OpenManage Integration for VMware vCenter Version 5.2

Benutzerhandbuch

October 2020
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

Kapitel 1: Einführung....10
Neues in dieser Version....10
OpenManage Integration for VMware vCenter-Funktionen....10

Kapitel 2: Bei Dell EMC OMIVV-Verwaltungskonsole anmelden....13
Neuen vCenter-Server registrieren....13
Registrieren eines vCenter-Servers mit einem Konto ohne Administratorrechte....14
Erforderliche Berechtigungen für Nicht-Administratornutzer....15
Dell Berechtigungen vorhandener Rolle zuweisen....16
Zertifikate für registrierte vCenter-Server aktualisieren....16
vCenter-Anmeldeinformationen ändern....16
Registrierung von Dell OpenManage Integration for VMware vCenter aufheben....17
Hochladen einer Lizenz auf die OMIVV-Verwaltungskonsole....17
OMIVV-Gerät verwalten....17
Globale Alarme einrichten....25
Informationen zur OMIVV VM-Konsole....26

Kapitel 3: Hosts und Gehäuse über das Dashboard überwachen....36

Kapitel 4: Hosts mit Host-Zugangsdatenprofil verwalten....39
Host-Zugangsdatenprofil....39
Host-Anmeldeinformationenprofil erstellen....39
Zugangsdatenprofil bearbeiten....40
Host-Zugangsdatenprofil anzeigen....42
Host-Zugangsdatenprofil testen....42
Host-Zugangsdatenprofil löschen....43

Kapitel 5: Gehäuse mit Chassis-Zugangsdatenprofil verwalten....44
Gehäuse-Zugangsdatenprofil....44
Gehäuse-Zugangsdatenprofil erstellen....44
Gehäuse-Zugangsdatenprofil bearbeiten....45
Gehäuse-Zugangsdatenprofil anzeigen....46
Gehäuse-Zugangsdatenprofil testen....46
Gehäuse-Zugangsdatenprofil löschen....46

Kapitel 6: Firmware- und Treiber-Repositorys mithilfe des Repository-Profils verwalten....48
Repository-Profil....48
Repository-Profil erstellen....48
Repository-Profil bearbeiten....49
Dell Standardkatalog bearbeiten oder anpassen....50
Validierten MX-Stapel-Katalog bearbeiten....50
Mit Repository-Speicherort synchronisieren....50
Repository-Profil anzeigen....50
Repository-Profil löschen....51

Kapitel 7: Basiskonfiguration mit Clusterprofil erfassen....52
Clusterprofil....52
Clusterprofil erstellen....52
Clusterprofil bearbeiten....53
Clusterprofil anzeigen....53
Clusterprofil aktualisieren....54
Clusterprofil löschen....54

Kapitel 8: Bare-Metal-Server verwalten....55
Bare-Metal-Server anzeigen....55
Geräteerkennung....55
Auto-Ermittlung....56
Voraussetzungen für Auto Discovery (Automatische Ermittlung)....56
Verwaltungskonten auf iDRAC aktivieren und deaktivieren....56
PowerEdge-Server manuell für die automatische Ermittlung konfigurieren....57
Manuelle Ermittlung von Bare-Metal-Servern....57
Bare-Metal-Server entfernen....58
Bare-Metal-Server aktualisieren....59
iDRAC-Lizenz erwerben oder erneuern....59

Kapitel 9: Bereitstellungsprofile verwalten....60
Systemprofil....60
Systemprofil erstellen....60
Systemprofil bearbeiten....62
Systemprofil anzeigen....63
Systemprofil löschen....63
ISO-Profil....63
ISO-Profil erstellen....63
ISO-Profil bearbeiten....63
Ein ISO-Profil anzeigen....64
ISO-Profil löschen....64
Benutzerdefinierte Dell EMC ISO-Images herunterladen....64

Kapitel 10: Bereitstellung eines Systemprofils und ISO-Profils....65
Bereitstellungsprüfliste....66
Systemprofil bereitstellen (Konfiguration der Hardware)....66
ISO-Profil bereitstellen (ESXi Installation)....67
Systemprofil und ISO-Profil bereitstellen....69
VLAN-Support....69
Festlegen der Zeit für den Bereitstellungs-Job....70

Kapitel 11: Konformität....71
Verwaltungs-Compliance....71
Nicht konforme Hosts anzeigen....71
Nicht konformen Host reparieren....72
Konfigurations-Compliance....74
Konfigurations-Compliance anzeigen....74
Abweichungsbericht anzeigen....75

Kapitel 12: OMIVV-Jobs verwalten..... 76
Bereitstellungs-Jobs..... 76
Ermittlungs-Jobs..... 77
Gehäuse-Firmwareupdates-Jobs..... 77
Host-Firmwareupdates-Jobs..... 78
Systemsperrmodus-Jobs..... 78
Abweichungserkennungsjob..... 79
Host-Bestandsaufnahme-Job anzeigen..... 80
Bestandsaufnahme-Job ausführen..... 80
Host-Bestandsaufnahme-Job ändern..... 81
Gehäuse-Bestandsaufnahme-Job anzeigen..... 81
Gehäuse-Bestandsaufnahme-Job ausführen..... 82
Host-Gewährleistung anzeigen..... 82
Host Service-Job ändern..... 82
Gehäuseservice anzeigen..... 83

Kapitel 13: Protokolle verwalten..... 84
Protokollverlauf anzeigen..... 84

Kapitel 14: OMIVV-Geräteeinstellungen verwalten..... 85
Mehrere Geräte verwalten..... 85
Serviceablaufbenachrichtigung einrichten..... 85
Benachrichtigung über aktuelle Geräteversion konfigurieren..... 86
Konfigurieren von Anmeldeinformationen für die Bereitstellung..... 86
Funktionszustand der Hardware-Komponentenredundanz – Proaktive HA..... 86
Proaktive HA-Ereignisse..... 87
Proactive HA für Rack- und Tower-Server konfigurieren..... 88
Proactive HA auf Clustern aktivieren..... 89
Schweregrad der Funktionszustands-Aktualisierungsbenachrichtigung überschreiben..... 90
Erstkonfiguration..... 90
Status der Erstkonfiguration anzeigen..... 91
Einstellungen für die Firmware-Update..... 91
Lizenzinformationen anzeigen..... 91
OpenManage Integration for VMware vCenter-Lizenzierung (OMIVV)..... 92
Eine Softwarelizenz erwerben..... 93
Auf Support-Informationen zugreifen..... 93
Fehlerbehebungsbundle erstellen und herunterladen..... 93
iDRAC zurücksetzen..... 94

Kapitel 15: vCenter-Einstellungen verwalten..... 95
Informationen zu Ereignissen und Alarmen..... 95
Konfigurieren von Ereignissen und Alarmen..... 96
Gehäuseereignisse anzeigen..... 96
Gehäusealarme anzeigen..... 96
Alarm- und Ereigniseinstellungen anzeigen..... 97
Ereignisse im Zusammenhang mit der Virtualisierung..... 97
Verwaltung der Zeitpläne für Datenabruf..... 108
Einen Bestandsaufnahme-Job planen..... 108

Serviceabfrage-Jobs planen ... 109

Kapitel 16: Gehäuseverwaltung ... 110
Dell EMC Gehäuseinformationen anzeigen ... 110
Gehäuse-Bestandsinformationen anzeigen ... 110
Anzeigen von Informationen zur Hardware-Bestandsliste für Gehäuse ... 111
Firmwarebestandsinformationen anzeigen ... 113
Management Controller-Informationen anzeigen ... 113
Bestandsinformationen anzeigen ... 114
Serviceinformationen anzeigen ... 115
Zugeordneten Host für Gehäuse anzeigen ... 116
Zugehörige Gehäuseinformationen anzeigen ... 116
PowerEdge MX Gehäuse verwalten ... 116
Gehäuse- und Host-Management mithilfe der einheitlichen Gehäuse-Management-IP ... 117
PowerEdge MX Gehäuse hinzufügen ... 117
MX-Gehäuse-Firmwareaktualisierung ... 118

Kapitel 17: Hostverwaltung ... 120
OMIVV-Hosts anzeigen ... 120
Einen einzelnen Host überwachen ... 120
Anzeigen der Hostzusammenfassungsinformationen ... 120
OMIVV Hostinformationen anzeigen ... 122
Hosts auf Clustern und in Rechenzentren überwachen ... 127
Firmware-Aktualisierung ... 133
Firmware und Treiber auf vSAN-Host aktualisieren ... 134
Firmware und Treiber auf vSAN-Cluster aktualisieren ... 136
Firmware auf vSphere-Host aktualisieren ... 139
Firmware auf vSphere-Cluster aktualisieren ... 140
Firmware-Komponenten des gleichen Typs aktualisieren ... 142
Überblick über vSphere Lifecycle Manager ... 143
Anzeigen des Status von vSphere Lifecycle Manager in Dell EMC-Verwaltungskonsole ... 143
Registrieren von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole ... 144
Aufheben der Registrierung von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole ... 144
Verwalten von Clustern mithilfe von vSphere Lifecycle Manager ... 144
Verwenden von OMIVV als Firmware-Add-on-Anbieter in vSphere LifeCycle Manager – Benutzeroberfläche ... 144
Anzeigen des Konformitätsstatus ... 145
Beheben von Konformitätsproblemen im Cluster ... 145
Hardware-Kompatibilitätsprüfung ... 146
Durchführen einer Korrektur-Vorabprüfung ... 146
Korrigieren eines Clusters in vSphere Lifecycle Manager ... 146
Verwenden von OMIVV als Firmware-Add-on-Anbieter in vSphere Lifecycle Manager – vSphere Automation APIs ... 147
Blinkanzeigelicht einrichten ... 150
Systemsperrmodus konfigurieren ... 151

Kapitel 18: Sicherheitsrollen und Berechtigungen ... 152
Datenintegrität ... 152
Zugriffskontrollauthentifizierung, -autorisierung und -rollen ... 152
Dell Vorgangsrolle ... 152

Dell Infrastrukturbereitstellungsrolle....153
Informationen zu Berechtigungen....153

Kapitel 19: Häufig gestellte Fragen – FAQs....155
Häufig gestellte Fragen – FAQs....155
iDRAC-Lizenztyp und -Beschreibung werden für nicht konforme vSphere Hosts falsch angezeigt....155
Dell Anbieter wird nicht als Anbieter für Funktionszustandsaktualisierung angezeigt....155
Aufgrund einer ungültigen oder unbekannten iDRAC-IP-Adresse ist die Host-Bestandsaufnahme oder Testverbindung fehlgeschlagen....156
Bei der Ausführung eines Fix-Assistenten für nicht konforme vSphere Hosts wird der Status eines spezifischen Hosts als „Unknown“ angezeigt....156
Dell Berechtigungen, die beim Registrieren des OMIVV-Geräts zugewiesen wurden, werden nach dem Aufheben der Registrierung von OMIVV nicht entfernt....156
Wie behebe ich den Fehlercode 2000000, der von der VMware Zertifizierungsstelle – VMCA – verursacht wird?....156
In der Verwaltungskonsole ist nach dem Zurücksetzen des Geräts auf die werksseitigen Einstellungen Aktualisierungs-Repository-Pfad nicht auf den Standard-Pfad eingestellt....157
Was soll ich tun, wenn ein Web-Kommunikationsfehler im vCenter HTML-5-Client nach dem Ändern der DNS-Einstellungen in OMIVV angezeigt wird?....157
Das Installationsdatum wird für einige Firmware-Versionen auf der Firmware-Seite als 31.12.1969 angezeigt....157
Warum wird das OpenManage Integration Symbol im HTML-5 Client nicht angezeigt, selbst wenn die Registrierung des Plug-ins im vCenter erfolgreich war?....158
Warum werden DNS-Konfigurationseinstellungen nach dem Neustart des Geräts auf die ursprünglichen Einstellungen zurückgesetzt, wenn die IP- und DNS-Einstellungen des Geräts mit DHCP-Werten überschrieben werden?....158
Wenn die Firmwareaktualisierung ausgeführt wird, wird möglicherweise die Fehlermeldung angezeigt, dass die Firmware-Repository-Datei nicht vorhanden oder ungültig ist....158
Die Verwendung von OMIVV zum Aktualisieren einer Intel-Netzwerkkarte mit der Firmwareversion 13.5.2 wird nicht unterstützt....158
Die Verwendung von OMIVV zum Aktualisieren einer Intel Netzwerkkarte von 14.5 oder 15.0 auf 16.x schlägt aufgrund der Bereitstellungsanforderung von DUP fehl....159
Warum zeigt das Administrationsportal einen nicht erreichbaren Aktualisierungs-Repository-Speicherort an?....159
Warum wechselt das System bei der Durchführung einer 1:n-Firmware-Aktualisierung nicht in den Servicemodus?....159
Die globale Gehäuse-Integrität ist immer noch funktionsfähig, obwohl sich einige der Netzteil-Status zu kritisch geändert haben....159
Die Prozessor-Version wird auf der Seite „System-Überblick“ als „Nicht verfügbar“ angezeigt....159
Unterstützt OMIVV vCenter im verknüpften Modus?....159
Erforderliche Porteinstellungen für OMIVV....159
Das Passwort für den Benutzer, der für die Bare-Metal-Erkennung verwendet wird, wird nach der erfolgreichen Anwendung des Systemprofils nicht geändert, das über den gleichen Benutzer mit neuen geänderten Anmeldeinformationen in der iDRAC-Benutzerliste verfügt....161
Die auf der Seite vCenter Hosts und Clusters aufgelisteten neuen iDRAC-Versionsdetails können nicht angezeigt werden....161
Unterstützt OMIVV ESXi mit aktiviertem Sperrmodus?....161
Beim Verwenden des Sperrmodus tritt ein Fehler auf....162
Versuch schlägt fehl, ESXi bei einem Serverausfall bereitzustellen....162
Automatisch ermittelte Systeme werden ohne Modellinformationen im Bereitstellungsassistenten angezeigt....162
Die NFS-Freigabe wurde mit dem ESXi-ISO-Image eingerichtet, die Bereitstellung schlägt jedoch mit Fehlern beim Laden des Freigabeortes fehl....162

So wird ein OMIVV-Gerät zwangsweise aus dem vCenter entfernt... 162
Beim Eingeben eines Kennworts im Bildschirm „Jetzt sichern“ wird eine Fehlermeldung angezeigt... 163
Was mache ich, wenn eine Aktualisierung fehlschlägt?... 163
Was kann ich tun, wenn die vCenter Registrierung fehlgeschlagen ist?... 163
Die Leistung ist während des Tests der Anmeldeinformationen im Host-Anmeldeprofil langsam oder die Anwendung reagiert nicht... 163
Unterstützt OMIVV die VMware vCenter Server Appliance?... 164
Ein Server kann als nicht konform mit dem CSIOR-Status „unbekannt“ angezeigt werden... 164
Der Firmware-Level wird nicht aktualisiert, obwohl ich eine Firmware-Aktualisierung mit der Option „Beim nächsten Neustart anwenden“ ausgeführt und das System neu gestartet habe... 164
Der Host wird auch nach dem Entfernen des Hosts aus der vCenter Struktur weiterhin unter dem Gehäuse angezeigt... 164
Nach der Sicherung und Wiederherstellung von OMIVV wurden die Alarmeinstellungen nicht wiederhergestellt... 164
Die BS-Bereitstellung schlägt fehl, wenn NPAR auf einem Zielknoten aktiviert und im Systemprofil deaktiviert ist... 164
Die verfügbare OMIVV-Geräteversion zeigt falsche Informationen an, wenn die verfügbare Version niedriger ist als die aktuelle Version... 165
Ausnahme 267027 wird beim Hinzufügen eines Bare-Metal-Servers der 12. Generation und höher ausgelöst... 165
Während der Bereitstellung schlägt das Anwenden des Systemprofils aufgrund eines iDRAC-Fehlers fehl... 165
OMIVV RPM-Upgrade schlägt fehl, wenn Proxy mit Domain-Benutzerauthentifizierung konfiguriert ist... 165
Ein Systemprofil kann nicht angewendet werden, das eine PCIe-Erweiterungskarte im FX-Gehäuse hat... 165
Die Abweichungserkennung zeigt nicht kompatible modulare Server an, die im FX-Gehäuse über eine PCIe-Karte verfügen... 165
Auf PowerEdge-Servern kann kein Betriebssystem bereitgestellt werden, wenn iDRAC die MAC-Adresse des ausgewählten NIC nicht anzeigt... 166
Beim Erstellen eines neuen Host-Anmeldeinformationenprofils für den Host mit ESXi 6.5U1 wird die Service-Tag-Nummer des Hosts nicht auf der Seite der ausgewählten Hosts angezeigt... 166
Das Dell EMC Symbol wird nach der Sicherung und Wiederherstellung einer früheren zu einer späteren OMIVV-Version nicht angezeigt... 166
Beim Aktualisieren oder Zurückstufen einiger iDRAC-Firmwareversionen über OMIVV meldet OMIVV möglicherweise, dass der Auftrag fehlgeschlagen ist, obwohl die Firmwareaktualisierung erfolgreich durchgeführt wurde... 166
Beim Konfigurieren des Systems im Sperrmodus auf Cluster-Ebene wird gelegentlich die Meldung „Kein Host unter dem Cluster verfügt über eine erfolgreiche Bestandsaufnahme“ angezeigt... 167
Manchmal werden bei der nachträglichen RPM-Aktualisierung des OMIVV-Geräts mehrere Einträge in den letzten Aufgaben des vCenter angezeigt... 167
Nach der Registrierung von vCenter wird das Dell EMC Logo von OMIVV nicht auf der Startseite von VMware angezeigt... 167
Nicht konforme 11G-PowerEdge-Server werden im OMIVV-Bestand nach der Sicherung und Wiederherstellung beibehalten... 167
VCenter kann nach dem Upgrade des OMIVV-Geräts vom Flex-Client nicht gestartet werden... 168
Beim Hinzufügen oder Entfernen von Netzwerkadaptern zu OMIVV verschwinden die vorhandenen NIC von der OMIVV-Konsole... 168
Nach dem Hinzufügen oder Entfernen des zweiten NIC werden auf der Seite „Netzwerkkonfiguration“ drei NIC angezeigt... 168
Ein Server mit unbekanntem Status in der älteren Version ist auf der Bare-Metal-Server-Seite nach der Sicherung und Wiederherstellung auf eine neueste OMIVV-Version nicht aufgeführt... 169
Nach der BS-Bereitstellung konnte OMIVV ESXi-Host nicht zu vCenter hinzufügen oder ein Host-Profil konnte nicht hinzugefügt werden oder der Wartungsmodus für den Host ist fehlgeschlagen... 169
Der iDRAC-Lizenzstatus wird auf der Seite „Verwaltungs-Compliance“ als konform angezeigt, wenn die IP-Adresse des iDRAC nicht erreichbar ist... 169

ESXi-Host ist nach erfolgreicher BS-Bereitstellung unter Verwendung von OMIVV entweder getrennt oder antwortet nicht ... 169
Zeitüberschreitung bei der Bereitstellung, wenn die Netzwerkschnittstellenkarte (NIC) von OMIVV nicht mit dem ESXi-Host-Netzwerk verbunden ist ... 169
Service-Job für bestimmte Hosts wird nicht ausgeführt ... 170
Die proaktive HA-Initialisierung erfolgt nach der Durchführung von Sicherungen und Wiederherstellungen nicht ... 170
OMIVV-Seite zeigt ungültige Sitzung oder Zeitüberschreitungs-Ausnahmefehler oder 2-Millionen-Fehler im Firefox-Browser an ... 170
In vCenter wird im Bereich „Letzte Tasks“ die Spalte „Details“ für einige OMIVV-Task-Benachrichtigungen nicht angezeigt ... 170
Bei Verwendung vCenter 6.5 U2 kann der Fehler 2000002 auf allen Seiten von OMIVV angezeigt werden ... 170
Der Fehler 2000002 wird auf allen Seiten von OMIVV nach der Durchführung von RPM-Aktualisierungen oder -Sicherungen und -Wiederherstellungen von einer früheren OMIVV-Version auf eine neuere OMIVV-Version angezeigt ... 170
Manchmal nimmt die Aufhebung der Registrierung des vCenter von OMIVV viel Zeit in Anspruch ... 171
Nach der Aktualisierung des OMIVV-Zertifikats wird die Fehlermeldung „Verbindung zur OMIVV-Appliance fehlgeschlagen. Das SSL-Zertifikat ist ungültig.“ angezeigt ... 171
Bereitstellungs-Job schlägt in OMIVV fehl ... 171
Testverbindung und Bestandsaufnahme in OMIVV nach der Änderung des vCenter-Kennworts fehlgeschlagen ... 171
Die OMIVV-Instanz wird nach dem Zurücksetzen der OMIVV-Appliance auf die Werkseinstellungen nicht aus vCenter entfernt ... 172
OMIVV zeigt nur BIOS- und iDRAC-Attribute auf der Seite für Profileinstellungen des Systemprofils an ... 172
Die BS-Bereitstellung wurde mit unbekanntem Fehler abgeschlossen ... 172
Chassis Management Controller (CMC)-Firmware-Updates schlägt im FX2-Gehäuse fehl ... 172
Die Bereitstellung des ISO-Profils schlägt in OMIVV fehl ... 172
Probleme bei der Bare-Metal-Bereitstellung ... 172
Aktivieren der automatischen Ermittlung auf einem neu erworbenen System ... 173

Anhang A: Systemspezifische Attribute ... 174

Anhang B: Weitere Informationen ... 178

Anhang C: Anpassungsattribute ... 179

Anhang D: Vergleich von Komponenten- und Baseline-Version - Matrix ... 180

Anhang E: Antwortcodes ... 182

1

Einführung

IT-Administratoren verwenden VMware vCenter als primäre Konsole zur Verwaltung und Überwachung von VMware vSphere-ESX/ESXi-Hosts. Mit OpenManage Integration for VMware vCenter (OMIVV) können Sie die Komplexität bei der Verwaltung Ihres Rechenzentrums reduzieren, indem Sie die Tasks rund um die Verwaltung und Überwachung der Dell EMC Serverinfrastruktur in der vSphere-Umgebung rationalisieren.

Neues in dieser Version

Diese Version von OpenManage Integration for VMware vCenter 5.2 bietet die folgenden Funktionen:

- Einführung von OMIVV RESTful APIs

  Weitere Informationen finden Sie im *API-Handbuch von OpenManage Integration for VMware vCenter Version 5.2* unter **https://www.dell.com/support/**.
- Unterstützung für vSphere 7.0 UI
- Unterstützung für XE2420-basierte PowerEdge-Server
- Unterstützung für IPv4 bereichsbasierte Bare-Metal-Ermittlung
- Sicherheitsverbesserung
- Hinzugefügte Filteroption auf den Seiten **Dell EMC Gehäuse** und **Dell EMC Hosts** zum Filtern von Hosts und Gehäusen basierend auf dem Funktionszustand
- Erweiterung des Service-Reporting für Hosts mit mehreren oder unterschiedlichen Garantien.

