanagement-Controller (CMC) klassifiziert.
- **MELDUNG**: Die tatsächliche Ursache eines Ereignisses. Ereignisse werden nur zu Informationszwecken oder im Fall eines Fehlers beim Durchführen von Aufgaben ausgelöst.
- **KATEGORIE**: Klasse, zu der die Fehlermeldung gehört. Informationen über die Kategorien finden Sie im *Referenzhandbuch zu Ereignis- und Fehlermeldungen für Dell EMC Power Edge-Server*, das auf der Support-Website verfügbar ist.
- **Empfohlene Maßnahme**: Lösung des Fehlers mithilfe der GUI-, RACADM- oder WS-Man-Befehle. Sofern erforderlich, wird empfohlen für weitere Informationen die Dokumente auf der Support-Website oder im TechCenter zu lesen.
- **Detaillierte Beschreibung**: Weitere Informationen über ein Problem für eine einfache und schnelle Lösung.

Sie können weitere Informationen zu einer Warnmeldung anzeigen, indem Sie mithilfe der Filter wie die Meldungs-ID, Meldungstext, Kategorie und Unterkategorie suchen. So zeigen die Warnungsdefinitionen an:

1. Klicken Sie im Menü **OpenManage Enterprise** unter **Warnungen** auf **Warnungsdefinitionen**.

   Unter **Warnungsdefinitionen** wird eine Liste aller standardmäßigen Warnmeldungen angezeigt.

2. Um eine Fehlermeldung schnell zu suchen, klicken Sie auf **Erweiterte Filter**.

Im rechten Fensterbereich werden Informationen zu Fehler- und Ereignismeldungen der Meldungs-ID angezeigt, die Sie in der Tabelle ausgewählt haben.

15

Überwachen von Auditprotokollen

Auf der Seite **OpenManage Enterprise** > **Überwachen** > **Auditprotokolle** sind die Protokolldaten aufgelistet, die für Sie oder die Dell EMC Support Teams beim Troubleshooting und bei der Analyse hilfreich sind. Ein Auditprotokoll wird aufgezeichnet, wenn:

- Eine Gruppe zugeordnet oder eine Zugangsberechtigung geändert wird.
- Eine Nutzerrolle geändert wird.
- Aktionen, die auf den Geräten ausgeführt wurden, die von OpenManage Enterprise überwacht werden.

Die Dateien der Auditprotokolle können in CSV-Dateiformat exportiert werden. Informationen dazu finden Sie unter Alle oder ausgewählte Daten exportieren auf Seite 68.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Bereichsbasierte Einschränkungen gelten nicht für die Auditprotokolle.

1. Um die Auditprotokolle anzuzeigen, wählen Sie **Audit** > **Auditprotokolle** aus.
   Die Auditprotokolle, die OpenManage Enterprise speichert und zu den mit der Appliance durchgeführten Aufgaben anzeigt, werden angezeigt. Zum Beispiel: Anmeldeversuche von Nutzern, Erstellung von Warnungsrichtlinien und Ausführung verschiedener Jobs.
2. Um Daten in einer beliebigen Spalte zu sortieren, klicken Sie auf den Spaltentitel.
3. Um Informationen zu einem Auditprotokoll schnell zu suchen, klicken Sie auf **Erweiterte Filter**.
   Die folgenden Felder werden angezeigt, die als Filter für die schnelle Suche nach Daten fungieren.
4. Geben Sie Daten in die folgenden Felder ein oder wählen Sie diese aus:
   - **Schweregrad**: Wählen Sie den Schweregrad eines Protokolldatensatzes aus. Die verfügbaren Optionen lauten „Info“, „Warnung“ und „Kritisch“.
     - Kritisch: Eine ungewöhnliche Aktion hat stattgefunden. Sofortige Maßnahmen sind erforderlich.
     - Warnung: Das Ereignis ist wichtig, es sind jedoch keine sofortigen Maßnahmen erforderlich.
     - Info: Eine Aktion wurde erfolgreich durchgeführt.
   - **Startzeit** und **Endzeit**: Zum Anzeigen der Auditprotokolle eines bestimmten Zeitraums.
   - **Nutzer**: Zum Anzeigen von Auditprotokollen für einen bestimmten Nutzer. Zum Beispiel Administrator, System, Device Manager und Betrachter.
   - **Quelladresse**: Zum Anzeigen der Auditprotokolle für ein bestimmtes System. Zum Beispiel das System, auf dem Sie sich bei OpenManage Enterprise angemeldet haben.
   - **Kategorie**: Zum Anzeigen der Auditprotokolle für einen bestimmen Audit- oder Konfigurationstyp.
     - Audit: Wird erzeugt, wenn sich ein Nutzer bei der OpenManage Enterprise-Appliance an- oder davon abmeldet.
     - Konfiguration: Wird erzeugt, wenn eine Aktion auf einem Zielgerät durchgeführt wird.
   - **Beschreibung enthält**: Geben Sie den Text oder eine in den Protokolldaten enthaltene Phrase ein, die Sie suchen. Alle Protokolle mit dem ausgewählten Text werden angezeigt. Wenn Sie z. B. `warningSizeLimit` eingeben, werden alle Protokolle mit diesem Text angezeigt.
   - **Meldungs-ID**: Geben Sie die Meldungs-ID ein. Wenn die Suchkriterien übereinstimmen, werden nur die Elemente mit der entsprechenden Nachrichten-ID angezeigt.
5. Um den Filter zu entfernen, klicken Sie auf **Alle Filter löschen**.
6. Um ein Auditprotokoll oder alle Auditprotokolle zu exportieren, wählen Sie **Exportieren** > **Ausgewählte exportieren** bzw. **Exportieren** > **Alle exportieren** aus. Weitere Informationen zum Exportieren der Auditprotokolle finden Sie unter Alle oder ausgewählte Daten exportieren auf Seite 68.
7. Um die neuesten Konsolen-Protokolle abzurufen und ein Archiv zu erstellen, das zum Download zur Verfügung steht, klicken Sie auf **Troubleshooting** > **Konsolenprotokollarchiv erstellen**.
8. Um die Konsolenprotokollarchive herunterzuladen, klicken Sie auf **Troubleshooting** > **Archivierte Konsolenprotokolle herunterladen**.

ANMERKUNG:

- Derzeit wird für jedes M1000e-Gehäuse, das mit der Gehäusefirmwareversion 5.1x und älteren Versionen erkannt wurde, das Datum in der Spalte ZEITSTEMPEL unter Hardware-Protokolle als JAN 12, 2013 angezeigt. Für alle Gehäuseversionen der VRTX- und FX2-Gehäuse wird jedoch das korrekte Datum angezeigt.
- Die Datei ist nicht sofort zum Herunterladen bereit, insbesondere in Fällen, in denen ein großer Satz von Protokollen erfasst wird. Der Erfassungsprozess findet im Hintergrund statt und eine Eingabeaufforderung zum Speichern der Datei wird angezeigt, wenn der Vorgang abgeschlossen ist.

Zugehörige Informationen

Auditprotokolle an Remote-Syslog-Server weiterleiten auf Seite 123

Themen:

- Auditprotokolle an Remote-Syslog-Server weiterleiten

Auditprotokolle an Remote-Syslog-Server weiterleiten

Um alle Auditprotokolle von OpenManage Enterprise von Syslog-Servern aus zu überwachen, können Sie eine Warnrichtlinie erstellen. Alle Auditprotokolle, z. B. Anmeldeversuche für Benutzer, das Erstellen von Warnrichtlinien und das Ausführen verschiedener Jobs, können an Syslog-Server weitergeleitet werden.

So erstellen Sie eine Warnungsrichtlinie zum Weiterleiten von Auditprotokollen an Syslog-Server:

1. Wählen Sie **Warnungen** > **Warnungsrichtlinien** > **Erstellen**.
2. Geben Sie im Dialogfeld **Warnungsrichtlinie erstellen** im Abschnitt **Name und Beschreibung** einen Namen und eine Beschreibung der Warnungsrichtlinie ein.
   a. Das Kontrollkästchen **Richtlinie aktivieren** ist standardmäßig aktiviert, um anzugeben, dass die Warnungsrichtlinie aktiviert wird, sobald sie erstellt wurde. Deaktivieren Sie das Kontrollkästchen, um die Warnungsrichtlinie zu deaktivieren. Weitere Informationen zum Aktivieren von Warnungsrichtlinien zu einem späteren Zeitpunkt finden Sie unter Konfigurieren und Verwalten von Warnungsrichtlinien auf Seite 121.
   b. Klicken Sie auf **Weiter**.
3. Erweitern Sie im Abschnitt **Kategorie** den Eintrag **Anwendung** und wählen Sie die Kategorien und Unterkategorien der Appliance-Protokolle aus. Klicken Sie auf **Weiter**.
4. Im Bereich **Ziel** ist die Option **Geräte auswählen** standardmäßig ausgewählt. Klicken Sie auf **Geräte auswählen** und wählen Sie im linken Bereich Geräte aus. Klicken Sie auf **Weiter**.

   ANMERKUNG: Die Auswahl von Zielgeräten oder -gruppen ist bei der Weiterleitung der Auditprotokolle an den Syslog-Server nicht möglich.

5. (Optional) Die Warnungsrichtlinien sind standardmäßig immer aktiv. Wählen Sie zur Einschränkung der Aktivität im Abschnitt **Datum und Uhrzeit** das Start- und Enddatum aus und wählen Sie dann den Zeitraum.
   a. Aktivieren Sie die Kontrollkästchen der entsprechenden Tage, an denen die Warnungsrichtlinien ausgeführt werden sollen.
   b. Klicken Sie auf **Weiter**.
6. Wählen Sie im Abschnitt **Schweregrad** den Schweregrad der Warnungen aus, für die diese Richtlinie aktiviert sein muss.
   a. Um alle Schweregradkategorien auswählen, aktivieren Sie das Kontrollkästchen **Alle**.
   b. Klicken Sie auf **Weiter**.
7. Wählen Sie unter **Aktionen** den Punkt **Syslog** aus.

   Wenn Syslog-Server nicht in OpenManage Enterprise konfiguriert sind, klicken Sie auf **Aktivieren** und geben Sie die Ziel-IP-Adresse oder den Hostnamen der Syslog-Server ein. Weitere Informationen zum Konfigurieren der Syslog-Server finden Sie unter SMTP-, SNMP- und Syslog-Warnungen konfigurieren auf Seite 124.
8. Klicken Sie auf **Weiter**.
9. Im Abschnitt **Zusammenfassung** werden die Details der Warnungsrichtlinie angezeigt, die Sie definiert haben. Lesen Sie die Informationen sorgfältig durch.
10. Klicken Sie auf **Fertigstellen**.

Die Warnungsrichtlinie wurde erfolgreich erstellt und wird im Abschnitt **Warnungsrichtlinien** aufgeführt.

Zugehörige Tasks

Konfigurieren und Verwalten von Warnungsrichtlinien auf Seite 121

Überwachen von Auditprotokollen auf Seite 127

16

Verwenden von Jobs zur Gerätesteuerung

Ein Job ist ein Satz von Anweisungen für die Durchführung einer Aufgabe auf einem oder mehreren Geräten. Zu den Jobs zählen Ermittlung, Firmwareupdate, Bestandsaktualisierung für Geräte, Gewährleistung usw. Sie können auf der Seite **Jobs** den Status und die Details von Jobs überwachen, die in den Geräten und ihren Komponenten initiiert werden. OpenManage Enterprise verfügt über viele interne Wartungsjobs, die nach einem festgelegten Zeitplan automatisch von der Appliance ausgelöst werden. Weitere Informationen zu den Standardjobs und deren Planung finden Sie unter OpenManage Enterprise-Standardjobs und -Planung auf Seite 132.

Voraussetzungen:

Um Jobs, wie z. B. Blinken, Stromsteuerung, Verwaltung von Firmware-Baselines und Verwaltung der Konfigurations-Compliance-Baseline, zu erstellen und zu verwalten, wenn die Geräteauswahl-Aufgabe beteiligt ist,

- müssen Sie über die notwendigen Nutzerberechtigungen verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16
- Jeder Jobtyp beschränkt sich auf Geräte, für die Sie Folgendes haben:
  - Zugriffsberechtigungen.
  - Fähigkeit zur Durchführung der erforderlichen Aktion.

Um Jobs zu erstellen und zu verwalten, wählen Sie **OpenManage Enterprise** > **Überwachen** > **Jobs** aus. Auf der Seite **Jobs** können Sie folgende Aufgaben ausführen:

- Anzeigen der Liste Jobs, die aktuell ausgeführt werden, fehlgeschlagen sind und erfolgreich abgeschlossen sind.
- Jobs zum Blinken von LEDs erstellen, die Stromversorgung des Geräts steuern und Remote-Befehle auf Geräten ausführen. Siehe Remote-Befehlsjob für die Geräteverwaltung erstellen auf Seite 135 Erstellen von Jobs zur Stromverwaltung der Geräte, und Erstellen eines Jobs zum Blinken von Geräte-LEDs. Sie können ähnliche Maßnahmen auf einem Server der Seite "Gerätedetails" durchführen. Informationen dazu finden Sie unter Anzeigen und Konfigurieren einzelner Geräte auf Seite 68.
- Verwalten von Jobs wie das Ausführen, Beenden, Aktivieren, Deaktivieren oder Löschen von Jobs.

Um weitere Informationen zu einem Job anzuzeigen, aktivieren Sie das Kontrollkästchen des entsprechenden Jobs und klicken Sie dann im rechten Fensterbereich auf **Details anzeigen**. Siehe Anzeigen Jobinformationen.

Themen:

Anzeigen von Joblisten

Klicken Sie in OpenManage Enterprise auf **Überwachen** > **Jobs**, um die Liste der vorhandenen Jobs anzuzeigen. Informationen zu Jobs finden Sie in den folgenden Spalten:

- **Jobstatus**: Gibt den Ausführungsstatus eines Jobs an.

  Informationen dazu finden Sie unter Beschreibung von Jobstatus und Jobtypen auf Seite 131.
- **Status**: Gibt den Status eines Jobs an. Die verfügbaren Optionen sind „Aktiviert" oder „Deaktiviert".
- **Jobname**: Name des Jobs.
- **Jobtyp**: Gibt den Typ des Jobs an.

  Informationen dazu finden Sie unter Beschreibung von Jobstatus und Jobtypen auf Seite 131.
- **Beschreibung**: Detaillierte Beschreibung eines Jobs.
- **Letzte Ausführung**: Letzte Ausführungsperiode eines Jobs.

Jobs können auch gefiltert werden, indem Sie die Werte im Abschnitt **Erweiterte Filter** eingeben oder auswählen. Die folgenden zusätzlichen Informationen können zum Filtern der Warnmeldungen bereitgestellt werden:

- **Startdatum der letzten Ausführung**: Startdatum der letzten Ausführung des Jobs.
- **Enddatum der letzten Ausführung**: Enddatum der letzten Ausführung des Jobs.
- **Quelle**: Die verfügbaren Optionen lauten „Alle“, „Nutzergeneriert“ (Standard) und „System“.

Um weitere Informationen zu einem Job anzuzeigen, wählen Sie einen Job aus und klicken Sie im rechten Fensterbereich auf **Details anzeigen**. Informationen dazu finden Sie unter Einzelne Jobinformationen anzeigen auf Seite 134.

OpenManage Enterprise bietet einen integrierten Bericht zum Anzeigen der geplanten Jobs. Klicken Sie auf **OpenManage Enterprise** > **Überwachen** > **Berichte** > **Geplante Jobs**. Klicken Sie auf **Ausführen**. Informationen dazu finden Sie unter Berichte ausführen auf Seite 141.

ANMERKUNG: Auf den Seiten **Ermittlungs- und Bestandsaufnahme-Zeitpläne** wird der Status eines geplanten Jobs durch **In Warteschlange** in der Spalte **STATUS** definiert. Jedoch wird derselbe Status als **Geplant** auf der Seite **Jobs** angezeigt.

Beschreibung von Jobstatus und Jobtypen

Tabelle 21. Jobstatus und Beschreibung

Jobstatus	Beschreibung
Geplant	Der Job wird zu einer späteren Zeit oder zu einem späteren Datum ausgeführt.
In Warteschlange	Jobs, die auf die Ausführung warten.
Wird gestartet	
Wird ausgeführt	Job wird mit **Jetzt ausführen** ausgelöst.
Abgeschlossen	Job wurde ausgeführt.
Fehlgeschlagen	Jobausführung war nicht erfolgreich.
Neu	Job wurde erstellt, aber nicht ausgeführt.
Mit Fehlern abgeschlossen	Die Jobausführung war teilweise erfolgreich und wurde mit Fehlern abgeschlossen.
Abgebrochen	Der Job wurde vom Nutzer angehalten.
Unterbrochen	Der Job wurde vom Nutzer unterbrochen.
Angehalten	Der Job wurde vom Nutzer unterbrochen.
Annuliert	
Nicht ausgeführt	Der Job wird entweder in die Warteschlange eingereiht oder geplant und muss noch ausgeführt werden.

Ein Job kann zu einem der folgenden Typen gehören:

Tabelle 22. Jobtypen und Beschreibung

Jobtyp	Beschreibung
Funktionszustand	Überprüft den Integritätsstatus der Geräte. Informationen dazu finden Sie unter Gerätefunktionsstatus auf Seite 40.
Bestandsaufnahme	Erzeugt einen Inventarbericht der Geräte. Informationen dazu finden Sie unter Verwalten von Geräteinventar auf Seite 74.
Device-Konfiguration	Erstellt die Baseline für die Device-Konfiguration. Informationen dazu finden Sie unter Verwalten der Device-Konfigurations-Compliance auf Seite 110.
Report_Task	Erstellt Berichte über Geräte mithilfe von integrierten oder benutzerdefinierten Datenfeldern. Informationen dazu finden Sie unter Berichte auf Seite 140.
Gewährleistung	Generiert Daten zum Gewährleistungsstatus von Geräten. Informationen dazu finden Sie unter Verwalten der Gerätegewährleistung auf Seite 138.

Tabelle 22. Jobtypen und Beschreibung (fortgesetzt)

Jobtyp	Beschreibung
Onboarding_Task	Integriert die ermittelten Geräte. Informationen dazu finden Sie unter Onboarding von Geräten auf Seite 45.
Ermittlung	Ermittelt Geräte. Informationen dazu finden Sie unter Ermitteln von Geräten für die Überwachung oder Verwaltung auf Seite 41.
Ausführung des Konsolenaktualisierungsjobs	Der Konsolen-Upgrade-Job wird mithilfe dieser Aufgabe nachverfolgt. Mit dieser Aufgabe können Sie feststellen, ob das Upgrade abgeschlossen wurde oder fehlgeschlagen ist.
Backup	
Gehäuseprofile	
Debug-Protokolle	Erfasst Debug-Protokolle der Aufgaben des Anwendungsmonitoring, der Ereignisse und des Aufgaben-Ausführungsverlaufs.
Geräteaktion	Erstellt Maßnahmen auf Geräten, wie z. B. Einschalten der LED, Ausschalten der LED, IPMI-CLI, RACADM-CLI usw.
Diagnostic_Task	Aufgaben zum Herunterladen/Ausführen von Diagnose/TSR oder Services (SupportAssist) sind mit der Diagnoseaufgabe verbunden. Siehe Diagnoseberichte ausführen und herunterladen.
VLAN-Definition importieren	Importieren von VLAN-Definitionen aus Excel oder MSM.
OpenID Connect-Anbieter	Konfiguration der OpenID-Verbindung. Siehe Anmelden bei OpenManage Enterprise über OpenID Connect-Anbieter.Anmelden bei OpenManage Enterprise über OpenID Connect-Anbieter auf Seite 160
PluginDownload_Task	Die Aufgabe zum Herunterladen des Plug-ins wird nachverfolgt und diese Aufgabe hilft, zu ermitteln, ob das Herunterladen von RPM-Plug-ins abgeschlossen wurde und sie für die Installation bereit sind. Siehe Überprüfen und Aktualisieren der Version von OpenManage Enterprise und der verfügbaren Plug-ins.
Post_Upgrade_Task	Die Aufgabe nach dem Upgrade wird nachverfolgt, um die Appliance-Einstellungen festzulegen, die in der Version N-1 oder N-2 vorgenommen wurden, wobei auch die Ermittlungsaufgabe ausgeführt wird, die in der vorherigen Version erstellt wurde, um sicherzustellen, dass alle Geräte aufgelistet werden.
Report_Task	Die Berichtsaufgabe wird nachverfolgt, wenn der Nutzer den Bericht ausführt („Muster“ und „Benutzerdefiniert“).
Wiederherstellen	
Einstellungen aktualisieren	Die Aufgabe zum Aktualisieren der Einstellungen wird nachverfolgt, wenn der Nutzer eine neue Einstellung unter „Anwendungseinstellungen“ anwendet.
Software-Rollback	Die Rollback-Aufgabe wird nachverfolgt, wenn der Nutzer einen Rollback-Vorgang auf einem Zielgerät ausführt.
Update	Die Aktualisierungsaufgabe wird nachverfolgt, wenn der Nutzer die Firmware- oder Treiber-Updates auf den Zielgeräten durchführt.
Upgrade_Bundle_Download_Task	Die Aufgabe zum Herunterladen des Bundle-Upgrades wird nachverfolgt und diese Aufgabe hilft, zu ermitteln, ob das Herunterladen von OMEnterprise RPM abgeschlossen wurde und für die Installation bereit ist.

OpenManage Enterprise-Standardjobs und -Planung

OpenManage Enterprise verfügt über viele interne Wartungsjobs, die nach einem festgelegten Zeitplan automatisch von der Appliance ausgelöst werden.

Tabelle 23. In der folgenden Tabelle sind die Namen der OpenManage Enterprise-Standardjobs und deren Planung aufgeführt.

Jobname	Cron-Ausdruck	Beschreibung des Cron-Ausdrucks	Beispiel
Konfigurationsbestandsaufnahme	0 0 0 1/1 * ? *	Um 00:00:00 Uhr, jeden Tag, beginnend am 1. eines jeden Monats	• Di, 18. Mai, 00:00:00 UTC, 2021 • Mi, 19. Mai, 00:00:00 UTC, 2021
Standard-Konsolen-Aktualisierungs-Task	0 0 12 ? * MO *	Um 12:00:00 Uhr, an jedem Montag, jeden Monat	• Mo, 24. Mai, 12:00:00 UTC, 2021 • Mo, 31. Mai, 12:00:00 UTC, 2021
Standard-Bestandsaufnahme-Task	0 0 5 * * ? *	Täglich um 05:00:00 Uhr	• Di, 18. Mai, 05:00:00 UTC, 2021 • Mi, 19. Mai, 05:00:00 UTC, 2021
Task zum Löschen der Gerätekonfiguration zur Bereinigung	0 0/1 * * * ? *	Zur Sekunde :00, jede Minute, beginnend zur Minute :00 einer jeden Stunde	• Mo, 17. Mai, 18:39:00 UTC, 2021 • Mo, 17. Mai, 18:40:00 UTC, 2021
Dateibereinigungs-Task für Nutzung von Freigaben	0 0 0 1/1 * ? *	Um 00:00:00 Uhr, jeden Tag, beginnend am 1. eines jeden Monats	• Di, 18. Mai, 00:00:00 UTC, 2021 • Mi, 19. Mai, 00:00:00 UTC, 2021
Dateibereinigungs-Task für einzelne DUP-Dateien	0 0 0/4 1/1 * ? *	Zur Sekunde :00, zur Minute :00, alle 4 Stunden ab 00 Uhr, jeden Tag ab dem 1. jeden Monats	• Mo, 17. Mai, 20:00:00 UTC, 2021 • Di, 18. Mai, 00:00:00 UTC, 2021 • Di, 18. Mai, 04:00:00 UTC, 2021 • Di, 18. Mai, 04:00:00 UTC, 2021
Globaler Integritäts-Task	0 0 0/1 1/1 * ? *	Zur Sekunde :00, zur Minute :00, jede Stunde ab 00 Uhr, jeden Tag ab dem 1. jeden Monats	• Mo, 17. Mai, 19:00:00 UTC, 2021 • Mo, 17. Mai, 20:00:00 UTC, 2021
Interner Synchronisierungs-Task	0 0/5 * 1/1 * ? *	Zur Sekunde :00, alle 5 Minuten ab Minute :00, jede Stunde, täglich ab dem 1. jeden Monats	• Mo, 17. Mai, 18:45:00 UTC, 2021 • Mo, 17. Mai, 18:50:00 UTC, 2021
Metriken-Lösch-Task	0 0 * ? * *	Zur Sekunde :00 der Minute :00, jede Stunde	• Mo, 17. Mai, 19:00:00 UTC, 2021 • Mo, 17. Mai, 20:00:00 UTC, 2021 • Mo, 17. Mai, 21:00:00 UTC, 2021
Metriken-Task	0 0/15 * 1/1 * ? *	Zur Sekunde :00, alle 15 Minuten ab Minute :00, jede Stunde, täglich ab dem 1. jeden Monats	• Mo, 17. Mai, 18:45:00 UTC, 2021 • Mo, 17. Mai, 19:00:00 UTC, 2021
Task für mobile Abonnements	0 0/2 * 1/1 * ? *	Zur Sekunde :00, alle 2 Minuten ab Minute :00, jede Stunde, täglich ab dem 1. jeden Monats	• Mo, 17. Mai, 18:54:00 UTC, 2021 • Mo, 17. Mai, 18:56:00 UTC, 2021
Ermittlungs-Task für initiierte Nodes	0 0/10 * 1/1 * ? *	Zur Sekunde :00, alle 10 Minuten ab Minute :00, jede Stunde, täglich ab dem 1. jeden Monats	• Mo, 17. Mai, 19:00:00 UTC, 2021 • Mo, 17. Mai, 19:10:00 UTC, 2021
Aufgabe zur Kennwort-Rotation	0 0 0/6 1/1 * ? *	Zur Sekunde :00, zur Minute :00, alle 6 Stunden ab 00 Uhr, jeden Tag ab dem 1. jeden Monats	• Di, 18. Mai, 00:00:00 UTC, 2021 • Di, 18. Mai, 06:00:00 UTC, 2021 • Di, 18. Mai, 12:00:00 UTC, 2021
Periodische Registrierung von Metriken	0 0 3 * * ?	Täglich um 03:00:00 Uhr	• Di, 18. Mai, 03:00:00 UTC, 2021 • Mi, 19. Mai, 03:00:00 UTC, 2021
On Demand-Funktionszustand-Lösch-Task für Tabelle: Task	0 0 0/5 1/1 * ? *	Zur Sekunde :00, zur Minute :00, alle 5 Stunden ab 00 Uhr, jeden Tag ab dem 1. jeden Monats	• Di, 18. Mai, 00:00:00 UTC, 2021 • Di, 18. Mai, 05:00:00 UTC, 2021 • Di, 18. Mai, 10:00:00 UTC, 2021
Lösch-Task Tabelle :Event_Archive	0 0 18/12 ? * * *	Zur Sekunde :00, zur Minute :00, alle 12 Stunden, beginnend täglich um 18 Uhr	• Di, 18. Mai, 18:00:00 UTC, 2021 • Mi, 19. Mai, 18:00:00 UTC, 2021 • Do, 20. Mai, 18:00:00 UTC, 2021

Tabelle 23. In der folgenden Tabelle sind die Namen der OpenManage Enterprise-Standardjobs und deren Planung aufgeführt. (fortgesetzt)

Jobname	Cron-Ausdruck	Beschreibung des Cron-Ausdrucks	Beispiel
Lösch-Task Tabelle :Group_Audit	0 0 0 1/1 * ? *	Um 00:00:00 Uhr, jeden Tag, beginnend am 1. eines jeden Monats	• Di, 18. Mai, 00:00:00 UTC, 2021 • Mi, 19. Mai, 00:00:00 UTC, 2021 • Do, 20. Mai, 00:00:00 UTC, 2021
Lösch-Task Tabelle :Task	0 0 0 1/1 * ? *	Um 00:00:00 Uhr, jeden Tag, beginnend am 1. eines jeden Monats	• Di, 18. Mai, 00:00:00 UTC, 2021 • Mi, 19. Mai, 00:00:00 UTC, 2021 • Do, 20. Mai, 00:00:00 UTC, 2021
Lösch-Task Tabelle :announced_target	0 0 0 1/1 * ? *	Um 00:00:00 Uhr, jeden Tag, beginnend am 1. eines jeden Monats	• Di, 18. Mai, 00:00:00 UTC, 2021 • Mi, 19. Mai, 00:00:00 UTC, 2021 • Do, 20. Mai, 00:00:00 UTC, 2021
Lösch-Task für Tabelle: Kern-Anwendungsprotokoll	0 0 0/5 1/1 * ? *	Zur Sekunde :00, zur Minute :00, alle 5 Stunden ab 00 Uhr, jeden Tag ab dem 1. jeden Monats	• Di, 18. Mai, 00:00:00 UTC, 2021 • Di, 18. Mai, 05:00:00 UTC, 2021
Lösch-Task für Tabelle: Ereignis	0 0/30 * 1/1 * ? *	Zur Sekunde :00, alle 30 Minuten ab Minute :00, jede Stunde, täglich ab dem 1. jeden Monats	• Mo, 17. Mai, 19:30:00 UTC, 2021 • Mo, 17. Mai, 20:00:00 UTC, 2021 • Mo, 17. Mai, 20:30:00 UTC, 2021
Lösch-Task für Tabelle: Infrastrukturgerät	0 0/30 * 1/1 * ? *	Zur Sekunde :00, alle 30 Minuten ab Minute :00, jede Stunde, täglich ab dem 1. jeden Monats	• Mo, 17. Mai, 19:30:00 UTC, 2021 • Mo, 17. Mai, 20:00:00 UTC, 2021 • Mo, 17. Mai, 20:30:00 UTC, 2021
Abonnement-Abfrage-Task	0 0/30 * 1/1 * ? *	Zur Sekunde :00, alle 30 Minuten ab Minute :00, jede Stunde, täglich ab dem 1. jeden Monats	• Mo, 17. Mai, 19:30:00 UTC, 2021 • Mo, 17. Mai, 20:00:00 UTC, 2021 • Mo, 17. Mai, 20:30:00 UTC, 2021

Einzelne Jobinformationen anzeigen

1. Aktivieren Sie auf der Seite **Jobs** das Kontrollkästchen des entsprechenden Jobs.
2. Klicken Sie im rechten Fensterbereich auf **Details anzeigen**.
   Auf der Seite **Jobdetails** werden die Jobinformationen angezeigt.
3. Klicken Sie auf **Job neu starten**, wenn der Jobstatus einer der folgenden ist: Gestoppt, Fehlgeschlagen oder Neu.
   Eine Meldung gibt an, dass der Job bereits ausgeführt wird.