OpenManage Integration for VMware vCenter-Funktionen

Im Folgenden werden die Funktionen des OpenManage Integration for VMware vCenter (OMIVV) Geräts genannt:

Tabelle 1. OMIVV-Funktionen

Funktionen	Beschreibung
Bestandsaufnahme	Die Bestandsaufnahmefunktion bietet Folgendes: PowerEdge-Serverdetails wie Speicher – Menge und Typ, NIC, PSU, Prozessoren und Remote Access Controller (RAC) Serviceinformationen auf Server-, Cluster-und Rechenzentrumsebene Gehäusedetails, z. B. Informationen zum Gehäuse-Verwaltungscontroller (CMC) oder Managementmodul, Gehäusenetzteil, KVM-Status, Lüfter-/Wärmeinformationen, Serviceinformationen, Informationen zu Switches/Server oder Speicher. Unterstützung für eine MX-Gehäuse-Beziehung in der MCM-(Multi-Chassis-Management-) Konfiguration. Fabric-Informationen zu einer MCM-Konfiguration für ein MX-Gehäuse QuickSync-Hardwareinformationen für ein MX-Gehäuse
Überwachen und Senden von Warnungen	Die Überwachung und die Warnmeldungen umfassen folgende Funktionalitäten:

Tabelle 1. OMIVV-Funktionen (fortgesetzt)

Funktionen	Beschreibung
	Erkennen wichtiger Hardware-Fehler und Durchführen virtualisierungsbezogener Maßnahmen. Zum Beispiel das Migrieren von Arbeitslasten oder das Versetzen von Hosts in den Wartungsmodus. Bereitstellung von zusätzlichen Informationen wie z. B. zum Bestand, zu Ereignissen und zu Alarmen zur Diagnose von Server- und Gehäuseproblemen. Unterstützung für die Funktion VMware HA Proactive.
Firmware-Updates	Die clusterfähige Server-Firmwareaktualisierung umfasst Folgendes: Aktualisieren der unterstützten Server auf die aktuellste Version des BIOS und der Firmware Sie können OMIVV auch mit vSphere Lifecycle Manager verwenden, um das Firmware-Update durchzuführen (gilt für vCenter 7.0 und höher).
Abweichungserkennung für Cluster	Firmware-Compliance für Cluster Treiber-Compliance für vSAN-Cluster Hardware-Konformität **ANMERKUNG:** Hardware-Konformität wird nicht für Hosts unterstützt, die über das Gehäuse-Anmeldeinformationenprofil verwaltet werden.
Treiberaktualisierungen	Treiberaktualisierungen für vSAN-Cluster
Bereitstellung	Die Bereitstellung umfasst Folgendes: Erstellen und Bereitstellen von Systemprofilen. Remote-Bereitstellung eines Betriebssystems auf Bare-Metal-Servern mithilfe von VMware vCenter ohne Verwendung von PXE.
Service-Informationen	Abrufen von Serviceinformationen für Dell EMC Server und deren Gehäuse aus der Dell Servicedatenbank und Ermöglichen einer einfachen Online-Serviceaktualisierung.
Sicherheitsrollen und Berechtigungen	Sicherheitsrollen und Berechtigungen umfassen die folgenden Funktionen: Integration mit Standardauthentifizierung, -rollen und -berechtigungen von vCenter. Unterstützung für iDRAC-Sperrmodus auf iDRAC9-basierten Servern. Eine Liste der iDRAC9-basierten Server finden Sie in der Compliance-Matrix.
Support für OEM-Server	Die folgenden OMIVV-Funktionen werden unterstützt: Bestandsaufnahme Überwachen und Senden von Warnungen Firmware-Updates Bereitstellung Service-Informationen

Tabelle 1. OMIVV-Funktionen (fortgesetzt)

Funktionen	Beschreibung
	Sicherheitsrollen und Berechtigungen
MX-Gehäuse-Firmwareaktualisierung	Bietet eine Option zum Aktualisieren der Managementmodul-Firmware für MX-Gehäuse.

ANMERKUNG: Ab OMIVV 5.0 wird nur der VMware vSphere Client (HTML-5) unterstützt und der vSphere Web Client (FLEX) wird nicht unterstützt.

2

Bei Dell EMC OMIVV-Verwaltungskonsole anmelden

Sie können OpenManage Integration für VMware vCenter und seine virtuelle Umgebung über eines der beiden unten genannten Administrationsportale verwalten:

- Webbasierte Administration Console
- Konsolenansicht für einen individuellen Server – die Konsole der virtuellen Maschine des OMIVV-Geräts

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.

   Die Dauer der Kontosperrung beträgt eine Minute.

   Sie können keine neue Sitzung starten, wenn das Konto gesperrt ist. Allerdings ist eine alte aktive Sitzung weiterhin aktiv.
2. Geben Sie das Kennwort ein.

   Die Eingabe eines ungültigen Kennworts führt zu einem erfolglosen Anmeldeversuch. Sechs aufeinanderfolgende fehlgeschlagene Anmeldeversuche führen zu einer Kontosperrung. Zu den sechs erfolglosen Anmeldeversuchen gehören fehlgeschlagene Anmeldeversuche in der Administrationskonsole oder REST-API oder die Verwendung eines ungültigen Tokens für den REST-API-Zugriff.

   Die Dauer der Kontosperrung beträgt eine Minute.

   Sie können während der Kontosperrdauer keine Sitzung erstellen, aber eine aktuell aktive Sitzung bleibt aktiv.

   Wenn Sie sich zum ersten Mal anmelden, werden Sie aufgefordert, die EULA zu akzeptieren.
3. Lesen Sie auf der Seite **Dell EMC Endnutzer-Lizenzvereinbarung** die allgemeinen Geschäftsbedingungen, und markieren Sie dann das Kontrollkästchen **Ich akzeptiere die Bedingungen der Lizenzvereinbarung**.

   Weitere Informationen zu den Telemetrie-EULA erhalten Sie, indem Sie auf **Dell EMC Telemetrie-EULA** klicken.
4. Klicken Sie auf **Akzeptieren**.

Neuen vCenter-Server registrieren

Ihr vCenter-Konto sollte über die erforderlichen Berechtigungen zum Erstellen eines Nutzers verfügen. Weitere Informationen über die erforderlichen Berechtigungen finden Sie unter Erforderliche Berechtigungen für Nicht-Administratornutzer auf Seite 15.

Sie können das OMIVV-Gerät nach der Installation des OMIVV registrieren. Die OMIVV verwendet ein Administrator- oder anderes Nutzerkonto mit den erforderlichen Berechtigungen für vCenter Operations. Eine einzelne OMIVV-Geräteinstanz unterstützt bis zu 15 vCenter-Server und bis zu 2.000 ESXi-Hosts.

Wenn Sie versuchen, mehr als 15 vCenter zu registrieren, wird die folgende Fehlermeldung angezeigt:

Ihre Lizenz erlaubt nur <x> vCenter und es sind bereits alle registriert.

Führen Sie folgende Schritte durch, um den neuen vCenter-Server zu registrieren:

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.
2. Klicken Sie auf der Seite **VCENTER-REGISTRIERUNG** im rechten Fensterbereich auf **Neuen vCenter-Server registrieren**. Die Seite **NEUES vCENTER REGISTRIEREN** wird angezeigt.
3. Führen Sie im Dialogfeld **NEUES VCENTER REGISTRIEREN** unter **vCenter-Name** die folgenden Schritte aus:
   a. Geben Sie die vCenter-IP-Adresse oder den FQDN des Hosts in das Feld **vCenter-Server-IP-Adresse oder Hostname** ein.

      Dell EMC empfiehlt, OMIVV beim VMware vCenter unter Verwendung eines FQDN (Fully Qualified Domain Name) zu registrieren. In allen Registrierungen muss der Hostname von vCenter vom DNS-Server korrekt auflösbar sein. Für DNS-Server werden die folgenden Vorgehensweisen empfohlen:

      - Weisen Sie eine statische IP-Adresse und einen Hostnamen zu, wenn Sie ein OMIVV-Gerät mit einer gültigen DNS-Registrierung bereitstellen. Bei einer statischen IP-Adresse ist sichergestellt, dass die IP-Adresse des OMIVV-Geräts beim Neustart des Systems gleich bleibt.

- Stellen Sie sicher, dass die OMIVV-Hostnamen-Informationen in der Vorwärts- und Rückwärtssuche Ihres DNS-Servers vorhanden sind.

b. Geben Sie im Feld **Beschreibung** eine Beschreibung ein – optional.

4. Unter **vCenter Nutzerkonto** führen Sie die folgenden Schritte aus:
   a. Geben Sie im Feld **vCenter Nutzername** den Nutzernamen des Administrators oder eines Nicht-Administrator-Benutzers mit entsprechenden Berechtigungen an.
   b. Geben Sie das Kennwort in das Feld **Kennwort** ein.
   c. Geben Sie das Kennwort zur Bestätigung in das Feld **Kennwort bestätigen** ein.
   d. Aktivieren Sie das Kontrollkästchen **vSphere Lifecycle Manager registrieren** .

      Wenn Sie das Kontrollkästchen **vSphere Lifecycle Manager registrieren** aktivieren, können Sie die vSphere Lifecycle Manager-Funktion ab vCenter 7.0 aufwärts verwenden.
5. Klicken Sie auf **Registrieren**.

   Die folgende Fehlermeldung wird angezeigt, wenn die vCenter-Registrierung fehlschlägt:

   Es konnte keine Verbindung mit dem angegebenen vCenter-Server <x> aufgrund falscher Zugangsdaten erfolgen. Überprüfen Sie den Nutzernamen und das Kennwort.

Nach der Registrierung des vCenter-Servers wird OMIVV als vCenter-Plug-in registriert und das Symbol „Dell EMC OpenManage Integration“ wird im vSphere-Client angezeigt, über den Sie die OMIVV-Funktionen aufrufen können.

ANMERKUNG: Für alle vCenter-Vorgänge von der OMIVV-Appliance verwendet OMIVV die Berechtigungen des registrierten Nutzers und nicht die Berechtigungen des bei VMware vCenter angemeldeten Nutzers oder der lokalen Konten der OMIVV-Appliance.

Nutzer X verfügt über die nötigen Berechtigungen und registriert OMIVV im vCenter. Nutzer Y verfügt nur über die Dell Berechtigungen. Nutzer Y kann sich nun bei VCenter anmelden und ein Firmwareupdate von OMIVV auslösen. Während die Aktualisierung durchgeführt wird, nutzt OMIVV die Berechtigungen von Nutzer X, um das Gerät in den Wartungsmodus zu setzten oder den Host neu zu starten.

ANMERKUNG: Wenn Sie ein benutzerdefiniertes, von einer Zertifizierungsstelle signiertes Zertifikat in OMIVV hochladen möchten, stellen Sie sicher, dass Sie das neue Zertifikat vor der vCenter-Registrierung hochladen. Wenn Sie das neue benutzerdefinierte Zertifikat nach der vCenter-Registrierung hochladen, werden im vSphere Client Kommunikationsfehler angezeigt. Um dieses Problem zu beheben, müssen Sie die Registrierung von vCenter rückgängig machen und sich erneut registrieren.

Registrieren eines vCenter-Servers mit einem Konto ohne Administratorrechte

Sie können vCenter Server für das OMIVV Gerät mit vCenter Administrator-Anmeldeinformationen oder mit einem Nicht-Administrator-Nutzer mit den Dell Berechtigungen registrieren.

Um einen Nicht-Administrator-Nutzer mit den erforderlichen Berechtigungen für die Registrierung eines vCenter Servers auszustatten, führen Sie folgende Schritte durch:

1. Erstellen Sie eine Rolle oder ändern Sie eine vorhandene Rolle mit den erforderlichen Berechtigungen für die Rolle.

   Weitere Informationen über die Liste der Berechtigungen, die für die Rolle erforderlich sind, erhalten Sie unter Erforderliche Berechtigungen für Nicht-Administrator-Nutzer.

   Die erforderlichen Schritte zum Erstellen oder Ändern einer Rolle und zum Auswählen von Berechtigungen im vSphere Client (HTML-5) finden Sie in der Dokumentation zu VMware vSphere.
2. Weisen Sie einen Nutzer zu der neu erstellten Rolle zu, nachdem Sie eine Rolle definiert und Berechtigungen für die Rolle ausgewählt haben.

   Weitere Informationen zum Zuweisen einer Rolle zu Berechtigungen finden Sie in der Dokumentation zu VMware vSphere.

   Ein Nicht-Administrator-Nutzer von vCenter Server mit den erforderlichen Berechtigungen kann jetzt vCenter registrieren und/oder die Registrierung aufheben, Anmeldeinformationen ändern oder das Zertifikat aktualisieren.
3. Registrieren Sie einen vCenter Server mit einem Nicht-Administrator-Nutzer mit den erforderlichen Berechtigungen.
4. Weisen Sie nach Abschluss der Registrierung der in Schritt 1 erstellten oder bearbeiteten Rolle Dell Berechtigungen zu. Informationen dazu finden Sie unter Dell Berechtigungen vorhandener Rolle zuweisen auf Seite 16.

Jetzt können Nicht-Administrator-Nutzer mit den erforderlichen Berechtigungen die OMIVV-Funktionen mit Dell EMC Hosts nutzen.

Erforderliche Berechtigungen für Nicht-Administratornutzer

Zum Registrieren von OMIVV mit vCenter benötigt ein Nicht-Administratornutzer die folgenden Berechtigungen:

Beim Registrieren eines vCenter Servers mit OMIVV durch einen Nicht-Administrator-Nutzer wird eine Meldung angezeigt, wenn die folgenden Berechtigungen nicht zugewiesen wurden.

- Alarme
  - Erstellen von Alarmen
  - Ändern von Alarmen
  - Entfernen von Alarmen
- Erweiterung
  - Registrieren von Erweiterungen
  - Aufheben der Registrierung von Erweiterungen
  - Aktualisieren von Erweiterungen
- Global
  - Abbrechen von Tasks
  - Protokollereignis
  - Einstellungen
- Funktionszustand-Update-Anbieter
  - Registrieren
  - Registrierung aufheben
  - Aktualisierung
- Host
  - CIM
    - CIM-Interaktion
- Host-Konfig.
  - Erweiterte Einstellungen
  - Einstellungen ändern
  - Verbindung
  - Wartung
  - Netzwerkkonfiguration
  - Abfragen von Patches
  - Sicherheitsprofil und Firewall
- Bestandsaufnahme
  - Hinzufügen von Hosts zu einem Cluster
  - Hinzufügen von eigenständigen Hosts
  - Cluster ändern
- Lifecycle Manager: allgemeine Berechtigungen
  - Lesen

  ANMERKUNG: Die allgemeinen Berechtigungen von vSphere Lifecycle Manager gelten nur für vCenter 7.0 und höher.
- Hostprofil
  - Bearbeiten
  - Ansicht
- Berechtigungen
  - Ändern von Berechtigungen
  - Ändern einer Rolle
- Sitzungen
  - Validieren einer Sitzung
- Task
  - Erstellen
  - Aktualisierung

ANMERKUNG: Wenn ein vCenter-Server unter Verwendung eines Nutzers, der kein Administrator ist, registriert wird, um auf OMIVV-Funktionen zuzugreifen, muss der Nutzer, der kein Administrator ist, über Dell Berechtigungen verfügen. Weitere Informationen über das Zuweisen von Dell Berechtigungen finden Sie unter Dell Berechtigungen vorhandener Rolle zuweisen auf Seite 16.

Dell Berechtigungen vorhandener Rolle zuweisen

Wenn auf bestimmte Seiten von OMIVV ohne zugewiesene Dell Berechtigungen des angemeldeten Benutzers zugegriffen wird, wird Fehler 2000000 angezeigt.

Sie können zum Zuweisen der Dell Berechtigungen zur Rolle eine vorhandene Rolle bearbeiten.

1. Melden Sie sich mit Administratorrechten am vSphere Client (HTML-5) an.
2. Erweitern Sie im vSphere Client (HTML-5) **Menü** und klicken Sie auf **Administration → Rollen**.
3. Wählen Sie aus der Dropdownliste **Rollenanbieter** einen vCenter-Server aus.
4. Wählen Sie in der Liste **Rollen Dell Betrieb** aus und klicken Sie dann auf **BERECHTIGUNGEN**.
5. Um die Dell Berechtigungen zuzuweisen, klicken Sie auf das Bearbeitungssymbol [ ].
   Die Seite **Rolle bearbeiten** wird angezeigt.
6. Klicken Sie im linken Bereich auf **Dell**, wählen Sie dann die folgenden Dell Berechtigungen für die ausgewählte Rolle aus und klicken Sie dann auf **WEITER**:
   - Dell.Configuration
   - Dell.Deploy-Provisioning
   - Dell.Inventory
   - Dell.Monitoring
   - Dell.Reporting

   Weitere Informationen über die verfügbaren OMIVV-Rollen in vCenter finden Sie unter Sicherheitsrollen und Berechtigungen im .
7. Bearbeiten Sie den Rollennamen und geben Sie falls erforderlich eine Beschreibung für die ausgewählten Rolle ein.
8. Klicken Sie auf **FERTIGSTELLEN**.
   Melden Sie sich ab und dann über das vCenter an. Der Nutzer mit erforderlichen Berechtigungen kann nun die OMIVV-Vorgänge durchführen.

Zertifikate für registrierte vCenter-Server aktualisieren

Dell OpenManage Integration for VMware vCenter erstellt mithilfe der OpenSSL API das CSR (Certificate Signing Request) mit dem RSA-Verschlüsselungsstandard und einer Schlüssellänge von 2048 Bit.

Das von OMIVV generierte CSR ruft ein digital signiertes Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ab. Mit dem digitalen Zertifikat aktiviert OMIVV auf dem Webserver HTTPS für die sichere Datenübertragung.

Wenn das Zertifikat auf einem vCenter-Server geändert wird, führen Sie die folgenden Schritte durch, um das neue Zertifikat für OMIVV zu importieren:

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.
2. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**.
   Die registrierten vCenter-Server werden im Arbeitsbereich angezeigt.
3. Zum Aktualisieren des Zertifikats für eine vCenter Server-IP-Adresse oder den Hostnamen klicken Sie auf **Aktualisierung**.

vCenter-Anmeldeinformationen ändern

Sie können die vCenter Anmeldeinformationen mit Administratorrechten oder einem Nicht-Administrator-Nutzer mit den erforderlichen Berechtigungen ändern.

Wenn eine proaktive Hochverfügbarkeitsfunktion für einen Cluster aktiviert ist, dürfen Sie den ihr zugeordneten Nutzer nicht ändern. Das Ändern der Registrierung mit einem anderen vCenter-Nutzer führt zum Verlust der proaktiven Hochverfügbarkeitsfunktionalität. Wenn die Anmeldeinformationen geändert werden müssen, heben Sie die Registrierung der alten Anmeldeinformationen auf und registrieren Sie sich mit den neuen Anmeldeinformationen.

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.

2. Geben Sie im Dialogfeld **Anmeldung** das Kennwort ein und klicken Sie dann auf **Anmeldung**.
3. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**.
   Die registrierten vCenter-Server werden im Arbeitsbereich angezeigt.
4. Um das Fenster **Modify USER Acct** unter **Anmeldeinformationen** zu öffnen, klicken Sie für ein registriertes vCenter auf **Ändern**.
5. Wenn falsche Anmeldeinformationen eingegeben werden, wird eine Meldung angezeigt. Geben Sie den gültigen vCenter-Nutzernamen und das Kennwort ein. Geben Sie das Kennwort zur Bestätigung dann erneut ein.
6. Um das Kennwort zu ändern, klicken Sie auf **Anwenden**. Um eine Aktualisierung abzubrechen, klicken Sie auf **Abbrechen**.

Registrierung von Dell OpenManage Integration for VMware vCenter aufheben

Stellen Sie sicher, dass Sie die Registrierung der OMIVV vom vCenter-Server nicht aufheben, wenn ein Job für die Bestandsaufnahme-/Serviceliste oder ein Bereitstellungsauftrag ausgeführt wird.

Deaktivieren Sie Proaktive HA auf Clustern, falls es aktiviert ist. Greifen Sie zum Deaktivieren der proaktiven HA auf den Bildschirm **Proaktive HA-Ausfälle und Antworten** eines Clusters zu, indem Sie **Konfigurieren** > **Dienste** > **vSphere-Verfügbarkeit** auswählen und dann auf **Bearbeiten**klicken. Um „Proaktive HA“ zu deaktivieren, entfernen Sie im Bildschirm **Proaktive HA-Ausfälle und Antworten** die Markierung aus dem Kontrollkästchen des **Dell Inc** Anbieters.

Um Dell OpenManage Integration for VMware vCenter zu deinstallieren, müssen Sie die Registrierung von OMIVV auf dem vCenter Server unter Verwendung der Administrationskonsole aufheben.

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.
2. Klicken Sie auf der Seite **VCENTER REGISTRIERUNG** in der Tabelle **vCenter Server IP- oder Hostname** auf **Registrierung aufheben**.

   ANMERKUNG: Achten Sie darauf, das richtige vCenter auszuwählen, da OMIVV mehr als einem vCenter zugeordnet sein kann.

3. Klicken Sie zur Bestätigung der Aufhebung der Registrierung auf den ausgewählten vCenter Server auf das Dialogfeld **VCENTER REGISTRIERUNG AUFHEBEN** und anschließend auf **Registrierung aufheben**.

   ANMERKUNG: Nachdem Sie die Registrierung von OMIVV aufgehoben haben, melden Sie sich am vSphere Client (HTML-5) ab und wieder an. Wenn das OMIVV-Symbol weiterhin angezeigt wird, starten Sie die Client Services für vSphere Client (HTML-5) und Web Client (FLEX) neu.

Hochladen einer Lizenz auf die OMIVV-Verwaltungskonsole

Stellen Sie sicher, dass Ihre Lizenzen im Dell Digital Locker unter **https://www.dell.com/support** zum Herunterladen bereit sind. Wenn Sie mehr als eine Lizenz bestellt haben, werden sie möglicherweise separat zu unterschiedlichen Zeitpunkten geliefert. Sie können den Status anderer Lizenzelemente unter „Bestellstatus“ auf **https://www.dell.com/support** prüfen. Die Lizenzdatei steht im .XML-Format zur Verfügung.

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.
2. Geben Sie im **Anmelde**-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**.
   Die registrierten vCenter-Server werden im Arbeitsbereich angezeigt.
4. Klicken Sie auf **Lizenz hochladen**.
5. Klicken Sie im Dialogfeld **LIZENZ HOCHLADEN** auf **Durchsuchen**, um zur Lizenzdatei zu navigieren, und klicken Sie auf **Upload**.

   ANMERKUNG: Wenn Sie die Lizenzdatei ändern oder bearbeiten, funktioniert die Lizenzdatei (XML-Datei) nicht. Sie können die XML-Datei (Lizenzschlüssel) über Dell Digital Locker herunterladen. Wenn Sie einen Lizenzschlüssel nicht herunterladen können, wenden Sie sich an den Dell Support. Die Telefonnummer für das regionale Dell Supportteam für Ihr Produkt finden Sie unter „Technischen Support kontaktieren“ auf **https://www.dell.com/support**.

OMIVV-Gerät verwalten

Das Verwalten des OMIVV-Geräts ermöglicht Ihnen, das Netzwerk, die NTP- und die HTTPS-Informationen für Dell OpenManage Integration for VMware vCenter zu verwalten und ermöglicht einem Administrator, folgende Aktionen auszuführen:

- Starten Sie die OMIVV-Appliance neu, Informationen dazu finden Sie unter Neustarten des OMIVV-Geräts auf Seite 18.
- Das OMIVV-Gerät aktualisieren und einen Speicherort für die Repository-Aktualisierung konfigurieren. Siehe . OMIVV-Appliance und Repository-Speicherort aktualisieren auf Seite 18
- OMIVV-Gerät über RPM aktualisieren. Informationen dazu finden Sie unter OMIVV-Appliance über RPM aktualisieren (mit Internet) auf Seite 19.
- OMIVV-Gerät durch Sichern und Wiederherstellen aktualisieren. Informationen dazu finden Sie unter OMIVV-Gerät durch Sichern und Wiederherstellen aktualisieren auf Seite 20.
- Erstellen und Herunterladen des Fehlerbehebungspakets. Informationen dazu finden Sie unter Erstellen und Herunterladen des Fehlerbehebungsbündels auf Seite 23.
- HTTP-Proxy einrichten. Informationen dazu finden Sie unter HTTP-Proxy einrichten auf Seite 23.
- Network Time Protocol (NTP)-Server einrichten. Informationen dazu finden Sie unter Einrichten von NTP-Servern (Network Time Protocol) auf Seite 23.
- Bereitstellungsmodus konfigurieren. Informationen dazu finden Sie unter Bereitstellungsmodus konfigurieren auf Seite 23.
- Erweiterte Überwachung; siehe Erweiterte Überwachung auf Seite 24.
- Zertifikatsignierungsanforderung (CSR) erstellen. Informationen dazu finden Sie unter Zertifikatsignierungsanforderung (CSR) erstellen auf Seite 25.
- HTTPS-Zertifikat hochladen. Informationen dazu finden Sie unter HTTPS-Zertifikat hochladen auf Seite 25.
- Globale Alarme einrichten. Informationen dazu finden Sie unter Globale Alarme einrichten auf Seite 25.

Auf das Gerätemanagement zugreifen

Führen Sie in OpenManage Integration for VMware vCenter die folgenden Schritte aus, um Zugriff auf die Seite **GERÄTEMANAGEMENT** über das Administration-Portal zu erlangen:

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.
2. Geben Sie im **Anmelde**-Dialogfeld Ihr Kennwort ein.
3. Für die Konfiguration des Geräts klicken Sie im Managementabschnitt im linken Fensterbereich auf **GERÄTEVERWALTUNG**.

Neustarten des OMIVV-Geräts

1. Klicken Sie auf der Seite **GERÄTE-MANAGEMENT** auf **Virtuelles Gerät neu starten**.
2. Klicken Sie zum Neustarten des OMIVV-Geräts im Dialogfeld **Virtuelles Gerät neu starten** auf **Anwenden**.

OMIVV-Appliance und Repository-Speicherort aktualisieren

- Um sicherzustellen, dass alle Daten geschützt sind, führen Sie vor dem Aktualisieren des OMIVVGeräts eine Sicherung der OMIVV-Datenbank aus. Informationen dazu finden Sie unter Backups und Wiederherstellungen verwalten auf Seite 21.
- Das OMIVV-Gerät benötigt eine Internetverbindung, um verfügbare Aktualisierungsmechanismen anzuzeigen und die RPM-Aktualisierung durchzuführen. Stellen Sie sicher, dass das OMIVV-Gerät über eine Internetverbindung verfügt. Wenn Sie ein Proxy-Netzwerk auf Basis der Netzwerk-Umgebungseinstellungen benötigen, aktivieren Sie die Proxy-Einstellungen und geben Sie die Proxydaten ein. Siehe das Thema Einrichten des HTTP-Proxy.
- Stellen Sie sicher, dass **Repository-Pfad aktualisieren** gültig ist.
- Stellen Sie sicher, dass Sie sich von allen vSphere Client (HTML-5)-Sitzungen an den registrierten vCenter-Servern abmelden.
- Stellen Sie vor der Anmeldung an einem registrierten vCenter-Server sicher, dass Sie alle Geräte gleichzeitig unter dem gleichen Platform Service Controller (PSC) aktualisieren. Andernfalls werden möglicherweise inkonsistente Informationen in den OMIVV-Instanzen angezeigt.

1. Im Abschnitt **GERÄTEAKTUALISIERUNG** der Seite **GERÄTEVERWALTUNG** überprüfen Sie die aktuelle und verfügbare OMIVV-Version.

   Für die verfügbare Version des OMIVV-Geräts werden die entsprechenden RPM- und OMIVV-Aktualisierungsmechanismen mit einem Häkchen angezeigt [✔].

   Im Folgenden werden die verfügbaren Optionen des Aktualisierungsmechanismus dargestellt. Sie können eine dieser Optionen für den Aktualisierungsmechanismus durchführen:

Option	Beschreibung
1	Wenn ein Häkchen neben RPM angezeigt wird, können Sie eine RPM-Aktualisierung von der vorhandenen Version auf die neueste verfügbare Version durchführen. Informationen dazu finden Sie unter OMIVV-Appliance über RPM aktualisieren (mit Internet) auf Seite 19.
2	Wenn ein Häkchen neben OVF angezeigt wird, können Sie eine Sicherungskopie der OMIVV-Datenbank von der vorhandenen Version erstellen und die Wiederherstellung in der neuesten verfügbaren Geräteversion ausführen. Informationen dazu finden Sie unter OMIVV-Gerät durch Sichern und Wiederherstellen aktualisieren auf Seite 20.
3	Wenn ein Häkchen neben RPM und OVF angezeigt wird, können Sie eine der genannten Optionen zur Aktualisierung Ihres Geräts ausführen. In diesem Szenario ist die empfohlene Option die RPM-Aktualisierung.

2. Zur Aktualisierung des OMIVV-Geräts führen Sie die genannten Aufgaben für die Upgrade-Mechanismen durch, je nach Version von OMIVV.

OMIVV-Aktualisierungsoptionen

Sichern und Wiederherstellen

Sie können Sicherungen und Wiederherstellungen von OMIVV 5.0 und höher auf die neueste Version durchführen (mit vCenter 6.5 und höher).

RPM-Aktualisierung

Sie können die RPM-Aktualisierung von OMIVV 5.0 auf die neueste Version durchführen.

OMIVV-Appliance über RPM aktualisieren (mit Internet)

Stellen Sie sicher, dass Sie ein Upgrade auf eine Version des Geräts durchführen, die größer als die aktuelle ist.

Es wird empfohlen, einen Snapshot der Appliance zu erstellen, bevor Sie das Upgrade der OMIVV-Appliance durchführen.

1. Aktivieren Sie auf der Seite **GERÄTEMANAGEMENT** die Option „Proxy“ entsprechend Ihren Netzwerkeinstellungen und rufen Sie bei Bedarf die Proxy-Einstellungen auf. Siehe das Thema Einrichten des HTTP-Proxy.

   Für die verfügbare Version des OMIVV-Geräts werden die entsprechenden RPM- und OMIVV-Aktualisierungsmechanismen mit einem Häkchen angezeigt [✔].

2. Zum Aktualisieren des OMIVV-Plug-ins von einer vorhandenen Version auf die verfügbare Version führen Sie einen der folgenden Schritte durch:

   - Für die Aktualisierung unter Verwendung von RPM, das unter **Repository-Pfad aktualisieren** verfügbar ist, stellen Sie sicher, dass **Repository-Pfad aktualisieren** auf folgenden Pfad eingestellt ist: https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/

   Klicken Sie andernfalls im Fenster **Gerätemanagement** im Bereich **Geräteaktualisierung** auf **Bearbeiten**, um den Pfad im Textfeld **Aktualisierungs-Repository-Pfad** in https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ zu ändern, und klicken Sie auf **Übernehmen**.

3. Vergleichen Sie die verfügbare OMIVV-Geräteversion und die aktuelle OMIVV-Geräteversion.
4. Klicken Sie unter **Geräteeinstellungen** auf **Virtuelles Gerät aktualisieren**, um die Aktualisierung des OMIVV-Geräts zu übernehmen.
5. Klicken Sie im Dialogfeld **GERÄTEAKTUALISIERUNG** auf **Aktualisieren**.
   Nachdem Sie auf **Aktualisieren** geklickt haben, werden Sie vom Fenster der **VERWALTUNGSKONSOLE** abgemeldet.
6. Schließen Sie den Internet-Browser.

   Während des Upgrade-Vorgangs wird das Gerät ein- oder zweimal neu gestartet. Nachdem der Geräte-RPM aktualisiert wurde, stellen Sie sicher, dass Sie den Browser-Cache leeren, bevor Sie sich beim Dell Administratorportal anmelden.

   Nach Abschluss der RPM-Aktualisierung wird der Anmeldebildschirm in der OMIVV Konsole angezeigt. Öffnen Sie einen Browser, geben Sie den Link*https:\\<AppliancelP|Hostname>* ein und navigieren Sie zum Bereich **GERÄTEAKTUALISIERUNG**. Prüfen Sie, ob die Versionen der verfügbaren und aktuellen OMIVV-Geräte gleich sind.

Alle Anpassungen, die auf den eingetragenen Dell Alarmen und dem Dell Funktionszustand-Update-Anbieter für PHA-Cluster durchgeführt werden, werden nach dem RPM-Upgrade auf die Standardeinstellung zurückgesetzt.

OMIVV-Gerät über RPM aktualisieren (ohne Internetverbindung)

Erstellen Sie eine HTTP- oder HTTPS-Freigabe. Stellen Sie sicher, dass die HTTP- oder HTTPS-Freigabe Dateinamen unterstützt, die Sonderzeichen wie ++ oder Leerzeichen enthalten.

OMIVV unterstützt nur HTTP- und HTTPS-Freigaben.

OMIVV unterstützt das Upgrade von Version 5.1 auf 5.2, ohne dass eine Internetverbindung besteht.

1. Laden Sie das Paket RPM.zip herunter, das Sie unter **https://www.dell.com/support** finden.
2. Entpacken Sie RPM.zip und kopieren Sie die Dateien und Ordner vom Entpackungsort auf die HTTP- bzw. HTTPS-Freigabe.
3. Klicken Sie auf der Seite **GERÄTEVERWALTUNG** im Bereich **GERÄTEAKTUALISIERUNG** auf **Bearbeiten**und geben Sie den Pfad der Freigabe unter **Repository-Pfad aktualisieren** ein.
4. Klicken Sie auf **Anwenden**.
5. Vergleichen Sie die verfügbare OMIVV-Geräteversion und die aktuelle OMIVV-Geräteversion.
6. Klicken Sie unter **Geräteeinstellungen** auf **Virtuelles Gerät aktualisieren**, um die Aktualisierung des OMIVV-Geräts zu übernehmen.
7. Klicken Sie im Dialogfeld **GERÄTEAKTUALISIERUNG** auf **Aktualisieren**.
   Nachdem Sie auf **Aktualisieren** geklickt haben, werden Sie vom Fenster der **OMIV VERWALTUNGSKONSOLE** abgemeldet.

   Es kann je nach Netzwerkgeschwindigkeit in etwa 40 Minuten dauern, bis die Aktualisierung abgeschlossen ist.
8. Schließen Sie den Internet-Browser.
   Nachdem die Geräteaktualisierung abgeschlossen ist, stellen Sie sicher, dass Sie den Browser-Cache leeren, bevor Sie sich bei der **OMIV VERWALTUNGSKONSOLE** anmelden.

OMIVV-Gerät durch Sichern und Wiederherstellen aktualisieren

Es wird empfohlen, Cluster oder Hosts, die von OMIVV verwaltet werden, nach dem Backup und vor der Wiederherstellung der Backupdatei nicht zu ändern oder zu entfernen. Wenn die von OMIVV verwalteten Cluster oder Hosts geändert oder entfernt werden, konfigurieren Sie nach der Wiederherstellung die Profile (z. B. Host-Anmeldeinformationen-Profil, Clusterprofil), die mit diesen Clustern und Hosts verknüpft sind.

Heben Sie die Registrierung des OMIVV-Plug-ins von vCenter nicht auf. Durch das Aufheben der Registrierung des Plug-ins von vCenter wird der Dell Funktionszustand-Update-Anbieter für proaktive HA-Cluster entfernt, die durch das OMIVV-Plug-in auf vCenter registriert sind.

Es wird empfohlen, einen Snapshot der Appliance zu erstellen, bevor Sie das Upgrade der OMIVV-Appliance durchführen.

Führen Sie die folgenden Schritte aus, um das OMIVV-Gerät von einer älteren Version auf die aktuelle Version zu aktualisieren:

1. Sichern Sie die Daten früherer Versionen.
2. Deaktivieren Sie das ältere OMIVV-Gerät im vCenter.
3. Stellen Sie das neue OpenManage Integration-Gerät OVF bereit.
4. Starten Sie das neue OpenManage Integration-Gerät.
5. Richten Sie das Netzwerk und die Zeitzone für das neue Gerät ein.

   ANMERKUNG: Es wird empfohlen, die Identität (IP oder FQDN) der älteren OMIVV-Appliance für die neue OMIVV-Appliance beizubehalten.
6. Im Lieferumfang des OMIVV-Geräts ist ein Standardzertifikat enthalten. Wenn Sie ein nutzerdefiniertes Zertifikat für Ihr Gerät möchten, aktualisieren Sie dasselbe. Siehe Zertifikatsignierungsanforderung (CSR) erstellen auf Seite 25 und HTTPS-Zertifikat hochladen auf Seite 25. Andernfalls überspringen Sie diesen Schritt.
7. Stellen Sie die Datenbank auf dem neuen OMIVV-Gerät wieder her. Siehe Wiederherstellen der OMIVV-Datenbank aus einem Backup.
8. Überprüfen des Geräts. Weitere Informationen finden Sie unter . das Thema Überprüfen der Installation imInstallationshandbuch
9. Nach dem Upgrade wird empfohlen, die Bestandsaufnahme auf allen Hosts erneut durchzuführen, die das OMIVV-Plug-in verwaltet.

   Die Einstellungen für Ereignisse und Alarme werden nach der Wiederherstellung des Geräts nicht aktiviert. Sie können die Einstellungen für Ereignisse und Alarme über die Registerkarte **Einstellungen** erneut aktivieren.

   Wenn Sie ein Upgrade von einer früheren Version von OMIVV auf die verfügbare Version durchführen, werden alle geplanten Jobs weiterhin ausgeführt.

Alle Anpassungen, die auf den eingetragenen Dell Alarmen und dem Dell Funktionszustand-Update-Anbieter für PHA-Cluster durchgeführt werden, werden nach dem Backup- und Wiederherstellungsvorgang auf die Standardeinstellungen zurückgesetzt.

Nach dem Backup und der Wiederherstellung von einer früheren OMIVV-Version auf eine neuere OMIVV-Version führen Sie die folgenden Aufgaben durch, wenn eines der folgenden Probleme auftritt:

- 200000-Meldung
- Dell EMC Logo fehlt.
- OMIVV-UI reagiert nicht.
- OMIVV-Plug-in wird nicht von vCenter entfernt.
- Das SSL-Zertifikat ist ungültig.

Auflösung:

- Starten Sie die vSphere Client Services für vSphere Client (HTML-5) und vSphere Web Client (FLEX) auf dem vCenter-Server neu.
- Wenn das Problem weiterhin besteht:
  - Navigieren Sie für VMware vCenter-Server-Geräte zu `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`. Rufen Sie für Windows vCenter die folgenden Ordner in der vCenter-Appliance auf und überprüfen Sie, ob die alten Daten der älteren Version vorhanden sind – `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` Ordner in der vCenter-Appliance und überprüfen Sie, ob die alten Daten, wie z. B. com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX vorhanden sind.
  - Löschen Sie den Ordner, der der früheren OMIVV-Version entspricht, manuell und starten Sie die vSphere Client Services für vSphere Client (HTML-5) und Web Client (FLEX) neu.

Wenn die IP-Adresse für die neue Appliance sich von der IP-Adresse der älteren Appliance unterscheidet, führen Sie Folgendes durch:

- Die proaktive Hochverfügbarkeitsfunktion funktioniert möglicherweise nicht ordnungsgemäß. Deaktivieren und aktivieren Sie in einem solchen Fall die proaktive HA für alle Cluster, in denen der Dell EMC Host vorhanden ist.
- Konfigurieren Sie das Trap-Ziel für die SNMP-Traps, sodass es auf die neue Appliance verweist. Die Identitätsänderung wird durch Ausführung der Bestandsaufname auf diesen Hosts korrigiert. Während der Ausführung der Bestandsaufnahme auf Hosts werden diese Hosts, falls die SNMP-Traps nicht auf die neue IP verweisen, als „nicht konform“ aufgelistet. Informationen zur Behebung von Problemen mit der Host-Compliance finden Sie im Abschnitt Nicht konformen Host reparieren auf Seite 72.

Backups und Wiederherstellungen verwalten

Mit der Verwaltungskonsole können Sie Sicherungs- und Wiederherstellungsaufgaben durchführen.

- Backup und Wiederherstellung konfigurieren
- Automatische Backups planen
- Sofortiges Backup durchführen
- Datenbank aus einem Backup wiederherstellen
- Sicherungs- und Wiederherstellungseinstellungen zurücksetzen auf Seite 23

Führen Sie folgende Schritte in OMIVV durch, um die Seite **EINSTELLUNGEN ZU BACKUP UND ZUR WIEDERHERSTELLUNG** über die Verwaltungskonsole aufzurufen:

1. Navigieren Sie zu `https:\\<ApplianceIP|hostname>`.
2. Geben Sie im **Anmelde**-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.

Backup und Wiederherstellung konfigurieren

Die Backup- und Wiederherstellungsfunktion dient zum Sichern der OMIVV-Datenbank an einem Remote-Speicherort (NFS und CIFS), von dem aus sie später wiederhergestellt werden kann. Die Profile, Konfiguration und Host-Informationen sind im Backup enthalten. Wir empfehlen, das Sie zum Schutz gegen Datenverlust automatische Backups planen.

ANMERKUNG: Die NTP-Einstellungen werden nicht gespeichert und wiederhergestellt.

1. Klicken Sie auf der Seite **EINSTELLUNGEN ZUM BACKUP UND ZUR WIEDERHERSTELLUNG** auf **Bearbeiten**.
2. Führen Sie im markierten Bereich **EINSTELLUNGEN UND DETAILS** die folgenden Schritte aus:
   a. Geben Sie in **Sicherungsverzeichnis** den Pfad der Sicherungsdateien an.

b. Geben Sie unter **Nutzername** den Nutzernamen ein.
c. Geben Sie in **Kennwort** das Kennwort ein.
d. Geben Sie das Verschlüsselungskennwort in das Feld **Kennwort für die Verschlüsselung von Backups** ein.
Das Verschlüsselungskennwort darf alphanumerische Zeichen und Sonderzeichen wie „!, @, #, $, % und *“ enthalten.
e. Geben Sie das Verschlüsselungskennwort im Feld **Kennwort bestätigen** erneut ein.
3. Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.
4. Konfigurieren Sie den Backup-Zeitplan. Weitere Informationen finden Sie unter Planen von automatischen Backups

Konfigurieren Sie nach diesem Verfahren einen Backup-Zeitplan.

Automatische Backups planen

Weitere Informationen zum Konfigurieren des Backup-Speicherorts und des Berechtigungsnachweises finden Sie unter Konfigurieren von Backup und Wiederherstellung.

1. Auf der Seite **EINSTELLUNGEN FÜR BACKUP UND WIEDERHERSTELLUNG** klicken Sie auf **Bearbeiten automatisch geplanter Backup**.
Die relevanten Felder sind aktiviert.
2. Klicken Sie auf **Aktiviert**, um Backups zu aktivieren.
3. Aktivieren Sie die Kontrollkästchen **Tage, an denen ein Backup durchgeführt werden soll** für die Tage, an denen eine Backup-Aufgabe durchgeführt werden soll.
4. Geben Sie die Zeit in dem Format SS: MM in **Uhrzeit für Backup (24 Stunden, SS: MM)** ein.
Das Feld **Nächster Backup** wird mit dem Datum und der Uhrzeit für den nächsten geplanten Backup ausgefüllt.
5. Klicken Sie auf **Anwenden**.

Sofortiges Backup durchführen

1. Klicken Sie auf der Seite **EINSTELLUNGEN ZUM BACKUP UND ZUR WIEDERHERSTELLUNG** auf **Jetzt sichern**.
2. Aktivieren Sie im Dialogfeld **JETZT SICHERN** das Kontrollkästchen **Speicherort und Verschlüsselungskennwort aus den Sicherungseinstellungen verwenden**, um den angezeigten Speicherort und das Verschlüsselungskennwort zu verwenden.
3. Geben Sie die Werte für **Sicherungsverzeichnis**, **Nutzername**, **Kennwort** und **Kennwort für Verschlüsselung** ein.
Das Verschlüsselungskennwort darf alphanumerische Zeichen und Sonderzeichen wie „!, @, #, $, % und *“ enthalten. Es gibt keine Längenbeschränkung für ein Passwort.
4. Klicken Sie auf **Sichern**.

OMIVV-Datenbank aus Backup wiederherstellen

Nach der Wiederherstellung von OMIVV von einer früheren Version gilt Folgendes:

- 11G-Server werden nicht unterstützt. Nur 12G-Server oder spätere Generationen bleiben nach der Wiederherstellung erhalten.
- Hardware Profile und Bereitstellungsvorlagen werden nicht unterstützt. Es wird empfohlen, das Systemprofil für die Bereitstellung zu verwenden.
- Bereitstellungsaufgaben, die auf 11G-Servern geplant sind und/oder Hardwareprofil-basierte Bereitstellungsvorlagen verwenden, werden abgebrochen.
- Alle 11G-Server werden aus den Berechtigungsprofilen entfernt und verbrauchte Lizenzen werden freigegeben.
- Repository-Profile verwenden nur 64-Bit-Pakete.
  ANMERKUNG: Wenn Sie Backups und Wiederherstellungen von 4.x auf 5.x durchführen, wird beim Namen des Clusterprofils ein Warnsymbol angezeigt, da OMIVV das 32-Bit-Firmware-Bundle in 5.x nicht unterstützt. Um die neuesten Änderungen für das Clusterprofil zu verwenden, bearbeiten Sie das Clusterprofil.
- Firmwareupdates-Jobs, die auf 11G-Servern geplant sind, werden abgebrochen.