   Im Abschnitt **Ausführungsverlauf** werden die Informationen über den Zeitpunkt der erfolgreichen Ausführung des Jobs aufgeführt. Im Abschnitt **Ausführungsdetails** werden die Geräte aufgeführt, auf denen der Job ausgeführt wurde sowie die benötigte Zeit für die Ausführung eines Jobs.

   ANMERKUNG: Wenn eine Konfigurationswartungsaufgabe gestoppt wird, wird der Gesamtstatus der Aufgabe als „Gestoppt" angezeigt, aber die Aufgabe läuft weiter. Der Status wird jedoch im Abschnitt **Task-Ausführungsverlauf** als „Wird ausgeführt" angezeigt.
4. Um Daten in eine Excel-Datei zu exportieren, aktivieren Sie das entsprechende oder alle Kontrollkästchen und klicken Sie dann auf **Exportieren**. Informationen dazu finden Sie unter Alle oder ausgewählte Daten exportieren auf Seite 68.

Job zum Schalten von Geräte-LEDs erstellen

Die folgenden Schritte beschreiben, wie Sie die LEDs der angegebenen Geräte mithilfe des Assistenten zum Blinken von Geräten blinken lassen.

Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16

1. Der Assistent zum Blinken von Geräten kann folgendermaßen aktiviert werden:

a. Klicken Sie auf der Seite „Jobs“ (**OpenManage Enterprise** > **Überwachen** > **Jobs**) auf **Erstellen** und wählen Sie dann **Blinken von Geräten**.
b. Wählen Sie auf der Seite „Alle Geräte“ (**OpenManage Enterprise** > **Geräte**) die Geräte aus, klicken Sie auf das Dropdown-Menü **Weitere Aktionen** und klicken Sie dann entweder auf **LED einschalten** oder auf **LED ausschalten**.

2. Im Dialogfeld **Assistent: Blinken von Geräten**:
   a. Im Abschnitt **Optionen**:
      i. Geben Sie in das Feld **Jobname** einen Jobnamen in.
      ii. Wählen Sie im Drop-Down-Menü **LED-Blinkdauer** die Optionen aus, um die Blinkdauer für eine LED festzulegen und diese ein- bzw. auszuschalten.
      iii. Klicken Sie auf **Weiter**.
   b. Wählen Sie im Abschnitt **Ziel** die Zielgeräte oder Zielgruppen aus und klicken Sie auf **Weiter**. Informationen dazu finden Sie unter Zielgeräte und Zielgerätegruppen auswählen auf Seite 136.
   c. Wählen Sie im Dropdown-Menü **Planen Jetzt ausführen**, **Später ausführen** oder **Nach Zeitplan ausführen** aus. Informationen dazu finden Sie unter Felddefinitionen für die Jobplanung auf Seite 182.
3. Klicken Sie auf **Fertigstellen**.
   Ein Blink-LED-Job wird erstellt und auf der Seite „Jobs“ (**OpenManage Enterprise** > **Überwachen** > **Jobs**) in der Spalte **JOBSTATUS** angezeigt.

Job zur Stromverwaltung der Geräte erstellen

ANMERKUNG: Energieverwaltungsaktionen können nur auf Geräten durchgeführt werden, die mithilfe von iDRAC (bandextern) ermittelt und verwaltet werden.

1. Klicken Sie auf **Erstellen** und wählen Sie dann **Stromregelung der Geräte**.
2. Im Dialogfeld **Stromregelungs-Assistent**:
   a. Im Abschnitt **Optionen**:
      i. Geben Sie den Jobnamen in **Jobname** ein.
      ii. Wählen Sie im Drop-Down-Menü **Energieoptionen** eine der Aufgaben auf: **Einschalten**, **Ausschalten** oder **Aus- und Einschalten**.
      iii. Klicken Sie auf **Weiter**.
   b. Wählen Sie im Abschnitt **Ziel** die Zielgeräte aus und klicken Sie auf **Weiter**. Informationen dazu finden Sie unter Zielgeräte und Zielgerätegruppen auswählen auf Seite 136.
   c. Führen Sie im Abschnitt **Zeitplan** den Job sofort aus oder planen Sie ihn für einen späteren Zeitpunkt. Informationen dazu finden Sie unter Felddefinitionen für die Jobplanung auf Seite 182.
3. Klicken Sie auf **Fertigstellen**.
   Der Job wird erstellt, in der Liste „Jobs“ aufgeführt und durch einen entsprechenden Status in der Spalte **JOBSTATUS** gekennzeichnet.
4. Wenn der Job für einen späteren Zeitpunkt geplant ist, Sie den Job jedoch sofort ausführen möchten:
   - Aktivieren Sie auf der Seite „Jobs“ das Kontrollkästchen des entsprechenden geplanten Jobs.
   - Klicken Sie auf **Jetzt ausführen**. Der Job wird ausgeführt und der Status wird aktualisiert.
   - Um die Jobdaten anzuzeigen, klicken Sie im rechten Bereich auf **Details anzeigen**. Informationen dazu finden Sie unter Einzelne Jobinformationen anzeigen auf Seite 134.

Remote-Befehlsjob für die Geräteverwaltung erstellen

Mithilfe des Befehlszeilen-Job-Assistenten können Sie Remote-Befehls-Jobs für die Remote-Verwaltung der Zielgeräte erstellen.

1. Klicken Sie auf **Erstellen** und wählen Sie dann **Remote-Befehl auf Geräten**.
2. Im Dialogfeld **Befehlszeilenjob-Assistent** im Abschnitt **Optionen**:
   a. Geben Sie den Jobnamen in **Jobname** ein.
   b. Wählen Sie aus dem Drop-Down-Menü „Schnittstelle“ je nach den Zielgeräten, die Sie verwalten möchten, eine der Schnittstellen aus:
      - **IPMI CLI** – für iDRACs-und nicht-Dell-Server.
      - **RACADM CLI** – für iDRACs, die mithilfe des WSMAN-Protokolls ermittelt wurden.
      - **SSH CLI** – für Linux-Server, die mithilfe des SSH-Protokolls ermittelt wurden.

c. Geben Sie den Befehl in das Feld **Argumente** ein. Bis zu 100 Befehle können eingegeben werden, wobei jeder Befehl in einer neuen Zeile sein muss.

   ANMERKUNG: Die Befehle im Feld „Argumente" werden nacheinander ausgeführt.

d. Klicken Sie auf **Weiter**.
   Ein grünes Häkchen neben **Optionen** gibt an, dass die benötigten Daten zur Verfügung stehen.

3. Wählen Sie im Abschnitt **Ziel** die Zielgeräte aus und klicken Sie auf **Weiter**. Informationen dazu finden Sie unter Zielgeräte und Zielgerätegruppen auswählen auf Seite 136.
4. Führen Sie im Abschnitt **Zeitplan** den Job sofort aus oder planen Sie ihn für einen späteren Zeitpunkt. Informationen dazu finden Sie unter Felddefinitionen für die Jobplanung auf Seite 182.
5. Klicken Sie auf **Fertigstellen**.
   Der Job wird erstellt, in der Liste „Jobs" aufgeführt und durch einen entsprechenden Status in der Spalte **JOBSTATUS** gekennzeichnet.
6. Wenn der Job für einen späteren Zeitpunkt geplant ist, Sie den Job jedoch sofort ausführen möchten:
   - Aktivieren Sie auf der Seite „Jobs" das Kontrollkästchen des entsprechenden geplanten Jobs.
   - Klicken Sie auf **Jetzt ausführen**. Der Job wird ausgeführt und der Status wird aktualisiert.
   - Um die Jobdaten anzuzeigen, klicken Sie im rechten Bereich auf **Details anzeigen**. Informationen dazu finden Sie unter Einzelne Jobinformationen anzeigen auf Seite 134.

Erstellen eines Jobs zum Ändern des Plugin-Typs der virtuellen Konsole

Sie können den Plugin-Typ der virtuellen Konsole bei mehreren Geräten in HTML5 ändern. Das Aktualisieren auf HTML5 kann zu einem besseren Browsererlebnis führen. Gehen Sie zum Aktualisieren wie folgt vor:

1. Klicken Sie auf **OpenManage Enterprise** > **Überwachen** > **Jobs**
2. Klicken Sie auf **Erstellen** und wählen Sie dann **Plug-in der virtuellen Konsole auf Geräten ändern** aus.
3. Führen Sie Folgendes im Dialogfeld **Assistent zum Ändern des Plug-ins der virtuellen Konsole** im Abschnitt **Optionen** durch:
   a. Geben Sie den Jobnamen in **Jobname** ein. Standardmäßig wird der Plug-in-Typ als HTML5 angezeigt.
   b. Klicken Sie auf **Weiter**.
4. Wählen Sie im Abschnitt **Job-Ziel** die Zielgeräte aus, und klicken Sie auf **Weiter**. Informationen dazu finden Sie unter Zielgeräte und Zielgerätegruppen auswählen auf Seite 136.
   a. Klicken Sie auf **Weiter**.
5. Führen Sie im Abschnitt **Zeitplan** den Job sofort aus oder planen Sie ihn für einen späteren Zeitpunkt. Informationen dazu finden Sie unter Felddefinitionen für die Jobplanung auf Seite 182.
6. Klicken Sie auf **Fertigstellen**.
   Der Job wird erstellt, in der Liste „Jobs" aufgeführt und durch einen entsprechenden Status in der Spalte **JOBSTATUS** gekennzeichnet.
7. Wenn der Job für einen späteren Zeitpunkt geplant ist, Sie den Job jedoch sofort ausführen möchten:
   - Aktivieren Sie auf der Seite „Jobs" das Kontrollkästchen des entsprechenden geplanten Jobs.
   - Klicken Sie auf **Jetzt ausführen**. Der Job wird ausgeführt und der Status wird aktualisiert.
   - Um die Jobdaten anzuzeigen, klicken Sie im rechten Bereich auf **Details anzeigen**. Informationen dazu finden Sie unter Einzelne Jobinformationen anzeigen auf Seite 134.

Zielgeräte und Zielgerätegruppen auswählen

Standardmäßig ist **Geräte auswählen** ausgewählt, um anzugeben, dass der Job auf den Geräten ausgeführt werden kann. Sie können einen Job auf der Gerätegruppen auch ausführen, indem Sie **Gruppen auswählen** wählen.

ANMERKUNG: Die angezeigten Gerätegruppen und Geräte unterliegen dem bereichsbasierten betrieblichen Zugriff, den der Nutzer für die Geräte hat. Weitere Informationen finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Klicken Sie auf **Geräte auswählen**.

Im Dialogfeld **Job-Ziel** werden im linken Fensterbereich die von OpenManage Enterprise überwachten Geräte aufgelistet.
Im Arbeitsbereich wird die Liste der jede Gruppe zugeordneten Geräte und die Gerätedetails angezeigt. Informationen zu Feldbeschreibungen finden Sie unter Geräteliste auf Seite 62. Weitere Informationen zu Gerätegruppen finden Sie unter Geräte in Gruppen organisieren auf Seite 55.

2. Aktivieren Sie das Kontrollkästchen des entsprechenden Geräts und klicken Sie auf **OK**.
   Die ausgewählten Geräte werden im Abschnitt **Alle ausgewählten Geräte** in der ausgewählten Gruppe angezeigt.

Verwalten von Jobs

Wenn Jobs erstellt und auf der Seite **Jobs** angezeigt werden, können Sie sie wie folgt verwalten.

- **Jobs ausführen**: Markieren Sie das entsprechende Kontrollkästchen eines Jobs und klicken Sie dann auf **Jetzt ausführen**, um die Aufgabe auf den Zielgeräten auszuführen. Sie können einen Job ausführen, wenn er sich im aktivierten Status befindet.
- **Jobs aktivieren**: Markieren Sie das entsprechende Kontrollkästchen eines Jobs und klicken Sie dann auf **Aktivieren**.
- **Jobs deaktivieren**: Markieren Sie das entsprechende Kontrollkästchen eines Jobs und klicken Sie dann auf **Deaktivieren**.

  ANMERKUNG: Die Ausführung kann nur für Jobs mit dem Status „Geplant“ deaktiviert werden. Jobs, die bereits aktiv sind und sich im Status „Wird ausgeführt“ befinden, können nicht mehr deaktiviert werden.
- **Jobs beenden**: Markieren Sie das entsprechende Kontrollkästchen eines Jobs und klicken Sie dann auf **Beenden**. Sie können einen Job beenden, wenn er sich im ausgeführten Status befindet.
- **Löschen**: Markieren Sie das entsprechende Kontrollkästchen eines Jobs und klicken Sie dann auf **Löschen**.

Verwalten der Gerätegewährleistung

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Indem Sie auf **OpenManage Enterprise** > **Überwachen** > **Service** klicken, können Sie den Gewährleistungsstatus aller von OpenManage Enterprise überwachten Geräte anzeigen, die sich in Ihrem Bereich befinden. Beispiel: Ein Administrator, der Zugriff auf alle Gerätegruppen hat, kann die Gewährleistungsdetails aller Geräte anzeigen. Die Geräte-Manager sehen jedoch die Gewährleistungsdetails nur für die Geräte, die sich in ihrem jeweiligen Bereich befinden.

Zu statistischen und Analysezwecken können Sie die ausgewählten oder alle Daten auch in ein Excel-Datenblatt exportieren. Die Gewährleistungsseite zeigt die folgenden Informationen an:

- **STATUS** der Gewährleistung

  ANMERKUNG: Der Gewährleistungsstatus wird von den Einstellungen bestimmt, die der Administrator auswählt. Siehe . Verwalten von Gewährleistungseinstellungen auf Seite 169

  - bedeutet **kritisch** und zeigt an, dass die Gewährleistung abgelaufen ist.
  - bedeutet eine **Warnung**, die darauf hinweist, dass die Gewährleistung bald abläuft.
  - bedeutet **normal** und zeigt an, dass die Gewährleistung aktiv ist.
- **SERVICE-TAG-NUMMER**
- **GERÄTEMODELL**
- **GERÄTETYP**
- **GEWÄHRLEISTUNGSTYP**:
  - Erstpaket: Die mit dem Kauf von OpenManage Enterprise zur Verfügung gestellte Gewährleistung.
  - Erweitert: Die Gewährleistung ist erweitert, da die ursprüngliche Gewährleistungsdauer abgelaufen ist.
- **SERVICE-LEVEL-BESCHREIBUNG**: Zeigt das Service Level Agreement (SLA) entsprechend der mit dem Gerät verknüpften Gewährleistung an.
- **VERBLEIBENDE TAGE** – Die Anzahl der verbleibenden Tage bis zum Ablauf der Gewährleistung. Sie können einstellen, wie viele Tage vorher eine Warnung ausgelöst wird. Informationen dazu finden Sie unter Verwalten von Gewährleistungseinstellungen auf Seite 169.

OpenManage Enterprise bietet einen integrierten Bericht zu den Services, die in den nächsten 30 Tagen ablaufen. Klicken Sie auf **OpenManage Enterprise** > **Überwachen** > **Berichte** > **Services, die in den nächsten 30 Tagen ablaufen**. Klicken Sie auf **Ausführen**. Informationen dazu finden Sie unter Berichte ausführen auf Seite 141.

Zum Filtern der in der Tabelle angezeigten Daten klicken Sie auf **Erweiterte Filter**. Lesen Sie den Abschnitt zu den erweiterten Filtern in Übersicht über die grafische Benutzeroberfläche von OpenManage Enterprise auf Seite 36.

Der Gewährleistungsstatus für alle ermittelten Geräte wird einmal pro Woche automatisch von einem integrierten Gewährleistungsjob erfasst. Sie können den Gewährleistungsjob auch manuell initiieren, indem Sie in der oberen rechten Ecke auf **Gewährleistung aktualisieren** klicken.

Zum Exportieren aller oder ausgewählter Gewährleistungsdaten klicken Sie auf **Export**. Informationen dazu finden Sie unter Alle oder ausgewählte Daten exportieren auf Seite 68.

Zugehörige Tasks

Anzeigen und Erneuern der Gerätegewährleistung auf Seite 139

Themen:

Anzeigen und Erneuern der Gerätegewährleistung

Klicken Sie auf **OpenManage Enterprise** > **Überwachen** > **Gewährleistung**. So erhalten Sie eine Liste des Gewährleistungsstatus aller von OpenManage Enterprise überwachten Geräte, zusammen mit ihrer Service-Tag--Nummer, Modellbezeichnung, Gerätetyp, zugeordneten Gewährleistung und Service-Level-Informationen.. Informationen zu Feldbeschreibungen finden Sie unter Verwalten der Gerätegewährleistung auf Seite 138.

Zum Anzeigen der Gewährleistungsinformationen und zum Erneuern der Gewährleistung für ein Gerät:

- Aktivieren Sie das Kontrollkästchen für das jeweilige Gerät. Im rechten Fensterbereich werden der Gewährleistungsstatus und andere wichtige Details des Geräts angezeigt, z. B. den Service-Level-Code, Serviceanbieter, Beginndatum der Gewährleistung, Enddatum der Gewährleistung usw.
- Abgelaufene Gewährleistungen können durch Klicken auf **Dell Gewährleistungsverlängerung für Gerät** verlängert werden. Dadurch werden Sie auf die Dell EMC Support-Website umgeleitet, damit Sie Ihre Gerätegewährleistung verwalten können.
- Klicken Sie auf **Gewährleistung aktualisieren** in der oberen rechten Ecke, um die Gewährleistungstabelle zu aktualisieren. Der Gewährleistungsstatus ändert sich automatisch von kritisch  zu normal , und zwar bei allen Geräten, deren Gewährleistungen erneuert sind. Bei jedem Klicken auf **Service aktualisieren** wird ein neues Warnungsprotokoll für den Geräteservice mit der Gesamtzahl der abgelaufenen Services in der Konsole generiert. Weitere Informationen zu Warnungsprotokollen finden Sie unter Anzeigen der Warnungsprotokolle.
- Zum Sortieren der Daten in der Tabelle basierend auf einer Spalte klicken Sie auf den Spaltentitel.
- Klicken Sie zum Anpassen auf die Schaltfläche **Erweiterte Filter**.

Zugehörige Informationen

Verwalten der Gerätegewährleistung auf Seite 138

18

Berichte

Indem Sie au f **OpenManage Enterprise** > **Überwachen** > **Berichte** klicken, können Sie benutzerdefinierte Berichte erstellen, um die Gerätedetails in der Tiefe anzuzeigen. Mithilfe von Berichten können Sie Daten über die Geräte, Jobs, Warnungen und anderen Elementen in Ihrem Rechenzentrum aufrufen. Berichte sind integriert und nutzerdefiniert. Sie können nur die nutzerdefinierten Berichte bearbeiten oder löschen. Definitionen und Kriterien, die für einen integrierten Bericht verwendet werden, können nicht bearbeitet oder gelöscht werden. Eine Vorschau für den Bericht, den Sie aus der Liste „Berichte" auswählen, wird im rechten Fensterbereich angezeigt.

Die Berichte und Daten, die auf der Seite „Berichte" angezeigt werden, hängen von den bereichsbasierten Nutzerberechtigungen ab, die Sie in OpenManage Enterprise haben. Beispiel: Geräte-Manager haben nur Zugriff auf die Berichte, die sie zusätzlich zu den integrierten Berichten erstellt haben. Außerdem enthält der von einem Nutzer erzeugte Bericht nur Daten von den Geräten, die im Bereich für diesen Nutzer sind. Beispiel: Berichte, die vom Administrator und dem „uneingeschränkten" Geräte-Managern erzeugt werden, enthalten Daten in allen Gerätegruppen. Berichte, die von Geräte-Managern erzeugt werden, die über einen eingeschränkten Bereich verfügen, enthalten Daten, die sich nur auf die Geräte und/oder Gerätegruppen beziehen, die im Bereich enthalten sind.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Tabelle 24. Die rollenbasierten Zugriffsberechtigungen für das Verwalten von Berichten auf OpenManage Enterprise

Benutzerrolle...	Zulässige Berichtsaufgaben...
Administratoren und Geräte-Manager	Ausführen, Erstellen, Bearbeiten, Kopieren, als E-Mail senden, Herunterladen und Exportieren
Anzeigen	Ausführen, als E-Mail senden, Exportieren, Anzeigen und Herunterladen

Vorteile der Berichtsfunktion:
- Sie können mithilfe von bis zu 20 Filtern Berichtskriterien erstellen.
- Sie können Daten filtern und nach Spaltennamen Ihrer Wahl sortieren.
- Sie können Berichte einsehen, herunterladen und per E-Mail versenden.
- Sie können Berichte an 20 bis 30 Empfänger gleichzeitig senden.
- Wenn Sie das Gefühl haben, dass die Berichterstellung viel Zeit benötigt, können Sie den Vorgang anhalten.
- Die generierten Berichte werden automatisch in die Sprache übersetzt, die während der Installation von OpenManage Enterprise eingestellt war.
- Jedes Mal, wenn Sie eine Berichtsdefinition erstellen, bearbeiten, löschen oder kopieren, wird ein Eintrag im Auditprotokoll gemacht.

Derzeit können die folgenden integrierten Berichte zum Extrahieren der folgenden Informationen erzeugt werden:

- Gerätekategorie: Bestand, FRU, Firmware, Firmware-/Treiber-Compliance, geplante Jobs, Warnungszusammenfassung, Festplatte, modulares Gehäuse, NIC, virtuelle Festplatte, Gewährleistung und Lizenz.
- Warnungskategorie: Wöchentlich Warnungen

Zugehörige Tasks

Berichte ausführen auf Seite 141
Ausführen und Senden von Berichten per E-Mail auf Seite 141
Berichte bearbeiten auf Seite 142
Berichte löschen auf Seite 142

Themen:

- Berichte bearbeiten
- Kopieren von Berichten
- Berichte löschen
- Erstellen von Berichten
- Exportieren ausgewählter Berichte

Berichte ausführen

Auf der Seite „Berichte“ (**OpenManage Enterprise** > **Monitor** > **Berichte**) können Sie die integrierten Berichte oder die Berichte, die Sie erstellt haben, ausführen, anzeigen und herunterladen.

Wenn Sie einen Bericht ausführen, werden die ersten 20 Zeilen angezeigt und Sie können die Ergebnisse durchblättern. Um alle Zeilen gleichzeitig anzuzeigen, laden Sie den Bericht herunter. Weitere Informationen zum Bearbeiten dieses Werts finden Sie unter Alle oder ausgewählte Daten exportieren auf Seite 68. Daten, die in der Befehlsausgabe angezeigt werden, können nicht sortiert werden, denn das wird in der Abfrage definiert, die zum Erstellen eines Berichts verwendet wird. Um die Daten zu sortieren, bearbeiten Sie den Abfragebericht oder exportieren Sie ihn in eine Excel-Tabelle. Es wird empfohlen, nicht mehr als fünf (5) Berichte auf einmal auszuführen, da die Berichterstattung Systemressourcen verbraucht. Dieser Wert von fünf Berichten hängt von den ermittelten Geräten, genutzten Feldern und der Anzahl der zur Erstellung des Berichts zusammengeführten Berichte ab. Ein Berichtsjob wird erstellt und ausgeführt, wenn eine Berichterstellung angefordert wird. So werden Berichte für rollenbasierte Berechtigungen erstellt, siehe Erstellen von Berichten auf Seite 143.

ANMERKUNG:
- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Berichte, die von Geräte-Managern erzeugt werden, haben nur Daten in Bezug auf die Geräte, die in ihrem Bereich enthalten sind.
- Es wird davon abgeraten, einen Bericht häufig auszuführen, denn es verbraucht Datenverarbeitungs- und Daten-Ressourcen.
- Bei einem Bericht, dessen Kategorie „Gerät“ ist, sind die ersten Spalten im Bericht standardmäßig Gerätename, Gerätemodell und Service-Tag-Nummer des Geräts. Sie können Spalten beim Anpassen Ihres Berichts ausschließen.

Um einen Bericht auszuführen, wählen Sie den Bericht aus und klicken Sie auf **Ausführen**. Auf der Seite **<report name> Berichte** wird der Bericht mithilfe der Felder, die für die Erstellung des Berichts definiert wurden, tabellarisiert.

So laden Sie einen Bericht herunter:

1. Klicken Sie auf **Herunterladen**.
2. Im Dialogfeld **Bericht Herunterladen** wählen Sie den Typ der Ausgabedatei und klicken auf **Fertigstellen**. Die gewählte Ausgabedatei wird angezeigt. Aktuell können Sie Berichte in die Formate XML, PDF, Excel und CSV exportieren. Es erfolgt ein Auditprotokoll-Eintrag, sobald Sie eine Berichtsdefinition erstellen, bearbeiten, löschen oder kopieren.

So senden Sie einen Bericht als E-Mail:

1. Klicken Sie auf **E-Mail**.
2. Wählen Sie im Dialogfeld **Bericht per E-Mail senden** das Dateiformat, geben Sie die E-Mail-Adresse des Empfängers ein und klicken Sie auf **Fertigstellen**. Der Bericht wird gesendet. Sie können Berichte per E-Mail an 20-30 Empfänger gleichzeitig senden.
3. Wenn die E-Mail-Adresse nicht konfiguriert ist, klicken Sie auf **Gehe zu SMTP-Einstellungen**. Weitere Informationen zum Festlegen von SMTP-Einstellungen finden Sie unter Einstellen der SNMP-Anmeldeinformationen auf Seite 169.

ANMERKUNG: Wenn Sie einen Bericht, der bereits erzeugt wurde, herunterladen oder ausführen und ein anderer Benutzer versucht, den Bericht zur gleichen Zeit zu löschen, werden beide Aufgaben erfolgreich abgeschlossen.

Zugehörige Informationen

Berichte auf Seite 140

Ausführen und Senden von Berichten per E-Mail

Sie können den Bericht ausführen und per E-Mail an 20-30 Empfänger gleichzeitig senden.

ANMERKUNG: Der E-Mail-Vorgang schlägt bei umfangreichen Berichten möglicherweise fehl, wenn die Nachrichtengröße die feste auf dem SMTP-Server eingestellte Nachrichtengröße überschreitet. Erwägen Sie in solchen Fällen, den Grenzwert für die Nachrichtengröße des SMTP-Servers zurücksetzen, und versuchen Sie es erneut.

1. Wählen Sie den Bericht und klicken Sie auf **Ausführen und per E-Mail senden**.
2. Im Dialogfeld **Bericht per E-Mail senden**:
   a. Wählen Sie im Drop-Down-Menü **Format** eines der Dateiformate aus, in dem der Bericht erstellt werden muss — HTML, CSV, PDF oder MS-Excel.
   b. Geben Sie im Feld **An** die E-Mail-Adresse des Empfängers ein. Wenn die E-Mail-Adresse nicht konfiguriert ist, klicken Sie auf **Gehe zu SMTP-Einstellungen**. Weitere Informationen zum Festlegen von SMTP-Einstellungen finden Sie unter Einstellen der SNMP-Anmeldeinformationen auf Seite 169.
   c. Klicken Sie auf **Fertigstellen**.
   Der Bericht wird per E-Mail gesendet und in den Überwachungsprotokollen aufgezeichnet.

Zugehörige Informationen

Berichte auf Seite 140

Berichte bearbeiten

Es können nur vom Benutzer erstellte Berichte bearbeitet werden.

1. Wählen Sie den Bericht aus und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Dialogfeld **Berichtsdefinition** die Einstellungen. Siehe Erstellen von Berichten.
3. Klicken Sie auf **Speichern**.
   Die aktualisierten Informationen werden gespeichert. Ein Überwachungsprotokolleintrag wird erzeugt, wenn Sie eine Berichtsdefinition generieren, bearbeiten, löschen oder kopieren.

   ANMERKUNG: Beim Bearbeiten eines benutzerdefinierten Berichts werden, falls die Kategorie geändert wird, die zugehörigen Felder ebenfalls entfernt.

Zugehörige Informationen

Berichte auf Seite 140

Kopieren von Berichten

Es können nur vom Benutzer erstellte Berichte kopiert werden.

1. Wählen Sie den Bericht, klicken Sie auf **Weitere Aktionen** und klicken Sie dann auf **Kopieren**.
2. Geben Sie im Dialogfeld **Berichtsdefinition kopieren** einen neuen Namen für den kopierten Bericht ein.
3. Klicken Sie auf **Speichern**.
   Die aktualisierten Informationen werden gespeichert. Es erfolgt ein Überwachungsprotokoll-Eintrag, sobald Sie eine Berichtsdefinition erstellen, bearbeiten, löschen oder kopieren.

Berichte löschen

Es können nur vom Benutzer erstellte Berichte gelöscht werden. Wenn eine Berichtsdefinition gelöscht wird, wird der zugehörige Berichtsverlauf gelöscht und sämtliche laufenden Berichte, die diese Berichtsdefinition ausführen, werden ebenfalls angehalten.

1. Klicken Sie im Menü **OpenManage Enterprise** unter **Überwachen** auf **Berichte**.
   Eine Liste der verfügbaren Berichte wird angezeigt.
2. Wählen Sie den Bericht, klicken Sie auf **Weitere Aktionen** und klicken Sie dann auf **Löschen**.

   ANMERKUNG: Wenn Sie einen Bericht, der bereits erzeugt wurde, herunterladen oder ausführen und ein anderer Benutzer versucht, den Bericht zur gleichen Zeit zu löschen, werden beide Aufgaben erfolgreich abgeschlossen.

3. Klicken Sie im Dialogfeld **Berichtsdefinition löschen** auf **Ja**, wenn Sie aufgefordert werden, auszuwählen, ob der Bericht gelöscht soll.

Der Bericht wird aus der Berichtsliste gelöscht und die Tabelle wird aktualisiert. Jedes Mal, wenn Sie eine Berichtsdefinition erstellen, bearbeiten, löschen oder kopieren, wird ein Eintrag im Überwachungsprotokoll erstellt.

Zugehörige Informationen

Berichte auf Seite 140

Erstellen von Berichten

ANMERKUNG:
- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Die Berichte, die von Geräte-Managern erzeugt werden, haben nur Daten in Bezug auf die Gerätegruppen, die in ihrem Bereich enthalten sind.
- Einige Tabellen enthalten gerätetypspezifische Daten, die den Bericht effektiv auf diesen Gerätetyp beschränken. Das Mischen von Spalten aus mehreren gerätespezifischen Tabellen verschiedener Typen (z. B. Server und Gehäuse) führt zu einem ungültigen Bericht ohne Ergebnisse.

Für integrierte Berichte gelten Standarddefinitionen (Filterkriterien) für die Erstellung von Berichten. Sie können die Kriterien anpassen, um Ihre eigenen Definitionen zu erstellen und anschließend angepasste Berichte zu generieren. Die Felder oder Spalten, die Sie in Ihrem Bericht anzeigen möchten, sind abhängig von der von Ihnen ausgewählten Kategorie. Sie können immer nur eine Kategorie gleichzeitig auswählen. Die Anordnung der Spalten in ein Bericht kann durch Ziehen und einfügen geändert werden. Auch:
- Berichtsnamen müssen eindeutig sein.
- Die Berichtsdefinition muss über mindestens eine Feld und eine Kategorie verfügen.
- Für Berichte mit den Kategorien „Gerät“ und „Warnung“ müssen die Pflichtfelder „Gerätename“ oder „Gerätegruppe“ vorhanden sein.

Standardmäßig ist **Geräte** als Kategorie ausgewählt, die Spalten „Gerätename“, „Service-Tag-Nummer des Geräts“ und „Gerätemodell“ werden im Arbeitsbereich angezeigt. Falls Sie während der Bearbeitung der Berichtskriterien eine andere Kategorie auswählen, wird eine Meldung angezeigt, die darauf hinweist, dass die Standardfelder entfernt werden. Alle Kategorien verfügen über vordefinierte Eigenschaften, die als Spaltentitel verwendet werden können und die Daten nach den von Ihnen festgelegten Kriterien gefiltert werden. Beispiel für Kategorietypen:
- Jobs: Aufgabenname, Aufgabentyp, Aufgabenstatus und interne Aufgabe.
- Gruppen, Gruppenstatus, Gruppendefinition, Gruppenmitgliedschaftstyp, Gruppenname und Gruppentyp.
- Warnungen: Warnungsstatus, Warnungsschweregrad, Katalogname, Warnungstyp, Warnungs-Unterkategorie und Geräteinformationen.
- Geräte: Warnung, Warnungskatalog, Gehäuselüfter, Device-Software usw. Diese Kriterien besitzen eine weitere Klassifizierung, auf deren Basis Daten gefiltert und Berichte generiert werden können.

Tabelle 25. Rollenbasierten Zugriffsrechte zur Erstellung von Berichten auf OpenManage Enterprise

Benutzerrolle...	Zulässige Berichtsaufgaben...
Administratoren und Geräte-Manager	Ausführen, Erstellen, Bearbeiten, Kopieren, als E-Mail senden, Herunterladen und Exportieren
Anzeigen	Ausführen, als E-Mail senden, Exportieren, Anzeigen und Herunterladen

1. Klicken Sie auf **Berichte** > **Erstellen**.
2. Im Dialogfeld **Berichtsdefinition**:
   a. Geben Sie den Namen und die Beschreibung des neuen Berichts ein, der definiert werden soll.
   b. Klicken Sie auf **Weiter**.
3. Im Abschnitt **Report Builder**:
   a. Wählen Sie aus dem Dropdown-Menü **Kategorie** die Berichtskategorie aus.
      - Wenn Sie „Gerät“ als Kategorie auswählen, wählen Sie außerdem die Gerätegruppe aus.
      - Bearbeiten Sie falls erforderlich die Filterkriterien. Informationen dazu finden Sie unter Abfragekriterien auswählen auf Seite 58.
   b. Aktivieren Sie im Abschnitt **Spalten auswählen** die Kontrollkästchen der Felder, die als Berichtsspalten angezeigt werden müssen.

Ausgewählte Feldnamen werden im Abschnitt **Spaltenreihenfolge** angezeigt.

c. Sie können den Bericht wie folgt anpassen:
   - Verwenden der Felder **Sortieren nach** und **Richtung**.
   - Ziehen Sie die Felder im Abschnitt **Spaltenreihenfolge** nach oben oder unten.

4. Klicken Sie auf **Fertigstellen**.
   Der Bericht wird erstellt und in der Liste der Berichte aufgeführt. Sie können Berichte zu Analysezwecken exportieren. Informationen dazu finden Sie unter Alle oder ausgewählte Daten exportieren auf Seite 68. Es erfolgt ein Auditprotokoll-Eintrag, sobald Sie eine Berichtsdefinition erstellen, bearbeiten, löschen oder kopieren.

Auswählen von Abfragekriterien beim Erstellen von Berichten

Definieren Sie Filter während des Erstellens von Abfragekriterien für:

- Erstellen benutzerdefinierter Berichte. Informationen dazu finden Sie unter Erstellen von Berichten auf Seite 143.
- Erstellen von abfragebasierten Gerätegruppen unter den BENUTZERDEFINIERTEN GRUPPEN. Informationen dazu finden Sie unter Abfrage-Gerätegruppe erstellen auf Seite 58.

Definieren Sie die Abfrage-Kriterien durch die Verwendung von zwei Optionen:

- **Wählen Sie vorhandene Abfrage zum Kopieren**: Standardmäßig bietet OpenManage Enterprise eine Liste integrierter Abfrage-Vorlagen, die Sie kopieren und Ihre eigenen Abfragekriterien und aufbauen können. Bei der Definition einer Abfrage können maximal 20 Kriterien (Filter) verwendet werden. Zum Hinzufügen von Filtern müssen Sie eine Option aus dem Drop-Down-Menü **Typ auswählen** wählen.
- **Typ auswählen**: Erstellen Sie ein Abfragekriterium von Grund auf, indem Sie Attribute aus diesem Drop-Down-Menü verwenden. Optionen im Menü hängen von den durch OpenManage Enterprise überwachten Geräten ab. Wenn ein Abfragetyp ausgewählt ist, werden nur entsprechende Operatoren, wie z. B. =, >, < und null angezeigt, basierend auf dem Abfragetyp. Diese Methode wird empfohlen für die Definition von Abfragekriterien bei der Erstellung von benutzerspezifischen Berichten.

  ANMERKUNG: Bei der Bewertung einer Abfrage mit mehreren Bedingungen ist die Reihenfolge der Auswertung die gleiche wie bei SQL. Zur Angabe einer bestimmten Reihenfolge für die Beurteilung der Bedingungen fügen Sie bei der Definition einer Abfrage Klammern hinzu bzw. entfernen diese.

ANMERKUNG: Bei Auswahl werden die Filterkriterien einer vorhandenen Abfrage nur virtuell kopiert, um ein neues Abfragekriterium zu erstellen. Die standardmäßigen Filterkriterien im Zusammenhang mit vorhandenen Abfragekriterien werden nicht geändert. Die Definition (Filter) von integrierten Abfragekriterien wird als Startpunkt für den Aufbau eines benutzerdefinierten Abfragekriteriums verwendet. Beispiel:

1. *Abfrage1* ist ein integriertes Abfragekriterium mit dem folgenden vordefinierten Filter: `Task Enabled=Yes`.
2. Kopieren Sie die Filter-Eigenschaften von *Abfrage1*, erstellen Sie *Abfrage2* und passen Sie die Abfragekriterien durch Hinzufügen eines weiteren Filters an: `Task Enabled=Yes` UND `(Task Type=Discovery)`.
3. Später öffnen Sie *Abfrage1*. Das Filterkriterium bleibt weiterhin `Task Enabled=Yes`.

1. Im Dialogfeld **Abfragekriterien-Auswahl** wählen Sie aus dem Drop-Down-Menü je nachdem, ob Sie ein Abfragekriterium für Abfrage-Gruppen oder für die Berichterstellung erstellen möchten.
2. Hinzufügen oder Entfernen eines Filters durch Klicken auf das Plus- oder Papierkorb-Symbol.
3. Klicken Sie auf **Fertigstellen**.
   Ein Abfragekriterium wird in der Liste der vorhandenen Abfragen erstellt und gespeichert. Ein Überwachungsprotokoll-Eintrag wird gemacht und in der Überwachungsprotokoll-Liste angezeigt. Informationen dazu finden Sie unter Überwachen von Auditprotokollen auf Seite 127.

Exportieren ausgewählter Berichte

1. Wählen Sie die Kontrollkästchen der entsprechenden zu exportierenden Berichte, klicken Sie auf **Weitere Aktionen** und klicken Sie dann auf **Ausgewählte exportieren**.

   Gegenwärtig können Sie nicht alle Berichte auf einmal exportieren.
2. Wählen Sie im Dialogfeld **Ausgewählte Berichte exportieren** eines der folgenden Dateiformate aus, in dem der Bericht erstellt werden muss — HTML, CSV oder PDF.
3. Klicken Sie auf **Fertigstellen**.
   Öffnen oder speichern Sie im Dialogfeld die Datei an einem bekannten Speicherort zu Analyse- und statistischen Zwecke.

19

Verwalten von MIB-Dateien

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Tools von Drittanbietern in Ihrem Rechenzentrum können Warnungen erzeugen, die entscheidend für Ihren Betriebsablauf sind. Solche Warnungen werden in Management Information Base-(MIB)-Dateien gespeichert, definiert und von den jeweiligen Tools verstanden. Jedoch ermöglicht OpenManage Enterprise Ihnen auch die Verwaltung solcher MIBs, sodass MIBs, die nicht von Dell EMC stammen, importiert, analysiert und von OpenManage Enterprise zum Gerätemanagement verwendet werden können. OpenManage Enterprise unterstützt SMI1 und SMI2. OpenManage Enterprise bietet integrierte MIB-Dateien, die für Dell EMC Geräte verwendet werden können. Dies sind schreibgeschützte MIB-Dateien, die nicht bearbeitet werden können.

ANMERKUNG: Nur gültige MIBs mit Traps werden von OpenManage Enterprise verarbeitet.

Sie verwalten von MIBs durch:

- Importieren von MIB-Dateien auf Seite 145
- Entfernen von MIB-Dateien auf Seite 147
- Auflösen von MIB-Typen auf Seite 147

Durch Klicken auf das Menü **OpenManage Enterprise** > **Überwachen** > **MIB** können Sie die MIB-Dateien verwalten, die von OpenManage Enterprise und anderen Systemmanagement-Tools im Rechenzentrum verwendet werden. Eine Tabelle listet die verfügbaren MIB-Dateien mit den folgenden Eigenschaften auf. Klicken Sie auf die jeweilige Spaltenüberschrift, um die Daten zu sortieren.

Tabelle 26. Rollenbasierter Zugriff für MIB-Dateien in OpenManage Enterprise

OpenManage Enterprise – Funktionen	Rollenbasierte Zugriffskontrolle für MIB-Dateien		
	Admin	**Device Manager**	**Viewer**
Traps oder MIBs anzeigen	J	J	J
MIB importieren. Traps bearbeiten.	J	N	N
MIB entfernen	J	N	N
Traps bearbeiten	J	N	N

Um die integrierten MIB-Dateien von OpenManage Enterprise herunterzuladen, klicken Sie auf **MIB herunterladen**. Die Dateien werden in den angegebenen Ordner gespeichert.

Themen:

Importieren von MIB-Dateien

Idealer Prozessablauf von MIB-Import: **Benutzer lädt MIBs auf OpenManage Enterprise hoch** > **OpenManage Enterprise analysiert MIBs** > **OpenManage Enterprise durchsucht die Datenbank nach bereits verfügbaren ähnlichen Traps** > **OpenManage Enterprise zeigt filebasierte MIB-Daten an**. Die maximale Dateigröße von MIB, die importiert werden kann, ist 3 MB. Der OpenManage Enterprise Auditprotokoll-Verlauf zeichnet jeden Import und das Entfernen von MIBs auf.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen rollenbasierten Nutzerberechtigungen und den bereichsbasierten betrieblichen Zugriff auf die Geräte verfügen. Siehe . Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16
- Es kann jeweils nur eine MIB-Datei gleichzeitig importiert werden.

1. Klicken Sie auf **MIB** > **MIB importieren**.
2. Klicken Sie im Dialogfeld **MIB importieren** im Abschnitt **MIB-Dateien hochladen** auf **Datei auswählen**, um eine MIB-Datei auszuwählen.

   Wenn MIB Importaussagen hat, die von der externen MIBs aufgelöst werden, wird eine Meldung angezeigt.

   a. Klicken Sie auf **Typen beheben**. Lösen Sie die MIB-Typen auf. Informationen dazu finden Sie unter Entfernen von MIB-Dateien auf Seite 147.
   b. Klicken Sie auf **Fertigstellen**. Wenn die MIB-Datei in Besitz von Dell EMC ist, wird eine Meldung angezeigt, die darauf hinweist, dass die MIB mit dem Produkt geliefert wird und nicht geändert werden kann.
3. Klicken Sie auf **Weiter**.
4. Im Bereich **Traps anzeigen** Abschnitt, wird eine Liste von MIB-Dateien mit den folgenden Informationen angezeigt:
   - Warnungskategorie des Trap. Sie können die Kategorie bearbeiten und sie mit den OpenManage Enterprise-Kategoriedefinitionen abgleichen. Informationen dazu finden Sie unter Bearbeiten von MIB-Traps auf Seite 146.
   - Der Trapname ist schreibgeschützt. Definiert vom Drittanbietergerät.
   - Schweregrad einer Warnung: Kritisch, Warnung, Information und Normal.
   - Warnmeldung, die zu einer Warnung gehört.
   - „Trap OID“ ist schreibgeschützt und einzigartig.
   - „Neu“ zeigt an, dass der Trap zum ersten Mal von OpenManage Enterprise importiert wird. Bereits importierte Traps werden immer als „Importiert“ angezeigt. „Überschreiben“ zeigt die Traps an, deren Definition aufgrund eines Importvorgangs neu geschrieben wird.

   Informationen, wie Sie die Standard-Warnungskategorien oder den Schweregrad einer-MIB-Datei bearbeiten finden Sie hier Bearbeiten von MIB-Traps auf Seite 146. Wählen sie zum Löschen von MIB-Dateien das entsprechende Kontrollkästchen aus und klicken Sie auf **Trap Löschen**. Die MIB-Dateien werden gelöscht und die Liste der MIB-Dateien wird aktualisiert.
5. Klicken Sie auf **Fertigstellen**. Die MIB-Dateien werden analysiert, in OpenManage Enterprise importiert und unter der Registerkarte **MIN** aufgelistet.

ANMERKUNG: Wenn Sie eine MIB importieren und dann erneut importieren, wird der MIB-Status angezeigt als **IMPORTIERT**. Wenn Sie eine gelöschte MIB-Datei erneut importieren wird der Trap-Status ist immer als **NEU** angezeigt.

ANMERKUNG: Traps, die bereits in OpenManage Enterprise importiert wurden, können nicht importiert werden.

ANMERKUNG: MIB-Dateien, die standardmäßig mit OpenManage Enterprise ausgeliefert werden, können nicht importiert werden.

ANMERKUNG: Ereignisse, die erzeugt werden, nachdem der Trap importiert wurde, werden formatiert und entsprechend der neuen Definition angezeigt.

Bearbeiten von MIB-Traps

1. Wählen Sie den Bericht aus und klicken Sie auf **Bearbeiten**.
2. Im Dialogfeld **MIB-Traps bearbeiten**:
   a. Wählen Sie einen Wert aus oder geben Sie Daten in die Felder ein:
      - Wählen Sie die neue Warnungskategorie aus, die der Warnung zugewiesen werden soll. Standardmäßig zeigt OpenManage Enterprise einige integrierte Warnungskategorien an.
      - Geben Sie die Warnungskomponente ein.
      - Der Trapname ist schreibgeschützt, da er durch das Tool eines Drittanbieters erstellt wurde.
      - Wählen Sie den Schweregrad aus, der der Warnung zugewiesen werden soll. Standardmäßig zeigt OpenManage Enterprise einige integrierte Warnungskategorien an.
      - Eine Meldung, in der die Warnung beschrieben wird.

   b. Klicken Sie auf **Fertigstellen**.
      Der Trap wird bearbeitet und die aktualisierte Trap-Liste wird angezeigt.

ANMERKUNG: Es können nicht mehrere Warnungen gleichzeitig ausgewählt werden. Die in OpenManage Enterprise importierten Traps können nicht bearbeitet werden.

3. Bearbeiten Sie im Dialogfeld **Berichtsdefinition** die Einstellungen. Siehe Erstellen von Berichten.
4. Klicken Sie auf **Speichern**.
   Die aktualisierten Informationen werden gespeichert.

Entfernen von MIB-Dateien

ANMERKUNG: Sie können keine MIB-Datei entfernen, die über Trap-Definitionen verfügt, die von einer der Warnrichtlinien verwendet wird. Informationen dazu finden Sie unter Warnungsrichtlinien auf Seite 121.

ANMERKUNG: Ereignisse, die vor dem Löschen einer MIB empfangen werden, sind von der entsprechenden MIB-Entfernung nicht betroffen. Ereignisse die jedoch nach der Entfernung generiert wurden, verfügen über unformatierte Traps.

1. Erweitern Sie in der Spalte **MIB-DATEINAME** den Ordner und wählen Sie die MIB-Dateien.
2. Klicken Sie auf **MIB entfernen**.
3. Aktivieren Sie das Kontrollkästchen der zu entfernenden MIBs im Dialogfeld **MIB entfernen**.
4. Klicken Sie auf **Entfernen**.
   Die MIB-Dateien werden entfernt und die MIB-Tabelle wird aktualisiert.

Auflösen von MIB-Typen

1. Importieren Sie die MIB-Dateien. Informationen dazu finden Sie unter Importieren von MIB-Dateien auf Seite 145.
   Wenn der MIB-Typ nicht aufgelöst wurde, werden im Dialogfeld **Nicht aufgelöste Typen** MIB-Typen aufgeführt, mit dem Hinweis, dass die MIB-Typen nur nach Auflösung importiert werden.
2. Klicken Sie auf **Typen beheben**.
3. Klicken Sie im Dialogfeld **Typen auflösen** auf **Dateien auswählen**, und wählen Sie dann die fehlenden Dateien aus.
4. Klicken Sie im Dialogfeld **MIB importieren** auf **Weiter**. Wenn immer noch MIB-Typen fehlen, werden diese im Dialogfeld **Nicht aufgelöste Typen** erneut aufgeführt. Wiederholen Sie die Schritte 1 bis 3.
5. Nachdem alle nicht aufgelösten MIB-Typen aufgelöst sind, klicken Sie auf **Fertig stellen**. Schließen Sie den Importvorgang ab. Informationen dazu finden Sie unter Importieren von MIB-Dateien auf Seite 145.

Laden Sie eine MIB-Datei für OpenManage Enterprise herunter

1. Klicken Sie auf der **Startseite** auf **MIB**.
2. Erweitern Sie eine MIB-Datei für OpenManage Enterprise und wählen Sie sie aus und klicken Sie dann auf **MIB herunterladen**.

   ANMERKUNG: Sie können nur die auf OpenManage Enterprise bezogenen MIB-Dateien herunterladen.

20

Verwalten von OpenManage Enterprise-Geräteeinstellungen

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

ANMERKUNG: Informationen zu unterstützten Browsern finden Sie in der *OpenManage Enterprise Supportmatrix* auf der Support-Website.

Indem Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen** klicken, können Sie:

- Die OpenManage Enterprise-Netzwerkeinstellungen konfigurieren und verwalten, wie beispielsweise IPv4, IPv6, Uhrzeit und Proxy-Einstellungen. Informationen finden Sie unter Konfigurieren der Netzwerkeinstellungen.
- Nutzer hinzufügen, aktivieren, bearbeiten und löschen. Siehe Verwalten von Nutzern.
- Den Gerätezustand und die Überwachungseigenschaften des Dashboard festlegen. Siehe Verwalten der Konsolen-Voreinstellungen.
- Nutzeranmeldung und Richtlinien für die Anmeldesperrung verwalten. Siehe Festlegen der Anmeldungs-Sicherheitseigenschaften.
- Anzeigen des aktuellen SSL-Zertifikats und anschließendes Erstellen einer CSR-Anfrage. Informationen dazu finden Sie unter Generieren und Herunterladen der Zertifikatsignierungsanforderung auf Seite 164.
- E-Mail-, SNMP und Syslog-Eigenschaften für Warnungsverwaltung konfigurieren. Informationen dazu finden Sie unter SMTP-, SNMP- und Syslog-Warnungen konfigurieren auf Seite 124.
- SNMP-Listener- und Trap-Weiterleitungseinstellungen festlegen. Siehe Verwalten eingehender Warnungen.
- Legen Sie die Anmeldeinformationen und die Uhrzeit für den Empfang von Benachrichtigungen über den Ablauf des Service fest. Siehe Verwalten von Garantieeinstellungen.
- Die Eigenschaften für die Suche nach Verfügbarkeit der aktualisierten Version festlegen und anschließend die OpenManage Enterprise-Version aktualisieren. Informationen dazu finden Sie unter Überprüfen und Aktualisieren der Version von OpenManage Enterprise und der verfügbaren Plug-ins auf Seite 170.
- Legen Sie die Anmeldeinformationen von Benutzern zum Ausführen des Remote-Befehls unter Verwendung von RACADM und IPMI fest. Siehe Ausführen von Remote-Befehlen & -Skripten.
- Festlegen und Empfangen von Warnbenachrichtigungen auf Ihrem Mobiltelefon. Informationen dazu finden Sie unter OpenManage Mobile-Einstellungen auf Seite 177.

Zugehörige Tasks

Löschen von Verzeichnisdiensten auf Seite 160

Themen:

- OpenManage Mobile-Einstellungen

OpenManage Enterprise-Netzwerkeinstellungen konfigurieren

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

1. Erweitern Sie das Feld **Aktuelle Einstellungen**, um nur die aktuellen Netzwerkeinstellungen aller aktiven Netzwerkverbindungen von OpenManage Enterprise, wie z. B. DNS-Domänenname, FQDN und IPv4- und IPv6-Einstellungen, anzuzeigen.
2. Um das Sitzungszeitlimit und die maximale Anzahl von Sitzungen für die Nutzer der OpenManage Enterprise API und der Webschnittstelle zu konfigurieren, erweitern Sie die Konfiguration für das **Sitzungsinaktivitätszeitlimit** und führen Sie folgende Schritte aus:
    a. Aktivieren Sie das Kontrollkästchen **Aktivieren**, um das universelle Zeitlimit zu aktivieren, und geben Sie den Wert für das **Inaktivitätszeitlimit (1–1440)** ein. Der Wert für das Inaktivitätszeitlimit kann auf zwischen 1 Minute und 1440 Minuten (24 Stunden) eingestellt werden. Standardmäßig ist das universelle Zeitlimit ausgegraut. Durch die Aktivierung des universellen Zeitlimits werden die API- und Webinterface-Felder deaktiviert.
    b. Ändern Sie das **Inaktivitätszeitlimit (1–1440)** der API und die Werte für **Maximale Anzahl von Sitzungen (1–100)**. Diese Attribute sind standardmäßig auf 30 Minuten bzw. 100 festgelegt.
    c. Ändern Sie das **Inaktivitätszeitlimit (1–1440)** der Weboberfläche und die Werte für **Maximale Anzahl von Sitzungen (1–100)**. Diese Attribute sind standardmäßig auf 30 Minuten bzw. 100 festgelegt.
    d. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern, oder wählen Sie **Verwerfen**, um die Standardwerte beizubehalten.
3. Die aktuelle Systemzeit und die lokale Zeitzone bzw. die NTP-Server-IP werden angezeigt. Wenn Sie Zeitzone, Datum Uhrzeit und NTP-Serversynchronisation für das System konfigurieren möchten, erweitern Sie **Zeitkonfiguration**.
    a. Wählen Sie die gewünschte Zeitzone aus der Dropdown-Liste aus.
    b. Geben Sie das Datum ein oder klicken Sie auf das **Kalender** Symbol, um ein Datum auszuwählen.
    c. Geben Sie die Uhrzeit im Format HH:MM:SS ein.
    d. Wählen Sie zur Synchronisierung mit einem NTP-Server das Kontrollkästchen **NTP verwenden** und geben Sie die Serveradresse des primären NTP-Servers ein.

        In OpenManage Enterprise können Sie bis zu drei NTP-Server konfigurieren.

        ANMERKUNG: Die Optionen **Datum** und **Uhrzeit** sind nicht verfügbar, wenn die **NTP verwenden** Option ausgewählt ist.

    e. Klicken Sie auf **Anwenden**.
    f. Um die Einstellungen auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.
4. Um die OpenManage Enterprise-Proxy-Einstellungen zu konfigurieren, erweitern Sie das Feld **Proxy-Konfiguration**.
    a. Wählen Sie **Aktivieren Sie die HTTP-Proxy Einstellungen** zum Konfigurieren der HTTP-Proxy aus und geben Sie dann HTTP-Proxy-Adresse und HTTP-Portnummer ein.
    b. Aktivieren Sie das Kontrollkästchen **Proxy-Authentifizierung aktivieren**, um die Proxy-Anmeldeinformationen zu aktivieren, und geben Sie dann den Nutzernamen und das Kennwort ein.
    c. Aktivieren Sie das Kontrollkästchen **Zertifikat-Validierung ignorieren**, wenn der konfigurierte Proxy den SSL-Datenverkehr abfängt und kein vertrauenswürdiges Drittanbieterzertifikat verwendet. Mit dieser Option werden die integrierten Zertifikat-Prüfungen ignoriert, die für die Gewährleistung und die Katalogsynchronisierung verwendet werden.
    d. Klicken Sie auf **Anwenden**.
    e. Um die Einstellungen auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.

Informationen zu den Aufgaben, die Sie mithilfe der Anwendungseinstellungen-Funktion durchführen können, finden Sie unter Verwalten von OpenManage Enterprise-Geräteeinstellungen auf Seite 148.

Verwalten von OpenManage Enterprise-Nutzern

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

- Jede Änderung an der Benutzerrolle wirkt sich nicht auf die aktive Sitzung der betroffenen Benutzer aus und wird bei der nächsten Anmeldung wirksam.
- Wenn ein Geräte-Manager-Benutzer (DM) zu einem Viewer heruntergestuft wird, verliert dieser DM den Zugriff auf alle Entitäten in seinem Besitz, z. B. Jobs, Firmware- oder Konfigurationsvorlagen, Baselines, Warnmeldungsrichtlinien und Profile. Diese Entitäten können nur vom Administrator verwaltet werden und können nicht wiederhergestellt werden, selbst wenn derselbe Benutzer von einem Viewer zum DM hochgestuft wird.

Indem Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Benutzer** klicken, können Sie:

- Lokale OpenManage Enterprise-Nutzer einsehen, hinzufügen, aktivieren, bearbeiten, deaktivieren oder löschen. Weitere Informationen finden Sie unter Hinzufügen und Bearbeiten von lokalen OpenManage Enterprise-Nutzern
- Weisen Sie Active Directory-Nutzern OpenManage Enterprise-Rollen zu, indem Sie die Verzeichnisgruppen importieren. Active Directory- und LDAP-Verzeichnis-Benutzern kann in OpenManage Enterprise eine Administrator-, eine Geräte-Manager- oder eine Viewer-Rolle zugewiesen werden. Weitere Informationen finden Sie unter Importieren von AD- und LDAP-Gruppen auf Seite 155
- Zeigen Sie die Details zu den angemeldeten Benutzern an und beenden Sie eine Benutzersitzung.
- Verwalten von Verzeichnisdiensten Weitere Informationen finden Sie unter Hinzufügen oder Bearbeiten von Active Directory-Gruppen zur Verwendung mit Verzeichnisdiensten auf Seite 158
- Sie können OpenID Connect-Anbieter (PingFederate und/oder Key Cloak) einsehen, hinzufügen, aktivieren, bearbeiten, deaktivieren oder löschen. Weitere Informationen finden Sie unter Anmelden bei OpenManage Enterprise über OpenID Connect-Anbieter auf Seite 160

Standardmäßig wird die Liste der Benutzer unter **Benutzer** angezeigt. Im rechten Fensterbereich werden die Eigenschaften eines im Arbeitsbereich ausgewählten Nutzernamens angezeigt.

- **BENUTZERNAME**: Neben den von Ihnen erstellten Benutzern zeigt OpenManage Enterprise die folgenden standardmäßigen Benutzerrollen an, die nicht bearbeitet oder gelöscht werden können: Admin, System und Root. Sie können die Anmeldeinformationen jedoch durch Auswahl des Standardbenutzernamens und klicken auf **Bearbeiten** bearbeiten. Informationen dazu finden Sie unter Aktivieren von OpenManage Enterprise-Benutzern auf Seite 154. Die empfohlenen Zeichen für Nutzernamen sind:
  - 0-9
  - A–Z
  - a–z
  - - ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >
  - Die empfohlenen Zeichen für Kennwörter sind:
    - 0-9
    - A–Z
    - a–z
    - ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >
- **BENUTZERTYP**: Gibt an, ob sich der Benutzer lokal oder remote angemeldet hat.
- **AKTIVIERT**: Gibt mit einem Häkchen an, ob der Benutzer für die Durchführung von OpenManage Enterprise-Verwaltungsaufgaben aktiviert ist. Siehe Aktivieren von OpenManage Enterprise-Benutzern auf Seite 154 und Deaktivieren von OpenManage Enterprise-Benutzern auf Seite 155.
- **ROLLE**: Gibt die Benutzerrolle in OpenManage Enterprise an. Zum Beispiel OpenManage Enterprise-Administrator und Device Manager. Informationen dazu finden Sie unter OpenManage Enterprise-Nutzerrollentypen auf Seite 15.