Stellen Sie sicher, dass der richtige Bereitstellungsmodus konfiguriert ist, bevor Sie den Wiederherstellungsvorgang durchführen. Weitere Informationen zur Konfiguration des Bereitstellungsmodus finden Sie unter Bereitstellungsmodus konfigurieren auf Seite 23.

1. Klicken Sie auf der Seite **EINSTELLUNGEN ZUM BACKUP UND ZUR WIEDERHERSTELLUNG** auf **Jetzt wiederherstellen**.
2. Geben Sie im Dialogfeld **JETZT WIEDERHERSTELLEN** einen Pfad für den **Dateispeicherort** zusammen mit der Datei backup .gz im CIFS oder NFS-Format ein.
3. Geben Sie den **Nutzernamen**, das **Kennwort** und das **Verschlüsselungskennwort** für die Backup-Datei ein.
Das Verschlüsselungskennwort darf alphanumerische Zeichen und Sonderzeichen wie „!, @, #, $, % und *“ enthalten.

4. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
   Bei einer Wiederherstellung wird das OMIVV-Gerät nach Abschluss der Wiederherstellung neu gestartet. Informationen zum Überprüfen der Installation finden Sie unter dem Thema Überprüfen der Installation im Installationshandbuch.

   Schließen Sie nach Abschluss der Wiederherstellung den Browser und löschen Sie den Browser-Cache, bevor Sie sich beim Admin-Portal anmelden.

Sicherungs- und Wiederherstellungseinstellungen zurücksetzen

Mithilfe der Funktion zum Zurücksetzen von Einstellungen können Sie Einstellungen auf den unkonfigurierten Status zurücksetzen.

1. Klicken Sie auf der Seite **EINSTELLUNGEN ZUR SICHERUNG UND WIEDERHERSTELLUNG** auf **Einstellungen zurücksetzen**.
2. Klicken Sie im Dialogfeld **Einstellungen zurücksetzen** auf **Anwenden**.

Erstellen und Herunterladen des Fehlerbehebungsbündels

Um das Fehlerbehebungspaket zu erzeugen, stellen Sie sicher, dass Sie sich beim Administratorportal anmelden.

Das Fehlerbehebungspaket enthält Protokollierungsinformationen von OMIVV, die zur Unterstützung bei der Behebung von Problemen verwendet oder an den technischen Support gesendet werden können.

1. Klicken Sie auf der Seite **GERÄTEMANAGEMENT** auf **Fehlerbehebungspaket erstellen**.
2. Klicken Sie auf **Fehlerbehebungspaket herunterladen**.

HTTP-Proxy einrichten

1. Scrollen Sie auf der Seite **GERÄTEVERWALTUNG** bis zu **HTTP-PROXY-EINSTELLUNGEN**, und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie **Aktiviert**, um die Verwendung der HTTP-Proxy-Einstellungen zu aktivieren.
3. Geben Sie die Proxy-Serveradresse in das **Feld Proxy-Serveradresse** ein.
4. Geben Sie den Proxyserver-Port in **Proxyserver-Port** ein.
5. Wählen Sie **Ja** aus, um die Proxy-Anmeldeinformationen zu verwenden.
6. Bei der Verwendung von Proxy-Anmeldeinformationen geben Sie den Nutzernamen in **Nutzername** ein.
7. Geben Sie das Kennwort in **Kennwort** ein.
8. Klicken Sie auf **Anwenden**.

Einrichten von NTP-Servern (Network Time Protocol)

Sie können das NTP zum Synchronisieren der Uhren der OMIVV-Geräte mit der Uhr eines NTP-Servers verwenden.

1. Klicken Sie in der Verwaltungskonsole auf der Seite **GERÄTE-MANAGEMENT** auf **Bearbeiten** im Bereich **NTP-Einstellungen**.
2. Wählen Sie **Aktiviert** aus. Geben Sie den Hostnamen oder die IP-Adresse eines bevorzugten und eines sekundären NTP-Server ein und klicken Sie auf **Anwenden**.
3. Nachdem Sie NTP konfiguriert haben, starten Sie die Terminalkonsole und aktivieren Sie das Kontrollkästchen **Datum und Uhrzeit über das Netzwerk synchronisieren**.

ANMERKUNG: Es kann etwa 10 Minuten dauern, bis die OMIVV-Uhr mit dem NTP-Server synchronisiert ist.

ANMERKUNG: Wenn das OMIVV-Verwaltungsportal eine lange Zeit in Anspruch nimmt, um Informationen zu laden, stellen Sie sicher, dass die NTP-Einstellungen korrekt sind und der NTP-Server über die virtuelle OMIVV-Maschine erreichbar ist.

Bereitstellungsmodus konfigurieren

Stellen Sie für jeden der genannten Bereitstellungsmodi sicher, dass Sie genügend Speicherressourcen für das OMIVV-Gerät zurückstellen, indem Sie Reservierungen verwenden. In der Dokumentation zu vSphere finden Sie die Schritte zum Reservieren von Speicherressourcen.

Stellen Sie sicher, dass die folgenden Systemvoraussetzungen für die erforderlichen Bereitstellungsmodi erfüllt sind, indem Sie diese Ressourcen der virtuellen OMIVV-Maschine zuweisen:

Tabelle 2. Systemanforderungen für Bereitstellungsmodi

Bereitstellungsmodi	Anzahl der Hosts	Anzahl der CPUs	Speicher (GB)	Mindestspeichergröße
Klein	Bis zu 250	2	8	95 GB
Mittel	Bis 500	4	16	95 GB
Groß	Bis zu 1000	8	32	95 GB
Extragroßer Modus	Bis zu 2.000	12	32	95 GB

ANMERKUNG: Die MX-Gehäuse-Firmwareaktualisierungsfunktion wird nur in den Bereitstellungsmodi „Mittel“, „Groß“ und „Extragroß“ unterstützt.

Sie können einen geeigneten Bereitstellungsmodus auswählen, um OMIVV so zu skalieren, dass es der Anzahl der Knoten in Ihrer Umgebung entspricht.

Um das OpenManage Management Pack for vRealize Operations (vROPS) in OMIVV zu integrieren, ist der minimale Bereitstellungsmodus **Medium**.

1. Scrollen Sie auf der Seite **GERÄTEMANAGEMENT** hinunter zu **Bereitstellungsmodus**.
   Die Konfigurationswerte des Bereitstellungsmodus wie **Klein**, **Mittel**, **Groß** und **Extragroß** werden angezeigt. Standardmäßig ist dieser Wert auf **Klein** gesetzt.
2. Um einen Bereitstellungsmodus basierend auf einer Umgebung zu bearbeiten, klicken Sie auf **Bearbeiten**.
3. Stellen Sie im **Bearbeiten**-Modus sicher, dass die Voraussetzungen erfüllt sind, und wählen Sie den gewünschten Bereitstellungsmodus aus.
4. Klicken Sie auf **Anwenden**.
   Die zugewiesene CPU und der Speicher werden mit der erforderlichen CPU und dem Speicher für die Einstellung des Bereitstellungsmodus verglichen.
   - Wenn die Überprüfung fehlschlägt, wird eine Fehlermeldung angezeigt.
   - Wenn die Überprüfung erfolgreich ist, wird das OMIVV-Gerät neu gestartet und der Bereitstellungsmodus geändert, nachdem Sie die Änderung bestätigt haben.
   - Wenn der erforderliche Bereitstellungsmodus bereits eingestellt ist, wird eine Meldung angezeigt.
5. Wenn der Bereitstellungsmodus geändert wird, müssen Sie die Änderungen bestätigen. Die OMIVV-Appliance wird anschließend neu gestartet, damit der Bereitstellungsmodus aktualisiert wird.

ANMERKUNG: Während das OMIVV-Gerät gestartet wird, wird die zugewiesene Systemressource mit dem eingestellten Bereitstellungsmodus verglichen und dahingehend geprüft. Wenn die zugewiesenen Systemressourcen unter dem Bereitstellungsmodus liegen, wird das OMIVV-Gerät nicht bis zur Anzeige der Anmeldeseite gestartet. Zum Starten des OMIVV-Geräts muss es heruntergefahren, die Systemressourcen auf die vorhandene Einstellung des Bereitstellungsmodus aktualisiert und das OMIVV-Gerät wieder eingeschaltet werden.

Bereitstellungsmodus zurückstufen

1. Melden Sie sich bei der Administratorkonsole an.
2. Ändern Sie den Bereitstellungsmodus im erforderlichen Maße.
3. Fahren Sie das OMIVV-Gerät herunter und ändern Sie die Systemressourcen im erforderlichen Maße.
4. Schalten Sie das OMIVV-Gerät ein.

Bereitstellungsmodus aktualisieren

1. Leeren Sie den Browser-Cache bevor Sie sich beim Dell Administratorportal anmelden.
2. Schalten Sie das OMIVV-Gerät ein.
3. Melden Sie sich bei der Administratorkonsole an.
4. Ändern Sie den Bereitstellungsmodus im erforderlichen Maße.

Erweiterte Überwachung

Stellen Sie sicher, dass die erweiterte Überwachung zur Unterstützung von OpenManage Management Pack for vRealize Operations Manager aktiviert ist. Es wird empfohlen, die erweiterte Überwachung über den Bereitstellungsmodus „Mittel“ durchzuführen.

Stellen Sie sicher, dass die SNMP-Trap-Überwachung zur Unterstützung von SNMP-Warnungen für OpenManage Management Pack for vRealize Operations Manager aktiviert ist. Dies ermöglicht dem Nutzer die Überwachung des Funktionszustands des Servers oder Gehäuses in Echtzeit.

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.
2. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
3. Scrollen Sie auf der Seite **Gerätemanagement** nach unten zu **Erweiterte Überwachung**.
4. Um die Einstellungen der erweiterten Überwachung zu ändern, klicken Sie auf **Bearbeiten**.
5. Aktivieren oder deaktivieren Sie im Bearbeitungsmodus die erweiterte Überwachung und SNMP-Trap-Überwachung und klicken Sie dann auf **Anwenden**.

Zertifikatsignierungsanforderung (CSR) erstellen

Bevor Sie eine OMIVV für ein vCenter registrieren, stellen Sie sicher, dass Sie die CSR hochladen.

Das Erstellen einer neuen CSR verhindert, dass Zertifikate mit zuvor erstellten CSR auf das Gerät hochgeladen werden. Um eine CSR zu erstellen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der Seite **GERÄTE-MANAGEMENT** auf **Zertifikatsignierungsanforderung erstellen** im Bereich **HTTPS-ZERTIFIKATE**.
   Eine Meldung zeigt an, dass wenn eine neue Anforderung erzeugt wird, mit dem vorherigen CSR erzeugte Zertifikate nicht mehr auf das Gerät hochgeladen werden. Um mit der Anforderung fortzufahren, klicken Sie auf **Weiter**.
2. Wenn Sie mit der Anforderung fortfahren, geben Sie im Dialogfenster **ZERTIFIKATSIGNIERUNGSANFORDERUNG ERSTELLEN** Informationen zum allgemeinen Namen, die Organisation, den Ort, das Bundesland, das Land und die E-Mail-Adresse ein. Klicken Sie auf **Weiter**.
3. Klicken Sie auf **Herunterladen** und speichern Sie das resultierende CSR an einem zugänglichen Speicherort.

HTTPS-Zertifikat hochladen

Stellen Sie sicher, dass das Zertifikat das PEM-Format verwendet.

Die HTTPS-Zertifikate werden für die sichere Kommunikation zwischen der OMIVV-Appliance und Hostsystemen oder vCenter verwendet. Um diese Art der sicheren Kommunikation einzurichten, senden Sie das CSR-Zertifikat an eine signierende Zertifizierungsstelle und laden Sie dann das resultierende CSR über die Verwaltungskonsole hoch. Darüber hinaus gibt es ein selbst-signiertes Standardzertifikat, das für die sichere Kommunikation verwendet werden kann; dieses Zertifikat ist bei jeder Installation einmalig.

1. Klicken Sie auf der Seite **GERÄTE-MANAGEMENT** auf **Zertifikat hochladen** im Bereich **HTTPS-ZERTIFIKATE**.
2. Klicken Sie auf **OK** im Dialogfeld **ZERTIFIKAT HOCHLADEN**.
3. Klicken Sie zum Hochladen des gewünschten Zertifikats auf **Durchsuchen** und dann auf **Hochladen**.
   Um den Status zu prüfen, rufen Sie die **Ereigniskonsole** des vSphere-Clients registrierter vCenter auf.

Während des Hochladens von Zertifikaten reagiert die OMIVV-Verwaltungskonsole bis zu 3 Minuten lang nicht mehr. Schließen Sie nach Abschluss der Aufgabe „HTTPS-Zertifikat hochladen“ die Browsersitzung und greifen Sie auf das Admin-Portal in einer neuen Browsersitzung zu.

Standardmäßiges HTTPS-Zertifikat wiederherstellen

1. Klicken Sie auf der Seite **GERÄTE-MANAGEMENT** auf **Standardzertifikat wiederherstellen** im Bereich **HTTPS-ZERTIFIKATE**.
2. Klicken Sie im Dialogfeld **STANDARDMÄSSIGES ZERTIFIKAT WIEDERHERSTELLEN** auf **Anwenden**.

Während der Wiederherstellung von Zertifikaten reagiert die OMIVV-Verwaltungskonsole bis zu 3 Minuten lang nicht mehr. Schließen Sie nach Abschluss der Aufgabe „HTTPS-Zertifikat-Standardeinstellungen wiederherstellen“ die Browsersitzung und greifen Sie auf das Admin-Portal in einer neuen Browsersitzung zu.

Globale Alarme einrichten

Mit der Alarmverwaltung können Sie die globalen Einstellungen, wie Alarme für alle vCenter-Instanzen unter OMIVV gespeichert werden, konfigurieren.

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.
2. Geben Sie im **Anmelde**-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **ALARMVERWALTUNG**. Klicken Sie auf **Bearbeiten**, um neue vCenter-Alarmeinstellungen festzulegen.
4. Geben Sie numerische Werte in die folgenden Felder ein:

   Standardmäßig wird die aktuelle Anzahl der Warnmeldungen angezeigt.

   - **Maximale Anzahl an Alarmen**
   - **Anzahl an Tagen, über die Alarme beibehalten werden sollen**
   - **Timeout für duplizierte Alarme (Sekunden)**
5. Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

Informationen zur OMIVV VM-Konsole

Die OMIVV VM-Konsole befindet sich innerhalb des vSphere-Clients auf einer virtuellen Maschine. Die Konsole arbeitet Hand in Hand mit der Verwaltungskonsole. Sie können mit der Verwaltungskonsole folgende Aufgaben ausführen:

- Konfiguration von Netzwerkeinstellungen
- Ändern des Kennworts des OMIVV-Geräts
- Konfigurieren von NTP und der Einstellungen zur lokalen Zeitzone
- Führen Sie einen Neustart des OMIVV-Geräts durch.
- Zurücksetzen des OMIVV-Geräts auf die werkseitigen Einstellungen
- Anmelden mit der schreibgeschützten Rolle
- Abmelden von der Konsole

OMIVV VM-Konsole öffnen

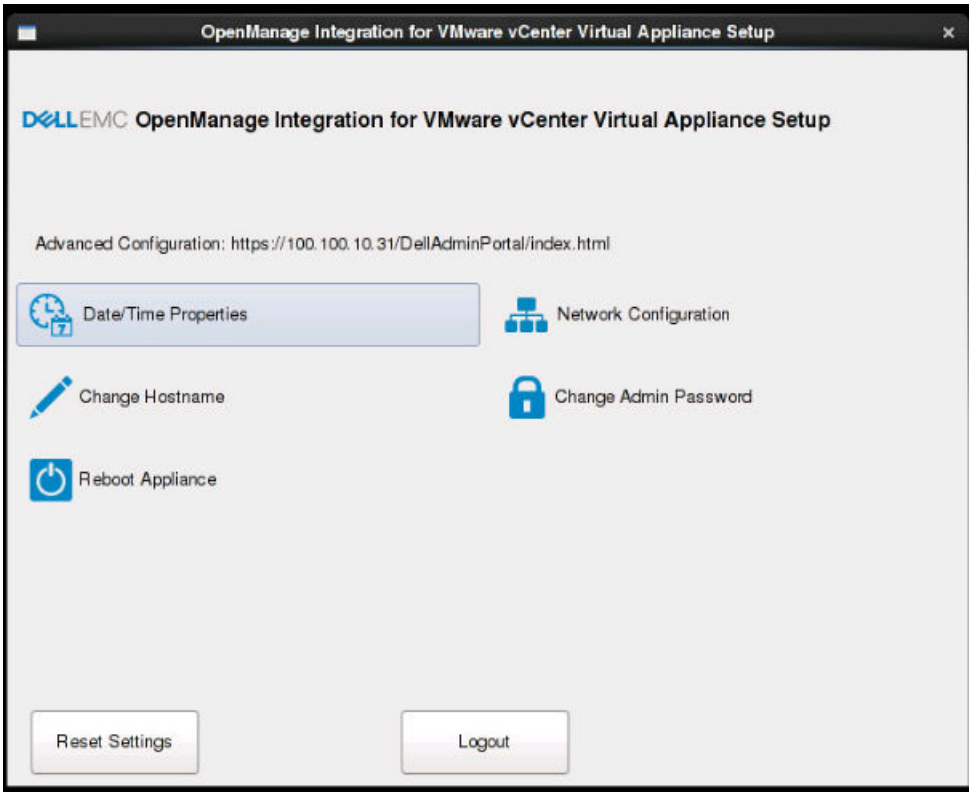
Starten Sie die Web- oder Remote-Konsole des OMIVV-Geräts, um die OMIVV-VM-Konsole zu öffnen.

Nach dem Öffnen der VM-Konsole und Eingabe der Anmeldeinformationen (Nutzername: `admin` und Kennwort: das Kennwort, das Sie während der Bereitstellung des Geräts eingerichtet haben), können Sie mit der Konfiguration der Konsole beginnen.

OMIVV-Gerät konfigurieren

1. Schalten Sie die virtuelle Maschine ein.
2. Klicken Sie im rechten Fensterbereich auf **Web-Konsole starten**.
3. Melden Sie sich als Administrator an (der Standardnutzername ist `admin`).
4. Wenn Sie sich zum ersten Mal anmelden, befolgen Sie die Anweisungen auf dem Bildschirm, um das Kennwort festzulegen (Admin- und ReadOnly-Nutzer).

   ANMERKUNG: Ein vergessenes Administratorkennwort kann von der OpenManage Integration for VMware vCenter-Appliance nicht wiederhergestellt werden.
5. Zum Konfigurieren der OMIVV-Zeitzoneninformationen klicken Sie auf **Datum/Uhrzeit-Eigenschaften**.



ANMERKUNG: Wenn das OMIVV-Gerät keine IP-Adresse aus dem Netzwerk abrufen kann (DHCP), wird `0.0.0.0` als IP-Adresse angezeigt. Um dies zu beheben, müssen Sie die statische IP manuell konfigurieren.

a. Aktivieren Sie auf der Registerkarte **Datum und Uhrzeit** das Kontrollkästchen **Datum und Uhrzeit über das Netzwerk synchronisieren**. Das Kontrollkästchen **Datum und Uhrzeit über das Netzwerk synchronisieren** ist nur aktiviert, wenn NTP über das Admin-Portal erfolgreich konfiguriert wurde. Weitere Informationen zum Konfigurieren von NTP finden Sie unter Einrichten von NTP-Servern (Network Time Protocol) auf Seite 23.

b. Klicken Sie auf **Zeitzone**, wählen Sie die entsprechende Zeitzone aus und klicken Sie dann auf **OK**.

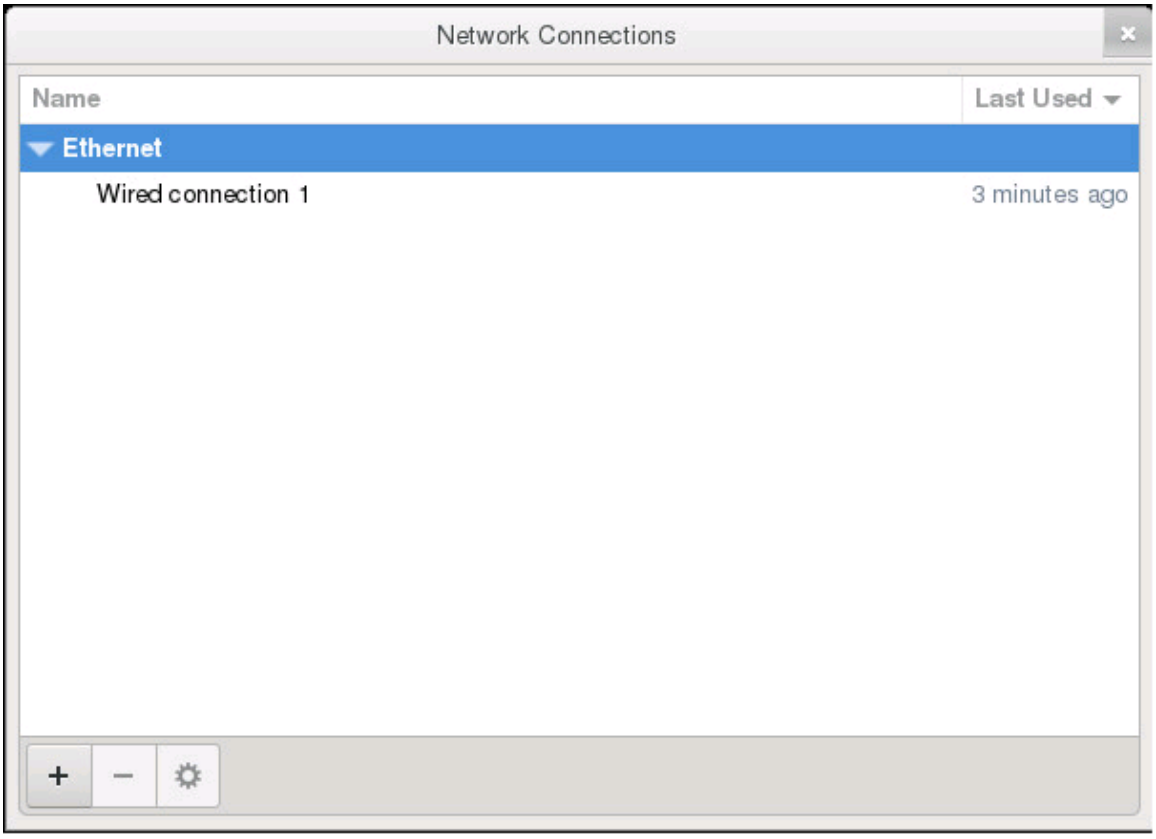
6. Um das Netzwerk des OMIVV-Geräts zu konfigurieren, klicken Sie auf **Netzwerkkonfiguration**.

   Zur Verwaltung der Dell EMC Server in Ihrer vSphere-Umgebung benötigt OMIVV Zugriff auf das vSphere-Netzwerk (vCenter und ESXi-Verwaltungsnetzwerk) und das Out-of-band-Netzwerk (iDRAC, CMC und OME-Modular).

   Wenn das vSphere-Netzwerk und das Out-of-band-Netzwerk in Ihrer Umgebung als separates isoliertes Netzwerk verwaltet werden, benötigt OMIVV Zugriff auf beide Netzwerke. In diesem Fall muss das OMIVV-Gerät mit zwei Netzwerkadaptern konfiguriert werden. Es wird empfohlen, beide Netzwerke im Rahmen der Erstkonfiguration zu konfigurieren.

   Wenn Sie über das vSphere-Netzwerk auf das Out-of-band-Netzwerk zugreifen können, konfigurieren Sie keine zwei Netzwerkadapter für das OMIVV-Gerät. Weitere Informationen zum Konfigurieren einer zweiten Netzwerkkarte finden Sie unter Konfigurieren der OMIVV-Appliance mit zwei Netzwerkschnittstellen-Controllern (NICs) auf Seite 29.

7. Wählen Sie **Kabelgebundene Verbindung 1** aus und klicken Sie auf  .



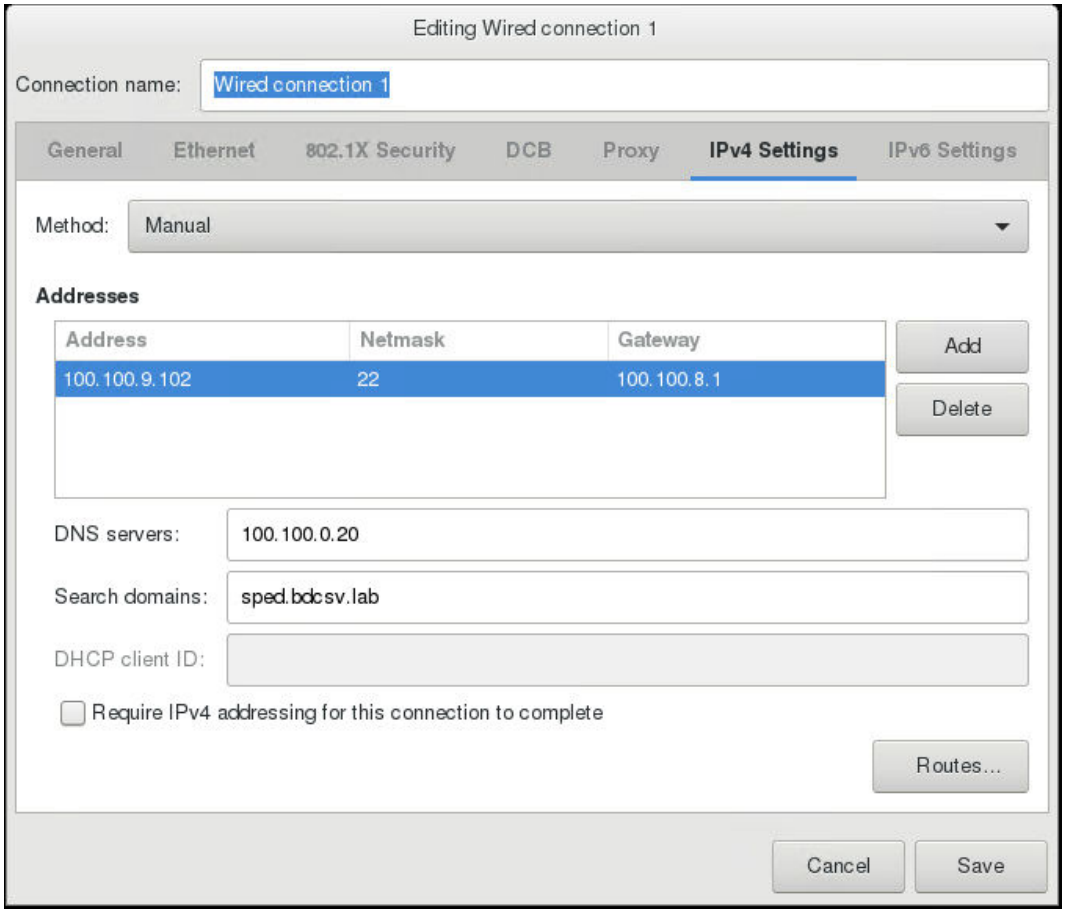
a. Klicken Sie auf die Registerkarte **IPv4-Einstellungen**, wählen Sie **Manuell** aus dem Dropdown-Menü **Methode** und klicken Sie auf **Hinzufügen**.

   ANMERKUNG: Wenn Sie Automatisch (DHCP) wählen, geben Sie keine IP-Adresse ein, da das OMIVV-Gerät die IP-Adresse beim nächsten Neustart automatisch vom DHCP-Server erhält.

b. Geben Sie eine gültige IP-Adresse, eine Netzmaske (im CIDR-Format (Classless Inter-Domain Routing)) und Gateway-Informationen ein.
   Wenn Sie im Feld **Netzmaske** eine IP-Adresse eingeben, wird diese automatisch in das entsprechende CIDR-Format umgewandelt.

c. Geben Sie die DNS-Server-IP und die zu suchenden Domänen jeweils in die Felder **DNS-Server** und **Domänen suchen** ein.

d. Aktivieren Sie das Kontrollkästchen **IPv4-Adressierung zum Abschließen dieser Verbindung erforderlich** und klicken Sie auf **Speichern**.



ANMERKUNG:

Nachdem Sie das OMIVV-Gerät mit einer statischen IP-Adresse konfiguriert haben, wird die OMIVV-Terminal-Hilfsprogramm-Seite manchmal nicht sofort aktualisiert, um die aktualisierte IP anzuzeigen. Um dieses Problem zu beheben, verlassen Sie das OMIVV-Terminal-Dienstprogramm und melden Sie sich erneut an.

8. Klicken Sie zum Ändern des Hostnamens des OMIVV-Geräts auf **Hostnamen ändern**.
   a. Geben Sie einen gültigen Hostnamen ein und klicken Sie auf **Hostnamen aktualisieren**.

   ANMERKUNG: Wenn bei der OMIVV-Appliance bereits vCenter-Server registriert sind, heben Sie die Registrierung auf und registrieren Sie alle vCenter-Instanzen erneut. Weitere Informationen finden Sie im Thema „Aufheben der Registrierung und erneute Registrierung verwalten“ im Installationshandbuch.

9. Starten Sie das System neu.

Konfigurieren der OMIVV-Appliance mit zwei Netzwerkschnittstellen-Controllern (NICs)

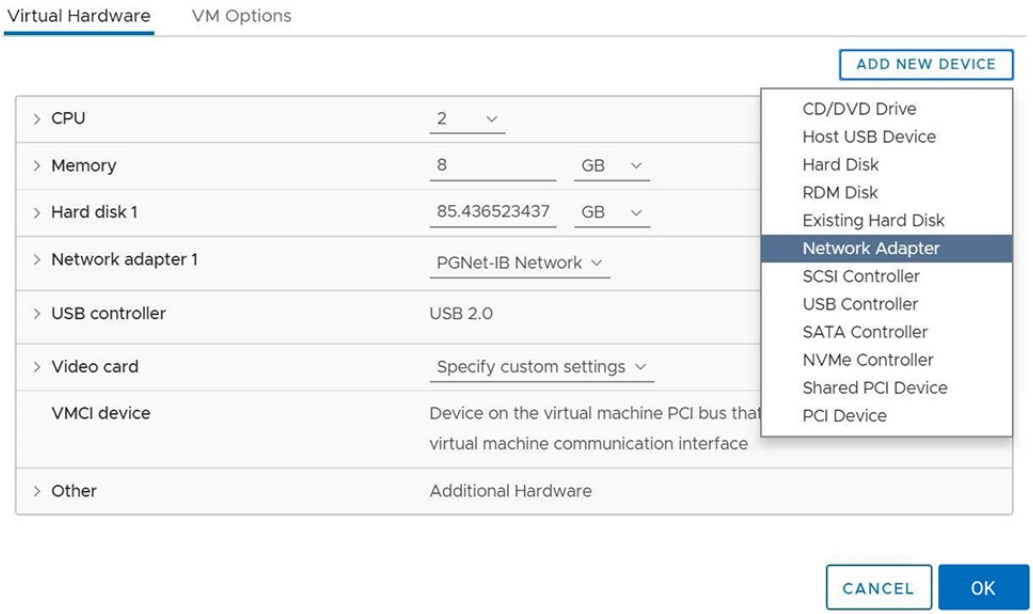
Zur Verwaltung der Dell EMC Server in Ihrer vSphere-Umgebung benötigt OMIVV Zugriff auf das vSphere-Netzwerk (vCenter und ESXi-Verwaltungsnetzwerk) und das Out-of-band-Netzwerk (iDRAC, CMC und OME-Modular). Wenn das vSphere-Netzwerk und das Out-of-band-Netzwerk in Ihrer Umgebung als separates isoliertes Netzwerk verwaltet werden, benötigt OMIVV Zugriff auf beide Netzwerke. In diesem Fall muss die OMIVV-Appliance mit zwei NICs konfiguriert werden. Wenn auf das Out-of-band-Netzwerk über das vSphere-Netzwerk zugegriffen werden kann, sollten Sie keine zwei NICs für die OMIVV-Appliance konfigurieren.

Stellen Sie sicher, dass Sie über die folgenden Informationen sowohl für das Out-of-band-Netzwerk als auch für das vSphere-Netzwerk verfügen:

- IP-Adresse, Netzmaske (im CIDR-Format) und Gateway des Geräts (falls statisch)
- Standard-Gateway: Es ist zwingend erforderlich, das Standard-Gateway nur für ein Netzwerk mit einer Internetverbindung zu konfigurieren. Es wird empfohlen, das vSphere-Netzwerk als Standardgateway zu verwenden.

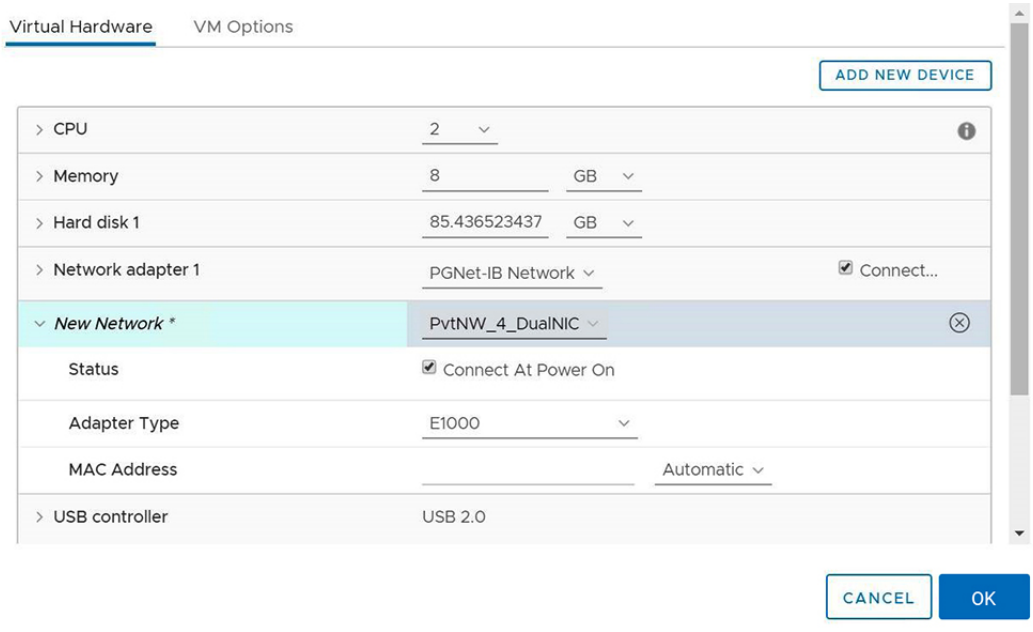
- Routing-Anforderungen (Netzwerk-IP, Netzmaske und Gateway): Für andere externe Netzwerke, die weder direkt noch über das Standard-Gateway erreichbar sind, konfigurieren Sie die statischen Routen.
- DNS-Anforderungen: OMIVV unterstützt DNS-Konfiguration nur für ein Netzwerk. Weitere Informationen zur DNS-Konfiguration finden Sie unter Schritt 9 (b) in diesem Thema.

1. Schalten Sie die OMIVV-Appliance aus.
2. Bearbeiten Sie die VM-Einstellungen mit dem vSphere Client (HTML-5) und fügen Sie den zusätzlichen Netzwerkadapter hinzu. Um die VM-Einstellungen zu bearbeiten, klicken Sie mit der rechten Maustaste auf die VM und klicken Sie dann auf **Einstellungen bearbeiten**.
3. Klicken Sie auf **NEUES GERÄT HINZUFÜGEN** und wählen Sie **Netzwerkadapter** aus.



a. Wählen Sie das entsprechende Netzwerk für den NIC aus und markieren Sie dann das Kontrollkästchen **Beim Einschalten verbinden**.
b. Wählen Sie im Drop-Down-Menü den **VMXNET3**-Adapter aus.

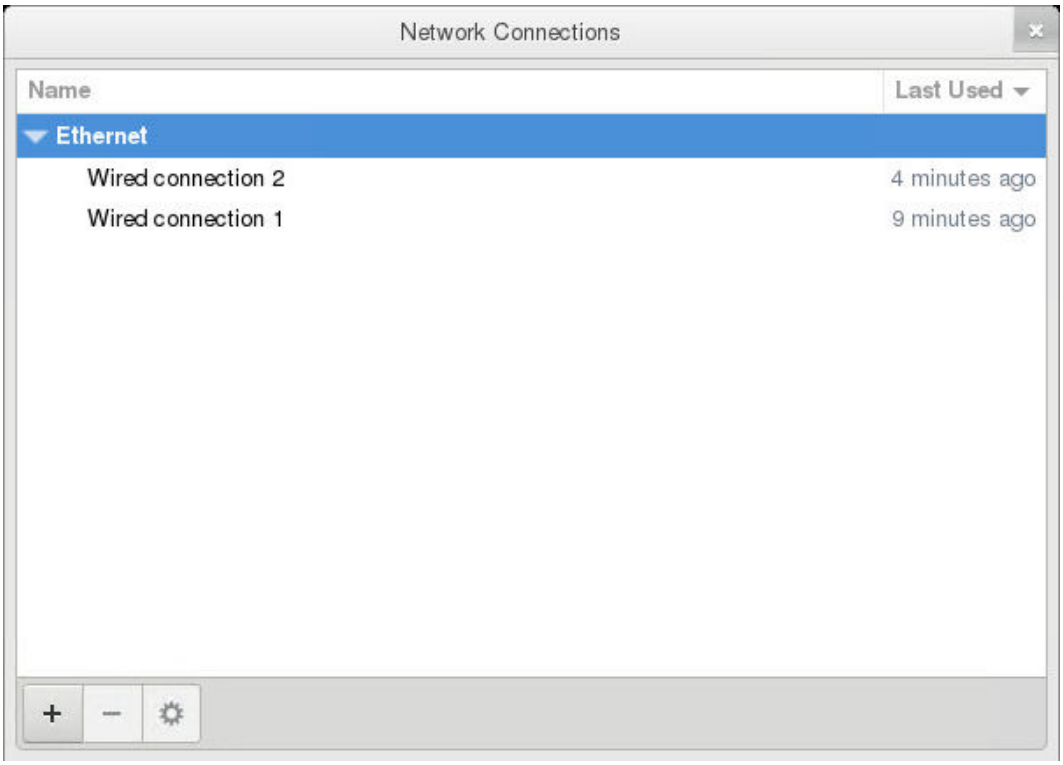
ANMERKUNG: OMIVV unterstützt den VMXNET3-NIC-Typ.



4. Schalten Sie das OMIVV-Gerät ein. Melden Sie sich als Administrator an (der Standardnutzername ist Admin) und drücken Sie dann die **Eingabetaste**.

5. Wählen Sie im Hilfsprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts Netzwerkkonfiguration**.

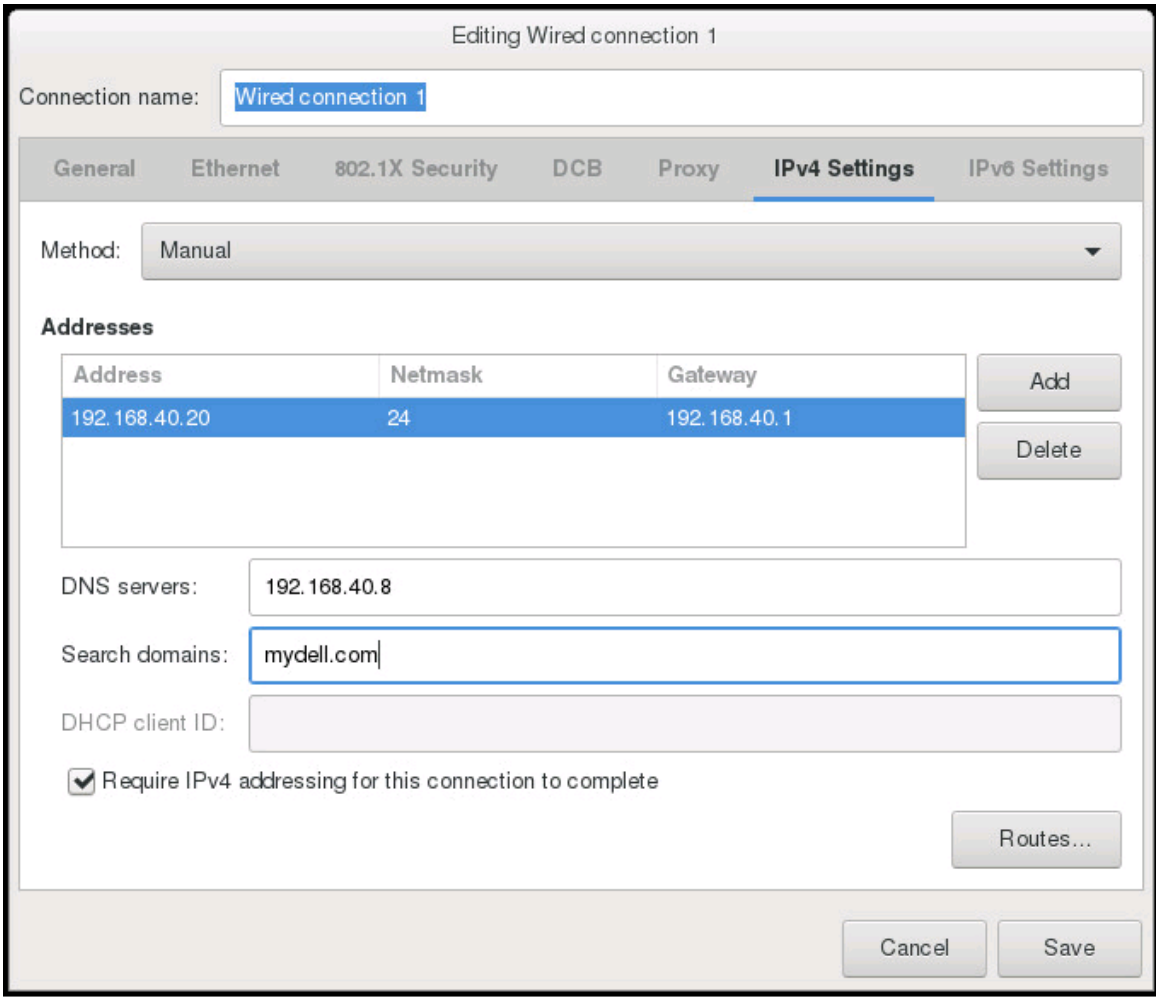
   Auf der Seite **Netzwerkverbindungen** werden zwei NICs angezeigt.



WARNUNG: Verwenden Sie „+“ nicht, um eine neue Netzwerkschnittstelle hinzuzufügen. Um einen NIC hinzuzufügen, muss „Einstellungen bearbeiten“ für vSphere verwendet werden.

6. Wählen Sie die NIC aus, die Sie konfigurieren möchten, und klicken Sie auf  .
7. Um die richtige NIC zu identifizieren, verwenden Sie die auf der Registerkarte **Ethernet** angezeigte MAC-ID und vergleichen Sie sie dann mit der im vSphere Client (HTML-5) angezeigten MAC-ID.

   Achten Sie darauf, dass Sie die auf der Registerkarte **Ethernet** angegebene Standard-MAC-Adresse nicht ändern.
8. Klicken Sie auf die Registerkarte **Allgemein** und aktivieren Sie das Kontrollkästchen **Automatische Verbindung zu diesem Netzwerk herstellen, wenn es verfügbar ist**.
9. Klicken Sie auf die Registerkarte **IPv4-Einstellungen** und gehen Sie wie folgt vor:



a. Wählen Sie **Manuell** oder **Automatisch (DHCP)** aus der Dropdown-Liste **Methode**.
b. Wenn Sie die Methode **Manuell** auswählen, klicken Sie auf **Hinzufügen** und geben Sie dann die gültige IP-Adresse, Netzmaske (im CIDR-Format) und Gateway-Details ein. Es wird empfohlen, die statische IP-Adresse für den Fall zu verwenden, dass Sie die Priorität der DNS-Server (primäre und sekundäre DNS-Einträge) steuern möchten.

   Typischerweise werden die vSphere-Elemente eines Rechenzentrums, wie vCenter- und ESXi-Hosts, über den Hostnamen oder FQDN verwaltet. iDRAC, CMC und OME-Modular werden über IP-Adressen verwaltet. In diesem Fall wird empfohlen, die DNS-Einstellungen nur für das vSphere-Netzwerk zu konfigurieren.