Verwandte Verweise

Deaktivieren von OpenManage Enterprise-Benutzern auf Seite 155

Aktivieren von OpenManage Enterprise-Benutzern auf Seite 154

Zugehörige Tasks

Löschen von Verzeichnisdiensten auf Seite 160

Löschen von OpenManage Enterprise-Benutzern auf Seite 155

Beenden von Benutzersitzungen auf Seite 157

Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise

OpenManage Enterprise verfügt über rollenbasierte Zugriffskontrolle (RBAC), die die Nutzerberechtigungen für die drei integrierten Rollen (Administrator, Device Manager und Viewer) eindeutig definiert. Darüber hinaus kann ein Administrator mithilfe der bereichsbasierten

Zugriffskontrolle (SBAC) die Gerätegruppen begrenzen, auf die ein Device Manager Zugriff hat. In den folgenden Themen werden die RBAC- und SBAC-Funktionen erläutert.

Berechtigungen der rollenbasierten Zugriffskontrolle (RBAC) in OpenManage Enterprise

Den Nutzern werden Rollen zugewiesen, die ihren Zugriff auf die Appliance-Einstellungen und Geräteverwaltungsfunktionen bestimmen. Diese Funktion wird als rollenbasierte Zugriffskontrolle (RBAC, Role-Based Access Control) bezeichnet. Die Konsole erzwingt die für eine bestimmte Aktion erforderliche Berechtigung, bevor die Aktion zugelassen wird. Weitere Informationen zum Verwalten von Nutzern auf OpenManage Enterprise finden Sie unter Verwalten von OpenManage Enterprise-Nutzern auf Seite 149.

In dieser Tabelle sind die verschiedenen Berechtigungen aufgeführt, die für jede Rolle aktiviert sind.

Tabelle 27. Rollenbasierte Nutzerberechtigungen in OpenManage Enterprise

OpenManage Enterprise – Funktionen	Beschreibung der Berechtigungen	Nutzerebenen für den Zugriff auf OpenManage Enterprise		
		Admin	Device Manager	Viewer
Appliance-Einrichtung	Globale Appliance-Einstellungen, einschließlich der Einrichtung der Appliance.	**J**	N	N
Sicherheitskonfiguration	Sicherheitseinstellungen der Appliance	**J**	N	N
Warnungsverwaltung	Warnungsmaßnahmen/-verwaltung	**J**	N	N
Fabric-Management	Fabric-Aktionen/-Management	**J**	N	N
Netzwerkverwaltung	Netzwerkmaßnahmen/-verwaltung	**J**	N	N
Gruppenverwaltung	Erstellen, Lesen, Aktualisieren und Löschen (CRUD) für statische und dynamische Gruppen	**J**	N	N
Ermittlungsverwaltung	CRUD für Ermittlungsaufgaben, Ausführen von Ermittlungsaufgaben	**J**	N	N
Bestandsverwaltung	CRUD für Bestandsaufnahmeaufgaben, Ausführen von Bestandsaufnahmeaufgaben	**J**	N	N
Trap-Management	MIB-Import, Trap-Bearbeitung	**J**	N	N
Verwaltung der automatischen Bereitstellung	Verwalten der automatischen Bereitstellung von Konfigurationsvorgängen	**J**	N	N
Überwachungskonfiguration	Warnmeldungsrichtlinien, Weiterleitung, SupportAssist usw.	**J**	**J**	N
Betriebsschalter	Neustart/Ein- und Ausschalten der Gerätestromversorgung	**J**	**J**	N
Device-Konfiguration	Device-Konfiguration, Anwendung von Vorlagen, Verwaltung/Migration der IO-Identität, Speicherzuordnung (für Speichergeräte) usw.	**J**	**J**	N
Betriebssystembereitstellung	Bereitstellen des Betriebssystems, Zuordnung zu LUN usw.	**J**	**J**	N
Geräteupdate	Geräte-Firmwareupdates, Anwendung aktualisierter Baselines usw.	**J**	**J**	N
Vorlagenverwaltung	Erstellen/Verwalten von Vorlagen	**J**	**J**	N

Tabelle 27. Rollenbasierte Nutzerberechtigungen in OpenManage Enterprise (fortgesetzt)

OpenManage Enterprise – Funktionen	Beschreibung der Berechtigungen	Nutzerebenen für den Zugriff auf OpenManage Enterprise		
		Admin	Device Manager	Viewer
Baseline-Management	Erstellen/Verwalten von Firmware/ Konfigurations-Baseline-Richtlinien	**J**	**J**	N
Energiemanagement	Festlegen von Energiebudgets	**J**	**J**	N
Jobverwaltung	Jobausführung/-verwaltung	**J**	**J**	N
Berichtsverwaltung	CRUD-Vorgänge für Berichte	**J**	**J**	N
Ausführen von Berichten	Berichte ausführen	**J**	**J**	**J**
Ansicht	Anzeigen aller Daten, Berichtausführung/-verwaltung usw.	**J**	**J**	**J**

Bereichsbasierte Zugriffskontrolle (SBAC) in OpenManage Enterprise

Mithilfe der Funktion der rollenbasierten Zugriffskontrolle (RBAC) können Administratoren Rollen zuweisen, während sie Nutzer erstellen. Die Rollen bestimmen den Zugriff der Nutzer auf die Appliance-Einstellungen und Gerätemanagementfunktionen. Die bereichsbasierte Zugriffskontrolle (SBAC) ist eine Erweiterung der RBAC-Funktion, die es einem Administrator ermöglicht, eine Device Manager-Rolle auf eine Teilmenge von Gerätegruppen, genannt Bereich, zu beschränken.

Beim Erstellen oder Aktualisieren eines Device Manager (DM) können Administratoren einen Bereich zuweisen, um den betrieblichen Zugriff des DM auf eine oder mehrere Systemgruppen, nutzerdefinierte Gruppen und/oder Plug-in-Gruppen zu beschränken.

Administrator- und Viewer-Rollen haben einen uneingeschränkten Bereichszugriff. Das bedeutet, dass Sie den betrieblichen Zugriff haben, wie durch RBAC-Berechtigungen für alle Geräte- und Gruppeneinheiten angegeben.

Der Bereich kann wie folgt implementiert werden:

1. Nutzer erstellen oder bearbeiten
2. DM-Rolle zuweisen
3. Bereich zur Beschränkung des betrieblichen Zugriffs zuweisen

Weitere Informationen zum Verwalten von Nutzern finden Sie unter Verwalten von OpenManage Enterprise-Nutzern auf Seite 149.

Wenn ein Device Manager (DM)-Nutzer mit einem zugewiesenen Bereich sich anmeldet, kann der DM nur dem Bereich zugeordnete Geräte anzeigen und verwalten. Außerdem kann der DM Einheiten wie Jobs, Firmware oder Konfigurationsvorlagen und Baselines, Warnungsrichtlinien, Profile und so weiter im Zusammenhang mit Bereichen zugeordneten Geräten anzeigen und verwalten, und zwar nur dann, wenn der DM die Einheit besitzt (DM hat die Einheit erstellt oder die Eigentumsrechte dieser Einheit sind ihm zugewiesen). Weitere Informationen zu den Einheiten, die ein DM erstellen kann, finden Sie unter *Berechtigungen der rollenbasierten Zugriffskontrolle (RBAC) in OpenManage Enterprise*.

Wenn Sie beispielsweise auf **Konfigurationen** > **Vorlagen** klicken, kann ein DM-Nutzer die standardmäßigen und nutzerdefinierten Vorlagen des DM-Nutzers anzeigen. Außerdem kann der DM-Nutzer andere Aufgaben für eigene Vorlagen durchführen, zu denen er von RBAC berechtigt wurde.

Durch Klicken auf **Konfiguration** > **Identitäts-Pools** kann ein DM-Nutzer alle Identitäten sehen, die von einem Administrator oder dem DM-Nutzer erstellt wurden. Der DM kann auch Aktionen für die durch RBAC-Berechtigung angegebenen Identitäten durchführen. Allerdings kann der DM nur die Nutzung der Identitäten anzeigen, die den Geräten im Bereich des DM zugeordnet sind.

In ähnlicher Weise können Sie durch Klicken auf **Konfiguration** > **VLAN-Pools** alle vom Administrator erstellten VLANs sehen und exportieren. Der DM kann keine anderen Vorgänge ausführen. Wenn der DM eine Vorlage hat, kann er die Vorlage bearbeiten, um die VLAN-Netzwerke zu verwenden, aber das VLAN-Netzwerk kann nicht bearbeitet werden.

In OpenManage Enterprise kann der Bereich beim Erstellen eines lokalen oder Importieren eines AD/LDAP-Nutzers zugewiesen werden. Die Bereichszuweisung für OIDC-Nutzer kann nur auf Open-ID Connect (OIDC)-Anbietern erfolgen.

SBAC für lokale Nutzer:

Beim Erstellen oder Bearbeiten eines lokalen Nutzers mit DM-Rolle kann der Administrator eine oder mehrere Gerätegruppen auswählen, die den Bereich für den DM definieren.

Sie können z. B. (als Administrator) einen DM-Nutzer mit dem Namen DM1 erstellen und die Gruppe *G1* in nutzerdefinierten Gruppen zuweisen. Dann hat DM1 nur betrieblichen Zugriff auf alle Geräte in *G1*. Der Nutzer DM1 kann nicht auf andere Gruppen oder Einheiten zugreifen, die mit anderen Geräten in Verbindung stehen.

Außerdem kann DM1 mit SBAC die Einheiten, die von anderen DMs (z. B. DM2) erstellt wurden, nicht in der gleichen Gruppe *G1* sehen. Das bedeutet, dass ein DM-Nutzer nur die Einheiten sehen kann, die im Besitz des Nutzers sind.

Sie können z. B. (als Administrator) einen anderen DM-Nutzer mit dem Namen DM2 erstellen und die gleiche Gruppe *G1* in nutzerdefinierten Gruppen zuweisen. Wenn DM2 Konfigurationsvorlagen, Konfigurations-Baselines oder Profile für die Geräte in *G1* erstellt, hat DM1 keinen Zugriff auf diese Einheiten und umgekehrt.

Ein DM mit Bereich für alle Geräte hat betrieblichen Zugriff, wie durch RBAC-Berechtigungen für alle Geräte- und Gruppeneinheiten im Besitz des DM festgelegt.

SBAC für AD/LDAP-Nutzer:

Beim Importieren oder Bearbeiten von AD/LDAP-Gruppen können Administratoren Bereiche zu Nutzergruppen mit DM-Rolle zuweisen. Wenn ein Nutzer Mitglied mehrerer AD-Gruppen ist, von denen jede eine DM-Rolle hat, und jede AD-Gruppe verschiedene Bereichszuweisungen hat, ist der Bereich des Nutzers die Vereinigung der Bereiche dieser AD-Gruppen.

Beispiel:

- Nutzer DM1 ist Mitglied von zwei AD-Gruppen (*RR5-Floor1-LabAdmins* und *RR5-Floor3-LabAdmins*). Beiden AD-Gruppen wurde die DM-Rolle zugewiesen, wobei die Bereichszuweisungen für die AD-Gruppen wie folgt lauten: *RR5-Floor1-LabAdmins* erhält *ptlab-Server* und *RR5-Floor3-LabAdmins* erhält *smdlab-Server*. Der Bereich des DM DM1 ist nun die Verbindung von *ptlab-Servern* und *smdlab-Servern*.
- Nutzer DM1 ist Mitglied von zwei AD-Gruppen (*adg1* und *adg2*). Beiden AD-Gruppen wurde die DM-Rolle zugewiesen, wobei die Bereichszuweisungen für die AD-Gruppen wie folgt erfüllt sind: *adg1* erhält Zugriff auf *g1* und *adg2* erhält Zugriff auf *g2*. Wenn *g1* die übergeordnete Menge von *g2* ist, ist der Bereich von DM1 der größere Bereich (*g1*, alle untergeordneten Gruppen und alle untergeordneten Geräte).

Wenn ein Nutzer Mitglied mehrerer AD-Gruppen ist, die über unterschiedliche Rollen verfügen, hat die Rolle mit der höheren Funktionalität Vorrang (in der Reihenfolge Administrator, DM, Viewer).

Ein DM mit uneingeschränktem Bereich hat betrieblichen Zugriff, wie durch RBAC-Berechtigungen für alle Geräte- und Gruppeneinheiten angegeben.

ANMERKUNG: Nach dem Upgrade von OpenManage Enterprise von den Versionen 3.5 oder früher müssen die Geräte-Manager AD/LDAP und OIDC (PingFederate oder KeyCloak) alle Vorgängerversionen neu erstellen, da diese Einheiten nur dem Administrator nach dem Upgrade zur Verfügung stehen. Weitere Informationen finden Sie in den Versionshinweisen unter https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

SBAC für OIDC-Nutzer:

Die Bereichszuweisung für OIDC-Nutzer erfolgt nicht innerhalb der OME-Konsole. Sie können für OIDC-Nutzer in einem OIDC-Anbieter während der Nutzerkonfiguration Bereiche zuweisen. Wenn der Nutzer sich mit den Anmeldeinformationen für den OIDC-Anbieter anmeldet, ist die Rollen- und Bereichszuweisung für OME verfügbar. Weitere Informationen zum Verwalten von Nutzerrollen und Bereichen finden Sie unter Konfigurieren Sie eine OpenID Connect-Anbieterrichtlinie in PingFederate für den rollenbasierten Zugriff auf OpenManage Enterprise auf Seite 162.

ANMERKUNG: Wenn PingFederate als OIDC-Anbieter verwendet wird, können nur Administratorrollen verwendet werden. Weitere Informationen finden Sie unter Konfigurieren Sie eine OpenID Connect-Anbieterrichtlinie in PingFederate für den rollenbasierten Zugriff auf OpenManage Enterprise auf Seite 162 und in den Versionshinweisen unter https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

Eigentumsübertragung: Der Administrator kann die Eigentümerressourcen von einem Device Manager (Quelle) zu einem anderen Device Manager übertragen. Ein Administrator kann z. B. alle zugewiesenen Ressourcen von einem Quell-DM1 auf DM2 übertragen. Ein Geräte-Manager mit eigenen Einheiten, z. B. Firmware- und/oder Konfigurations-Baselines, Konfigurationsvorlagen, Warnungsrichtlinien und Profilen, wird als berechtigter Quellnutzer betrachtet. Mit der Eigentumsübertragung werden nur die Einheiten und nicht die Gerätegruppen (Bereich), die Eigentum eines Geräte-Managers sind, übertragen. Weitere Informationen finden Sie unter Eigentumsübertragung von Geräte-Manager-Einheiten auf Seite 156.

Verwandte Verweise

OpenManage Enterprise-Nutzerrollentypen auf Seite 15

Hinzufügen und Bearbeiten von lokalen OpenManage Enterprise-Nutzern

Dieses Verfahren ist spezifisch für das Hinzufügen und Bearbeiten der lokalen Benutzer. Beim Bearbeiten von lokalen Benutzern können Sie alle Benutzereigenschaften bearbeiten. Bei Verzeichnisnutzern können hingegen nur die Rolle und Gerätegruppen (im Falle eines Device Managers) bearbeitet werden. Informationen zum Integrieren von Verzeichnisdiensten in OpenManage Enterprise und zum Importieren der Verzeichnisnutzer finden Sie unter Integration von Verzeichnisdiensten in OpenManage Enterprise auf Seite 157 und Importieren von AD- und LDAP-Gruppen auf Seite 155.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Sie können Admin/System/Root-Benutzer nicht aktivieren, deaktivieren oder löschen. Sie können nur das Kennwort ändern. Klicken Sie dazu auf **Bearbeiten** im rechten Fensterbereich.

1. Wählen Sie **Anwendungseinstellungen** > **Nutzer** > **Nutzer** > **Hinzufügen**.
2. Im Dialogfeld **Benutzer hinzufügen**:
   a. Wählen Sie unter **Nutzerdetails** im Drop-Down-Menü **Nutzerrolle** „Administrator", „Device Manager" oder „Betrachter" aus. Weitere Informationen finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

      Standardmäßig ist das Kontrollkästchen **Aktiviert** aktiviert, um anzugeben, dass die Benutzerberechtigungen, die derzeit eingerichtet werden, für einen Benutzer aktiviert sind.

   b. Für die Device Manager-Rollen wird der Bereich auf **Alle Geräte** (uneingeschränkter Bereich) eingestellt. Allerdings kann der Administrator den Bereich einschränken, indem er die Option **Gruppen auswählen** gefolgt von der Auswahl der Gerätegruppe(n) auswählt.
   c. Geben Sie unter **Nutzerzugangsdaten** den **Nutzernamen** und das **Kennwort** ein und geben Sie das Kennwort unter **Kennwort bestätigen** erneut ein.

      ANMERKUNG: Der Nutzername darf nur alphanumerische Zeichen enthalten (Unterstrich ist jedoch zulässig) und das Kennwort muss mindestens ein Zeichen in Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.

3. Klicken Sie auf **Fertigstellen**.
   Eine Meldung wird angezeigt, dass der Benutzer erfolgreich gespeichert wurde. Es wird ein Job zum Anlegen eines neuen Benutzers gestartet. Nach dem Ausführen des Jobs ist der neue Benutzer erstellt und erscheint in der Liste der Benutzer.

Bearbeiten der OpenManage Enterprise-Benutzereigenschaften

1. Aktivieren Sie auf der Seite **Anwendungseinstellungen** unter **Benutzer** das Kontrollkästchen des entsprechenden Benutzers.
2. Schließen Sie die Aufgaben in Hinzufügen und Bearbeiten von lokalen OpenManage Enterprise-Nutzern auf Seite 154 ab.
   Die aktualisierten Daten werden gespeichert.

   ANMERKUNG: Wenn Sie die Rolle eines Benutzers ändern, werden die für die neue Rolle verfügbaren Berechtigungen automatisch angewendet. Wenn Sie einen Geräte-Manager zum Administrator machen, werden die Zugriffsrechte und Berechtigungen für einen Administrator automatisch diesem Geräte-Manager zugewiesen.

Aktivieren von OpenManage Enterprise-Benutzern

Aktivieren Sie das Kontrollkästchen des entsprechenden Benutzernamens und klicken Sie auf **Aktivieren**. Der Benutzer wird aktiviert und ein Häkchen wird in der entsprechenden Zelle der Spalte **AKTIVIERT** angezeigt. Wenn der Benutzer während der Erstellung des Benutzernamens bereits aktiviert wurde, ist die Schaltfläche **Aktivieren** ausgegraut.

Zugehörige Tasks

Löschen von Verzeichnisdiensten auf Seite 160
Löschen von OpenManage Enterprise-Benutzern auf Seite 155
Beenden von Benutzersitzungen auf Seite 157

Zugehörige Informationen

Verwalten von OpenManage Enterprise-Nutzern auf Seite 149

Deaktivieren von OpenManage Enterprise-Benutzern

Aktivieren Sie das Kontrollkästchen des entsprechenden Benutzernamens und klicken Sie dann auf **Deaktivieren**. Der Benutzer wird deaktiviert, und ein Häkchen verschwindet aus der entsprechenden Zelle der Spalte **AKTIVIERT**. Wenn der Benutzer während der Erstellung des Benutzernamens deaktiviert ist, wird die Schaltfläche **Deaktivieren** ausgegraut angezeigt.

Zugehörige Tasks

Löschen von Verzeichnisdiensten auf Seite 160
Löschen von OpenManage Enterprise-Benutzern auf Seite 155
Beenden von Benutzersitzungen auf Seite 157

Zugehörige Informationen

Verwalten von OpenManage Enterprise-Nutzern auf Seite 149

Löschen von OpenManage Enterprise-Benutzern

1. Aktivieren Sie das Kontrollkästchen des entsprechenden Benutzernamens und klicken Sie auf **Löschen**.
2. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**.

Verwandte Verweise

Deaktivieren von OpenManage Enterprise-Benutzern auf Seite 155
Aktivieren von OpenManage Enterprise-Benutzern auf Seite 154

Zugehörige Informationen

Verwalten von OpenManage Enterprise-Nutzern auf Seite 149

Importieren von AD- und LDAP-Gruppen

ANMERKUNG:

- Die Nutzer ohne Administratorrechte können die Active Directory (AD)- und Lightweight Directory Access Protocol (LDAP)-Nutzer nicht aktivieren oder deaktivieren.
- Bevor Sie AD-Gruppen in OpenManage Enterprise importieren, müssen Sie die Nutzergruppen bei der Konfiguration des AD in eine UNIVERSALGRUPPE einschließen.
- AD und LDAP Verzeichnisnutzer können importiert werden und einer der OpenManage Enterprise-Rollen zugewiesen werden (Admin, DeviceManager oder Betrachter). Die einfache Anmeldung (SSO) stoppt bei der Anmeldung an der Konsole. Auf den Geräten ausgeführte Aktionen erfordern ein dazu berechtigtes Konto auf dem Gerät.
- Nach dem Upgrade von OpenManage Enterprise von Version 3.5 oder früher müssen der Gerätemanager von AD/LDAP und OIDC (PingFederate oder KeyCloak) alle Vorgängerversionen neu erstellen, da diese Einheiten nur dem Administrator nach dem Upgrade zur Verfügung stehen. Weitere Informationen finden Sie in den Versionshinweisen unter https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs

1. Klicken Sie auf **Verzeichnisgruppe importieren**
2. Im Dialogfeld **Active Directory importieren**:
   a. Wählen Sie im Drop-Down-Menü **Verzeichnisquelle** eine AD- oder LDAP-Quelle aus, die zum Hinzufügen von Gruppen importiert werden muss. Informationen zum Hinzufügen von Verzeichnissen finden Sie unter Hinzufügen oder Bearbeiten von Active Directory-Gruppen zur Verwendung mit Verzeichnisdiensten auf Seite 158.
   b. Klicken Sie auf **Anmeldeinformationen eingeben**.

c. Geben Sie im angezeigten Dialogfeld den Nutzernamen und das Kennwort der Domäne ein, in der das Verzeichnis gespeichert ist. Verwenden Sie die Tooltips, damit Sie die richtige Syntax eingeben.
d. Klicken Sie auf **Fertigstellen**.
3. Im Abschnitt **Verfügbare Gruppen**:
a. Geben Sie im Feld **Gruppe suchen** die ersten Buchstaben des Gruppennamens ein, der im getesteten Verzeichnis verfügbar ist. Alle Gruppennamen, die mit dem eingegebenen Text beginnen, werden unter GRUPPENNAME aufgeführt.
b. Klicken Sie auf die Kontrollkästchen für die zu importierenden Gruppen, und klicken Sie dann auf die Schaltflächen **>> oder <<**, um die Gruppen hinzuzufügen oder zu entfernen.
4. Im Abschnitt **Zu importierende Gruppen**:
a. Wählen Sie die Kontrollkästchen der Gruppen aus und wählen Sie dann eine Rolle aus dem Drop-Down-Menü „Gruppenrolle zuweisen“ aus. Weitere Informationen zum rollenbasierten Zugriff finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
b. Klicken Sie auf **Rolle zuweisen**.
Den Benutzern in der Gruppe unter dem ausgewählten Verzeichnisdienst werden die ausgewählten Benutzerrollen zugewiesen.
c. Für die Rolle des Geräte-Managers wird der Bereich standardmäßig auf **Alle Geräte** eingestellt. Allerdings kann der Administrator den Bereich einschränken, indem er die Option **Bereich zuweisen** gefolgt von der Auswahl der Gerätegruppe(n) auswählt.
5. Wiederholen Sie die Schritte 3 und 4 nach Bedarf.
6. Klicken Sie auf **Importieren**.
Die Verzeichnisgruppen werden importiert und in der Benutzerliste angezeigt. Trotzdem melden sich alle Benutzer in diesen Gruppen mit ihrem Domänennutzernamen und -kennwort bei OpenManage Enterprise an.

Ein Domänennutzer, z. B. john_smith kann Mitglied mehrerer Verzeichnisgruppen und in diesen Gruppen unterschiedlichen Rollen zugewiesen sein. In diesem Fall werden mehrere Rollen, wie z. B. Device Manager und Viewer, über dem Benutzernamen in der rechten Ecke der Appliance angezeigt. Solch ein Nutzer erhält in den Verzeichnisgruppen, in denen er Mitglied ist, die Rolle mit der höchsten Stufe.

- Beispiel 1: Der Benutzer ist Mitglied von drei Gruppen mit den Rollen Admin, DM und Betrachter. In diesem Fall wird der Benutzer ein Administrator.
- Beispiel 2: Der Benutzer ist Mitglied von drei DM-Gruppen und einer Betrachtergruppe. In diesem Fall wird der Benutzer ein DM mit Zugriff auf den Verband der Gerätegruppen aller drei DM Rollen.

Eigentumsübertragung von Geräte-Manager-Einheiten

In diesem Thema wird beschrieben, wie ein Administrator Einheiten wie Jobs, Firmware- oder Konfigurationsvorlagen, Baselines, Warnungsrichtlinien und Profile, die von einem Geräte-Manager erstellt wurden, zu einem anderen Geräte-Manager übertragen kann. Der Administrator kann eine „Eigentumsübertragung“ initiieren, wenn ein Geräte-Manager das Unternehmen verlässt.

ANMERKUNG:

- Zum Ausführen dieser Aufgabe in OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Mit der Eigentumsübertragung werden nur die Einheiten und nicht die Gerätegruppen (Bereich), die Eigentum eines Geräte-Managers sind, übertragen.
- Bevor eine Eigentumsübertragung der Einheiten initiiert wird, muss der Administrator zuerst die Gerätegruppen, die dem vorherigen Geräte-Manager gehören, dem Geräte-Manager zuweisen, der übernehmen wird.
- Wenn die Eigentumsrechte an den Einheiten an eine Active Directory-Nutzergruppe übertragen werden, werden die Eigentumsrechte an alle Mitglieder dieser AD-Gruppe übertragen.

Gehen Sie wie folgt vor, um die Eigentumsrechte an Einheiten wie Jobs, Firmware- oder Konfigurationsvorlagen und Baselines, Warnungsrichtlinien und Profilen von einem Geräte-Manager auf einen anderen zu übertragen:

1. Starten Sie den Assistenten zum Übertragen von Eigentumsrechten, indem Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Nutzer** > **Eigentumsrechte übertragen** klicken.
2. Wählen Sie aus der Dropdown-Liste **Quellnutzer** den Geräte-Manager aus, von dem die Eigentumsrechte an Einheiten übertragen werden sollen.

   ANMERKUNG: Unter „Quellnutzer“ sind nur die lokalen, Active Directory-, OIDC- oder gelöschten Geräte-Manager aufgelistet, denen Einheiten wie Jobs, FW- oder Konfigurationsvorlagen, Warnungsrichtlinien und-Profile zugeordnet sind.

3. Wählen Sie aus der Dropdown-Liste **Zielnutzer** den Geräte-Manager aus, an den die Eigentumsrechte an Einheiten übertragen werden sollen.
4. Klicken Sie auf **Fertigstellen** und dann auf **Ja** in der Eingabeaufforderung.

Alle Einheiten im Besitz des „Quell"-Geräte-Managers, z. B. Jobs, Firmware- oder Konfigurationsvorlagen, Warnungsrichtlinien und Profile, werden an den „Ziel"-Geräte-Manager übertragen.

Beenden von Benutzersitzungen

1. Aktivieren Sie das Kontrollkästchen des entsprechenden Benutzernamens und klicken Sie dann auf **Beenden**.
2. Wenn Sie dazu aufgefordert werden, den Löschvorgang zu bestätigen, klicken Sie auf **JA**.
   Die ausgewählte Benutzersitzung ist beendet und der Benutzer abgemeldet.

Verwandte Verweise

Deaktivieren von OpenManage Enterprise-Benutzern auf Seite 155
Aktivieren von OpenManage Enterprise-Benutzern auf Seite 154

Zugehörige Informationen

Verwalten von OpenManage Enterprise-Nutzern auf Seite 149

Integration von Verzeichnisdiensten in OpenManage Enterprise

Verzeichnisdienste ermöglichen Ihnen den Import von Verzeichnisgruppen von AD oder LDAP für die Verwendung in der Konsole. OpenManage Enterprise unterstützt die Integration der folgenden Verzeichnisdienste:

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

Voraussetzungen/unterstützte Attribute für LDAP-Integration

Tabelle 28. Voraussetzungen/unterstützte Attribute für die LDAP-Integration in OpenManage Enterprise

	Attribut der Nutzeranmeldung	Attribut der Gruppenmitgliedschaft	Zertifikatanforderung
AD/LDAP	Cn, sAMAccountName	Mitglied	• Das Domain-Controller-Zertifikat muss einen FQDN haben. Das SAN-Feld kann IPv4 und/oder IPv6 oder einen FQDN haben. • Nur das Base64-Zertifikatformat wird unterstützt.
OpenLDAP	UID, SN	Uniquemember	Nur das PEM-Zertifikatformat wird unterstützt.
PHP LDAP	UID	MemberUid	

Nutzer-Voraussetzungen für die Verzeichnisdienst-Integration

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

1. Der BindDN-Nutzer und der für die Testverbindung verwendete Nutzer sollten identisch sein.
2. Wenn das Attribut der Nutzeranmeldung bereitgestellt wird, ist nur der entsprechende Nutzername, der dem Attribut zugewiesen ist, für die Gerät-Anmeldung zulässig.
3. Der für die Testverbindung verwendete Nutzer sollte Teil einer nicht standardmäßigen Gruppe in LDAP sein.

4. Das Attribut der Gruppenmitgliedschaft sollte entweder den „Nutzer-DN“ oder den (für die Anmeldung verwendeten) Kurznamen des Nutzers haben.
5. Wenn MemberUid als „Attribut der Gruppenmitgliedschaft“ verwendet wird, wird beim Nutzernamen, der in der Gerät-Anmeldung verwendet wird, in einigen LDAP-Konfigurationen zwischen Groß- und Kleinschreibung unterschieden.
6. Wenn der Suchfilter in der LDAP-Konfiguration verwendet wird, ist die Nutzeranmeldung für diejenigen Nutzer, die nicht Teil der angegebenen Suchkriterien sind, nicht erlaubt.
7. Die Gruppensuche funktioniert nur, wenn den Gruppen Nutzer unter dem angegebenen Attribut der Gruppenmitgliedschaft zugewiesen sind.

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

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

Um die Verzeichnisdienste nutzen zu können, treffen Sie folgende Vorbereitungen:

- Fügen Sie eine Verzeichnisverbindung hinzu. Informationen dazu finden Sie unter Hinzufügen oder Bearbeiten von Active Directory-Gruppen zur Verwendung mit Verzeichnisdiensten auf Seite 158.
- Importieren Sie Verzeichnisgruppen, und ordnen Sie alle Nutzer in der Gruppe einer bestimmten Rolle zu. Informationen dazu finden Sie unter Importieren von AD- und LDAP-Gruppen auf Seite 155.
- Bearbeiten Sie bei DM-Nutzern die Verzeichnisgruppe, um die Gruppen hinzuzufügen, die der DM verwalten kann. Informationen dazu finden Sie unter Hinzufügen und Bearbeiten von lokalen OpenManage Enterprise-Nutzern auf Seite 154.

Hinzufügen oder Bearbeiten von Active Directory-Gruppen zur Verwendung mit Verzeichnisdiensten

1. Klicken Sie auf **Anwendungseinstellungen** > **Benutzer** > **Verzeichnisdienste** und dann auf **Hinzufügen**.
2. Im Dialogfeld **Verbindung zum Verzeichnisdienst** ist **AD** standardmäßig aktiviert, um als Verzeichnistyp Active Directory (AD) anzugeben:

   ANMERKUNG: Weitere Informationen zum Erstellen einer LDAP-Benutzergruppe unter Verwendung von Verzeichnisdiensten finden Sie unter Hinzufügen oder Bearbeiten von Lightweight Directory Access Protocol-Gruppen zur Verwendung mit Verzeichnisdiensten auf Seite 159.

   a. Geben Sie den gewünschten Namen für das AD-Verzeichnis ein.
   b. Wählen Sie die Domain-Controller-Suchmethode aus:
      - **DNS**: Geben Sie im Feld **Methode** den Domänennamen ein, um DNS nach den Domain-Controllern abzufragen.
      - **Manuell**: Geben Sie im Feld **Methode** den FQDN oder die IP-Adresse des Domain-Controllers ein. Wenn Sie mehrere Server haben, werden maximal drei Server unterstützt, verwenden Sie eine durch Kommas getrennte Liste.
   c. Geben Sie im Feld **Gruppendomäne** die Gruppendomäne ein, die in der Tooltip-Syntax vorgeschlagen wurde.
3. Im Abschnitt **Erweiterte Optionen**:
   a. Die Portnummer der Adresse des globalen Katalogs wird standardmäßig mit 3269 befüllt. Geben Sie für den Domain-Controller-Zugriff 636 für die Portnummer ein.

      ANMERKUNG: Nur LDAPS-Ports werden unterstützt.

   b. Geben Sie die Dauer für die Netzwerkzeitüberschreitung und für die Zeitüberschreitung bei einer Suchanfrage in Sekunden ein. Das maximal unterstützte Zeitlimit beträgt 300 Sekunden.
   c. Wählen Sie zum Hochladen eines SSL-Zertifikats die Option **Zertifikatsvalidierung** und klicken Sie auf **Eine Datei auswählen**. Das Zertifikat sollte ein Stamm-CA-Zertifikat sein, das im Base64-Format kodiert ist.

   Die Registerkarte **Verbindung testen** wird angezeigt.
4. Klicken Sie auf **Verbindung testen**.
5. Geben Sie in dem angezeigten Dialogfeld den **Benutzernamen** und das **Kennwort** der Domäne ein, mit der Sie eine Verbindung herstellen möchten.

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

6. Klicken Sie auf **Verbindung testen**.
   Im Dialogfeld **Verzeichnisdienstinformationen** wird eine Meldung angezeigt, um anzugeben, ob die Verbindung erfolgreich hergestellt wurde.
7. Klicken Sie auf **Ok**.
8. Klicken Sie auf **Fertigstellen**.
   Es wird ein Job erstellt und ausgeführt, um das angeforderte Verzeichnis zur Liste der Verzeichnisdienste hinzuzufügen.

1. Wählen Sie in der Spalte **Verzeichnisname** das Verzeichnis aus. Die Verzeichnisdienst-Eigenschaften werden im rechten Fensterbereich angezeigt.
2. Klicken Sie auf **Bearbeiten**.
3. Bearbeiten Sie im Dialogfeld **Verbindung zum Verzeichnisdienst** die Daten und klicken Sie auf **Fertig stellen**. Die Daten werden aktualisiert und gespeichert.

Hinzufügen oder Bearbeiten von Lightweight Directory Access Protocol-Gruppen zur Verwendung mit Verzeichnisdiensten

1. Klicken Sie auf **Anwendungseinstellungen** > **Benutzer** > **Verzeichnisdienste** und dann auf **Hinzufügen**.
2. Wählen Sie im Dialogfeld **Verbindung zum Verzeichnisdienst LDAP** als Verzeichnistyp aus.

   ANMERKUNG: Weitere Informationen zum Erstellen einer AD-Benutzergruppe unter Verwendung von Verzeichnisdiensten finden Sie unter Hinzufügen oder Bearbeiten von Active Directory-Gruppen zur Verwendung mit Verzeichnisdiensten auf Seite 158.

   a. Geben Sie den gewünschten Namen für das LDAP-Verzeichnis ein.
   b. Wählen Sie die Domain-Controller-Suchmethode aus:
      - **DNS**: Geben Sie im Feld **Methode** den Domänennamen ein, um DNS nach den Domain-Controllern abzufragen.
      - **Manuell**: Geben Sie im Feld **Methode** den FQDN oder die IP-Adresse des Domain-Controllers ein. Wenn Sie mehrere Server haben, werden maximal drei Server unterstützt, verwenden Sie eine durch Kommas getrennte Liste.
   c. Geben Sie den Distinguished Name (DN) der LDAP-Bindung und das zugehörige Kennwort ein.

      ANMERKUNG: Anonyme Bindung wird für AD LDS nicht unterstützt.

3. Im Abschnitt **Erweiterte Optionen**:
   a. Die LDAP-Portnummer wird standardmäßig mit 636 befüllt. Geben Sie eine Portnummer ein, um diese zu ändern.

      ANMERKUNG: Nur LDAPS-Ports werden unterstützt.

   b. Geben Sie zur Übereinstimmung mit der LDAP-Konfiguration auf dem Server den Gruppenbasis-DN ein, nach dem gesucht werden soll.
   c. Geben Sie die im LDAP-System bereits konfigurierten **Benutzerattribute** ein. Es wird empfohlen, dass es sich hierbei um einen spezifischen Eintrag innerhalb des ausgewählten Basis-DN handelt. Andernfalls konfigurieren Sie einen Suchfilter, um sicherzustellen, dass dieser eindeutig ist. Wenn der Benutzer-DN nicht eindeutig durch die Suchkombination von Attribut und Suchfilter identifiziert werden kann, schlägt die Anmeldung fehl.

      ANMERKUNG: Die Benutzerattribute sollten in dem LDAP-System konfiguriert sein, das für Abfragen vor der Integration in die Verzeichnisdienste verwendet wird.

      ANMERKUNG: Sie müssen die Benutzerattribute als **cn** oder **sAMAccountName** für die AD-LDS-Konfiguration und als **UID** für die LDAP-Konfiguration eingeben.

   d. Geben Sie im Feld **Attribut der Gruppenmitgliedschaft** das Attribut ein, das die Gruppen- und Mitgliedsinformationen im Verzeichnis speichert.
   e. Geben Sie die Dauer für die Netzwerkzeitüberschreitung und für die Zeitüberschreitung bei einer Suchanfrage in Sekunden ein. Das maximal unterstützte Zeitlimit beträgt 300 Sekunden.
   f. Wählen Sie zum Hochladen eines SSL-Zertifikats die Option **Zertifikatsvalidierung** und klicken Sie auf **Eine Datei auswählen**. Das Zertifikat sollte ein Stamm-CA-Zertifikat sein, das im Base64-Format kodiert ist.

   Die Registerkarte **Verbindung testen** wird aktiviert.

4. Klicken Sie auf **Verbindung testen** und geben Sie dann die Anmeldeinformationen des Bind-Benutzers für die Domäne ein, mit der eine Verbindung hergestellt werden soll.

   ANMERKUNG: Stellen Sie beim Testen der Verbindung sicher, dass **Test-Benutzername** den Wert für **Attribut der Benutzeranmeldung** enthält, der zuvor eingegeben wurde.
5. Klicken Sie auf **Verbindung testen**.
   Im Dialogfeld **Verzeichnisdienstinformationen** wird eine Meldung angezeigt, um anzugeben, ob die Verbindung erfolgreich hergestellt wurde.
6. Klicken Sie auf **Ok**.
7. Klicken Sie auf **Fertigstellen**.
   Es wird ein Job erstellt und ausgeführt, um das angeforderte Verzeichnis zur Liste der Verzeichnisdienste hinzuzufügen.

1. Wählen Sie in der Spalte **Verzeichnisname** das Verzeichnis aus. Die Verzeichnisdienst-Eigenschaften werden im rechten Fensterbereich angezeigt.
2. Klicken Sie auf **Bearbeiten**.
3. Bearbeiten Sie im Dialogfeld **Verbindung zum Verzeichnisdienst** die Daten und klicken Sie auf **Fertig stellen**. Die Daten werden aktualisiert und gespeichert.

Löschen von Verzeichnisdiensten

Aktivieren Sie das Kontrollkästchen des entsprechenden Verzeichnisdienstes und klicken Sie dann auf **Löschen**.

Verwandte Verweise

Deaktivieren von OpenManage Enterprise-Benutzern auf Seite 155
Aktivieren von OpenManage Enterprise-Benutzern auf Seite 154

Zugehörige Informationen

Verwalten von OpenManage Enterprise-Geräteeinstellungen auf Seite 148
Verwalten von OpenManage Enterprise-Nutzern auf Seite 149

Anmelden bei OpenManage Enterprise über OpenID Connect-Anbieter

Sie können sich mit OpenID Connect (OIDC) Anbietern anmelden. OpenID Connect-Anbieter sind die Identitäts- und Nutzerverwaltungssoftware, mit der Nutzer sicher auf Anwendungen zugreifen können. Derzeit bietet OpenManage Enterprise Unterstützung für PingFederate und Keycloak.

WARNUNG: Nutzerrollen und -bereiche werden bei der erneuten Registrierung des Clients mit OIDC-Anbieter PingFederate (PingIdentity) auf „Standard“ zurückgesetzt. Dieses Problem könnte dazu führen, dass die Berechtigungen und der Umfang der nicht-Administrator-Rollen (DM und Viewer) auf die des Administrators zurückgesetzt werden. Die erneute Registrierung der Appliance-Konsole mit dem OIDC-Anbieter wird im Falle eines Upgrades der Appliance, der Änderung der Netzwerkkonfiguration oder der Änderung des SSL-Zertifikats ausgelöst.

Um Sicherheitsbedenken nach einer der oben genannten erneuten Registrierungen zu vermeiden, muss der Administrator alle OpenManage Enterprise Client-IDs auf der PingFederate-Website neu konfigurieren. Außerdem wird dringend empfohlen, dass Client-IDs nur für Administratornutzer mit Pingfederate erstellt werden, bis dieses Problem behoben ist.

ANMERKUNG:

- Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- In der Appliance können nur maximal vier OpenID Connect-Anbieter-IDs hinzugefügt werden.
- Nach dem Upgrade von OpenManage Enterprise von Version 3.5 oder früher müssen der Gerätemanager von AD/LDAP und OIDC (PingFederate oder KeyCloak) alle Vorgängerversionen neu erstellen, da diese Einheiten nur dem Administrator nach dem

Upgrade zur Verfügung stehen. Weitere Informationen finden Sie in den Versionshinweisen unter https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs

Voraussetzungen:

Bevor Sie die Anmeldung eines OpenID Connect-Anbieters aktivieren, müssen Sie Folgendes:

1. Einen OIDC-Anbieter in OpenManage Enterprise hinzufügen: Fügen Sie in den Anwendungseinstellungen von OpenManage Enterprise einen Anbieter für OpenID Connect hinzu. Wenn Sie den den OpenID Connect-Anbieter hinzufügen, wird eine Client-ID für den OpenID Connect-Anbieter generiert. Weitere Informationen finden Sie unter Hinzufügen eines OpenID Connect-Anbieters zu OpenManage Enterprise auf Seite 161.
2. **Konfigurieren Sie den OpenID Connect-Anbieter unter Verwendung der Client-ID**: Suchen Sie im OpenID Connect-Anbieter die Client-ID und definieren Sie eine Anmelderolle (Administrator, Device Manager oder Viewer), indem Sie den Bereich namens **dxcua** (Dell erweiterter Anspruch für Nutzerauthentifizierung) hinzufügen und zuordnen. Für weitere Informationen, siehe:
   - Konfigurieren Sie eine OpenID Connect-Anbieterrichtlinie in PingFederate für den rollenbasierten Zugriff auf OpenManage Enterprise auf Seite 162
   - Konfigurieren Sie eine OpenID Connect Provider-Richtlinie in Keycloak für den rollenbasierten Zugriff auf OpenManage Enterprise auf Seite 163

Wenn Sie einen OpenID Connect-Anbieter in OpenManage Enterprise hinzufügen, wird er auf der Seite **Anwendungseinstellungen** > **Nutzer** > **OpenID Connect Anbieter** aufgeführt. Die folgenden OIDC-Anbieterdetails werden angezeigt:

- Name: Der Name des OpenID Connect-Anbieters, als er in der Appliance hinzugefügt wurde
- Aktiviert: Ein „Haken" in diesem Feld zeigt an, dass der OpenID Connect-Anbieter in der Appliance aktiviert ist
- Ermittlungs-URI: Der URI (Uniform Resource Identifier) des OpenID Connect-Anbieters
- Registrierungsstatus: Kann einer der folgenden sein:
  - Erfolgreich: Zeigt eine erfolgreiche Registrierung beim OpenID Connect-Anbieter an
  - Fehlgeschlagen: Zeigt eine fehlgeschlagene Registrierung beim OpenID Connect-Anbieter an. Die „fehlgeschlagene" OpenID Connect-Anbieter-Registrierung wird nicht zugelassen, selbst sie aktiviert sind.
  - In Bearbeitung: Dieser Status wird angezeigt, wenn die Appliance versucht, sich beim OpenID Connect-Anbieter zu registrieren.

Im rechten Fensterbereich werden für den ausgewählten OpenID Connect-Anbieter Kunden-ID, Registrierungsstatus und Ermittlungs-URI Sie können auf **Details anzeigen** klicken, um die Zertifikatdetails des OpenID Connect-Anbieters anzuzeigen.

Auf der Seite **Anwendungseinstellungen** > **Nutzer** > **OpenID Connect-Anbieter** können Sie Folgendes:

- Hinzufügen eines OpenID Connect-Anbieters zu OpenManage Enterprise auf Seite 161
- Bearbeiten der Details eines OpenID Connect-Anbieters in OpenManage Enterprise auf Seite 163
- Testen Sie den Registrierungsstatus von OpenManage Enterprise mit dem OpenID Connect-Anbieter auf Seite 163
- OpenID Connect-Anbieter aktivieren auf Seite 164
- OpenID Connect-Anbieter deaktivieren auf Seite 164
- OpenID Connect-Anbieter löschen auf Seite 164

Hinzufügen eines OpenID Connect-Anbieters zu OpenManage Enterprise

Das Hinzufügen, Aktivieren und Registrieren eines OpenID Connect-Anbieters (Keycloak oder PingFederate) ermöglicht die Anmeldung eines autorisierten Clients bei OpenManage Enterprise. Dies generiert eine Client-ID.

Um einen OpenID Connect-Anbieter zu OpenManage Enterprise hinzuzufügen, gehen Sie zu der Seite **Anwendungseinstellungen** > **Benutzer** > **OpenID Connect Providers** und führen die folgenden Schritte aus:

ANMERKUNG: Es können nur maximal vier OpenID Connect-Anbieter-Clients hinzugefügt werden.

1. Klicken Sie auf **Hinzufügen**, um die Seite „Neuen OpenID Connect-Anbieter hinzufügen" zu aktivieren.
2. Geben Sie folgende Informationen in die entsprechenden Felder ein:
   a. Name: Name des OIDC-Clients.
   b. Discovery URI - Uniform Resource Identifier des OIDC-Anbieters
   c. Authentifizierungstyp - Wählen Sie eine der folgenden Methoden aus, die das Zugriffstoken verwenden muss, um auf die Appliance zuzugreifen:
      i. Erstzugriffstoken - Bereitstellen des Erstzugriffstokens
      ii. Benutzername und Passwort - Geben Sie den Benutzernamen und das Passwort ein
   d. (Optional) Kontrollkästchen für die Zertifikatsvalidierung - Sie können das Kontrollkästchen aktivieren und das Zertifikat des OIDC-Anbieters hochladen, indem Sie auf **Durchsuchen** klicken und das Zertifikat suchen oder indem Sie das Zertifikat per Drag & Drop in das Feld „Gestrichelte Linie" ziehen.

e. (Optional) Verbindung testen - Klicken Sie auf **URI- und SSL-Verbindung testen**, um die Verbindung mit dem OpenID Connect-Anbieter zu testen.

ANMERKUNG: Die Testverbindung hängt nicht vom Benutzernamen und Kennwort oder den Angaben des Erstzugriffstokens ab, da nur die Gültigkeit der angegebenen Discovery URI überprüft wird.

f. (Optional) Aktiviertes Kontrollkästchen - Sie können das Kontrollkästchen aktivieren, um den autorisierten Client-Zugriffstoken die Anmeldung bei der Appliance zu ermöglichen.

3. Klicken Sie auf **Fertigstellen**.

Der neu hinzugefügte OpenID-Connect-Anbieter ist auf der Seite Anwendungseinstellungen > Benutzer > OpenID-Connect-Anbieter aufgelistet, und die Client-ID befindet sich im rechten Fensterbereich.

Nächste Schritte:

Konfigurieren Sie eine OpenID Connect-Anbieterrichtlinie in PingFederate für den rollenbasierten Zugriff auf OpenManage Enterprise auf Seite 162

Konfigurieren Sie eine OpenID Connect Provider-Richtlinie in Keycloak für den rollenbasierten Zugriff auf OpenManage Enterprise auf Seite 163

Konfigurieren Sie eine OpenID Connect-Anbieterrichtlinie in PingFederate für den rollenbasierten Zugriff auf OpenManage Enterprise

Um die OpenManage Enterprise OpenID Connect-Anmeldung mit PingFederate zu aktivieren, müssen Sie der Client-ID einen Bereich **dxcua** (Dell erweiterter Claim für die Benutzerauthentifizierung) hinzufügen und zuordnen und die Benutzerberechtigungen wie folgt definieren:

WARNUNG: Benutzerrollen und -bereiche werden bei der erneuten Registrierung des Clients mit dem OIDC-Anbieter PingFederate (PingIdentity) auf „Standard“ zurückgesetzt. Dieses Problem kann die Berechtigungen und den Umfang der Nicht-Administrator-Rollen (DM und Viewer) auf die des Administrators zurücksetzen. Die erneute Registrierung der Appliance-Konsole mit dem OIDC-Anbieter wird im Falle eines Upgrades der Appliance, der Änderung der Netzwerkkonfiguration oder der Änderung des SSL-Zertifikats ausgelöst.

Um Sicherheitsbedenken nach einem der oben erwähnten Neuregistrierungsereignisse zu vermeiden, muss der Administrator alle OpenManage Enterprise Client-IDs auf der PingFederate-Website neu konfigurieren. Außerdem wird dringend empfohlen, dass Client-IDs nur für Administrator-Benutzer mit Pingfederate erstellt werden, bis dieses Problem behoben ist.

ANMERKUNG:

- Der Standardalgorithmus für die Zuweisung sollte RS256 (RSA-Signatur mit SHA-256) sein.

1. Fügen Sie einen „exklusiven“ oder „Standard“-Bereich namens dxcua unter Bereichsverwaltung in den OAuth-Einstellungen hinzu.
2. Erstellten Bereich zuweisen in **OpenID Connect Richtlinienmanagment** > **Richtlinie** mit folgenden Schritten:
    a. Aktivieren Sie **Benutzerinfo in Token einschließen**
    b. Fügen Sie im Attributbereich den Bereich und den Attributwert als **dxcua** hinzu.
    c. Fügen Sie unter „Vertragserfüllung“ dxcua hinzu und wählen Sie den Typ als „Text“ aus. Definieren Sie dann die Benutzerprivilegien für die OpenManage Enterprise OpenID Connect Anbieteranmeldung mit einem der folgenden Attribute:
        i. Administrator: `dxcua : [{"Role": "AD"}]`
        ii. Device Manager: `dxcua : [{"Role": "DM"}]`

        ANMERKUNG: Um den Zugriff des Geräte-Managers auf die Auswahl von Gerätegruppen zu beschränken (z. B. G1 und G2), verwenden Sie in OpenManage Enterprise `dxcua : [{"Role": "DM", "Entity":"G1, G2"}]`

        iii. Viewer: `dxcua : [{"Role": "VE"}]`
    d. Wenn nach der Client-Registrierung in OpenManage Enterprise ein „ausschließender“ Bereich konfiguriert wird, bearbeiten Sie den konfigurierten Client in PingFederate und aktivieren Sie den erstellten ausschließenden Bereich „dxcua“.
3. Die dynamische Client-Registrierung sollte in PingFederate für die OpenManage Enterprise Client-Registrierung aktiviert werden. Wenn die Option „Token für Erstzugriff anfordern“ in den Client-Einstellungen des OpenID Connect-Anbieters nicht ausgewählt ist, funktioniert die Registrierung mit Nutzername und Kennwort. Wenn die Option aktiviert ist, dann funktioniert die Registrierung nur mit dem Erstzugriffs-Token.

Konfigurieren Sie eine OpenID Connect Provider-Richtlinie in Keycloak für den rollenbasierten Zugriff auf OpenManage Enterprise

Um die OpenManage Enterprise OpenID Connect-Anmeldung mit Keycloak zu aktivieren, müssen Sie zunächst einen Bereich dxcua zur Client-ID hinzufügen und zuordnen und die Benutzerrechte wie folgt definieren:

ANMERKUNG: Für den im Konfigurationsassistenten für OpenID Connect Provider angegebenen Discovery URI sollte ein gültiger Endpunkt des Providers aufgeführt sein.

1. Definieren Sie im Abschnitt „Attribute von Keycloak-Benutzern" den „Schlüssel und Wert" für OpenManage Enterprise-Anmelderollen unter Verwendung eines der folgenden Attribute:
   - Administrator : `dxcua : [{"Role": "AD"}]`
   - Device Manager: `dxcua : [{"Role": "DM"}]`

     ANMERKUNG: Um den Zugriff des Geräte-Managers auf die Auswahl von Gerätegruppen zu beschränken (z. B. G1 und G2), verwenden Sie in OpenManage Enterprise `dxcua : [{"Role": "DM", "Entity":"G1, G2"}]`
   - Viewer: `dxcua : [{"Role": "VE"}]`
2. Sobald der Client in Keycloak registriert ist, fügen Sie im Abschnitt Mapper einen Mapper-Typ „Benutzerattribut" mit folgenden Werten hinzu:
   - Name: dxcua
   - Mapper-Typ: Benutzerattribut
   - Benutzerattribut: dxcua
   - Token Claim-Name: dxcua
   - Claim Json-Typ: Zeichenfolge
   - Zu ID-Token hinzufügen: Aktivieren
   - Zu Zugriffs-Token hinzufügen: Aktivieren
   - Hinzufügen zu Benutzerinformationen: Aktivieren

Testen Sie den Registrierungsstatus von OpenManage Enterprise mit dem OpenID Connect-Anbieter

Gehen Sie auf der Seite **Anwendungseinstellungen** > **Benutzer** > **OpenID Connect-Anbieter** wie folgt vor:

1. Wählen Sie einen OpenID Connect-Anbieter aus.
2. Klicken Sie im rechten Fensterbereich auf **Registrierungsstatus testen**.

   ANMERKUNG: Die Testverbindung hängt nicht von Benutzername und Kennwort oder den Details des Erstzugriffstokens ab, sie prüft nur die Gültigkeit der Discovery-URI.

Der letzte Registrierungsstatus („erfolgreich" oder „fehlgeschlagen") beim OIDC-Anbieter wird aktualisiert.

Bearbeiten der Details eines OpenID Connect-Anbieters in OpenManage Enterprise

Gehen Sie auf der Seite **Anwendungseinstellungen** > **Benutzer** > **OpenID Connect-Anbieter** wie folgt vor:

1. Wählen Sie einen OpenID Connect-Anbieter aus.
2. Klicken Sie im rechten Fensterbereich auf **Bearbeiten**.
3. Je nach Registrierungsstatus des OpenID Connect Anbieter-Clients können Sie Folgendes tun:
   a. Wenn der Registrierungsstatus „Erfolgreich" ist, können nur die Kontrollkästchen „Verbindung testen" und „Aktiviert" bearbeitet werden.
   b. Wenn der Registrierungsstatus „fehlgeschlagen" ist, können Sie das Kontrollkästchen „Benutzername", „Passwort", „Zertifizierungsvalidierung", „Verbindung testen" und „Aktiviert bearbeiten".
4. Zum Implementieren klicken Sie auf **Fertigstellen** oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.

OpenID Connect-Anbieter aktivieren

Wenn die Anmeldung eines OpenID Connect-Anbieters zu dem Zeitpunkt, zu dem er der Appliance hinzugefügt wurde, nicht aktiviert wurde, müssen Sie die Anmeldung in der Appliance aktivieren.

Gehen Sie auf der Seite **Anwendungseinstellungen** > **Benutzer** > **OpenID Connect-Anbieter** wie folgt vor:

1. Wählen Sie den/die OpenID Connect-Anbieter aus.
2. Klicken Sie auf **Aktivieren**.

Die Aktivierung der OpenID Connect Provider in OpenManage Enterprise ermöglicht es den autorisierten Client-Zugriffstoken, sich bei der Appliance anzumelden.

OpenID Connect-Anbieter löschen

Gehen Sie auf der Seite **Anwendungseinstellungen** > **Benutzer** > **OpenID Connect-Anbieter** wie folgt vor:

1. Wählen Sie den/die OpenID Connect-Anbieter aus.
2. Klicken Sie auf **Löschen**.

OpenID Connect-Anbieter deaktivieren

Gehen Sie auf der Seite **Anwendungseinstellungen** > **Benutzer** > **OpenID Connect-Anbieter** wie folgt vor:

1. Wählen Sie den/die OpenID Connect-Anbieter aus.
2. Klicken Sie auf **Deaktivieren**.

Das Client-Zugriffstoken von den „deaktivierten“ OIDC-Anbietern wird von der Appliance abgelehnt.

Sicherheitszertifikate

Durch Klicken auf **Anwendungseinstellungen SicherheitZertifikate** können Sie Informationen über das derzeit zur Verfügung stehende SSL-Zertifikat für das Gerät anzeigen.

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Benutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Zum Erstellen einer Zertifikatsignierungsanforderung (CSR) siehe Generieren und Herunterladen der Zertifikatsignierungsanforderung auf Seite 164.

Generieren und Herunterladen der Zertifikatsignierungsanforderung

So erstellen Sie eine Zertifikatsignierungsanforderung (CSR) für Ihr Gerät und fordern dann ein SSL an:

ANMERKUNG: Sie können die CSR nur aus der OpenManage Enterprise-Appliance heraus generieren.

1. Klicken Sie auf **Zertifikatsignierungsanforderung erstellen**.
2. Geben Sie im Dialogfeld **Zertifikatsignierungsanforderung erstellen** die erforderlichen Informationen in die Felder ein.
3. Klicken Sie auf **Erstellen**.
   Eine CSR wird erstellt und im Dialogfeld **Zertifikatsignierungsanforderung** angezeigt. Eine Kopie der CSR wird auch an die von Ihnen in der Anforderung angegebenen E-Mail-Adresse gesendet.
4. Im Dialogfeld **Zertifikatsignierungsanforderung** kopieren Sie die CSR-Daten und senden diese an die Zertifizierungsstelle (CA), wenn Sie ein SSL-Zertifikat anfordern.
   - Um die CSR herunterzuladen, klicken Sie auf **Zertifikatsignierungsanforderung herunterladen**.
   - Klicken Sie auf **Fertigstellen**.

Zuweisen eines Webserverzertifikats zu OpenManage Enterprise unter Verwendung von Microsoft Certificate Services

1. Erstellen Sie die Zertifikatsignierungsanforderung (CSR) in OpenManage Enterprise und laden Sie sie herunter. Siehe . Generieren und Herunterladen der Zertifikatsignierungsanforderung auf Seite 164
2. Öffnen Sie eine Websitzung zum Zertifizierungsserver (https://x.x.x.x/certsrv) und klicken Sie auf den Link **Zertifikat anfordern**.
3. Klicken Sie auf der Seite „Zertifikat anfordern" auf den Link **Erweiterte Zertifikatsanforderung senden**.
4. Klicken Sie auf der Seite „Erweiterte Zertifikatsanforderung" auf den Link **Eine Zertifikatsanforderung mittels einer Base-64-kodierten CMC- oder PKCS#10-Datei senden oder eine Verlängerungsanforderung mittels einer Base-64-kodierten PKCS#7-Datei senden**.
5. Gehen Sie auf der Seite „Zertifikatsanforderung oder Verlängerungsanforderung senden" wie folgt vor:
    a. Kopieren Sie den gesamten Inhalt der heruntergeladenen CSR und fügen Sie ihn in das Feld **Base-64-kodierte Zertifikatsanforderung (CMC- oder PKCS#10-Datei oder PKCS#7)** ein.
    b. Wählen Sie für die **Zertifikatvorlage Webserver** aus.
    c. Klicken Sie auf **Senden**, um ein Zertifikat zu erstellen.
6. Wählen Sie auf der Seite „Zertifikat ausgestellt" die Option **Base-64-kodiert** aus und klicken Sie dann auf den Link **Zertifikat herunterladen**, um das Zertifikat herunterzuladen.
7. Laden Sie das Zertifikat in OpenManage hoch, indem Sie zur Seite **Anwendungseinstellungen** > **Sicherheit** > **Zertifikate** navigieren und dann auf **Hochladen** klicken.