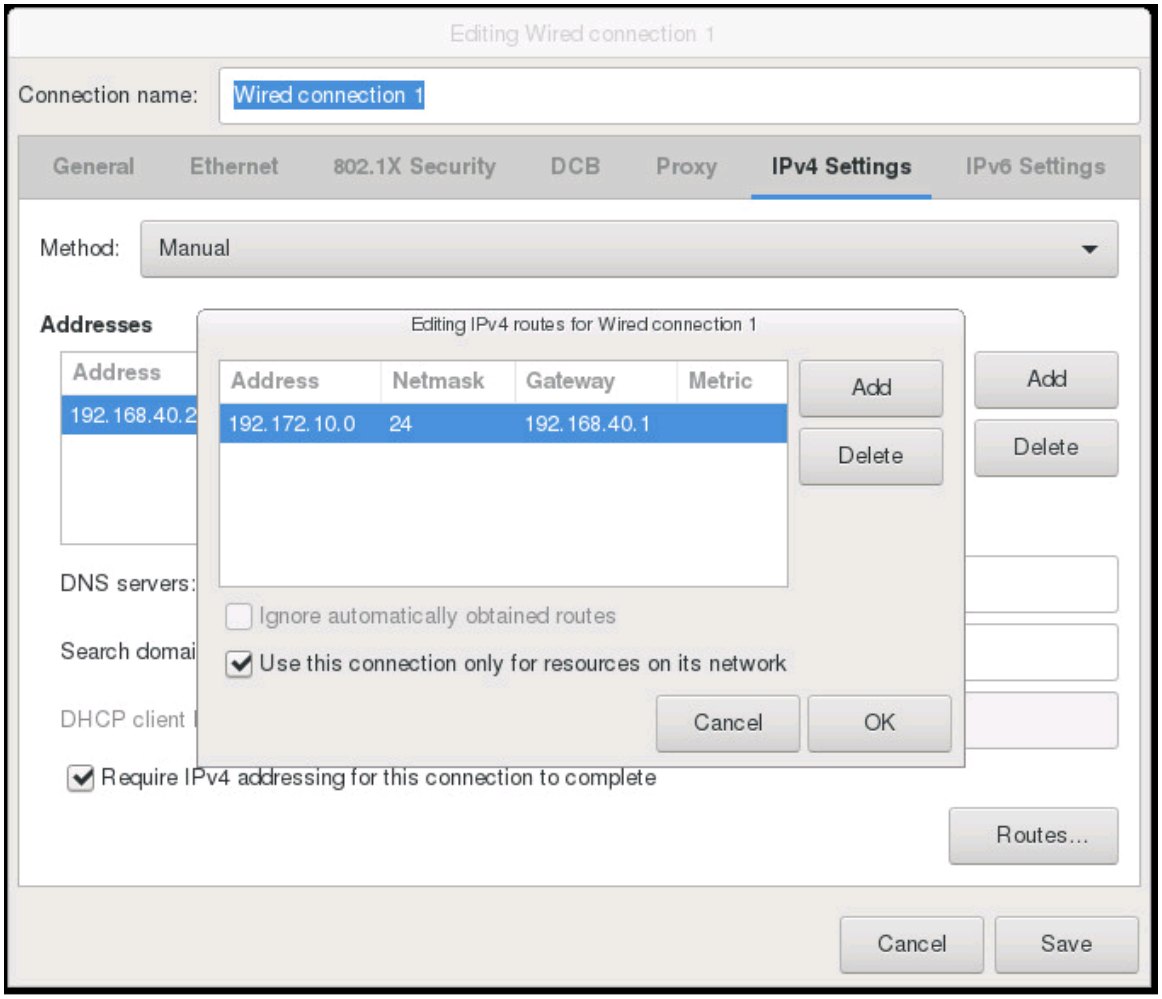
   Wenn sowohl das vSphere-Netzwerk als auch das iDRAC-Verwaltungsnetzwerk über den Hostnamen oder FQDN verwaltet werden, muss der DNS-Server so konfiguriert werden, dass er den Hostnamen oder FQDN für beide Netzwerke auflöst. Weitere Informationen finden Sie in der CentOS-Dokumentation.

   ANMERKUNG: Der zuletzt konfigurierte DNS-Server wird zum primären DNS, unabhängig davon, für welches Netzwerk der DNS konfiguriert ist.

c. Geben Sie die DNS-Server-IP und die zu suchenden Domänen in die Felder **DNS-Server** und **Domänen suchen** ein.
d. Aktivieren Sie das Kontrollkästchen **IPv4-Adressierung zum Abschließen dieser Verbindung erforderlich** und klicken Sie auf **SPEICHERN**.
e. Wenn Sie dieses Netzwerk nicht als Standardnetzwerk (Gateway) verwenden möchten, klicken Sie auf **Routen**, und aktivieren Sie dann das Kontrollkästchen **Diese Verbindung nur für Ressourcen in ihrem Netzwerk verwenden**.

   ANMERKUNG: Das Hinzufügen mehrerer Netzwerke als Standardgateways kann zu Netzwerkproblemen führen, sodass OMIVV-Funktionen beeinträchtigt sind.

f. Wenn Sie über die bekannten Gateways zu einem externen Netzwerk gelangen möchten, klicken Sie auf der gleichen Seite auf **Hinzufügen** und fügen Sie dann die Netzwerk-IP-Adresse, die Netzmaske (im CIDR-Format) und die Gateway-Details hinzu.



In der Regel erfordert das Netzwerk, das Sie als Standard-Gateway konfiguriert haben, keine manuelle Routingkonfiguration, da das Gateway die Erreichbarkeit gewährleisten kann. Bei Netzwerken, für die das Standard-Gateway nicht konfiguriert ist (für die das Kontrollkästchen **Diese Verbindung nur für Ressourcen in ihrem Netzwerk verwenden** aktiviert wurde), kann jedoch eine manuelle Routingkonfiguration erforderlich sein. Da das Standard-Gateway nicht so konfiguriert ist, dass dieses Netzwerk externe Netzwerke erreicht, sind manuelle Routingkonfigurationen erforderlich.

ANMERKUNG: Eine falsche Routingonfiguration kann dazu führen, dass die Netzwerkschnittstelle unvermittelt nicht mehr reagiert. Achten Sie darauf, die Routing-Einträge entsprechend zu konfigurieren.

g. Klicken Sie auf **OK**.

10. Klicken Sie auf **Speichern**. Zum Konfigurieren einer anderen NIC wiederholen Sie die Schritte 6–10.
11. Navigieren Sie zu **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** und klicken Sie auf **Gerät neu starten**. Die Netzwerkkonfiguration ist erst nach einem Neustart des OMIVV-Geräts abgeschlossen.

    Nachdem das Gerät erfolgreich neu gestartet wurde, funktionieren die NICs gemäß der Konfiguration. Der Status von NICs kann eingesehen werden, indem Sie sich als **schreibgeschützter** Nutzer anmelden und die folgenden Befehle ausführen: `ifconfig`, `ping` und `route -n`.

Kennwort des OMIVV-Geräts ändern

Sie können das Kennwort des OMIVV-Geräts im vSphere-Client unter Verwendung der Konsole ändern.

1. Öffnen Sie die OMIVV-Webkonsole.
2. Klicken Sie im Dienstprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** auf **Admin-Kennwort ändern**.

   Folgen Sie den Anweisungen auf dem Bildschirm, um das Kennwort festzulegen.
3. Geben Sie im Textfeld **Aktuelles Kennwort** das aktuelle Administratorkennwort ein.
4. Geben Sie ein neues Kennwort im Textfeld **Neues Kennwort** ein.

5. Geben Sie das neue Kennwort erneut im Textfeld **Neues Kennwort bestätigen** ein.
6. Klicken Sie auf **Administratorkennwort**.

Konfigurieren des Network Time Protocol (NTP) und Einstellen der lokalen Zeitzone

1. Öffnen Sie die OMIVV-Webkonsole.
2. Klicken Sie im Dienstprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** auf **Datum/Uhrzeit-Eigenschaften**.

   Geben Sie die NTP-Details in die Admin-Konsole ein. Weitere Informationen finden Sie unter Einrichten von NTP-Servern (Network Time Protocol) auf Seite 23.
3. Wählen Sie auf der Registerkarte **Datum und Uhrzeit Datum und Uhrzeit über das Netzwerk synchronisieren**.
   Das **NTP-Server**-Feld wird angezeigt.
4. Zum Hinzufügen einer weiteren NTP-Server-IP oder eines Hostnamens klicken Sie auf die Schaltfläche **Hinzufügen**, und drücken Sie die **Tabulatortaste**.
5. Klicken Sie auf **Zeitzone**, und wählen Sie dann die entsprechende Zeitzone aus. Klicken Sie dann Sie auf **OK**.

Hostnamen des OMIVV-Geräts ändern

1. Klicken Sie im Dienstprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** auf **Hostname ändern**.

   ANMERKUNG: Wenn irgendwelche vCenter-Server beim OMIVV-Gerät registriert sind, heben Sie die Registrierung auf und registrieren Sie alle vCenter-Instanzen erneut.
2. Geben Sie einen aktualisierten Hostnamen ein.
   Geben Sie den Domänennamen im folgendem Format an: *<Hostname>*.
3. Klicken Sie auf **Hostnamen aktualisieren**.
   Der Hostname des Geräts wird aktualisiert und die Hauptmenü-Seite wird angezeigt.
4. Um das Gerät neu zu starten, klicken Sie auf **Neustart des Geräts**.

ANMERKUNG: Stellen Sie sicher, dass Sie alle Referenzen auf das virtuelle Gerät in Ihrer Umgebung manuell aktualisieren, wie z. B. Bereitstellungsserver in iDRAC und Dell EMC Repository Manager (DRM).

Neustart des OMIVV-Geräts durchführen

1. Öffnen Sie die OMIVV-Webkonsole.
2. Klicken Sie im Dienstprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** auf **Gerät neu starten**.
3. Um das Gerät neu zu starten, klicken Sie auf **Ja**.

OMIVV-Appliance auf werkseitige Einstellungen zurücksetzen

1. Öffnen Sie die OMIVV-Webkonsole.
2. Klicken Sie im Dienstprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** auf **Einstellungen zurücksetzen**.

   Die folgende Meldung wird angezeigt:

   ```
   All the settings in the appliance will be Reset to Factory Defaults and the appliance will
   be rebooted. Do you still wish to continue?
   ```
3. Um das Gerät zurückzusetzen, klicken Sie auf **Ja**.
   Wenn Sie auf **Ja** klicken, wird das OMIVV-Gerät auf die Werkseinstellungen zurückgesetzt und alle anderen Einstellungen und vorhandenen Daten werden gelöscht.

   Nachdem die Zurücksetzung auf die Werkseinstellungen abgeschlossen ist, registrieren Sie die vCenters erneut bei dem OMIVV-Gerät.

ANMERKUNG: Wenn das OMIVV-Gerät auf die Werkseinstellungen zurückgesetzt wird, werden alle Aktualisierungen an der Netzwerkkonfiguration beibehalten. Diese Einstellungen werden nicht zurückgesetzt.

Schreibgeschützte Benutzerrolle

Es gibt einen Nutzer ohne Rechte mit der Bezeichnung „schreibgeschützt“ mit Shell-Zugriff für Diagnosezwecke. Der Nutzer mit schreibgeschützter Rolle verfügt über eingeschränkte Rechte zum Ausführen einiger Befehle.

3

Hosts und Gehäuse über das Dashboard überwachen

Das Dashboard zeigt Folgendes an:

- Funktionszustand von Hosts und Gehäusen
- Servicestatus von Hosts und Gehäusen
- Lizenzinformationen von Hosts und vCenter
- Konfigurations-Compliance-Status der Hosts
- Status der mit OMIVV geplanten Jobs
- Bare-Metal-Server, die für die Bereitstellung verfügbar sind
- Kurzhinweise zu OMIVV-Funktionen

Funktionszustand

Der Abschnitt **Zustand** zeigt die Integrität aller von OMIVV verwalteten Hosts und Gehäuse an. Alle Hosts, die hier angezeigt werden, werden mithilfe desselben Platform Service Controller (PSC) konfiguriert.

Der Status der einzelnen Hosts und Gehäuse wird nach Abschluss einer periodischen Integritäts-Metrik-Aufgabe oder eines SNMP-Ereignisses von Host und Gehäuse aktualisiert (startet Integritätsmetrik-Job für spezifischen Host oder Gehäuse).

Standardmäßig wird der Task „Integritätsmetrik-Job“ nach jeder Stunde ausgeführt. Die angezeigten Daten werden verwendet, um die proaktive HA-Integrität und Funktionszustandsaktualisierung für Server und Gehäuse im Dashboard zu überwachen. Die Details des Jobs sind unter „Protokolle“ verfügbar.

Die folgende Liste beschreibt die verschiedenen Zustände von Hosts und Gehäusen:

- **Fehlerfrei**: Zeigt die Anzahl der Hosts und Gehäuse an, die sich in einem fehlerfreien Zustand befinden.
- **Warnung**: Zeigt die Anzahl der Hosts und Gehäuse an, die eine Korrekturmaßnahme erfordern, aber sich nicht unmittelbar auf das System auswirken.
- **Kritisch**: Zeigt die Anzahl der Hosts und Gehäuse an, die kritische Probleme mit einer oder mehreren Komponenten haben und eine sofortige Aktion erfordern.
- **Unbekannt**: Zeigt die Gesamtzahl der Hosts und Gehäuse an, die sich in einem unbekannten Zustand befinden. Der Host oder das Gehäuse zeigt den Status „Unbekannt“ an, wenn der Host oder das Gehäuse nicht erreichbar ist oder der Integritätsstatus unbekannt ist.

Um weitere Informationen zu Hosts anzuzeigen, klicken Sie auf der Seite **Dashboard** im Abschnitt **Integrität** auf **HOST ANZEIGEN**.

Um weitere Informationen zu Gehäusen anzuzeigen, klicken Sie auf der Seite **Dashboard** im Abschnitt **Integrität** auf **GEHÄUSE ANZEIGEN**.

Gewährleistung

Die Anzahl der Hosts, die unter dieser Servicekategorie angezeigt werden, bezeichnet die Hosts, die vCenter-Servern angehören, die mit dem PSC konfiguriert wurden. Um die Serviceinformationen zu Host und Gehäuse zu erhalten, stellen Sie sicher, dass Sie die Benachrichtigung zum Ablauf des Service auf der Seite **Einstellungen** aktiviert haben.

Für Hosts mit mehreren oder unterschiedlichen Gewährleistungen (z. B. Servicetypen wie Next Business Day (NBD) und Party Only Warranty (POW)) zeigt OMIVV den Status basierend auf dem Servicetyp an, der die geringste Anzahl an Gewährleistungstagen hat.

Der Abschnitt **Service** enthält die folgenden Informationen zu Hosts und Gehäusen:

- **Fehlerfrei**: Zeigt die Anzahl der Hosts und Gehäuse an, für die die verbleibenden Servicetage über dem Warnungsschwellenwert liegen.
- **Warnung**: Zeigt die Anzahl der Hosts und Gehäuse an, für die die verbleibenden Servicetage unter dem Warnungsschwellenwert liegen.

- **Kritisch**: Zeigt die Anzahl der Hosts und Gehäuse an, für die die verbleibenden Servicetage unterhalb des kritischen Schwellenwerts liegen.
- **Unbekannt**: Zeigt die Anzahl der Hosts und Gehäuse an, deren Service unbekannt ist.

Gehen Sie wie folgt vor, um die Hosts zu identifizieren, die sich in einem der folgenden Zustände befinden: **Fehlerfrei**, **Warnung**, **Kritisch** und **Unbekannt**:

1. Gehen Sie zu **Hosts und Cluster**.
2. Wählen Sie zum Anzeigen des Funktionszustands von Hosts auf Cluster-Ebene ein Cluster aus und klicken Sie dann auf **Überwachen** > **OMIVV-Cluster-Informations** > **gewährleistung**.
3. Um den Funktionszustand des Hosts auf Rechenzentrumsebene anzuzeigen, wählen Sie ein Rechenzentrum aus und klicken dann auf **Überwachen** > **OMIVV Datacenter-Informations** > **gewährleistung**.

Lizenzen

Im Abschnitt **Lizenzen** werden die folgenden Informationen angezeigt:

- Anzahl aller Host- und vCenter-Lizenzen
- Anzahl der verfügbaren Host- und vCenter-Lizenzen
- Anzahl der Host- und vCenter-Lizenzen, die verwendet werden.

Um eine Lizenz zu erwerben, klicken Sie auf der Seite **Dashboard** im Abschnitt **Lizenzen** auf **LIZENZ KAUFEN**.

Bereit zur Bereitstellung

In diesem Abschnitt werden nur die konformen Bare-Metal-Server, die mit OMIVV erkannt werden, angezeigt. Um die Bare-Metal-Server bereitzustellen, klicken Sie auf **Bereitstellen**.

Konfigurations-Compliance

In diesem Abschnitt werden die Hosts angezeigt, die Teil des Clusters sind, der dem Clusterprofil zugeordnet ist. Die Hosts, die hier angezeigt werden, werden mithilfe desselben Platform Service Controller (PSC) konfiguriert.

Um den Status der Konfigurations-Compliance von Hosts anzuzeigen, klicken Sie auf **COMPLIANCE ANZEIGEN**.

Jobs

Im Abschnitt Jobs werden die Jobs angezeigt, die mithilfe von OMIVV geplant werden. Sie können die Job-Details nur für die letzten 7 Tage anzeigen.

Das Kreisdiagramm zeigt die Gesamtzahl der Jobs in den Status **Erfolgreich**, **In Bearbeitung**, **Fehlgeschlagen**, **Geplant** und **Abgebrochen** an. Um den Jobstatus aus dem Kreisdiagramm zu filtern, klicken Sie auf die Jobstatus.

Sie können die Anzahl der folgenden Jobs anzeigen, die sich in den Status **Erfolgreich**, **In Bearbeitung**, **Fehlgeschlagen**, **Geplant** und **Abgebrochen** befinden:

- Bereitstellungs-Jobs

  Weitere Informationen finden Sie unter Bereitstellungs-Jobs auf Seite 76.
- Host-Firmwareupdates-Jobs

  Weitere Informationen finden Sie unter Host-Firmwareupdates-Jobs auf Seite 78.
- Gehäuse-Firmwareupdates-Jobs

  Weitere Informationen finden Sie unter Gehäuse-Firmwareupdates-Jobs auf Seite 77.
- Systemsperrmodus-Jobs

  Weitere Informationen finden Sie unter Systemsperrmodus-Jobs auf Seite 78.

Um den Status aller Jobs anzuzeigen, klicken Sie auf **ALLE JOBS ANZEIGEN**.

Schnellreferenzhandbuch

Dieser Abschnitt enthält die Schnellreferenzen auf die folgenden Funktionen:

- Erst-Konfigurationsassistenten starten

  Weitere Informationen finden Sie unter . Erstkonfiguration auf Seite 90
- Host-Zugangsdatenprofil

  Weitere Informationen finden Sie unter . Host-Zugangsdatenprofil auf Seite 39
- Verwaltungs-Compliance

  Weitere Informationen finden Sie unter . Verwaltungs-Compliance auf Seite 71
- Gehäuse-Zugangsdatenprofil

  Weitere Informationen finden Sie unter . Gehäuse-Zugangsdatenprofil auf Seite 44
- Clusterprofil

  Weitere Informationen finden Sie unter . Clusterprofil auf Seite 52
- Bereitstellung

  Weitere Informationen finden Sie unter . Bereitstellungsprüfliste auf Seite 66

4

Hosts mit Host-Zugangsdatenprofil verwalten

Host-Zugangsdatenprofil

Ein Host-Zugangsdatenprofil speichert die iDRAC- und die Host-Anmeldeinformationen, die OMIVV für die Kommunikation mit den Servern verwendet. OMIVV verwaltet die Hosts, die einem Host-Zugangsdatenprofil zugeordnet sind. Sie können einem einzigen Host-Zugangsdatenprofil mehrere Server zuordnen.

Der PowerEdge MX-Gehäuse-Host kann mit einer einzigen einheitlichen Chassis-Management-IP verwaltet werden. Hosts in einem PowerEdge MX-Gehäuse mit deaktiviertem iDRAC IP müssen über ein Gehäuseprofil verwaltet werden. Informationen zur Verwaltung des PowerEdge MX-Gehäuses mithilfe eines Gehäuse-Zugangsdatenprofils finden Sie unter Gehäuse-Zugangsdatenprofil erstellen auf Seite 44. Um vollständige OMIVV-Funktionen zu erhalten, wird die Verwaltung von PowerEdge MX-Gehäuse-Hosts über eine iDRAC-IP mit Host-Zugangsdatenprofil empfohlen.

Host-Anmeldeinformationenprofil erstellen

Wenn die Anzahl der hinzugefügten Hosts die Lizenzgrenze überschreitet, kann kein Host-Anmeldeinformationenprofil erstellt werden.

Bevor Sie die Active Directory (AD)-Anmeldeinformationen mit einem Host-Anmeldeinformationen Profil verwenden, stellen Sie Folgendes sicher:

- Das Benutzerkonto ist in AD vorhanden.
- Der iDRAC oder der Host müssen für die AD-basierte Authentifizierung konfiguriert sein.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Host-Anmeldeinformationenprofil**.
2. Klicken Sie auf der Seite **Host-Anmeldeinformationenprofil** auf **NEUES PROFIL ERSTELLEN**.
3. Lesen Sie auf der Seite **Host-Anmeldeinformationenprofil** die Anweisungen und klicken Sie dann auf **ERSTE SCHRITTE**.
4. Führen Sie auf der Seite **Name und Anmeldeinformationen** folgende Schritte aus:
   a. Geben Sie den Profilnamen und die Beschreibung an. Die Beschreibung ist optional.
   b. Wählen Sie in der Liste **vCenter-Name** eine Instanz von vCenter aus, auf der Sie das Host-Anmeldeinformationenprofil erstellen möchten.
   c. Geben Sie im Bereich **iDRAC-Anmeldeinformationen** die lokalen iDRAC-Anmeldeinformationen oder die AD-Anmeldeinformationen ein.
      - Gehen Sie wie folgt vor, um die lokalen Anmeldeinformationen für iDRAC einzugeben:
        - Geben Sie den Benutzernamen im Feld **Benutzername** ein. Der Benutzername ist auf 16 Zeichen beschränkt.

          Informationen zur Definition von Benutzernamen finden Sie im *iDRAC-Benutzerhandbuch*, das unter **https://www.dell.com/support** verfügbar ist.
        - Geben Sie das Kennwort ein.

          Weitere Informationen zu den empfohlenen Zeichen in Benutzernamen und Kennwörtern finden Sie im *iDRAC Benutzerhandbuch*, das unter **https://www.dell.com/support** verfügbar ist.
      - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
      - Um die Anmeldeinformationen für einen iDRAC einzugeben, der bereits für AD konfiguriert und aktiviert ist, aktivieren Sie das Kontrollkästchen **Active Directory verwenden**.

        ANMERKUNG: Das iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware und die Bereitstellung eines Betriebssystems (BS).
        - Geben Sie den Benutzernamen im Feld **Active Directory-Benutzername** ein.

Geben Sie den Benutzernamen in einem dieser Formate ein: `domain\username` oder `username@domain`. Der Benutzername ist auf 256 Zeichen beschränkt. Informationen zu Nutzernamen-Einschränkungen finden Sie in der **Dokumentation zum Microsoft Active Directory**.

- Geben Sie das Kennwort ein.

  Die AD-Anmeldeinformationen können für den iDRAC und den Host dieselben oder unterschiedlich sein.

d. Geben Sie im **Host-Stamm**-Bereich die lokalen Host-Anmeldeinformationen oder AD-Anmeldeinformationen ein.