Verwalten der Konsolen-Voreinstellungen

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Benutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Durch Klicken auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Konsolen-Voreinstellungen** können Sie die Standardeigenschaften der OpenManage Enterprise-GUI festlegen. Z. B. die Standardzeit, nach deren Ablauf ein Gerätezustand automatisch geprüft und auf dem Dashboard aktualisiert wird, und die bevorzugten Einstellungen beim Ermitteln eines Geräts. Die folgenden Optionen stehen zur Verfügung:

1. **Berichteinstellungen**: So stellen Sie die maximale Anzahl der Zeilen für die Anzeige in OpenManage Enterprise ein:
    a. Erweitern Sie die **Berichtseinstellungen**.
    b. Geben Sie eine Zahl in das Feld für die **Maximale Anzahl an Berichtszeilen** ein. Das Standardlimit wird auf 1.000 Zeilen eingestellt, die maximal zulässige Anzahl von Zeilen beträgt jedoch 2 Milliarden.
    c. Klicken Sie auf **Anwenden**. Ein Job wird ausgeführt und die Einstellung wird angewendet.
2. **Gerätezustand**: So stellen Sie die Zeit ein, nach deren Ablauf der Funktionszustand von Geräten automatisch auf dem OpenManage Enterprise-Dashboard überwacht und aktualisiert werden muss:
    a. Erweitern Sie **Geräte-Funktionszustand**.
    b. Geben Sie die Häufigkeit an, mit der der Gerätezustand aufgezeichnet und Daten gespeichert werden müssen.
    c. Wählen Sie:
        - **Letzte bekannte**: den letzten aufgezeichneten Gerätezustand bei einem Verlust der Stromverbindung anzeigen.
        - **Unbekannt**: Anzeige des letzten aufgezeichneten Gerätezustands, als der Gerätestatus zu „Unbekannt" wechselte. Ein Gerät wird für OpenManage Enterprise unbekannt, wenn die Verbindung mit iDRAC unterbrochen und das Gerät nicht mehr von OpenManage Enterprise überwacht wird.
    d. Klicken Sie auf **Anwenden**, um die Änderungen an den Einstellungen zu speichern, oder wählen Sie **Verwerfen**, um die Standardwerte anzuwenden.
3. **Ermittlungseinstellung**: Erweitern Sie die Ermittlungseinstellung, um die von OpenManage Enterprise verwendete Gerätebenennung zu nutzen, um die erkannten iDRACs und andere Geräte über die Einstellungen für **Allgemeine Gerätebenennung** und **Server-Gerätebenennung** zu identifizieren.

    ANMERKUNG: Die Auswahl der Gerätebenennung für Allgemeine Gerätebenennung und Server-Gerätebenennung sind unabhängig voneinander und beeinflussen einander nicht.

    a. **Allgemeine Gerätebenennung** gilt für alle ermittelten Geräte außer iDRACs. Wählen Sie einen der folgenden Benennungsmodi aus:
        - **DNS**, um den DNS-Namen zu verwenden.
        - **Instrumentation (NetBIOS)**, um den NetBIOS-Namen zu verwenden.

ANMERKUNG:

- Die Standardeinstellung für Allgemeine Gerätebenennung ist **DNS**.
- Wenn eines der ermittelten Geräte nicht über den DNS-oder den NetBIOS-Namen verfügt, der für die Einstellung erforderlich ist, erkennt die Anwendung diese Geräte anhand der IP-Adressen.
- Wenn die Option **Instrumentation (NetBIOS)** unter **Allgemeine Gerätebenennung** ausgewählt ist, wird für Geräte im Gehäuse der **Gehäusename** auf der Seite „Alle Geräte“ als Gerätenameneintrag angezeigt.

b. **Server-Gerätebenennung** gilt nur für iDRACs. Wählen Sie einen der folgenden Benennungsmodi für die ermittelten iDRACs aus:
   - **iDRAC-Hostname**, um den iDRAC-Hostnamen zu verwenden.
   - **System-Hostname**, um den System-Hostnamen zu verwenden.

   ANMERKUNG:

   - Die standardmäßige Benennungspräferenz für iDRAC-Geräte ist der **System-Hostname**.
   - Wenn eines der iDRACs nicht über einen iDRACs- bzw. einen System-Hostnamen verfügt, der für die Einstellung erforderlich ist, erkennt die Anwendung diese iDRACs anhand der IP-Adressen.

c. Zur Eingabe der ungültigen Geräte-Hostnamen und der gängigen MAC-Adresse erweitern Sie **Erweiterte Einstellungen**:
   i. Geben Sie in **Ungültiger Geräte-Hostname** einen oder mehrere ungültige Hostnamen mit Kommatrennung ein. Standardmäßig wird eine Liste mit ungültigen Geräte-Hostnamen erstellt.
   ii. Geben Sie in **Gemeinsame MAC-Adressen** die gemeinsamen MAC-Adressen mit Kommatrennung ein. Standardmäßig wird eine Liste der gemeinsamen MAC-Adressen erstellt.

d. Klicken Sie auf **Anwenden**, um die Änderungen an den Einstellungen zu speichern, oder wählen Sie **Verwerfen**, um die Standardwerte anzuwenden.

4. **Server-initiierte Ermittlung**. Wählen Sie eine der folgenden Ermittlungs-Genehmigungs-Richtlinien aus:
   - **Automatisch**: damit Server mit iDRAC-Firmware-Version 4.00.00.00, die sich im selben Netzwerk wie die Konsole befinden, automatisch von der Konsole erkannt werden.
   - **Manuell**: die Server müssen manuell vom Benutzer erkannt werden.
   - Klicken Sie auf **Anwenden**, um die Änderungen an den Einstellungen zu speichern, oder wählen Sie **Verwerfen**, um die Standardwerte anzuwenden.
5. **MX7000 Integrations-Einstellungen**: Geben Sie bei der Integration eines der folgenden Warnmeldungs-Weiterleitungsverhalten auf MX7000-Gehäusen an:
   - Empfangen aller Warnmeldungen
   - Nur Warnmeldungen der Kategorie „Gehäuse“ empfangen
6. **SMB-Einstellung** So wählen Sie die Server Message Block (SMB)-Version, die für die Netzwerkkommunikation verwendet werden muss.
   - **V1 deaktivieren**: SMBv1 ist deaktiviert. Dies ist die Standardauswahl in der Appliance.
   - **V1 aktivieren** so aktivieren Sie SMBv1.

   ANMERKUNG: Sie müssen SMBv1 in den **SMB Einstellungen** aktivieren, bevor Sie mit Aufgaben beginnen, die Kommunikation mit einem beliebigen Gehäuse oder PowerEdge YX2X- und YX3X-Servern mit iDRAC-Version 2.50.50.50 und früheren Versionen erfordern. Weitere Informationen erhalten Sie unter Verwalten der Konsolen-Voreinstellungen auf Seite 165 und Generische Benennungskonvention für Dell EMC PowerEdge-Server auf Seite 187.
7. **E-Mail-Absender-Einstellungen**: So legen Sie die Adresse des Benutzers fest, der eine E-Mail-Nachricht sendet:
   a. Geben Sie eine E-Mail-Adresse in das Feld **Absender-E-Mail-ID** ein.
   b. Klicken Sie auf **Anwenden**, um die Änderungen an den Einstellungen zu speichern, oder wählen Sie **Verwerfen**, um die Standardwerte anzuwenden.
8. **Trap-Weiterleitungs-Format**: So legen Sie das Trap-Weiterleitungsformat fest –
   a. Wählen Sie eine der folgenden Optionen:
      - **Ursprüngliches Format (gilt nur für SNMP-Traps)**: Um die Trap-Daten so beizubehalten, wie sie sind.
      - **Normalisiert (gilt für alle Ereignisse)**: Um die Trap-Daten zu normalisieren. Wenn das Format für die Trap-Weiterleitung auf „Normalisiert“ festgelegt ist, empfängt der empfangende Agent, wie z. B. das Syslog, ein Tag mit der Geräte-IP-Adresse, von der die Warnmeldung weitergeleitet wurde.
   b. Klicken Sie auf **Anwenden**, um die Änderungen an den Einstellungen zu speichern, oder wählen Sie **Verwerfen**, um die Standardwerte anzuwenden.
9. **Einstellungen für die Kennzahlenerfassung**: Um die Häufigkeit der Wartung und Säuberung der PowerManager-Erweiterungsdaten einzustellen, gehen Sie wie folgt vor:
   a. Geben Sie im Feld **Daten-Säuberungsintervall** die Häufigkeit ein, mit der die PowerManager-Daten gelöscht werden sollen. Geben Sie Werte innerhalb von 30 bis 365 Tagen ein.
   b. Klicken Sie auf **Anwenden**, um Änderungen an den Einstellungen zu speichern, oder wählen Sie **Verwerfen**, um die Standardwerte anzuwenden.

Einstellen der Sicherheitseigenschaften für die Anmeldung

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Benutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

ANMERKUNG: AD und LDAP Verzeichnisbenutzer können importiert werden und einer der OpenManage Enterprise-Rollen zugewiesen werden (Admin, DeviceManager oder Betrachter).

Indem Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Sicherheit** klicken, können Sie Ihr OpenManage Enterprise entweder durch Angabe von **Zulässigen IP-Bereich einschränken** oder durch **Richtlinie zum Sperren von Anmeldungen** festlegen.

- Erweitern Sie **Zulässigen IP-Bereich einschränken**:

  ANMERKUNG: Wenn in der Appliance „Eingeschränkter zulässiger IP-Bereich" konfiguriert ist, werden alle eingehenden Verbindungen zur Appliance, wie z. B. der Empfang von Warnmeldungen, die Firmware-Aktualisierung und Netzwerkidentitäten für die Geräte blockiert, die sich außerhalb des angegebenen Bereichs befinden. Allerdings funktioniert jede Verbindung, die von der Appliance ausgeht, auf allen Geräten.

  1. Zur Angabe der IP-Adressen, für die der Zugang zu OpenManage Enterprise gewährt werden muss, wählen Sie das Kontrollkästchen **IP-Bereich aktivieren**.
  2. Im Feld **IP-Bereichs-Adresse (CIDR)** geben Sie den IP-Adressenbereich ein.

     ANMERKUNG: Es ist nur ein IP-Bereich zulässig.
  3. Klicken Sie auf **Anwenden**. Um auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.

     ANMERKUNG: Die Schaltfläche **Anwenden** wird nicht aktiviert, wenn mehrere IP-Bereiche in das Feld **IP-Bereichs-Adresse (CIDR)** eingegeben werden.
- Erweitern Sie das Feld **Richtlinie für Anmeldesperrung** :
  1. Wählen Sie das Kontrollkästchen **Nach Benutzernamen**, um die Anmeldung eines bestimmten Benutzernamens bei OpenManage Enterprise zu verhindern.
  2. Wählen Sie das Kontrollkästchen **Nach IP-Adresse**, um die Anmeldung einer bestimmten IP-Adresse bei OpenManage Enterprise zu verhindern.
  3. Geben Sie im Feld **Fehlversuche bis Sperrung** die Anzahl der erfolglosen Versuche ein, nach welchen der Benutzer von OpenManage Enterprise an weiteren Anmeldungen gehindert wird. Standardmäßig sind 3 Versuche eingestellt.
  4. Geben Sie im Feld **Fenster für Fehlversuche bis Sperrung** den Zeitraum ein, in dem OpenManage Enterprise Informationen über einen fehlgeschlagenen Versuch anzeigen muss.
  5. Geben Sie in das Feld **Sperrungsdauer** die Dauer ein, wie lange der Benutzer nach mehreren erfolglosen Versuchen an der Anmeldung gehindert wird.
  6. Klicken Sie auf **Anwenden**. Um die Einstellungen auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.

Anpassen der Warnungsanzeige

1. Klicken Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen>Warnungen** und erweitern Sie die **Anzeigeeinstellungen für Warnmeldungen**.
2. Wählen Sie eine der folgenden Optionen:
   a. **Alle** – ermöglicht das Anzeigen sowohl bestätigter als auch nicht bestätigter Warnungen.
   b. **Unbestätigt** – zum Aktivieren der Anzeige von ausschließlich unbestätigten Warnungen.

      ANMERKUNG: Standardmäßig sind die **Anzeigeeinstellungen für Warnmeldungen** auf **Unbestätigt** eingestellt.

   c. **Bestätigt** – zum Aktivieren der Anzeige von ausschließlich bestätigten Warnungen.
3. Klicken Sie auf **Anwenden**.

   Änderungen an der Anzeigeeinstellungen für Warnungen wirken sich auf die folgenden Seiten von OpenManage Enterprise aus:
   - Die obere rechte Ecke aller Seiten von OpenManage Enterprise. Informationen dazu finden Sie unter Übersicht über die grafische Benutzeroberfläche von OpenManage Enterprise auf Seite 36.
   - Die Dashboard-Seite. Informationen dazu finden Sie unter Überwachen Sie Geräte mit dem OpenManage Enterprise-Dashboard auf Seite 38.

- Die Geräte-Seite. Informationen dazu finden Sie unter Ringdiagramm auf Seite 40.
- Die Tabelle **Warnungsprotokoll** unter der Warnungen-Seite. Informationen dazu finden Sie unter Anzeigen von Warnungsprotokollen auf Seite 118.

SMTP-, SNMP- und Syslog-Warnungen konfigurieren

Indem Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Warnungen** klicken, können Sie die E-Mail-Adresse (SMTP) konfigurieren, die Systemwarnungen, SNMP-Warnungs-Weiterleitungsziele und die Syslog-Weiterleitungseigenschaften empfängt. Zum Verwalten dieser Einstellungen müssen Sie über OpenManage Enterprise-Anmeldeinformationen auf Administratorebene verfügen.

So konfigurieren und authentifizieren Sie den SMTP-Server, der die E-Mail-Kommunikation zwischen Nutzern und OpenManage Enterprise verwaltet:

ANMERKUNG: OpenManage Enterprise kann keine E-Mails an einen internen SMTP-Server senden, auf dem sich ein Zertifikat befindet, das von einer internen Stammzertifizierungsstelle ausgestellt wurde.

1. Erweitern Sie **E- Mail-Konfiguration**.
2. Geben Sie die SMTP-Server-Netzwerkadresse ein, von der aus E-Mail-Nachrichten gesendet werden.
3. Um den SMTP-Server zu authentifizieren, aktivieren Sie die Kontrollkästchen **Authentifizierung aktivieren** und geben Sie den Nutzernamen und das Kennwort ein.
4. Standardmäßig ist die SMPT-Portnummer, auf den zugegriffen wird, 25. Bearbeiten Sie dies gegebenenfalls.
5. Aktivieren Sie das Kontrollkästchen **SSL verwenden**, um Ihre SMTP-Transaktion zu sichern.
6. Um zu überprüfen, ob der SMTP-Server ordnungsgemäß funktioniert, klicken Sie auf das Kontrollkästchen **Test-E-Mail senden** und geben Sie einen **E-Mail-Empfänger** ein.
7. Klicken Sie auf **Anwenden**.
8. Um die Einstellungen auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.

So konfigurieren Sie die SNMP-Warnungsweiterleitung:

1. Erweitern Sie **SNMP-Warnungs-Weiterleitungskonfiguration**.
2. Aktivieren Sie das Kontrollkästchen **AKTIVIERT**, damit die entsprechenden SNMP-Traps Warnungen im Fall von vordefinierten Ereignisse senden können.
3. Geben Sie im Feld **ZIELADRESSE** die IP-Adresse des Zielgeräts ein, das die Warnung empfangen soll.

   ANMERKUNG: Die Eingabe der Konsolen-IP ist nicht erlaubt, um eine Duplizierung von Warnmeldungen zu vermeiden.
4. Wählen Sie im Menü **SNMP-VERSION** den Typ der SNMP-Version als SNMPv1, SNMPv2 oder SNMPv3 aus und füllen Sie die folgenden Felder aus:
   a. Geben Sie im Feld COMMUNITIYSTRING den Communitystring des Geräts ein, das die Warnung empfangen soll.
   b. Bearbeiten Sie bei Bedarf die PORTNUMMER. Die standardmäßige Portnummer für SNMP-Traps=162. Informationen dazu finden Sie unter Unterstützte Protokolle und Schnittstellen in OpenManage Enterprise auf Seite 32.
   c. Wenn SNMPv3 ausgewählt ist, geben Sie die folgenden zusätzlichen Details ein:
      i. NUTZERNAME: Geben Sie einen Nutzernamen ein.
      ii. AUTHENTIFIZIERUNGSTYP: Wählen Sie in der Dropdown-Liste SHA, MD_5 oder „Keine“ aus.
      iii. AUTHENTIFIZIERUNGS-PASSPHRASE: Geben Sie eine Authentifizierungs-Passphrase mit mindestens acht Zeichen an.
      iv. DATENSCHUTZTYP: Wählen Sie in der Dropdown-Liste DES, AES_128 oder „Keine“ aus.
      v. DATENSCHUTZ-PASSPHRASE: Geben Sie eine Datenschutz-Passphrase an, die mindestens acht Zeichen enthält.
5. Um eine SNMP-Meldung zu testen, klicken Sie auf die Schaltfläche **Senden** des entsprechenden Traps.
6. Klicken Sie auf **Anwenden**. Um die Einstellungen auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.

So aktualisieren Sie die Syslog-Weiterleitungskonfiguration:

1. Erweitern Sie **Syslog-Weiterleitungskonfiguration**.
2. Aktivieren Sie das Kontrollkästchen, um die Syslog-Funktion auf dem entsprechenden Server in der Spalte **SERVER** zu aktivieren.
3. Geben Sie im Feld **ZIELADRESSE/HOSTNAME** die IP-Adresse des Geräts ein, das die Syslog-Meldungen empfangen soll.
4. Die standardmäßige Portnummer mittels UPD=514. Bearbeiten Sie dies bei Bedarf durch Eingabe in das Feld oder Auswahl aus dem Feld. Informationen dazu finden Sie unter Unterstützte Protokolle und Schnittstellen in OpenManage Enterprise auf Seite 32.
5. Klicken Sie auf **Anwenden**.
6. Um die Einstellungen auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.

Verwalten von eingehenden Warnungen

ANMERKUNG: Zum Ausführen beliebiger Aufgaben auf OpenManage Enterprise müssen Sie über die erforderlichen Nutzerberechtigungen verfügen. Informationen dazu finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Durch Klicken auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Eingehende Warnmeldungen** können Sie die TrapForward-Eigenschaften festlegen und den Nutzer definieren, der die eingehenden SNMPv3-Warnmeldungen empfängt.

- Um die SNMP-Anmeldeinformationen für eingehende Warnungen festzulegen:

1. Aktivieren Sie das Kontrollkästchen **SNMPV3 aktiviert**.
2. Klicken Sie auf **Anmeldeinformationen**
3. Im Dialogfeld für **SNMP-Anmeldeinformationen**:
    a. Geben Sie im Feld **Nutzername** die Anmelde-ID des Benutzers ein, der die OpenManage Enterprise-Einstellungen verwaltet.
    b. Wählen Sie im Drop-Down-Menü **Authentifizierungstyp** entweder den Algorithmus **SHA** oder **MD_5** als Authentifizierungstyp aus.
    c. Geben Sie im Feld **Authentifizierungspassphrase** entsprechend Ihrer Auswahl die Passphrase für SHA oder MD_5 ein.
    d. Wählen Sie im Drop-Down-Menü **Datenschutztyp** entweder DES oder AES_128 als Verschlüsselungsstandard aus.
    e. Geben Sie im Feld **Sicherheitspassphrase** die Ihrem Datenschutztyp entsprechende Passphrase ein.
    f. Klicken Sie auf **Speichern**.
4. Geben Sie im Feld **Community** die Community-Zeichenfolge für den Empfang der SNMP-Traps ein.
5. Standardmäßig lautet die SNMP-Portnummer für die eingehenden Traps 162. Dies zum Ändern der Portnummer bearbeiten.
6. Klicken Sie auf **Anwenden**.
    SNMP-Anmeldeinformationen und -Einstellungen werden gespeichert.
7. Um die Einstellungen auf die Standardattribute zurückzusetzen, klicken Sie auf **Verwerfen**.

    ANMERKUNG: Wenn SNMPv3-Warnungseinstellungen vor dem Upgrade der Appliance konfiguriert werden, müssen Sie die Einstellungen neu konfigurieren. Geben Sie hierzu den Nutzernamen, die Passphrase für die Authentifizierung und die Sicherheitspassphrase ein, um weiterhin Warnmeldungen zu erhalten. Wenn das Problem weiterhin besteht, starten Sie die Services mithilfe der Text-Benutzeroberfläche (TUI) neu.

8. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern, oder auf **Verwerfen**, um den Vorgang abzubrechen.

Einstellen der SNMP-Anmeldeinformationen

1. Klicken Sie auf **Anmeldeinformationen**
2. Im Dialogfeld für **SNMP-Anmeldeinformationen**:
    a. Geben Sie im Feld **Benutzername** die Anmelde-ID des Benutzers ein, der die OpenManage Enterprise-Einstellungen verwaltet.
    b. Wählen Sie im Drop-Down-Menü **Authentifizierungstyp** entweder den Algorithmus **SHA** oder **MD_5** als Authentifizierungstyp aus.
    c. Geben Sie im Feld **Authentifizierungspassphrase** entsprechend Ihrer Auswahl die Passphrase für SHA oder MD_5 ein.
    d. Wählen Sie im Drop-Down-Menü **Datenschutztyp** entweder DES oder AES_128 als Authentifizierungstyp aus.
    e. Geben Sie im Feld **Sicherheitspassphrase** die Ihrem Datenschutztyp entsprechende Passphrase ein.
3. Klicken Sie auf **Speichern**.

Verwalten von Gewährleistungseinstellungen

Gewährleistungseinstellungen bestimmen die Anzeige von Servicestatistiken durch OpenManage Enterprise im Warnungs-Widget auf der Startseite, dem Scoreboard auf allen Seiten, der Serviceseite und den Berichten.

So ändern Sie die Gewährleistungseinstellungen:

1. Klicken Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Gewährleistung**.
2. Klicken Sie auf **Gewährleistungseinstellungen**, um das Dialogfeld zu aktivieren.

3. Geben Sie im Feld **Warnung anzeigen, wenn Services ablaufen** die Anzahl der Tage ein. Sie können einen Wert von 0–1000 eingeben (beide enthalten). Der Standardwert ist 90 Tage. Die auf dieser Einstellung beruhenden Services werden angezeigt als im Bericht und im Widget.
4. Über die Optionen **Abgelaufene Garantien ausblenden** können Sie eine der folgenden Optionen auswählen:
   a. **Alle**: zum Ausblenden der Anzeige aller „anfänglichen" und „erweiterten" Garantien, die abgelaufen sind.
   b. **Nur anfänglich**: Nur die anfänglichen Garantien, die abgelaufen sind, werden ausgeblendet.
   c. **Keine**: Alle abgelaufenen Garantien werden angezeigt.
5. Klicken Sie auf **Anwenden** oder **Verwerfen**, um die Gewährleistungseinstellungen zu speichern oder die Änderungen zu verwerfen und die alten Einstellungen beizubehalten.

Überprüfen und Aktualisieren der Version von OpenManage Enterprise und der verfügbaren Plug-ins

Auf der Seite **Konsole und Plug-ins** können Sie die OpenManage Enterprise-Version überprüfen und aktualisieren sowie Plug-ins installieren und aktualisieren. Um zur Seite **Konsole und Plug-ins** zu navigieren, klicken Sie auf **Anwendungseinstellungen** > **Konsole und Plug-ins**.

Auf der Seite **Konsole und Plug-ins** können Sie folgende Aktionen ausführen:

- Anzeigen Ihrer aktuellen Version von OpenManage Enterprise, Suche nach verfügbaren Updates und Upgrade auf neuere Versionen. Sie können auf die Schaltfläche **Updateeinstellungen** klicken, um Folgendes durchzuführen:
  - Automatische oder manuelle Suche nach Updates.
  - Wählen Sie für das Update der Appliance zwischen Dell.com (online) oder Netzwerkfreigabe (offline) aus.

    Weitere Informationen zum Upgrade von dell.com oder einer Netzwerkfreigabe finden Sie unter Konfigurieren und Upgrade von OpenManage Enterprise mithilfe der Online-Methode auf Seite 171 oder Konfigurieren von OpenManage Enterprise und Durchführen eines Offline-Upgrades mithilfe der Netzwerkfreigabe auf Seite 172.
- Klicken Sie für das Plug-in, das Sie installieren möchten auf **Installieren**, um die Funktionalität der Appliance zu verbessern. Weitere Informationen zum Installieren von Plug-ins finden Sie unter Plug-in.

  ANMERKUNG:
  - Die OpenManage Enterprise Advanced-Lizenz ist erforderlich, damit die Plug-ins nach der Installation voll funktionsfähig sind. Weitere ausführliche Informationen zu den Plug-ins finden Sie in der entsprechenden Dokumentation auf der Dell Support-Website.
  - Durch die Installation eines Plug-ins in OpenManage Enterprise werden die Appliance-Services neu gestartet.
- Mit den bereits installierten Plug-ins können Sie Folgendes tun:
  - Plug-in deaktivieren. Siehe Deaktivieren eines Plug-ins auf Seite 175
  - Plug-in aktivieren. Siehe Aktivieren eines Plug-ins auf Seite 175
  - Plug-in deinstallieren. Siehe Deinstallieren eines Plug-ins auf Seite 175

Upgrade-Empfehlungen und -Voraussetzungen

Administratoren müssen Folgendes berücksichtigen, bevor sie auf die neueste Version aktualisieren:

- Machen Sie einen VM-Snapshot der Konsole als Backup für den Fall, dass etwas Unerwartetes eintritt. Weisen Sie zusätzliche Ausfallzeiten dafür zu, falls erforderlich.
- Planen Sie mindestens eine Stunde für den Aktualisierungsvorgang ein. Planen Sie mehr Zeit ein, wenn das Update durch die Verwendung einer langsameren Netzwerkverbindung heruntergeladen werden muss.
- Stellen Sie sicher, dass keine Device-Konfigurations-, Bereitstellungs- oder Erweiterungs-(Plug-in-)Aufgaben ausgeführt werden oder für die Zeit während der geplanten Ausfallzeit geplant werden. Aktive oder geplante Aufgaben oder Richtlinien werden während des Updates ohne weitere Warnmeldungen beendet.
- Benachrichtigen Sie andere Konsolen-Nutzer über das bevorstehende geplante Update.
- Wenn das Upgrade fehlschlägt, wird die Appliance neu gestartet. Es wird empfohlen, den VM-Snapshot zurückzusetzen und das Upgrade erneut durchzuführen.

ANMERKUNG:
- Nur OpenManage Enterprise-Versionen ab Version 3.5 können über die Methode **Automatisch** > **Online** direkt auf Version 3.7 aktualisiert werden.

- OpenManage Enterprise-Versionen vor Version 3.4, z. B. Version 3.3.x und Version 3.2, müssen zuerst auf Version 3.4 und dann auf Version 3.5 aktualisiert werden, bevor ein Upgrade auf 3.7 durchgeführt werden kann.
- OpenManage Enterprise: TechRelease-Versionen sollten zunächst auf OpenManage Enterprise Version 3.0 oder 3.1 aktualisiert werden.
- Wenn Sie OpenManage Enterprise mit mehr als 8000 ermittelten Geräten aktualisieren, wird der Aktualisierungsvorgang in zwei bis drei Stunden abgeschlossen. Während dieser Zeit reagieren die Services möglicherweise nicht. Es wird empfohlen, die Appliance erneut zu starten. Nach dem Neustart wird die normale Funktionalität der Appliance wiederhergestellt.
- Das Hinzufügen einer zweiten Netzwerkschnittstelle sollte erst nach Abschluss der Upgradeaufgaben nach der Konsole durchgeführt werden. Der Versuch, eine zweite NIC hinzuzufügen, während die Aufgaben nach dem Upgrade noch durchgeführt werden, wäre ineffektiv.
- Sie können sich unmittelbar nach dem Update der Appliance anmelden und müssen nicht warten, bis die gesamte Bestandsaufnahme abgeschlossen wurde. Nach dem Update wird der Ermittlungstask im Hintergrund ausgeführt und Sie können den Fortschritt gelegentlich sehen.
- Durch Klicken auf **Aktualisieren** wird ein Job zum Herunterladen des Upgrade-Bundle initialisiert. Dieser Job wird nach dem Herunterladen aller Updatedateien von selbst abgeschlossen und kann nicht durch den Nutzer beendet werden.
- Nachdem das Upgrade von OpenManage Enterprise auf Version 3.7 durchgeführt wurde, haben die migrierten Device Manager-Nutzer uneingeschränkte Berechtigung und standardmäßig Zugriff auf alle Geräte. Falls erforderlich, können Administratoren mithilfe der SBAC-Funktion Berechtigungen entsprechend zuweisen. Weitere Informationen zur SBAC-Funktion finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.

Konfigurieren und Upgrade von OpenManage Enterprise mithilfe der Online-Methode

OpenManage Enterprise kann entweder automatisch oder manuell von Dell.com (https://downloads.dell.com/openmanage_enterprise) online aktualisiert werden.

- Sie müssen Administratorrechte besitzen, um das Upgrade auszuführen. Weitere Informationen zu Berechtigungen finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Sie müssen sicherstellen, dass die OpenManage Enterprise-Appliance auf Dell.com und die erwartete Aktualisierung zugreifen kann.

Das Upgrade von OpenManage Enterprise ist ein zweistufiger Prozess. Zunächst Konfigurieren der Appliance für das Online-Update auf Seite 171, um festzulegen, wie die Updates abgerufen werden sollen und die Update-Methode auszuwählen, und anschließend Upgrade von OpenManage Enterprise mithilfe der Online-Methode auf Seite 172 über die Seite Konsole und Plug-ins. Die Konfiguration der Update-Einstellungen ist ein einmaliger Prozess. Sobald die Update-Einstellungen konfiguriert sind, können Sie auf das Aktualisierungssymbol im Abschnitt „Update“ klicken, um festzustellen, ob eine aktualisierte Version zum Herunterladen verfügbar ist.