Der Standardbenutzername lautet root.

- Um die lokalen Host-Anmeldeinformationen einzugeben, führen Sie die folgenden Schritte durch:
  - Geben Sie das Kennwort ein.

    Das Host-Kennwort ist nur für Hosts erforderlich, auf denen ESXi 6.5 U3 und frühere Versionen ausgeführt werden.

    Um diesen Schritt für ESXi 6.7 und neuere Versionen zu überspringen, stellen Sie sicher, dass das Kontrollkästchen **Host-Anmeldeinformationen verwenden** deaktiviert ist. Wenn für einen Host, auf dem ESXi 6.7 oder höher ausgeführt wird, ein Kennwort eingegeben wurde, wird das Kennwort ignoriert.

    Für Hosts, auf denen ESXi 6.7 oder höherausgeführt werden, wird empfohlen, keine Anmeldeinformationen für ESXi einzugeben. OMIVV kann die iDRAC mit dem ESXi Host verbinden, selbst wenn falsche Host-Anmeldeinformationen eingegeben wurden.

- Um die Anmeldeinformationen für Hosts einzugeben, die bereits für AD konfiguriert und aktiviert sind, aktivieren Sie das Kontrollkästchen **Active Directory verwenden**.
  - Geben Sie den Benutzernamen im Feld **Active Directory-Benutzername** ein. Geben Sie den Benutzernamen in einem dieser Formate ein: `domain\username` oder `username@domain`. Der Benutzername ist auf 256 Zeichen beschränkt. Informationen zu Nutzernamen-Einschränkungen finden Sie in der **Dokumentation zum Microsoft Active Directory**.
  - Geben Sie das Kennwort ein.

- Um das Host-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.

5. Klicken Sie auf **Weiter**.
   Die Seite **Hosts auswählen** wird angezeigt.
6. Erweitern Sie auf der Seite **Hosts auswählen** die Strukturansicht, wählen Sie die Hosts aus, und klicken Sie dann auf **OK**.
   - Klicken Sie auf **HOST HINZUFÜGEN**, um Hosts auf der Seite **Zugeordnete Hosts** hinzuzufügen oder zu entfernen.
     ANMERKUNG: Fügen Sie keine PowerEdge MX-Server mit deaktiviertem iDRAC-IPv4 zu einem Host-Anmeldeinformationenprofil hinzu. Diese Server werden mit einem Gehäuse-Anmeldeinformationenprofil verwaltet.

   Die ausgewählten Hosts werden auf der Seite **Zugeordnete Hosts** angezeigt.
7. Um die Verbindung zu testen, wählen Sie einen oder mehrere Hosts aus und klicken Sie auf **TEST STARTEN**.
   Es wird empfohlen, dass Sie die Verbindung für alle konfigurierten Hosts testen.

   Während der Testverbindung aktiviert OMIVV den WBEM-Service und deaktiviert ihn dann nach dem Abrufen der iDRAC-IP-Adresse für Hosts, auf denen ESXi 6.5 und höher ausgeführt wird.

   ANMERKUNG: Nach der Eingabe gültiger Anmeldeinformationen kann es vorkommen, dass der Testverbindungsvorgang für den Host fehlschlägt und eine Meldung angezeigt wird, die darauf hinweist, dass ungültige Anmeldeinformationen eingegeben wurden. Dieses Problem tritt auf, wenn ESXi den Zugriff blockiert. Bei mehreren Anmeldeversuchen am ESXi mit den falschen Anmeldeinformationen wird Ihr Zugang zu ESXi 15 Minuten lang gesperrt. Warten Sie 15 Minuten und versuchen Sie den Vorgang erneut.

   - Um den Testverbindungsprozess zu beenden, klicken Sie auf **TEST ABBRECHEN**.

   Sie können die Ergebnisse der Testverbindung im Bereich **TESTERGEBNISSE** anzeigen.
8. Klicken Sie auf **Fertigstellen**.

Zugangsdatenprofil bearbeiten

Sie können die Anmeldeinformationen mehrerer Host-Zugangsdatenprofile gleichzeitig bearbeiten.

1. Führen Sie auf der Seite **Name und Anmeldeinformationen** folgende Schritte aus:
   a. Bearbeiten des Profilnamens und der Beschreibung.
   b. Bearbeiten Sie im Bereich **iDRAC-Anmeldeinformationen** die lokalen iDRAC-Anmeldeinformationen oder AD-Anmeldeinformationen.
      - Zum Konfigurieren der lokalen iDRAC-Anmeldeinformationen führen Sie die folgenden Tasks aus:
        - Ändern Sie den Nutzernamen im Feld **Nutzername**. Der Nutzername ist auf 16 Zeichen beschränkt.

          Informationen zur Definition von Nutzernamen finden Sie im *iDRAC-Benutzerhandbuch*, das unter **dell.com/support** verfügbar ist.
        - Ändern Sie das Kennwort.
        - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
      - Um die Anmeldeinformationen für einen iDRAC zu ändern, der bereits für AD konfiguriert und aktiviert ist, aktivieren Sie das Kontrollkästchen **Active Directory verwenden**.

        ANMERKUNG: Das iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware und die Bereitstellung eines Betriebssystems (BS).

        - Ändern Sie den Nutzernamen im Feld **Active Directory-Nutzername**.

          Geben Sie den Nutzernamen in einem dieser Formate ein: `domain\username` oder `username@domain`. Der Nutzername ist auf 256 Zeichen beschränkt. Weitere Informationen zur Definition von Nutzernamen finden Sie in der *Microsoft Active Directory-Dokumentation*.
        - Geben Sie das Kennwort ein.
        - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.

   c. Geben Sie im **Host-Stamm**-Bereich die lokalen Host-Anmeldeinformationen oder AD-Anmeldeinformationen ein.
      - Um die lokalen Host-Anmeldeinformationen einzugeben, führen Sie die folgenden Schritte durch:

        Der Standardnutzername lautet root.

        - Geben Sie das Kennwort ein.

          Das Host-Kennwort ist nur für Hosts erforderlich, auf denen ESXi 6.5 U3 und frühere Versionen ausgeführt werden.

          Um diesen Schritt für ESXi 6.7 und neuere Versionen zu überspringen, stellen Sie sicher, dass das Kontrollkästchen **Host-Anmeldeinformationen verwenden** deaktiviert ist. Wenn für einen Host, auf dem ESXi 6.7 oder höher ausgeführt wird, ein Kennwort eingegeben wurde, wird das Kennwort ignoriert.

          Für Hosts, auf denen ESXi 6.7 oder höherausgeführt werden, wird empfohlen, keine Anmeldeinformationen für ESXi einzugeben. OMIVV kann die iDRAC mit dem ESXi Host verbinden, selbst wenn falsche Host-Anmeldeinformationen eingegeben wurden.
      - Um die Anmeldeinformationen für Hosts zu ändern, die bereits für AD konfiguriert und aktiviert sind, aktivieren Sie das Kontrollkästchen **Active Directory verwenden**.
        - Ändern Sie den Nutzernamen im Feld **Active Directory-Nutzername**.

          Geben Sie den Nutzernamen in einem dieser Formate ein: `domain\username` oder `username@domain`. Der Nutzername ist auf 256 Zeichen beschränkt. Siehe
          Informationen zu Nutzernamen-Einschränkungen in der *Dokumentation zum Microsoft Active Directory*.
        - Ändern Sie das Kennwort.
      - Um das Host-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.

2. Klicken Sie auf **Weiter**.
   Die Seite **Zugeordnete Gehäuse** wird angezeigt.
3. Um die Hosts zur Liste der zugeordneten Hosts hinzuzufügen oder zu entfernen, klicken Sie auf der Seite **Zugeordnete Hosts** auf **HOST HINZUFÜGEN**.

   ANMERKUNG: Fügen Sie keine PowerEdge MX-Server mit deaktiviertem iDRAC-IPv4 zu einem Host-Zugangsdatenprofil hinzu. Diese Server werden mit einem Gehäuse-Zugangsdatenprofil verwaltet.

   Die ausgewählten Hosts werden auf der Seite **Zugeordnete Hosts** angezeigt.
4. Um die Verbindung zu testen, wählen Sie einen oder mehrere Hosts aus, und klicken Sie dann auf **TEST STARTEN**. Es wird empfohlen, dass Sie die Verbindung für alle konfigurierten Hosts testen.

ANMERKUNG: Nach der Eingabe gültiger Anmeldeinformationen kann es vorkommen, dass der Testverbindungsvorgang für den Host fehlschlägt und eine Meldung angezeigt wird, die darauf hinweist, dass ungültige Anmeldeinformationen eingegeben wurden. Dieses Problem tritt auf, wenn ESXi den Zugriff blockiert. Bei mehreren Anmeldeversuchen am ESXi mit den falschen Anmeldeinformationen wird Ihr Zugang zu ESXi 15 Minuten lang gesperrt. Warten Sie 15 Minuten und versuchen Sie den Vorgang erneut.

- Um die Testverbindung zu beenden, klicken Sie auf **TEST ABBRECHEN**.

Sie können die Ergebnisse der Testverbindung im Bereich **TESTERGEBNISSE** anzeigen.

Während der Testverbindung aktiviert OMIVV den WBEM-Service und deaktiviert ihn dann nach dem Abrufen der iDRAC-IP-Adresse für Hosts, auf denen ESXi 6.5 und höher ausgeführt wird.

5. Klicken Sie auf **Fertigstellen**.

ANMERKUNG: Die Felder „Änderungsdatum“ und „Zuletzt geändert von“ beinhalten Änderungen, die Sie über die vSphere Client-Benutzeroberfläche für ein Host-Zugangsdatenprofil vornehmen. Änderungen, die das OMIVV-Gerät auf dem entsprechenden Host-Zugangsdatenprofil vornimmt, haben keinen Einfluss auf diese beiden Felder.

Host-Zugangsdatenprofil anzeigen

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Host-Anmeldeinformationsprofil**.
   Eine Tabelle zeigt alle Host-Zugangsdatenprofile zusammen mit den folgenden Informationen an:
   - **Profilname**: Name des Host-Zugangsdatenprofils
   - **Beschreibung**: Beschreibung des Profils, falls angegeben
   - **vCenter**: FQDN oder Hostname bzw. IP-Adresse des zugehörigen vCenters
   - **Zugeordnete Hosts**: Die Hosts, die dem Host-Zugangsdatenprofil zugeordnet sind. Gibt es mehr als einen zugeordneten Host, können Sie alle über das Erweiterungssymbol anzeigen.
   - **iDRAC-Zertifikatsprüfung**: Zeigt an, ob das iDRAC-Zertifikat beim Erstellen eines Host-Zugangsdatenprofils überprüft wird.
   - **Host-Stamm-Zertifikatsüberprüfung**: Zeigt an, ob das Host-Root-Zertifikat beim Erstellen eines Host-Zugangsdatenprofils überprüft wird.
   - **Erstellungsdatum**: Datum, an dem das Host-Zugangsdatenprofil erstellt wurde.
   - **Änderungsdatum**: Datum, an dem das Host-Zugangsdatenprofil geändert wurde.
   - **Zuletzt geändert von**: Details des Benutzers, der das Host-Zugangsdatenprofil geändert hat.

   ANMERKUNG: Wenn der PowerEdge MX-Host über das Gehäuse-Zugangsdatenprofil verwaltet wird, zeigt die OMIVV ihn als einem Gehäuse-Zugangsdatenprofil zugeordnet an. Weitere Informationen finden Sie unter Gehäuse-Zugangsdatenprofil anzeigen auf Seite 46.
2. Wenn Sie die Spaltennamen aus dem Assistenten entfernen oder hinzufügen möchten, klicken Sie auf .
   Standardmäßig sind die Spalten **Änderungsdatum** und **Zuletzt geändert** nicht markiert. Um diese Spalten auszuwählen, klicken Sie auf das .
3. Um die Informationen der Host-Anmeldeinformationen-Profile zu exportieren, klicken Sie auf das .

Host-Zugangsdatenprofil testen

Mit der Funktion zum Testen des Zugangsdatenprofils können Sie die Host- und iDRAC-Anmeldeinformationen testen. Es wird empfohlen, alle Hosts auszuwählen.

1. Wählen Sie auf der OMIVV-Startseite ein Host-Zugangsdatenprofil mit zugehörigen Hosts aus und klicken Sie dann auf **TESTEN**.
   Die Seite **Host-Zugangsdatenprofil testen** wird angezeigt.
2. Wählen Sie alle zugehörigen Hosts aus und klicken Sie auf **TEST STARTEN**.
   a. Um die Testverbindung zu beenden, klicken Sie auf **TEST ABBRECHEN**.

   Testverbindungsergebnisse für die iDRAC- und Host-Anmeldeinformationen werden angezeigt.

Host-Zugangsdatenprofil löschen

Stellen Sie sicher, dass Sie kein Host-Zugangsdatenprofil löschen, das einem Host zugeordnet ist, wenn ein Job für die Bestandsaufnahme-/Serviceliste oder ein Bereitstellungsauftrag ausgeführt wird.

OMIVV verwaltet jedoch keine Hosts, die Bestandteil des Host-Zugangsdatenprofils sind, das Sie gelöscht haben, bis diese Hosts einem anderen Host-Zugangsdatenprofil hinzugefügt werden.

1. Wählen Sie auf der Seite **Host-Zugangsdatenprofil** ein Profil aus und klicken Sie auf **LÖSCHEN**.
2. Wenn Sie dazu aufgefordert werden, den Löschvorgang zu bestätigen, klicken Sie auf **LÖSCHEN**.
   Das ausgewählte Profil wird aus der Liste der Host-Zugangsdatenprofile entfernt.

5

Gehäuse mit Chassis-Zugangsdatenprofil verwalten

Gehäuse-Zugangsdatenprofil

Ein Gehäuse-Zugangsdatenprofil speichert die Gehäuse-Anmeldeinformationen, die OMIVV für die Kommunikation mit dem Gehäuse verwendet. OMIVV verwaltet und überwacht die Gehäuse, die einem Gehäuse-Zugangsdatenprofil zugewiesen sind. Sie können einem einzigen Gehäuse-Zugangsdatenprofil mehrere Gehäuse zuweisen.

Der PowerEdge MX-Gehäuse-Host kann mit einer einzigen einheitlichen Chassis-Management-IP verwaltet werden. Hosts in einem PowerEdge MX-Gehäuse mit deaktiviertem iDRAC IP müssen über ein Gehäuseprofil verwaltet werden. Um vollständige OMIVV-Funktionen zu erhalten, wird die Verwaltung von PowerEdge MX-Gehäuse-Hosts über eine iDRAC-IP mit Host-Zugangsdatenprofil empfohlen. Weitere Informationen zum Verwalten von MX-Gehäusen finden Sie unter PowerEdge MX Gehäuse verwalten auf Seite 116.

Gehäuse-Zugangsdatenprofil erstellen

- Um ein Gehäuse-Zugangsdatenprofil zu erstellen, müssen Sie über die folgenden Berechtigungen verfügen:
  - M1000e-, VRTX- und FX2-Gehäuse – SNMP-Trap-Ziel lesen und festlegen
  - PowerEdge MX-Gehäuse – Administrator
- Bevor Sie die Active Directory (AD)-Anmeldeinformationen mit einem Host-Anmeldeinformationen Profil verwenden, stellen Sie Folgendes sicher:
  - Das Nutzerkonto ist in AD vorhanden.
  - Der CMC oder OME-Modular müssen für die Ad-basierte Authentifizierung konfiguriert sein.
- Stellen Sie für PowerEdge MX-Gehäuse sicher, dass Sie über mindestens einen MX-Host im eingetragenen vCenter verfügen, damit die Testverbindung erfolgreich ist.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Gehäuse-Zugangsdatenprofil** > **NEUES PROFIL ERSTELLEN**.
2. Lesen Sie auf der Seite **Gehäuse-Zugangsdatenprofil** die Anweisungen und klicken Sie dann auf **ERSTE SCHRITTE**.
3. Führen Sie auf der Seite **Name und Anmeldeinformationen** folgende Schritte aus:
   a. Geben Sie den Profilnamen und eine Beschreibung an. Die Beschreibung ist optional.
   b. Geben Sie im Textfeld **Nutzername** den Nutzernamen mit Administratorrechten ein, der in der Regel für die Anmeldung am Chassis Management Controller (CMC) oder OpenManage Enterprise-Modular (OME-Modular) verwendet wird.
   c. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
   d. Geben Sie im Textfeld **Kennwort überprüfen** dasselbe Kennwort ein, das Sie im Textfeld **Kennwort** eingegeben haben. Die Kennwörter müssen übereinstimmen.
4. Wählen Sie auf der Seite **Gehäuse auswählen** ein einzelnes oder mehrere Gehäuse mithilfe der Kontrollkästchen neben der Spalte **IP/Hostname** und klicken Sie dann auf **OK**.
   Das ausgewählte Gehäuse wird auf der Seite **Zugeordnete Gehäuse** angezeigt. Klicken Sie zum Hinzufügen oder Entfernen des Gehäuses aus der zugehörigen Gehäuseliste auf **GEHÄUSE HINZUFÜGEN**.

   Wenn das ausgewählte Gehäuse bereits einem Gehäuse-Zugangsdatenprofil zugeordnet ist, wird die folgende Meldung angezeigt:

   Wenn Sie ein Gehäuse auswählen, das derzeit einem anderen Profil zugeordnet ist, wird das Gehäuse von diesem Gehäuse-Zugangsdatenprofil entfernt. Ein Gehäuse-Zugangsdatenprofil ohne zugeordnete Gehäuse wird gelöscht.

   Sie haben z. B. ein Profil Test, das Chassis A zugordnet ist. Wenn Sie ein anderes Profil, Test 1, erstellen und versuchen, Gehäuse A Test 1 zuzuordnen, wird eine Warnmeldung angezeigt.

   Das Testen der Verbindung wird für das ausgewählte Gehäuse automatisch ausgeführt.

Der Verbindungstest wird automatisch ausgeführt:

- Zum ersten Mal nach Auswahl des Gehäuses.
- Wenn die Anmeldeinformationen geändert werden
- Wenn das Gehäuse neu ausgewählt wurde

Das Testergebnis wird in der Spalte **Testergebnisse** als **Erfolgreich** oder **Fehlgeschlagen** angezeigt. Um die Konnektivität des Gehäuses manuell zu testen, wählen Sie das Gehäuse aus und klicken Sie auf **TEST STARTEN**.

Für ein mit einer MCM-Gruppe konfiguriertes PowerEdge MX-Gehäuse wird das Management aller Lead- und Mitgliedsgehäuse unter Verwendung des Lead-Gehäuses empfohlen. Der Verbindungstest für Mitgliedsgehäuse schlägt fehl, und der Testergebnisstatus wird als **Fehlgeschlagen** angezeigt. Der Link für die Hauptgehäuse-IP-Adresse wird angezeigt. Klicken Sie auf den IP-Link des Hauptgehäuses, um die gesamte MCM-Gruppe zu ermitteln.

5. Klicken Sie auf **FERTIGSTELLEN**.

   Stellen Sie sicher, dass Sie über mindestens ein erfolgreich überprüftes Gehäuse verfügen, um die Schritte des Assistenten abzuschließen. Nur erfolgreich geprüfte Gehäuse werden dem Gehäuse-Zugangsdatenprofil zugeordnet.

   Informationen zum Hinzufügen des PowerEdge MX-Gehäuses finden Sie unter PowerEdge MX Gehäuse hinzufügen auf Seite 117.

Gehäuse-Zugangsdatenprofil bearbeiten

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Gehäuse-Zugangsdatenprofil**.
2. Klicken Sie auf der Seite **Gehäuse-Anmeldeinformationsprofil** auf **BEARBEITEN**.
3. Führen Sie auf der Seite **Name und Anmeldeinformationen** folgende Schritte aus:
   a. Bearbeiten des Profilnamens und der Beschreibung. Die Beschreibung ist optional.
   b. Geben Sie im Textfeld **Nutzername** den Nutzernamen mit Administratorrechten ein, der in der Regel für die Anmeldung beim Chassis Management Controller (CMC) oder OpenManage Enterprise-Modular (OME-Modular) verwendet wird.
   c. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.

      Wenn Sie das Kennwortfeld leer lassen, berücksichtigt OMIVV das Kennwort, das während des Erstellungs-Workflows eingegeben wurde.
   d. Geben Sie im Textfeld **Kennwort überprüfen** dasselbe Kennwort ein, das Sie im Textfeld **Kennwort** eingegeben haben. Die Kennwörter müssen übereinstimmen.
4. Aktivieren oder entfernen Sie auf der Seite **Gehäuse auswählen** das Gehäuse mithilfe der Kontrollkästchen neben der Spalte **IP/Hostname** und klicken Sie dann auf **OK**.
   Das ausgewählte Gehäuse wird auf der Seite **Zugeordnete Gehäuse** angezeigt. Klicken Sie zum Hinzufügen oder Entfernen des Gehäuses aus der zugehörigen Gehäuseliste auf **GEHÄUSE HINZUFÜGEN**.

   Wenn das ausgewählte Gehäuse bereits einem Host-Zugangsdatenprofil zugeordnet ist, wird die folgende Meldung angezeigt:

   Wenn Sie ein Gehäuse auswählen, das derzeit einem anderen Profil zugeordnet ist, wird das Gehäuse von diesem Gehäuse-Zugangsdatenprofil entfernt. Ein Gehäuse-Zugangsdatenprofil ohne zugeordnete Gehäuse wird gelöscht.

   Sie haben z. B. ein Profil Test, das Chassis A zugordnet ist. Wenn Sie ein anderes Profil, Test 1, erstellen und versuchen, Gehäuse A Test 1 zuzuordnen, wird eine Warnmeldung angezeigt.

   Das Testen der Verbindung wird für das ausgewählte Gehäuse automatisch ausgeführt.

   Der Verbindungstest wird automatisch ausgeführt:

   - Zum ersten Mal nach Auswahl des Gehäuses.
   - Wenn die Anmeldeinformationen geändert werden
   - Wenn das Gehäuse neu ausgewählt wurde

   Das Testergebnis wird in der Spalte **Testergebnisse** als **Erfolgreich** oder **Fehlgeschlagen** angezeigt. Um die Konnektivität des Gehäuses manuell zu testen, wählen Sie das Gehäuse aus und klicken Sie auf **TEST STARTEN**.

   Für ein mit einer MCM-Gruppe konfiguriertes PowerEdge MX-Gehäuse empfiehlt Dell EMC die Verwaltung aller Führungs- und Mitgliedsgehäuse unter Verwendung des Hauptgehäuses. Der Vorgang des Verbindungstests für Mitgliedsgehäuse schlägt fehl und der Testergebnisstatus wird als Fehlgeschlagen angezeigt. Der Link für die Hauptgehäuse-IP-Adresse wird angezeigt. Klicken Sie auf den IP-Link des Hauptgehäuses, um die gesamte MCM-Gruppe zu ermitteln.