Konfigurieren der Appliance für das Online-Update

1. Klicken Sie auf **Anwendungseinstellungen** > **Konsole und Erweiterungen** > **Update-Einstellungen**.
2. Wählen Sie unter **Wie Sie auf Updates prüfen** eine der folgenden Optionen aus:
   - **Automatisch**: Die Appliance prüft jeden Montag auf die Verfügbarkeit der Aktualisierungen von der Quelle, die im **Wo nach Updates suchen** angegeben ist.
   - **Manuell**: Der Nutzer muss manuell prüfen, ob das Update von der Quelle verfügbar ist, die unter **Wo nach Updates suchen** angegeben ist, indem er auf das Symbol „Liste aktualisieren“ im Abschnitt „Updates“ auf der Seite Konsole und Plug-ins klickt.
3. Wählen Sie unter **Wo nach Updates suchendell.com** aus, um den Speicherort anzugeben, an dem die Appliance nach Updates sucht.
4. Optional: Aktivieren Sie das Kontrollkästchen **Automatisches Starten des Konsolen-Updates, wenn Downloads abgeschlossen sind**, um eine Installation des Konsolen-Updates unmittelbar nach dem Herunterladen des Update-Pakets zu initiieren. Andernfalls kann das Update manuell initiiert werden.
5. Klicken Sie auf **Anwenden**.

   Die Appliance sucht direkt auf https://downloads.dell.com/openmanage_enterprise nach Updates.

Aktualisieren Sie die Appliance mithilfe der Online-Methode.

Upgrade von OpenManage Enterprise mithilfe der Online-Methode

Bevor Sie mit dem Update von dell.com beginnen, stellen Sie Folgendes sicher:

- Stellen Sie sicher, dass die Update-Einstellungen für das Online-Update konfiguriert sind. Informationen dazu finden Sie unter Konfigurieren und Upgrade von OpenManage Enterprise mithilfe der Online-Methode auf Seite 171.
- Stellen Sie sicher, dass Sie alle Upgrade-Voraussetzungen und -Empfehlungen wie in Upgrade-Empfehlungen und -Voraussetzungen auf Seite 170 beschrieben, durchgegangen sind.
- Machen Sie einen VM-Snapshot der Konsole als Backup für den Fall, dass etwas Unerwartetes eintritt. Weisen Sie zusätzliche Ausfallzeiten dafür zu, falls erforderlich.

1. Basierend auf den Aktualisierungseinstellungen prüft die Appliance auf die Verfügbarkeit einer Aktualisierung. Wenn eine neue Version verfügbar ist, wird ein Banner mit den neuen Informationen zur Upgradeversion angezeigt. Über den Banner kann der Administrator auswählen, ob die Benachrichtigung geschlossen oder später erneut angezeigt werden soll, oder er kann auf **Jetzt anzeigen** klicken, um Details wie Version und Größe des Updates, das auf der Seite **Anwendungseinstellungen** > **Konsole und Plug-ins** verfügbar ist, anzuzeigen. Im Abschnitt „OpenManage Enterprise" auf der Seite Konsole und Plug-ins werden alle neuen Funktionen und Verbesserungen des verfügbaren Updates angezeigt.
2. Klicken Sie auf **Update** und dann auf **Konsole herunterladen**, um das Paket von der angegebenen Quelle herunterzuladen.

   ANMERKUNG:

   - Durch Klicken auf **Aktualisieren** wird ein Job zum Herunterladen des Upgrade-Bundle initialisiert. Dieser Job wird nach dem Herunterladen aller Updatedateien von selbst abgeschlossen und kann nicht beendet werden.
   - Wenn das Upgrade fehlschlägt, wird die Appliance neu gestartet. Es wird empfohlen, den VM-Snapshot zurückzusetzen und das Upgrade erneut durchzuführen.

3. Wenn das Kontrollkästchen **Automatisches Starten des Konsolen-Updates, wenn Downloads abgeschlossen sind** in den Update-Einstellungen aktiviert ist, wird das Upgrade automatisch gestartet, nachdem das Update-Paket heruntergeladen wurde. Klicken Sie andernfalls auf **Konsole aktualisieren**, um das Update durchzuführen.

Konfigurieren von OpenManage Enterprise und Durchführen eines Offline-Upgrades mithilfe der Netzwerkfreigabe

Sie müssen eine lokale Netzwerkfreigabe einrichten und das Aktualisierungspaket manuell herunterladen, wenn Sie nicht automatisch mit Dell.com verbunden sind. Jedes Mal, wenn manuell nach einem Update gesucht wird, wird ein Auditprotokoll erstellt.

Bevor Sie mit dem Update über eine Netzwerkfreigabe beginnen:

- Sie müssen Administratorrechte besitzen, um das Upgrade auszuführen. Weitere Informationen zu Berechtigungen finden Sie unter Rollen- und bereichsbasierte Zugriffskontrolle in OpenManage Enterprise auf Seite 16.
- Stellen Sie sicher, dass Sie die allgemeinen Upgrade-Empfehlungen und -Voraussetzungen, wie in Upgrade-Empfehlungen und -Voraussetzungen auf Seite 170 beschrieben, gelesen haben.
- Für Offline-Updates (Netzwerkfreigabe) sollte der Administrator je nachdem, ob ein minimales oder ein vollständiges Upgrade erforderlich ist, entsprechende Ordnerstrukturen erstellen und dann die entsprechenden Dateien von https://downloads.dell.com herunterladen und auf der Netzwerkfreigabe speichern. Ausführlichere Informationen zur Aktualisierung von OpenManage Enterprise auf die neueste Version und zulässige Ordnerstruktur für Updates finden Sie im technischen Whitepaper „Upgrade der Dell OpenManage EMC Enterprise Appliance-Version" (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) auf der Support-Website.
- Machen Sie einen VM-Snapshot der Konsole als Backup für den Fall, dass etwas Unerwartetes eintritt. (Weisen Sie zusätzliche Ausfallzeiten dafür zu, falls erforderlich).
- Wenn das Upgrade fehlschlägt, wird die Appliance neu gestartet. Es wird empfohlen, den VM-Snapshot zurückzusetzen und das Upgrade erneut durchzuführen.
- Das Hinzufügen einer zweiten Netzwerkschnittstelle sollte erst nach Abschluss der Upgradeaufgaben nach der Konsole durchgeführt werden. Der Versuch, eine zweite NIC hinzuzufügen, während die Aufgaben nach dem Upgrade noch durchgeführt werden, wäre ineffektiv.
- Sie müssen sicherstellen, dass die Sicherheitszertifikate von einer vertrauenswürdigen Drittanbieter-Zertifizierungsstelle signiert wurde, wenn Sie die HTTPS-Aktualisierungsmethode verwenden.

ANMERKUNG:

- OpenManage Enterprise-Versionen vor Version 3.4, z. B. Version 3.3x und Version 3.2, müssen zuerst auf Version 3.4 und dann auf Version 3.5 aktualisiert werden, bevor eine Aktualisierung auf 3.7 über eine freigegebene Netzwerkdateifreigabe (NFS) durchgeführt werden kann.

- Das direkte Aktualisieren von der Version „OpenManage Enterprise – Tech Release“ wird nicht unterstützt. TechRelease-Versionen sollten zunächst auf OpenManage Enterprise Version 3.0 oder 3.1 aktualisiert werden.
- Beim Aktualisieren von lokalen Freigaben für ein manuelles Upgrade von Versionen ohne installierte Erweiterungen/Plug-ins (z. B. 3.1 und 3.2) werden im Auditprotokoll Warnmeldungseinträge angezeigt, wie z. B. „Die Quelldatei vom Typ Erweiterungskatalog kann nicht abgerufen werden, weil die Datei nicht vorhanden ist“ und „Der Status des Downloads des Erweiterungskatalogs lautet fehlgeschlagen“. Diese Fehlermeldungen haben keine funktionalen Auswirkungen auf den Upgradeprozess und können ignoriert werden.

Das Upgrade von OpenManage Enterprise von einer Netzwerkfreigabe ist ein zweistufiger Prozess. Zunächst Konfigurieren der Appliance für das Update von einer Netzwerkfreigabe auf Seite 173, um festzulegen, wie die Updates abgerufen werden sollen und die Update-Methode auszuwählen, und anschließend Update der Appliance von einer Netzwerkfreigabe auf Seite 173 über die Seite Konsole und Plug-ins.

Konfigurieren der Appliance für das Update von einer Netzwerkfreigabe

1. Laden Sie die benötigten Dateien von https://downloads.dell.com herunter und speichern Sie sie auf einer Netzwerkfreigabe unter Beibehaltung derselben Ordnerstruktur, auf die von der Konsole aus zugegriffen werden kann.

   Ausführlichere Informationen zur Aktualisierung von OpenManage Enterprise auf die neueste Version und zulässige Ordnerstruktur für Updates finden Sie im technischen Whitepaper „Upgrade der Dell OpenManage EMC Enterprise Appliance-Version“ (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) auf der Support-Website.
2. Klicken Sie auf **Anwendungseinstellungen** > **Konsole und Erweiterungen** > **Update-Einstellungen**.
3. Wählen Sie in **Wie Sie auf Updates prüfen** eine der folgenden Optionen aus:
   - **Automatisch**: Die Appliance prüft jeden Montag auf die Verfügbarkeit der Aktualisierungen von der Quelle, die im **Wo nach Updates suchen** angegeben ist.
   - **Manuell**: Der Nutzer muss manuell prüfen, ob das Update von der Quelle verfügbar ist, die unter **Wo nach Updates suchen** angegeben ist, indem er auf das Symbol „Liste aktualisieren“ im Abschnitt „Updates“ auf der Seite Konsole und Plug-ins klickt.
4. Wählen Sie unter **Wo nach Updates suchenNetzwerkfreigabe** aus, um den Speicherort anzugeben, an dem die Appliance nach Updates sucht.
   a. Geben Sie unter **Lokaler Pfad** einen NFS-, HTTP- oder HTTPS-Pfad an, der die heruntergeladenen Dateien enthält. Das Format einer Netzwerkfreigabe lautet: `nfs://<IP Address>/<Folder_Name>, http://<IP Address>/<Folder_Name>, or https://<IP Address>/<Folder_Name>.`
   b. Um die Verbindung zur angegebenen Netzwerkfreigabe zu überprüfen, klicken Sie auf **Jetzt testen**.
5. Optional: Aktivieren Sie das Kontrollkästchen **Automatisches Starten des Konsolen-Updates, wenn Downloads abgeschlossen sind**, um eine Installation des Konsolen-Updates unmittelbar nach dem Herunterladen des Update-Pakets zu initiieren. Andernfalls kann das Update manuell initiiert werden.
6. Klicken Sie auf **Anwenden**.

Update der Appliance von einer Netzwerkfreigabe

- Stellen Sie sicher, dass Sie die Voraussetzungen und Empfehlungen wie in Upgrade-Empfehlungen und -Voraussetzungen auf Seite 170 beschrieben, gelesen haben.
- Stellen Sie sicher, dass die Update-Einstellungen für das Update von einer Netzwerkfreigabe konfiguriert sind. Siehe *Konfigurieren der Appliance für das Update von einer Netzwerkfreigabe.*

1. Basierend auf den Aktualisierungseinstellungen prüft die Appliance auf die Verfügbarkeit einer Aktualisierung. Wenn eine neue Version verfügbar ist, wird ein Banner mit den neuen Informationen zur Upgradeversion angezeigt. Über den Banner kann der Administrator auswählen, ob die Benachrichtigung geschlossen und später erneut angezeigt werden soll, oder er kann auf **Jetzt anzeigen** klicken, um Details wie Version und Größe des Updates, das auf der Seite **Anwendungseinstellungen** > **Konsole und Plug-ins** verfügbar ist, anzuzeigen. Im Abschnitt „OpenManage Enterprise“ auf der Seite Konsole und Plug-ins werden alle neuen Funktionen und Verbesserungen des verfügbaren Updates angezeigt.
2. Klicken Sie auf **Update** und dann auf **Konsole herunterladen**, um das Paket von der angegebenen Quelle herunterzuladen.

   ANMERKUNG:
   - Durch Klicken auf **Aktualisieren** wird ein Job zum Herunterladen des Upgrade-Bundle initialisiert. Dieser Job wird nach dem Herunterladen aller Updatedateien von selbst abgeschlossen und kann nicht beendet werden.

- Wenn beim Upgrade-Download ein Problem bei der Verbindung über den Proxy auftritt, deaktivieren Sie die Proxy-Einstellungen und führen Sie dann den Download durch.

3. Wenn das Kontrollkästchen **Automatisches Starten des Konsolen-Updates, wenn Downloads abgeschlossen sind** in den Update-Einstellungen aktiviert ist, wird das Upgrade automatisch gestartet, nachdem das Update-Paket heruntergeladen wurde. Klicken Sie andernfalls auf **Konsole aktualisieren**, um das Update durchzuführen.

Melden Sie sich nach dem Update an und bestätigen Sie, dass das Produkt wie erwartet funktioniert. Überprüfen Sie das Auditprotokoll auf Warnmeldungen oder Fehler im Zusammenhang mit der Aktualisierung. Sollten Fehler vorhanden sein, exportieren Sie das Auditprotokoll und speichern es für den technischen Support.

Nach dem Update der Appliance:

- Löschen Sie den Browser-Cache. Wenn der Browser-Cache nicht gelöscht wird, kann dies zu einem Fehlschlagen von neuen Tasks nach dem Update führen.
- Wenn Sie ein Upgrade von OpenManage Enterprise Version 3,1 durchführen, wird empfohlen, dass Sie die Active Directory-Gruppen neu konfigurieren oder importieren, um die Performance zu verbessern.
- Sie können sich unmittelbar nach dem Update der Appliance anmelden und müssen nicht warten, bis die gesamte Bestandsaufnahme abgeschlossen wurde. Nach dem Update wird der Ermittlungstask im Hintergrund ausgeführt und Sie können den Fortschritt gelegentlich sehen.

Installieren eines Plug-ins

Sie können die Plug-ins CloudIQ, Power Manager, OpenManage Enterprise Services (vormals SupportAssist-Enterprise) und Update Manager basierend auf Ihren Anforderungen installieren, um die Funktionalität von OpenManage Enterprise zu verbessern.

- Um OpenManage Enterprise Plug-ins von dell.com zu installieren, müssen Sie sicherstellen, dass die OpenManage Enterprise-Appliance auf downloads.dell.com zugreifen kann.
- Um OpenManage Enterprise Plug-ins aus einer lokalen Netzwerkfreigabe zu installieren, müssen Sie das Paket manuell auf die Netzwerkfreigabe herunterladen und den Speicherort auf der Seite Updateeinstellungen in OpenManage Enterprise aktualisieren.

Weitere Informationen zur Konfiguration von Systemaktualisierungen finden Sie unter Überprüfen und Aktualisieren der Version von OpenManage Enterprise und der verfügbaren Plug-ins auf Seite 170.

ANMERKUNG: Durch die Installation eines Plug-ins in OpenManage Enterprise werden die Appliance-Services neu gestartet.

Führen Sie die folgenden Schritte aus, um das Plug-in zu installieren:

1. Klicken Sie in OpenManage Enterprise auf **Anwendungseinstellungen** > **Konsole und Plug-ins**.
   Daraufhin wird die Seite **Konsole und Plug-ins** angezeigt.
2. Klicken Sie im Bereich **Plug-ins** auf **Installieren** für die Plug-ins, die Sie installieren möchten.
   Der Assistent **Plug-in installieren** wird angezeigt.
3. Wählen Sie in der Liste **Verfügbare Version(en)** die Version aus, die Sie installieren möchten.
4. Überprüfen Sie die Liste der Voraussetzungen, die im Abschnitt **Voraussetzungen** aufgeführt sind, und klicken stellen Sie sicher, dass Sie diese erfüllen. Klicken Sie dann auf **Plug-in herunterladen**.

   ANMERKUNG: Die Liste der Voraussetzungen ändert sich, wenn Sie die Version des Plug-ins auswählen, das Sie installieren möchten.

   Der Installationsvorgang validiert die Voraussetzungen für die Installation des Plug-ins. Wenn die Installationsvoraussetzungen nicht erfüllt sind, wird eine entsprechende Fehlermeldung angezeigt.

   Nachdem das Plug-in erfolgreich heruntergeladen wurde, ändert sich der Status im oberen Bereich von **Verfügbar** in **Heruntergeladen**.
5. Um das OpenManage Enterprise-Plug-in zu installieren, klicken Sie im Assistenten **Plug-in installieren** auf **Plug-in installieren**.
6. Es wird ein Zustimmungsformular angezeigt, um Sie über die Endnutzer-Lizenzvereinbarung (EULA) zu informieren. Klicken Sie auf **Akzeptieren**, um mit der Installation des Plug-ins fortzufahren.
   Die Details zur Anzahl der Nutzer, die bei OpenManage Enterprise angemeldet sind, Tasks in Bearbeitung und geplanten Jobs werden im Dialogfeld **Bestätigung** angezeigt.
7. Um die Installation zu bestätigen, wählen Sie die Option **Ich bestätige, dass ich den Snapshot der OpenManage Enterprise-Appliance vor dem Ausführen einer Plug-in-Aktion erstellt habe** und klicken Sie dann auf **Installation bestätigen**.
   Der Status des Installationsvorgangs wird angezeigt. Nach der erfolgreichen Installation des Plug-ins ändert sich der Status, der oben im Plug-in-Abschnitt angezeigt wird, von **Verfügbar** oder **Heruntergeladen** in **Installiert**.

Deaktivieren eines Plug-ins

Deaktiviert alle Funktionen des Plug-ins in OpenManage Enterprise.

ANMERKUNG: Durch die Deaktivierung eines Plug-ins in OpenManage Enterprise werden die Appliance-Services neu gestartet.

1. Klicken Sie in OpenManage Enterprise auf **Anwendungseinstellungen** > **Konsole und Plug-ins**.
   Daraufhin wird die Registerkarte **Konsole und Plug-ins** angezeigt.
2. Klicken Sie im Bereich **Plug-ins** auf **Deaktivieren** für die Plug-ins, die Sie deaktivieren möchten.
   Der Assistent **Plug-in deaktivieren** wird angezeigt.
3. Um das Plug-in zu deaktivieren, klicken Sie auf **Plug-in deaktivieren**.
   Die Details zur Anzahl der Nutzer, die bei OpenManage Enterprise angemeldet sind, Tasks in Bearbeitung und geplanten Jobs werden im Dialogfeld **Bestätigung** angezeigt.
4. Wählen Sie zur Bestätigung die Option **Ich bestätige, dass ich den Snapshot der OpenManage Enterprise Appliance vor dem Ausführen der Plug-in-Aktion erstellt habe.** und klicken Sie dann auf **Deaktivieren bestätigen**.

ANMERKUNG: Nach dem Deaktivieren des Plug-ins können Sie keine Informationen oder Seiten im Zusammenhang mit dem Plug-in in OpenManage Enterprise sehen.

Deinstallieren eines Plug-ins

Deinstalliert und löscht alle Daten, die vom Plug-in gesammelt wurden.

1. Klicken Sie in OpenManage Enterprise auf **Anwendungseinstellungen** > **Konsole und Plug-ins**.
   Daraufhin wird die Registerkarte **Konsole und Plug-ins** angezeigt.
2. Klicken Sie im Bereich **Plug-ins** auf **Deinstallieren** für die Plug-ins, die Sie deinstallieren möchten.
   Der Assistent **Plug-in deinstallieren** wird angezeigt.
3. Um das Plug-in von OpenManage Enterprise zu deinstallieren, klicken Sie auf **Plug-in deinstallieren**.
   Die Details zur Anzahl der Nutzer, die bei OpenManage Enterprise angemeldet sind, Tasks in Bearbeitung und geplanten Jobs werden im Dialogfeld **Bestätigung** angezeigt.
4. Wählen Sie zur Bestätigung der Deinstallation die Option **Ich bestätige, dass ich den Snapshot der OpenManage Enterprise Appliance vor dem Ausführen der Plug-in-Aktion erstellt habe.** und klicken Sie dann auf **Deinstallieren bestätigen**.

Alle Funktionen und Daten im Zusammenhang mit dem Plug-in werden deinstalliert.

Aktivieren eines Plug-ins

Alle Plug-in-Seiten werden in OpenManage Enterprise angezeigt und Plug-in-Funktionen sind für OpenManage Enterprise aktiviert.

ANMERKUNG: Durch Aktivieren eines Plug-ins in OpenManage Enterprise werden die Appliance-Services neu gestartet.

1. Klicken Sie in OpenManage Enterprise auf **Anwendungseinstellungen** > **Konsole und Plug-ins**.
   Daraufhin wird die Registerkarte **Konsole und Plug-ins** angezeigt.
2. Klicken Sie im Bereich **Plug-ins** auf **Aktivieren** für das Plug-in, das Sie aktivieren möchten.
   Der Assistent **Plug-in aktivieren** wird angezeigt.
3. Klicken Sie auf **Plug-in aktivieren**, um das Plug-in zu aktivieren.
   Die Details zur Anzahl der Nutzer, die bei OpenManage Enterprise angemeldet sind, Tasks in Bearbeitung und geplanten Jobs werden im Dialogfeld **Bestätigung** angezeigt.
4. Wählen Sie zur Bestätigung die Option **Ich bestätige, dass ich den Snapshot der OpenManage Enterprise Appliance vor dem Ausführen der Plug-in-Aktion erstellt habe.** und klicken Sie dann auf **Aktivieren bestätigen**.

Aktualisieren eines Plug-ins

Basierend auf den Update-Einstellungen prüft die Appliance die Verfügbarkeit eines Updates der installierten Plug-ins. Wenn eine neue Version verfügbar ist, wird ein Banner mit Informationen zur neuen Upgrade-Version angezeigt. Über den Banner kann der Administrator auswählen, ob die Benachrichtigung geschlossen oder später erneut angezeigt werden soll, oder er kann auf **Jetzt anzeigen** klicken, um Details wie Version und Größe des Updates, das auf der Seite **Anwendungseinstellungen** > **Konsole und Plug-ins** verfügbar ist, anzuzeigen. Im Abschnitt „Plug-in" auf der Seite „Konsole und Plug-ins" werden alle neuen Funktionen und Verbesserungen des verfügbaren Plug-in-Updates angezeigt.

Bevor Sie ein Plug-in aktualisieren, stellen Sie sicher, dass die Aktualisierungseinstellungen wie in Überprüfen und Aktualisieren der Version von OpenManage Enterprise und der verfügbaren Plug-ins auf Seite 170 beschrieben konfiguriert sind.

Um ein Plug-in zu erstellen, führen Sie die folgenden Schritte aus:

1. Klicken Sie im Abschnitt „Plug-in" auf **Update verfügbar** für das Plug-in, das Sie aktualisieren möchten.
   Die Seite **Plug-in aktualisieren** wird angezeigt.
2. Wählen Sie die Plug-in-Version aus und klicken Sie dann auf **Plug-in herunterladen**.
   Das Plug-in wird heruntergeladen und der Status des Downloads wird in einem grünen Band angezeigt.
3. Klicken Sie zum Aktualisieren des Plug-ins auf **Plug-in aktualisieren**.
   Wählen Sie im Fenster **Bestätigung** die Option **Ich bestätige, dass ich einen Snapshot der OpenManage Enterprise-Appliance vor dem Ausführen der Plug-in-Aktion erstellt habe** und klicken Sie dann auf **Aktualisieren**.

Nachdem der Aktualisierungsvorgang abgeschlossen ist, wird die Version im Abschnitt „Plug-in" angezeigt.

Befehle und Skripts ausführen

Bei Erhalt eines SNMP-Traps können Sie auf OpenManage Enterprise ein Skript ausführen. Dadurch wird eine Richtlinie eingerichtet, die ein Ticket auf Ihrem Drittanbieter-Ticketing-System für die Warnungsverwaltung öffnet. Sie können nur bis zu **vier** Remote-Befehle erstellen und speichern.

ANMERKUNG: Die Verwendung der folgenden Sonderzeichen als RACADM- und IPMI-CLI-Parameter wird nicht unterstützt: **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, * und **'**.

1. Klicken Sie auf **Anwendungseinstellungen** > **Skriptausführung**.
2. Gehen Sie im Abschnitt **Remote-Befehl – Einstellung** wie folgt vor:
   a. Zum Hinzufügen eines Remote-Befehls klicken Sie auf **Erstellen**.
   b. Geben Sie den in das Feld **Befehlsname** den Befehlsnamen ein.
   c. Wählen Sie einen der folgenden Befehlstypen aus:
      i. Skript
      ii. RACADM
      iii. IPMI Tool
   d. Wenn Sie **Skript** auswählen, gehen Sie wie folgt vor:
      i. Geben Sie in das Feld **IP-Adresse** die IP-Adresse ein.
      ii. Wählen Sie die Authentifizierungsmethode: **Kennwort** oder **SSH-Schlüssel**.
      iii. Geben Sie **Benutzername** und **Kennwort** oder **SSH-Schlüssel** ein.
      iv. Im Feld **Befehl** geben Sie die Befehle ein.
         - Bis zu 100 Befehle können eingegeben werden, wobei jeder Befehl in einer neuen Zeile sein muss.
         - Token-Ersetzung in Scripts ist möglich. Siehe . Token-Ersetzung in Remote-Skripts und Warnmeldungsrichtlinien auf Seite 184
      v. Klicken Sie auf **Fertigstellen**.
   e. Wenn Sie **RACADM** auswählen, gehen Sie wie folgt vor:
      i. Geben Sie den in das Feld **Befehlsname** den Befehlsnamen ein.
      ii. Im Feld **Befehl** geben Sie die Befehle ein. Bis zu 100 Befehle können eingegeben werden, wobei jeder Befehl in einer neuen Zeile sein muss.
      iii. Klicken Sie auf **Fertigstellen**.
   f. Wenn Sie **IPMI Tool** auswählen, gehen Sie wie folgt vor:
      i. Geben Sie den in das Feld **Befehlsname** den Befehlsnamen ein.
      ii. Im Feld **Befehl** geben Sie die Befehle ein. Bis zu 100 Befehle können eingegeben werden, wobei jeder Befehl in einer neuen Zeile sein muss.
      iii. Klicken Sie auf **Fertigstellen**.
3. Zum Bearbeiten der Einstellung eines Remote-Befehls wählen Sie den Befehl aus und klicken dann auf **Bearbeiten**.
4. Zum Löschen der Einstellung eines Remote-Befehls wählen Sie den Befehl aus und klicken dann auf **Löschen**.

OpenManage Mobile-Einstellungen

OpenManage Mobile (OMM) ist eine Systems Management-Anwendung, die Ihnen ermöglicht, einen Teilbereich von Rechenzentrumsüberwachungs- und Fehlerbehebungstasks auf einer oder mehreren OpenManage Enterprise-Konsolen und/oder einem integrierten Dell Remote Access Controller (iDRAC) unter Verwendung Ihres Android- oder iOS-Geräts auszuführen. Mithilfe von OMM können Sie Folgendes tun:

- Warnungsbenachrichtigungen von OpenManage Enterprise empfangen.
- Gruppe, Gerät, Warnung, und Protokollinformationen anzeigen.
- Einen Server ein-/ausschalten oder neu starten.

Standardmäßig sind Push-Benachrichtigungen für alle Warnungen und kritischen Warnungen aktiviert. Dieses Kapitel enthält Informationen über die OMM-Einstellungen, die Sie über OpenManage Enterprise konfigurieren können. Es stellt außerdem Informationen bereit, die Sie benötigen, um Fehler in OMM zu beheben.

ANMERKUNG: Weitere Informationen über die Installation und Verwendung von OMM finden Sie im *OpenManage Mobile-Benutzerhandbuch* unter Dell.com/OpenManageManuals.

Zugehörige Tasks

Aktivieren oder Deaktivieren von Warnbenachrichtigungen für OpenManage Mobile auf Seite 177
Aktivieren oder Deaktivieren von OpenManage Mobile-Abonnenten auf Seite 178
Löschen eines OpenManage Mobile-Abonnenten auf Seite 178
Anzeigen des Status des Warnungs-Benachrichtigungs-Dienstes auf Seite 178
Fehlerbehebung bei OpenManage Mobile auf Seite 180

Zugehörige Informationen

Aktivieren oder Deaktivieren von Warnbenachrichtigungen für OpenManage Mobile auf Seite 177
Aktivieren oder Deaktivieren von OpenManage Mobile-Abonnenten auf Seite 178
Fehlerbehebung bei OpenManage Mobile auf Seite 180

Aktivieren oder Deaktivieren von Warnbenachrichtigungen für OpenManage Mobile

Standardmäßig ist OpenManage Enterprise so konfiguriert, dass Warnungsbenachrichtigungen an die OpenManage Mobile-Anwendung gesendet werden. Warnungsbenachrichtigungen werden jedoch nur von OpenManage Enterprise gesendet, wenn ein OpenManage Mobile-Benutzer OpenManage Enterprise zur OpenManage Mobile-Anwendung hinzufügt.

ANMERKUNG: Die Administrator-Berechtigungen sind erforderlich zur Aktivierung oder Deaktivierung von Warnbenachrichtigungen für OpenManage Mobile.

ANMERKUNG: Damit OpenManage Enterprise Warnungsbenachrichtigungen an OpenManage Mobile senden kann, stellen Sie sicher, dass der OpenManage Enterprise-Server über ausgehenden (HTTPS-) Internetzugang verfügt.

So aktivieren oder deaktivieren Sie Warnungsbenachrichtigungen von OpenManage Enterprise an OpenManage Mobile:

1. Klicken Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Mobile**.
2. Markieren Sie das Kontrollkästchen **Pushbenachrichtigungen aktivieren**.
3. Klicken Sie auf **Anwenden**.

Zugehörige Tasks

OpenManage Mobile-Einstellungen auf Seite 177

Zugehörige Informationen

OpenManage Mobile-Einstellungen auf Seite 177
Löschen eines OpenManage Mobile-Abonnenten auf Seite 178

Aktivieren oder Deaktivieren von OpenManage Mobile-Abonnenten

Die Kontrollkästchen in der Spalte **Aktiviert** der Liste **Mobile-Abonnenten** ermöglichen Ihnen die Aktivierung oder Deaktivierung der Übertragung von Warnungsbenachrichtigungen an OpenManage Mobile-Abonnenten.

ANMERKUNG:

- Administrator-Berechtigungen sind erforderlich zur Aktivierung oder Deaktivierung von OpenManage Mobile-Abonnenten.
- OpenManage Mobile-Abonnenten werden möglicherweise automatisch von OpenManage Enterprise deaktiviert, wenn der Push-Benachrichtigungsdienst ihres Mobilfunkanbieters angibt, dass das Gerät dauerhaft nicht erreichbar ist.
- Selbst wenn ein OpenManage Mobile-Abonnent in der Liste **Mobile-Abonnenten** aktiviert ist, kann dieser den Empfang von Warnungsbenachrichtigungen in seinen OpenManage Mobile-Anwendungseinstellungen deaktivieren.

So aktivieren oder deaktivieren Sie Warnungsbenachrichtigungen an OpenManage Mobile-Abonnenten:

1. Klicken Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Mobile**.
2. Wählen Sie zur Aktivierung das entsprechende Kontrollkästchen und klicken Sie auf **Aktivieren**. Wählen Sie zur Deaktivierung das entsprechende Kontrollkästchen und klicken Sie auf **Deaktivieren**.

   Es können mehrere Abonnenten gleichzeitig ausgewählt werden.

Zugehörige Tasks

OpenManage Mobile-Einstellungen auf Seite 177

Zugehörige Informationen

OpenManage Mobile-Einstellungen auf Seite 177
Löschen eines OpenManage Mobile-Abonnenten auf Seite 178

Löschen eines OpenManage Mobile-Abonnenten

Das Löschen eines OpenManage Mobile-Abonnenten entfernt den Benutzer aus der Liste der Abonnenten. Dadurch wird verhindert, dass der Benutzer Warnungsbenachrichtigungen von OpenManage Enterprise erhält. Der OpenManage Mobile-Benutzer kann später erneut Warnungsbenachrichtigungen von der OpenManage Mobile-Anwendung abonnieren.

ANMERKUNG: Die Administrator-Berechtigungen sind erforderlich für das Löschen eines OpenManage Mobile-Abonnenten.

So löschen Sie einen OpenManage Mobile-Abonnenten:

1. Klicken Sie auf **OpenManage Enterprise** > **Anwendungseinstellungen** > **Mobile**.
2. Aktivieren Sie das Kontrollkästchen des entsprechenden Abonnentennamens und klicken Sie auf **Löschen**.
3. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**.

Zugehörige Tasks

Aktivieren oder Deaktivieren von Warnbenachrichtigungen für OpenManage Mobile auf Seite 177
Aktivieren oder Deaktivieren von OpenManage Mobile-Abonnenten auf Seite 178
Löschen eines OpenManage Mobile-Abonnenten auf Seite 178
Anzeigen des Status des Warnungs-Benachrichtigungs-Dienstes auf Seite 178

Zugehörige Informationen

OpenManage Mobile-Einstellungen auf Seite 177
Löschen eines OpenManage Mobile-Abonnenten auf Seite 178

Anzeigen des Status des Warnungs-Benachrichtigungs-Dienstes

OpenManage Enterprise leitet Warnungsbenachrichtigungen über den jeweiligen Geräteplattform-Warnungsbenachrichtigungsdienst an OpenManage Mobile-Abonnenten weiter. Wenn der OpenManage Mobile-Abonnent keine Warnungsbenachrichtigungen erhält, können Sie den **Benachrichtigungsdienststatus** überprüfen, um die Fehler bei der Lieferung von Warnungsbenachrichtigungen zu beheben.

Um den Status des Warnungs-Benachrichtigungs-Dienstes anzuzeigen, klicken Sie auf **AnwendungseinstellungenMobile**.

Zugehörige Tasks

Anzeigen des Status des Warnungs-Benachrichtigungs-Dienstes auf Seite 178

Zugehörige Informationen

OpenManage Mobile-Einstellungen auf Seite 177
Löschen eines OpenManage Mobile-Abonnenten auf Seite 178
Anzeigen des Status des Warnungs-Benachrichtigungs-Dienstes auf Seite 178

Status des Benachrichtigungsdiensts

Die folgende Tabelle enthält Informationen über den **Benachrichtigungsservicestatus**, der auf der Seite **Anwendungseinstellungen** > **Mobile** angezeigt wird.

Tabelle 29. Status des Benachrichtigungsdiensts

Statussymbol	Statusbeschreibung
	Der Service läuft und funktioniert normal. **ANMERKUNG:** Dieser Servicestatus gibt nur die erfolgreiche Kommunikation mit dem Plattform-Benachrichtigungsdienst wieder. Wenn das Gerät des Abonnenten nicht mit dem Internet oder einem mobilen Datendienst verbunden ist, werden Benachrichtigungen erst gesendet, wenn die Verbindung wiederhergestellt ist.
	Der Service hatte einen Fehler beim Liefern einer Nachricht, was möglicherweise vorübergehender Natur ist. Wenn das Problem weiterhin besteht, befolgen Sie die Schritte zur Fehlerbehebung oder wenden sich an den technischen Support.
	Im Service ist ein Fehler beim Liefern einer Nachricht aufgetreten. Befolgen Sie die Schritte zur Fehlerbehebung oder wenden Sie sich nach Bedarf an den Support.

Anzeigen von Informationen zu OpenManage Mobile-Abonnenten

Nachdem ein OpenManage Mobile-Benutzer erfolgreich OpenManage Enterprise hinzugefügt hat, wird der Benutzer der **Mobile-Abonnenten**-Tabelle in OpenManage Enterprise hinzugefügt. Zur Anzeige von Informationen zu Mobile-Abonnenten in OpenManage Enterprise klicken Sie auf **Anwendungseinstellungen** > **Mobile**.

Sie können die Informationen zu Mobile-Abonnenten auch über die die Dropdown-Liste **Exportieren** in eine .CSV-Datei exportieren.

Informationen über OpenManage Mobile-Abonnenten

Die folgende Tabelle enthält Informationen über die Tabelle **Mobile-Abonnenten**, die auf der Seite **Anwendungseinstellungen** > **Mobile** angezeigt wird.

Tabelle 30. Informationen über OpenManage Mobile-Abonnenten

Feld	Beschreibung
AKTIVIERT	Aktivieren oder deaktivieren Sie das Kontrollkästchen und klicken Sie dann auf **Aktivieren** bzw. **Deaktivieren**, um die Warnungsbenachrichtigungen für einen OpenManage Mobile Abonnenten zu aktivieren oder deaktivieren.
STATUS	Zeigt den Status des Abonnenten an, der angibt, ob OpenManage Enterprise Warnungsbenachrichtigungen erfolgreich an den Warnungsweiterleitungsdienst senden kann.
STATUSMELDUNG	Statusbeschreibung der Statusanzeige.

Tabelle 30. Informationen über OpenManage Mobile-Abonnenten (fortgesetzt)

Feld	Beschreibung
BENUTZERNAME	Name des OpenManage Mobil-Benutzers.
GERÄTE-ID	Eindeutige Kennung des mobilen Geräts.
BESCHREIBUNG	Beschreibung des mobilen Geräts.
FILTER	Filter sind Richtlinien, die der Abonnent für Warnungsbenachrichtigungen konfiguriert hat.
LETZTER FEHLER	Datum und Uhrzeit des letzten Fehlers beim Senden einer Warnungsbenachrichtigung an den OpenManage Mobile-Benutzer.
LETZTER PUSH	Datum und Uhrzeit, zu denen die letzte Warnungsbenachrichtigung erfolgreich von OpenManage Enterprise an den Warnungsweiterleitungsdienst gesandt wurde.
LETZTE VERBINDUNG	Datum und Uhrzeit des letzten Benutzerzugriffs auf OpenManage Enterprise über OpenManage Mobile.
REGISTRIERUNG	Datum und Uhrzeit, zu der der Benutzer OpenManage Enterprise in OpenManage Mobile hinzugefügt hat.

Fehlerbehebung bei OpenManage Mobile

Wenn OpenManage Enterprise nicht in der Lage ist, sich beim Meldungsweiterleitungsdienst zu registrieren oder Benachrichtigungen erfolgreich weiterzuleiten, stehen folgende Lösungen zur Verfügung:

Tabelle 31. Fehlerbehebung bei OpenManage Mobile

Problem	Ursache	Lösung
OpenManage Enterprise kann keine Verbindung zum Dell Meldungsweiterleitungsdienst herstellen. [Code 1001/1002]	Keine ausgehende Internet (HTTPS)-Verbindung.	Stellen Sie über einen Web-Browser fest, ob die ausgehende Internet-Konnektivität verfügbar ist. Wenn die Verbindung nicht verfügbar ist, führen Sie die folgenden Netzwerkaufgaben zur Fehlerbehebung durch: ● Überprüfen Sie, ob die Netzwerkkabel angeschlossen sind. ● Überprüfen Sie die IP-Adresse und DNS-Server-Einstellungen ● Überprüfen Sie, ob die Firewall darauf konfiguriert ist, ausgehenden Datenverkehr zuzulassen ● Überprüfen Sie, ob das Internetdienstanbieter-Netzwerk ordnungsgemäß funktioniert.
	Proxy-Einstellungen sind falsch.	Stellen Sie Proxy-Host, Schnittstelle, Benutzername und Kennwort wie erforderlich ein.
	Der Meldungsweiterleitungsdienst ist vorübergehend nicht verfügbar.	Warten Sie, bis der Service verfügbar ist.
Der Meldungsweiterleitungsdienst ist nicht in der Lage, eine Verbindung zu einem Gerätplattform-Benachrichtigungsdienst herzustellen. [Code 100-105, 200-202, 211-212]	Der Plattform-Anbieterdienst ist vorübergehend nicht für den Meldungsweiterleitungsdienst verfügbar.	Warten Sie, bis der Service verfügbar ist.

Tabelle 31. Fehlerbehebung bei OpenManage Mobile (fortgesetzt)

Problem	Ursache	Lösung
Das Gerätekommunikations-Token ist nicht mehr mit dem Plattform-Anbieter-Service eingetragen. [Code 203]	Die OpenManage Mobile-Anwendung wurde aktualisiert, wiederhergestellt, deinstalliert, oder das Gerätebetriebssystem wurde erweitert bzw. wiederhergestellt.	Installieren Sie OpenManage Mobile neu auf dem Gerät oder befolgen Sie die OpenManage Mobile Vorgehensweisen zur Fehlerbehebung im *OpenManage Mobile-Benutzerhandbuch* und verbinden Sie das Gerät erneut mit OpenManage Enterprise. Wenn das Gerät nicht mehr mit OpenManage Enterprise verbunden ist, entfernen Sie den Abonnenten.
Die OpenManage Enterprise-Registrierung wird vom Meldungsweiterleitungsdienst abgelehnt. [Code 154]	Eine veraltete Version von OpenManage Enterprise wird verwendet.	Upgrade auf eine neuere Version von OpenManage Enterprise.

Zugehörige Tasks

OpenManage Mobile-Einstellungen auf Seite 177

Zugehörige Informationen

OpenManage Mobile-Einstellungen auf Seite 177

21

Andere Referenzen und Feldbeschreibungen

Definitionen über bestimmte häufig angezeigte Felder auf der OpenManage Enterprise-Benutzeroberfläche (GUI) sind in diesem Kapitel aufgelistet und definiert. Hier finden Sie auch weitere nützliche Informationen.

Themen:

Zeitplan-Referenz

- **Jetzt aktualisieren**: Die Firmware-Version wird aktualisiert und auf die im zugeordneten Katalog verfügbare Version abgestimmt. Damit die Aktualisierung beim nächsten Neustart des Geräts wirksam wird, aktivieren Sie das Kontrollkästchen **Für nächsten Neustart des Servers einplanen**.
- **Später planen**: Wählen Sie diese Option, um ein Datum und die Uhrzeit für die Aktualisierung der Firmware Version anzugeben.

Feld-Definitionen Firmware-Baseline

- **Kompatibilität**: der Integritätsstatus der Firmware-Baseline. Sobald ein Gerät in Verbindung mit einer Firmware-Baseline einen kritischen Integritätsstatus aufweist, wird der Baseline-Status selbst als kritisch eingestuft. Dies wird der Rollup-Integritätsstatus genannt, der dem Status der Baseline mit höchstem Schweregrad entspricht. Weitere Informationen über den Rollup-Funktionsstatus finden Sie im Whitepaper *MANAGING THE ROLLUP HEALTH STATUS BY USING IDRAC ON THE DELL EMC 14TH GENERATION AND LATER POWEREDGE SERVERS* (VERWALTEN DES ROLLUP-FUNKTIONSSTATUS MITHILFE VON IDRAC AUF DELL EMC-SERVERN DER 14. GENERATION UND NEUER) auf der Website von Dell TechCenter.
- **NAME**: Name der Firmware-Baseline. Klicken Sie auf diese Option, um den Baseline-Kompatibilitätsbericht auf der Seite **Kompatibilitätsbericht** anzuzeigen. Weitere Informationen zum Erstellen einer Firmware-Baseline finden Sie unter Erstellen einer Firmware-/Treiber-Baseline auf Seite 81.
- **KATALOG**: der Firmwarekatalog, zu dem die Firmware-Baseline gehört. Informationen dazu finden Sie unter Firmware- und Treiber-Kataloge verwalten auf Seite 78.
- **ZEITPUNKT DER LETZTEN AUSFÜHRUNGTIME**: Der Zeitpunkt, zu dem der Baseline-Kompatibilitätsbericht zuletzt ausgeführt wurde. Informationen dazu finden Sie unter Überprüfen von Geräte-Firmware- und -Treiber-Compliance auf Seite 82.

Felddefinitionen für die Jobplanung

- **Jetzt ausführen**, um den Job sofort zu starten.
- **Später ausführen**, um ein späteres Datum und eine spätere Uhrzeit anzugeben.

- **Nach Zeitplan ausführen** zur wiederholten Ausführung in ausgewählter Häufigkeit. Wählen Sie **Täglich** und wählen Sie dementsprechend die Häufigkeit aus.

ANMERKUNG: Standardmäßig wird die Uhr für den Auftragsplaner täglich um 12:00 Uhr zurückgesetzt. Das Format „cron" berücksichtigt bei der Berechnung der Auftragshäufigkeit nicht die Auftragserstellungszeit. Beispiel: Wird ein Auftrag um 10:00 Uhr gestartet, um alle 10 Stunden ausgeführt zu werden, wird der Auftrag das nächste Mal um 20:00 Uhr ausgeführt Die nachfolgende Zeit ist jedoch nicht 06:00 Uhr des nächsten Tages, sondern 12:00 Uhr. Das liegt daran, dass die Auftragsplaneruhr täglich um 12:00 Uhr zurückgesetzt wird.

Warnungskategorien nach EEMI-Verlagerung

Tabelle der EEMI-Verlagerungen

Tabelle 32. Warnungskategorien in OpenManage Enterprise

Vorherige Kategorie	Vorherige Unterkategorie	Neue Kategorie	Neue Unterkategorie
Audit	Geräte	Systemzustand	Geräte
Audit	Geräte	Konfiguration	Geräte
Audit	Geräte	Konfiguration	Geräte
Audit	Geräte	Konfiguration	Geräte
Audit	Geräte	Konfiguration	Geräte
Audit	Anwendung	Konfiguration	Anwendung
Audit	Anwendung	Konfiguration	Anwendung
Audit	Anwendung	Konfiguration	Anwendung
Audit	Anwendung	Konfiguration	Anwendung
Audit	Geräte	Audit	Benutzer
Audit	Vorlagen	Konfiguration	Vorlagen
Audit	Vorlagen	Konfiguration	Vorlagen
Audit	Vorlagen	Konfiguration	Vorlagen
Audit	Vorlagen	Konfiguration	Vorlagen
Audit	Vorlagen	Konfiguration	Vorlagen
Konfiguration	Bestandsaufnahme	Konfiguration	Aufträge
Konfiguration	Bestandsaufnahme	Konfiguration	Aufträge
Konfiguration	Bestandsaufnahme	Konfiguration	Aufträge
Konfiguration	Bestandsaufnahme	Konfiguration	Geräte
Konfiguration	Bestandsaufnahme	Konfiguration	Geräte
Konfiguration	Bestandsaufnahme	Konfiguration	Geräte
Konfiguration	Firmware	Konfiguration	Jobs
Konfiguration	Firmware	Konfiguration	Jobs
Verschiedenes	Jobs	Konfiguration	Jobs
Verschiedenes	Jobs	Konfiguration	Jobs
Verschiedenes	Jobs	Konfiguration	Jobs
Verschiedenes	Allgemein	Konfiguration	Allgemein

Tabelle 32. Warnungskategorien in OpenManage Enterprise (fortgesetzt)

Vorherige Kategorie	Vorherige Unterkategorie	Neue Kategorie	Neue Unterkategorie
Verschiedenes	Allgemein	Konfiguration	Allgemein
Verschiedenes	Allgemein	Konfiguration	Allgemein
Verschiedenes	Allgemein	Konfiguration	Allgemein
Verschiedenes	Allgemein	Konfiguration	Allgemein
Verschiedenes	Allgemein	Konfiguration	Allgemein
Verschiedenes	Allgemein	Konfiguration	Allgemein
Verschiedenes	Allgemein	Konfiguration	Allgemein
Verschiedenes	Geräte	Konfiguration	Geräte
Verschiedenes	Geräte	Konfiguration	Geräte
Audit	Sicherheit	Konfiguration	Sicherheit
Audit	Sicherheit	Konfiguration	Sicherheit
Audit	Sicherheit	Konfiguration	Sicherheit

Token-Ersetzung in Remote-Skripts und Warnmeldungsrichtlinien

OpenManage Enterprise unterstützt die Verwendung von Token, um das Remote-Scripting und die Erstellung von Warnrichtlinien zu verbessern.

Tabelle 33. In OpenManage Enterprise unterstützte Token

Token	Beschreibung
`$IP`	Geräte-IP-Adresse
`$MSG`	Meldung
`$DATE`	Datum
`$TIME`	Uhrzeit
`$SEVERITY`	Schweregrad
`$SERVICETAG`	Service-Tag-Nummer
`$RESOLUTION`	Empfohlene Auflösung
`$CATEGORY`	Name der Warnungskategorie
`$ASSETTAG`	Bestands-Tag
`$MODEL`	Modellname
`$HOSTNAME`	FQDN oder Hostname (wenn FQDN nicht vorhanden ist)

Kundendienst-Debugging-Workflow

In OpenManage Enterprise können Sie das Konsolen-Debugging unter Verwendung der Option „Field Service Debug" (FSD) autorisieren.

Mithilfe von FSD können Sie folgende Aufgaben ausführen:

- Zulassen der Aktivierung und Vervielfältigung von Fehlersuchprotokollen
- Zulassen der Vervielfältigung von Echtzeitprotokollen
- Zulassen der Sicherung oder Wiederherstellung der Datenbank auf einer VM.

Die in den einzelnen Tasks referenzierten Themen enthalten detaillierte Anweisungen. Führen Sie folgende Tasks aus, um FSD zu aktivieren:

1. Entsperren Sie die FSD-Fähigkeit. Informationen dazu finden Sie unter FSD-Funktion entsperren auf Seite 185.
2. Installieren oder gewähren Sie die signierte FSD-DAT.ini-Datei. Informationen dazu finden Sie unter Eine signierte FSD-DAT.ini-Datei installieren oder bewilligen auf Seite 185.
3. Rufen Sie FSD auf. Informationen dazu finden Sie unter FSD aufrufen auf Seite 186.
4. Deaktivieren Sie FSD. Informationen dazu finden Sie unter FSD deaktivieren auf Seite 186.

FSD-Funktion entsperren

Über den Bildschirm TUI können Sie die FSD-Funktion entsperren.

1. Navigieren Sie zum TUI-Hauptmenü.
2. Um die FSD-Option zu verwenden, wählen Sie im TUI-Bildschirm **FSD-Modus (Field Service Debug) aktivieren**.
3. Um eine neue FSD-Entsperrungsanforderung zu erzeugen, wählen Sie im Bildschirm **FSD-Funktionen** die Option **FSD-Funktionen entsperren**.
4. Wählen Sie ein Start- und Enddatum, um die Dauer der angeforderten Debug-Funktionen zu bestimmen.
5. Wählen Sie auf dem Bildschirm **Anforderte Debug-Funktionen auswählen** eine Debug-Funktion aus einer Liste von speziell für die Konsole verfügbaren Debug-Funktionen aus. Wählen Sie in der rechten unteren Ecke die Option **Generieren**.

   ANMERKUNG: Die aktuell unterstützte Debug-Funktion ist `RootShell`

6. Lesen Sie auf dem Bildschirm **DAT-Datei herunterladen** die Signierungsanweisungen und die URL-Adresse der Freigabe, über die die DAT.ini-Datei verfügbar ist.
7. Verwenden Sie einen externen Client, um die DAT.ini-Datei aus der URL-Adresse der in Schritt 6 genannten Freigabe zu extrahieren.

   ANMERKUNG: Das Freigabeverzeichnis für den Download verfügt über Leseberechtigung und unterstützt nur jeweils eine DAT. ini-Datei.

8. Führen Sie eine der folgenden Aufgaben aus, je nachdem, ob Sie ein externer Benutzer oder ein interner Dell EMC Benutzer sind:
   - Senden Sie die DAT.ini-Datei zum Signieren an einen Dell EMC Kontakt, wenn Sie ein externer Benutzer sind.
   - Laden Sie die DAT.ini-Datei zur entsprechenden Dell Außendienst-Debug-Authentifizierungsstelle (FSDAF, Dell Field Service Debug Authentication Facility) hoch und senden Sie sie ab.
9. Warten Sie auf die Rücksendung einer von Dell EMC signierten und genehmigten DAT.ini-Datei.

Eine signierte FSD-DAT.ini-Datei installieren oder bewilligen

Stellen Sie sicher, dass Sie die Datei DAT.ini erhalten haben, die von Dell EMC zugelassenen und unterzeichnet ist.

ANMERKUNG: Nachdem Dell EMC die DAT.ini-Datei genehmigt hat, müssen Sie die Datei in das Konsolen-Gerät hochladen, das den ursprünglichen Befehl zum Entblocken generiert hat.

1. Zum Hochladen einer signierten DAT.ini-Datei auf den Bildschirm **FSD-Funktionen** wählen Sie **Installieren/Signierte FSD-DAT-Datei bewilligen** .

   ANMERKUNG: Das Hochladen-Freigabeverzeichnis hat nur lesegeschützte Berechtigungen und unterstützt lediglich jeweils nur eine DAT.ini-Datei. Die Größe der Datei DAT.ini liegt bei 4 KB.

2. Befolgen Sie auf dem Bildschirm **Hochladen signierte Datei DAT** die Anweisungen zum Hochladen der Datei DAT.ini für eine bestimmte Dateifreigabe-URL.
3. Verwenden Sie einen externen Client zum Hochladen der Datei DAT.ini zu einem Freigabespeicherort.
4. Wählen Sie auf dem Bildschirm **Hochladen signierte Datei DAT Ich habe die FSD DAT-Datei hochgeladen**.

Falls keine Fehler vorliegen, während die DAT.ini-Datei hochgeladen wird, wird eine Bestätigungsmeldung der erfolgreichen Installation des Zertifikats angezeigt. Klicken Sie auf **OK**, um fortzufahren.

Das Hochladen der Datei DAT.ini kann möglicherweise wegen der folgenden Gründe nicht ausgeführt werden:

- Das Hochlade-Freigabeverzeichnisses hat unzureichenden Speicherplatz.

- Die hochgeladene Datei DAT.ini entspricht nicht der vorherigen Debug-Funktion-Anfrage.
- Die von Dell EMC zur Verfügung gestellte Signatur für die Datei DAT.ini ist nicht gültig.

FSD aufrufen

Stellen Sie sicher, dass die DAT.ini-Datei signiert, von Dell EMC zurückgegeben und in OpenManage Enterprise hochgeladen wurde.

1. Zum Aufrufen einer Debug-Funktion auf dem Bildschirm **FSD-Funktionen** wählen Sie **Aufrufen von FSD-Funktionen**.
2. Wählen Sie auf dem Bildschirm **Aufrufen angefragter Debug-Funktionen** eine Debug-Funktion aus einer Liste mit Debug-Funktionen, die in der von Dell EMC signierten DAT.ini-Datei genehmigt ist. In der rechten unteren Ecke klicken Sie auf **Aufrufen**.

   ANMERKUNG: Die Debug-Funktion, die momentan unterstützt wird, ist `RootShell`.

Während der Befehl `invoke` ausgeführt wird, kann OpenManage Enterprise einen SSH-Daemon starten. Der externe SSH-Client kann mit OpenManage Enterprise für das Debuggen eine Verbindung herstellen.

FSD deaktivieren

Nach dem Aufrufen einer Debug-Funktion auf einer Konsole wird sie so lange ausgeführt, bis die Konsole neu gestartet oder die Debug-Funktion gestoppt wird. Andernfalls wird die aus dem Anfangs- und Enddatum ermittelte Dauer überschritten.

1. Um die Debug-Funktionen zu stoppen, wählen Sie auf dem Bildschirm **FSD-Funktionen** die Option **Debug-Funktionen deaktivieren**.
2. Wählen Sie im Bildschirm **Aufgerufene Debug-Funktionen deaktivieren** aus einer Liste aktuell aufgerufener Debug-Funktionen eine oder mehrere Debug-Funktionen aus. Wählen Sie in der rechten unteren Ecke des Bildschirms **Deaktivieren**.

Stellen Sie sicher, dass Sie alle SSH-Daemon- oder SSH-Sitzungen stoppen, die derzeit die Debug-Funktion nutzen.

Felddefinitionen Katalogverwaltung

KATALOGNAME: Name des Katalogs. Integrierte Kataloge können nicht bearbeitet werden.

DOWNLOAD: Zeigt die Downloadstatus von Katalogen von seinem Repository-Ordner an. Status sind: abgeschlossen, wird ausgeführt und fehlgeschlagen.

REPOSITORY: Repository-Typen wie z. B. Dell.com, CIFS und NFS.

Repository-Speicherort: Speicherort, an dem die Kataloge gespeichert werden. Beispiele sind Dell.com CIFS und NFS. Gibt außerdem den Fertigstellungsstatus für einen laufenden Job an, der auf dem Katalog ausgeführt wird.

KATALOGDATEI: Art der Katalogdatei.

ERSTELLUNGSDATUM: Datum, an dem die Katalogdatei erstellt wurde.

Firmware/Treiber-Compliance-Baseline-Berichte: Geräte mit dem Konformitätsstatus „Unbekannt“

Der Firmware-oder Treiber-Compliance-Status der folgenden Speicher-, Netzwerk- und Hyperkonvergente-Infrastruktur-Geräte (HCI) wird in den Firmware/Treiber-Baseline-Compliance-Berichten als unbekannt angezeigt, da der Dell Firmware-/Treiberkatalog die Firmware- oder Software-Updates für diese Geräte nicht unterstützt.

Tabelle 34. Firmware/Treiber-Compliance-Baseline-Berichte – „falsch“-konforme Geräte

Gerätekategorie	Geräteliste
Speicher	• SC-Serie • MD-Serie • ME-Serie
Netzwerkgeräte im FX2-, VRTX- und M1000e-Gehäuse	• F10-Switches

Tabelle 34. Firmware/Treiber-Compliance-Baseline-Berichte – „falsch"-konforme Geräte (fortgesetzt)

Gerätekategorie	Geräteliste
	• EAAs (Eingabe/Ausgabe-Aggregatoren) • EAMs (Eingabe/Ausgabe-Module)
Hyperkonvergente Appliances (HCI)	• VxRail • XC Serie
Geräte, die über einzelne Dell Update Packages (DUP) aktualisiert werden können, aber nicht direkt vom Dell Katalog unterstützt werden	• MX9116n Fabric Engine • MX5108n Ethernetswitch • PowerEdge MX5000s
Geräte, die nicht mit dem Dell Katalog oder einem einzelnen DUP aktualisiert werden können **ANMERKUNG:** Informationen zum Firmware/Treiber-Update dieser Geräte finden Sie im Installationshandbuch für das jeweilige Gerät.	• MX7116n Fabric Expander Module • PowerEdge MX 25GbE PTM

ANMERKUNG: Eine vollständige Liste der Geräte der Serien SC, MD, ME und XC finden Sie unter https://topics-cdn.dell.com/pdf/dell-openmanage-enterprise_compatibility-matrix2_en-us.pdf

Generische Benennungskonvention für Dell EMC PowerEdge-Server

Um eine Reihe von Servermodellen abzudecken, werden PowerEdge-Server jetzt mithilfe der generischen Benennungskonvention anstelle ihrer Generation benannt.

In diesem Thema wird erläutert, wie Sie die Generation eines PowerEdge-Servers identifizieren, der mithilfe der generischen Benennungskonvention benannt wurde.

Beispiel:

Beim R740-Servermodell handelt es sich um ein Rack-System mit zwei Prozessoren der 14. Generation von Servern mit Intel-Prozessoren. In der Dokumentation wird für R740 die generische Benennungskonvention **YX4X** verwendet. Dabei gilt Folgendes:

- Der Buchstabe **Y** (Alphabet) wird verwendet, um die folgenden Server-Formfaktoren zu kennzeichnen:
  - **C** = Cloud – modulare Server-Nodes für Hyperscale-Umgebungen
  - **F** = Flexibel – hybride Rack-basierte Schlitten für Rack-basierte FX2/FX2s-Gehäuse
  - **M** oder **MX** * = Modular – Blade-Server für die modularen Gehäuse MX7000, M1000e und/oder VRTX
  - **R** = Rack-montierbare Server
  - **T** = Tower-Server
- Der Buchstabe **X** (Ziffer) steht für die Klasse (Anzahl der Prozessoren) des Servers.
- Die Ziffer **4** steht für die Generation des Servers.
- Der Buchstabe **X** (Ziffer) steht für die Bauart des Prozessors.

Tabelle 35. Benennungskonvention für PowerEdge-Server und Beispiele

YX3X-Server	YX4X-Systeme
PowerEdge M630	PowerEdge M640
PowerEdge M830	PowerEdge R440
PowerEdge T130	PowerEdge R540