   ANMERKUNG: Wenn keine Hosts in den registrierten vCenters vorhanden sind, die dem hinzugefügten PowerEdge MX-Gehäuse zugeordnet sind, schlägt die Testverbindung für das Gehäuse fehl.
5. Klicken Sie auf **FERTIGSTELLEN**.

Stellen Sie sicher, dass Sie über mindestens ein erfolgreich überprüftes Gehäuse verfügen, um die Schritte des Assistenten abzuschließen. Nur erfolgreich geprüfte Gehäuse werden dem Gehäuse-Zugangsdatenprofil zugeordnet.

Informationen zum Hinzufügen eines PowerEdge MX-Gehäuses finden Sie unter PowerEdge MX Gehäuse hinzufügen auf Seite 117.

Gehäuse-Zugangsdatenprofil anzeigen

Nach dem Erstellen eines oder mehrerer Gehäuse-Zugangsdatenprofile können Sie das Gehäuse und die zugeordneten Gehäuse auf der Seite „Gehäuse-Zugangsdatenprofil“ anzeigen.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Gehäuse-Zugangsdatenprofil**.

   Eine Tabelle zeigt alle Gehäuse-Zugangsdatenprofile zusammen mit den folgenden Informationen an:

   - **Profilname**: Der Name des Gehäuse-Zugangsdatenprofils
   - **Beschreibung**: Die Beschreibung des Profils
   - **Gehäuse-IP/Hostname**: Der Link für die Gehäuse-IP-Adresse oder den Hostnamen.

     Für eine MCM-Gruppe (Multi-Chassis Management) werden das Lead-Gehäuse ( ) und die Mitgliedsgehäuse ( ) hierarchisch aufgelistet.

     ANMERKUNG: Für ein PowerEdge MX-Gehäuse in einer MCM-Konfiguration verwaltet OMIVV alle Lead- und Mitgliedsgehäuse nur unter Verwendung des Lead-Gehäuses. Alle Haupt- und Mitgliedsgehäuse sind demselben Gehäuse-Zugangsdatenprofil zugeordnet, dem das Hauptgehäuse zugeordnet ist.

     Für ein Mitgliedsgehäuse in der MCM-Gruppe (mit deaktiviertem IPv4) wird eine IPv4-Adresse des Lead-Gehäuses angezeigt. Die Service-Tag-Nummer des Mitgliedsgehäuses wird zudem in Klammern angezeigt.
   - **Gehäuse-Service-Tag-Nummer**: Die dem Gehäuse zugewiesene eindeutige Kennung.
   - **Änderungsdatum**: Datum, an dem das Gehäuse-Zugangsdatenprofil geändert wurde.
2. Die folgenden Informationen zu den zugeordneten Hosts werden in der oberen Tabelle angezeigt:

   - **Profilname**
   - **Zugeordnete Hosts**
   - **Service-Tag**
   - **Gehäuse-IP/Hostname**
   - **Service-Tag-Nummer des Gehäuses**
3. Um die Informationen des Gehäuse-Zugangsdatenprofils zu exportieren, klicken Sie auf das .

Gehäuse-Zugangsdatenprofil testen

Mithilfe der Funktion „Gehäuse-Zugangsdatenprofil testen“ können Sie die Zugangsdaten für ein Gehäuse testen, das dem Gehäuse-Zugangsdatenprofil zugeordnet ist. Es wird empfohlen, alle Gehäuse auszuwählen.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Gehäuse-Zugangsdatenprofil**.
2. Wählen Sie ein Gehäuse-Zugangsdatenprofil aus und klicken Sie auf **TESTEN**.
3. Wählen Sie auf der Seite **Gehäuse-Zugangsdatenprofil testen** das zugehörige Gehäuse aus und klicken Sie auf **TEST STARTEN**.
   a. Um die Testverbindung zu beenden, klicken Sie auf **TEST ABBRECHEN**.

   Das Testergebnis wird in der Spalte **Testergebnis** angezeigt.

Gehäuse-Zugangsdatenprofil löschen

Stellen Sie vor dem Löschen eines Gehäuse-Zugangsdatenprofils sicher, dass die Gehäuseinstanzen nicht Teil anderer vCenter sind, bei denen OMIVV registriert ist.

Wenn das Gehäuse-Zugangsdatenprofil gelöscht wird, überwacht OMIVV nicht die Gehäuse, die im gelöschten Gehäuse-Zugangsdatenprofil vorhanden sind, bis Sie das Gehäuse zu einem anderen Gehäuse-Zugangsdatenprofil hinzufügen.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Gehäuse-Zugangsdatenprofil** > **LÖSCHEN**.

2. Wählen Sie ein Gehäuse-Zugangsdatenprofil aus, das Sie löschen möchten.
3. Wenn Sie dazu aufgefordert werden, den Löschvorgang zu bestätigen, klicken Sie auf **LÖSCHEN**.

   Wenn alle einem Gehäuse-Zugangsdatenprofil zugeordneten Gehäuse entfernt oder zu anderen Profilen verschoben wurden, wird eine Bestätigungsmeldung über das Löschen angezeigt. Die Meldung weist darauf hin, dass das Gehäuse-Zugangsdatenprofil keine zugeordneten Gehäuse aufweist und gelöscht wird.

   Klicken Sie auf **OK**, um das Gehäuse-Zugangsdatenprofil zu löschen und die Bestätigungsmeldung zu erhalten.

6

Firmware- und Treiber-Repositorys mithilfe des Repository-Profils verwalten

Repository-Profil

Mit einem Repository-Profil können Sie Treiber- oder Firmware-Repositorys erstellen und verwalten.

Sie können die Profile für Firmware- und Treiber-Repository wie folgt verwenden:

- Aktualisieren der Firmware von Hosts
- Aktualisieren der Treiber von Hosts, die vSAN-Clustern angehören.
- Erstellen des Clusterprofils und der Baseline der Cluster.

Die standardmäßigen OMIVV-Firmware-Kataloge sind:

- **Dell EMC Standardkatalog**: Ein werkseitig erstelltes Firmware-Repository-Profil, das den Dell EMC Onlinekatalog verwendet, um die neuesten Firmware-Informationen zu beziehen. Wenn das Gerät keine Internetverbindung hat, ändern Sie dieses Repository, um auf eine lokale CIFS- oder NFS- bzw. HTTP- oder HTTPs-basierte Freigabe zu verweisen. Weitere Informationen zum Ändern dieses Katalogs finden Sie unter Dell Standardkatalog bearbeiten oder anpassen auf Seite 50.

  Sie können den Dell EMC Standardkatalog als Standardkatalog auswählen, um die Firmware der vSphere Hosts zu aktualisieren, die keinem Clusterprofil zugeordnet sind.
- **Validierter Katalog für MX-Stapel**: Ein werkseitig erstelltes Firmware-Repository-Profil, das den Dell EMC Onlinekatalog verwendet, um die validierten Firmware-Informationen für MX-Gehäuse und die zugehörigen Schlitten abzurufen. Weitere Informationen zum Ändern dieses Katalogs finden Sie unter Validierten MX-Stapel-Katalog bearbeiten auf Seite 50. Weitere Informationen zum validierten MX-Stapel-Katalog finden Sie im technischen Whitepaper unter MX7000-Firmwareaktualisierung.

  ANMERKUNG: Sie können den Dell EMC Standardkatalog und validierte MX-Stapel-Katalog-Repository-Profile nicht als Baseline der vSAN-Cluster verwenden.

Repository-Profil erstellen

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Profile** > **Repository-Profil**.
2. Lesen Sie auf der Seite **Repository-Profil** des Assistenten die Anweisungen und klicken Sie dann auf **ERSTE SCHRITTE**.
3. Geben Sie auf der Seite **Profilname und -beschreibung** den Profilnamen und die Beschreibung ein. Das Beschreibungsfeld ist optional und auf 255 Zeichen begrenzt.
4. Klicken Sie auf **WEITER**.
   Die Seite **Profileinstellungen** wird angezeigt.
5. Wählen Sie auf der Seite **Profileinstellungen** die Option **Firmware** oder **Treiber**.

   Folgendes gilt für das Treiber-Repository Profil:

   - Ein Treiber-Repository-Profil kann maximal 10 Treiber besitzen. Falls weitere Dateien vorhanden sind, ist die Auswahl des Treibers zufällig.
   - Es werden nur Offline-Treiberpakete (.zip-Dateien) verwendet.
   - Laden Sie die Offline-Treiber-Pakete (.zip-Dateien) herunter und geben Sie den vollständigen Pfad des Freigabespeicherorts an, um sie am Freigabespeicherort zu speichern. OMIVV erstellt automatisch den Katalog im Inneren des OMIVV-Geräts. Treiberpakete sind verfügbar unter https://my.vmware.com/web/vmware/downloads
   - OMIVV benötigt Schreibzugriff auf CIFS oder NFS.
   - Dateien in den Unterordnern werden ignoriert.
   - Dateien mit einer Größe von mehr als 10 MB werden ignoriert.
   - Das Treiber-Repository gilt nur für vSAN-Cluster.

6. Führen Sie im Bereich **Repository-Freigabespeicherort** folgende Schritte aus:
   a. Geben Sie den Repository-Freigabespeicherort an (NFS oder CIFS).
   b. Geben Sie bei CIFS die Anmeldeinformationen ein.

      OMIVV unterstützt nur Server Message Block(SMB)-Version 1.0- und SMB-Version 2.0-basierte CIFS-Freigaben.

      ANMERKUNG: Fügen Sie bei SMB-1.0-Freigaben, die als Treiber-Repository verwendet werden, das Dateitrennzeichen am Ende des Verzeichnispfades hinzu.

7. Klicken Sie auf **TEST STARTEN**, um den Katalogpfad und die Anmeldeinformationen zu validieren.

   Um die Erstellung eines Repository-Profils fortzusetzen, müssen Sie diesen Validierungsprozess abschließen.

   Die Ergebnisse der Testverbindung werden angezeigt.
8. Klicken Sie auf **WEITER**.
   Daraufhin wird die Seite **Mit Repository-Speicherort synchronisieren** angezeigt.
9. Klicken Sie auf **WEITER**.
   Die Seite **Zusammenfassung** wird angezeigt. Diese Seite zeigt die Informationen zum Repository-Profil an.
10. Klicken Sie auf **FERTIGSTELLEN**.
    Nach dem Erstellen des Katalogs werden der Download sowie das Parsen gestartet und der Status wird auf der Startseite des Repository-Profils angezeigt.

    Erfolgreich geparste Repository-Profile stehen während der Cluster-Profilerstellung und während der Firmwareaktualisierung zur Verfügung.

Repository-Profil bearbeiten

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Repository-Profil** > **BEARBEITEN**.
2. Bearbeiten Sie auf der Seite **Profilname und -beschreibung** den Profilnamen und die Beschreibung und klicken Sie dann auf **WEITER**.
3. Wählen Sie auf der Seite **Profileinstellungen** die Option **Firmware** oder **Treiber**.

   Folgendes gilt für das Treiber-Repository Profil:

   - Ein Treiber-Repository-Profil kann maximal 10 Treiber besitzen. Falls weitere Dateien vorhanden sind, ist die Auswahl des Treibers zufällig.
   - Es werden nur Offline-Treiberpakete (.zip-Dateien) verwendet.
   - Laden Sie die Offline-Treiber-Pakete (.zip-Dateien) herunter und geben Sie den vollständigen Pfad des Freigabespeicherorts an, um sie am Freigabespeicherort zu speichern. OMIVV erstellt automatisch den Katalog im Inneren des OMIVV-Geräts. Treiberpakete sind verfügbar unter https://my.vmware.com/web/vmware/downloads
   - OMIVV benötigt Schreibzugriff auf CIFS oder NFS.
   - Dateien in den Unterordnern werden ignoriert.
   - Dateien mit einer Größe von mehr als 10 MB werden ignoriert.
   - Das Treiber-Repository gilt nur für vSAN-Cluster.

4. Führen Sie im Bereich **Repository-Freigabespeicherort** folgende Schritte aus:
   a. Geben Sie den Repository-Freigabespeicherort an (NFS oder CIFS).
   b. Geben Sie bei CIFS die Anmeldeinformationen ein.

      ANMERKUNG: OMIVV unterstützt nur Server Message Block(SMB)-Version 1.0- und SMB-Version 2.0-basierte CIFS-Freigaben.

5. Klicken Sie auf **TEST STARTEN**, um den Katalogpfad und die Anmeldeinformationen zu validieren.

   Diese Validierung ist zwingend erforderlich, um fortzufahren.

   Die Ergebnisse der Testverbindung werden angezeigt.
6. Klicken Sie auf **WEITER**.
   Daraufhin wird die Seite **Mit Repository-Speicherort synchronisieren** angezeigt.
7. Aktivieren Sie auf der Seite **Mit Repository-Speicherort synchronisieren** das Kontrollkästchen **Mit Repository-Speicherort synchronisieren** und klicken Sie dann auf **WEITER**.
   Um nur den Profilnamen zu aktualisieren oder Informationen zu überprüfen, deaktivieren Sie das Kontrollkästchen **Mit Repository-Speicherort synchronisieren**, damit der Katalog in OMIVV unverändert bleibt. Weitere Informationen über „Mit Repository-Speicherort synchronisieren“ finden Sie unter Mit Repository-Speicherort synchronisieren auf Seite 50.
8. Überprüfen Sie die Profil-Informationen auf der Seite **Zusammenfassung** und klicken Sie dann auf **FERTIGSTELLEN**.

Dell Standardkatalog bearbeiten oder anpassen

1. Wählen Sie auf der Seite **Repository-Profil** die Option **Dell Standardkatalog**.
2. Bearbeiten Sie auf der Seite **Profilname und -beschreibung** die Profilbeschreibung und klicken Sie dann auf **WEITER**.
3. Wählen Sie im Abschnitt **Repository-Speicherort angeben** einen der folgenden Speicherorte aus:
   - **Dell Default Online**: Das Repository-Profil ist auf **Dell Online** festgelegt (`https://downloads.dell.com/catalog/Catalog.gz`). OMIVV verwendet Dell EMC Online als Quelle für Katalog- und Aktualisierungspakete.
   - **Custom Online**: OMIVV verwendet **Custom Online** (http oder HTTPS Share) als Quelle für Katalog- und Aktualisierungspakete. Wenn Sie ein benutzerdefiniertes Repository unter Verwendung des Server Update Utility (SUU) erstellen, stellen Sie sicher, dass die Signaturdatei für den Katalog (`catalog.xml.gz.sign`) im Katalogdatei-Ordner vorhanden ist.
   - **Freigegebener Netzwerkordner**: OMIVV verwendet den gemeinsam genutzten Netzwerkordner (CIFS oder NFS) als Quelle für Katalog- und Aktualisierungspakete.

   a. Wenn Sie **Custom Online** wählen, geben Sie den Onlinepfad für den Katalog ein.
   b. Wenn Sie **Freigegebener Netzwerkordner** ausgewählt haben, dann geben Sie den Speicherort der Katalogdatei ein (NFS oder CFS):
4. Klicken Sie auf **TEST STARTEN**, um den Katalogpfad und die Anmeldeinformationen zu validieren.
   Die Ergebnisse der Testverbindung werden angezeigt.
5. Aktivieren Sie auf der Seite **Mit Repository-Speicherort synchronisieren** das Kontrollkästchen **Mit Repository-Speicherort synchronisieren** und klicken Sie dann auf **WEITER**.
   Um nur den Profilnamen zu aktualisieren oder Informationen zu überprüfen, deaktivieren Sie das Kontrollkästchen **Mit Repository-Speicherort synchronisieren**, damit der Katalog in OMIVV unverändert bleibt. Weitere Informationen über „Mit Repository-Speicherort synchronisieren“ finden Sie unter Mit Repository-Speicherort synchronisieren auf Seite 50.
6. Überprüfen Sie die Profil-Informationen auf der Seite **Zusammenfassung** und klicken Sie dann auf **FERTIGSTELLEN**.

Validierten MX-Stapel-Katalog bearbeiten

1. Wählen Sie auf der Seite **Repository-Profil** die Option **Validierter MX-Stapel-Katalog** und klicken Sie dann auf **BEARBEITEN**.
2. Sie können nur Folgendes bearbeiten:
   a. die Katalogbeschreibung.
   b. Das Kontrollkästchen **Mit Repository-Speicherort synchronisieren**.

   Um nur den Profilnamen zu aktualisieren oder Informationen zu überprüfen, deaktivieren Sie das Kontrollkästchen **Mit Repository-Speicherort synchronisieren**, damit der Katalog in OMIVV unverändert bleibt. Weitere Informationen über „Mit Repository-Speicherort synchronisieren“ finden Sie unter Mit Repository-Speicherort synchronisieren auf Seite 50.

Mit Repository-Speicherort synchronisieren

Der Dell Standardkatalog und die validierten MX Stack-Repository-Profile prüfen automatisch alle 24 Stunden oder bei jedem Neustart, ob Änderungen durchgeführt wurden, und werden automatisch aktualisiert.

Um die Offline-Kataloge zu aktualisieren, führen Sie die folgenden Schritte aus:

1. Aktualisieren Sie den Katalog im Offlinespeicher (CIFS oder NFS) mit Dell EMC Repository Manager (DRM) oder Server Update Utility (SUU). Ersetzen Sie bei vorhandenen Treibern die Treiberpakete.
2. Bearbeiten Sie das Repository-Profil und aktivieren Sie das Kontrollkästchen **Mit Repository-Speicherort synchronisieren**, um Änderungen für die OMIVV zu erfassen. Dieser Vorgang dauert einige Minuten.
3. Um die Firmware in der Compliance-Baseline einer Konfiguration zu aktualisieren, stellen Sie sicher, dass Sie die jeweiligen Clusterprofile bearbeiten und speichern.

Repository-Profil anzeigen

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Repository-Profil**.
   Eine Tabelle zeigt alle Repository-Profile zusammen mit den folgenden Informationen an:
   - **Profilname**: Der Name des Repository-Profils
   - **Beschreibung**: Die Beschreibung des Profils

- **Typ**: Der Typ des Repositorys (Firmware oder Treiber)
- **Freigabepfad**: Der NFS-, CIFS-, HTTP- oder HTTPS-Pfad
- **Zuletzt erfolgreich aktualisierte Zeit**: Datum und Uhrzeit, an dem/zu der ein Repository-Profil aktualisiert wurde.
- **Status der letzten Aktualisierung**: Der Download- und Parsing-Status des Katalogs

2. Wenn Sie die Spaltennamen aus dem Assistenten entfernen oder hinzufügen möchten, klicken Sie auf .
3. Um die Repository-Profilinformationen zu exportieren, klicken Sie auf das .

Repository-Profil löschen

Stellen Sie vor dem Löschen eines Repository-Profils sicher, dass Sie die Zuweisung des Repository-Profils zu den zugehörigen Cluster-Profilen aufheben.

1. Wählen Sie auf der Seite **Repository-Profil** ein Repository-Profil aus und klicken Sie auf **LÖSCHEN**.
2. Klicken Sie im Dialogfeld zur Bestätigung des Löschvorgangs auf **LÖSCHEN**.

7

Basiskonfiguration mit Clusterprofil erfassen

Clusterprofil

Ein Clusterprofil ermöglicht Ihnen, die Konfigurations-Baseline wie (Hardwarekonfiguration, Firmware- oder Treiberversionen) zu erfassen und dann den erforderlichen Zustand für Cluster aufrechtzuerhalten, indem Sie alle Abweichungen von der Konfigurations-Baseline ermitteln.

Um ein Clusterprofil zu erstellen, stellen Sie sicher, dass Sie eines dieser Profile haben: Systemprofil, Firmware-Repository-Profil, Treiber-Repository-Profil oder eine Kombination davon. Es wird die Verwendung homogener Server (das gleiche Modell, die gleiche Hardwarekonfiguration und die gleiche Firmware-Stufe) für Baseline-Cluster empfohlen.

- Nachdem das Clusterprofil erstellt wurde, müssen die Firmware- und Treiber-Repository-Profile analysiert werden, bevor sie für die Erstellung eines Clusterprofils verwendet werden können.
- Nach der Erstellung des Clusterprofils wird ein aktueller Snapshot des zugehörigen Firmware- und Treiber-Repositorys für die Baseline erstellt. Wenn sich die Original-Repositorys ändern, muss das Clusterprofil erneut aktualisiert werden, um die Änderungen widerzuspiegeln. Andernfalls werden alle Aktualisierungen, die an den ursprünglichen Repositorys durchgeführt werden, nicht auf den Clusterprofil-Snapshots aktualisiert.
- Nachdem das Clusterprofil erstellt wird, löst es den Abweichungserkennung-Job aus.
- Wenn ein Cluster mit einem Clusterprofil verknüpft wird, werden etwaige vorherige Clusterprofil-Zuordnungen überschrieben.
- Wenn mehrere eigenständige vCenter in OMIVV registriert sind, wird empfohlen, getrennte Cluster-Profile für die einzelnen vCenter zu erstellen.
- Baselining von Treibern wird nur auf vSAN-Clustern unterstützt.

  ANMERKUNG: Die Treiber, die außerhalb von OMIVV installiert sind, kommen nicht für Baselines infrage.

Clusterprofil erstellen

Stellen Sie folgende Punkte sicher:

- Sie haben eines dieser Profile: Systemprofil, Firmware-Repository-Profil, Treiber-Repository-Profil oder eine Kombination davon.
- Der Cluster ist im vCenter vorhanden.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Profile** > **Clusterprofil** > **NEUES PROFIL ERSTELLEN**.
2. Lesen Sie auf der Seite **Clusterprofil** des Assistenten die Anweisungen und klicken Sie auf **ERSTE SCHRITTE**.
3. Geben Sie sie auf der Seite **Profilname und -beschreibung** den Profilnamen und die Beschreibung ein und klicken Sie auf **WEITER**. Profilnamen können bis zu 200 Zeichen, Beschreibungen bis zu 400 Zeichen enthalten.
4. Wählen Sie auf der Seite **Profil(e) zuordnen** eines der folgenden Profile oder seine Kombinationen aus:
   - Systemprofil: Durch die Auswahl eines Systemprofils wird die Konfigurations-Baseline für die Hosts im Cluster festgelegt. Für grundlegende und erweiterte Systemprofiltypen wird der Systemprofilname im folgenden Format angezeigt: Grundlegend_<Systemprofilname>, Erweitert_<Systemprofilname>
   - Firmware-Repository-Profil: Durch die Auswahl eines Firmware-Repositorys wird die Firmware oder BIOS-Baseline für die Hosts im Cluster erstellt. Online-Repositorys werden für die Erstellung von Baselines von vSAN-Clustern nicht unterstützt.
   - Treiber-Repository-Profil: Durch die Auswahl eines Treiber-Repository wird die Treiber-Baseline für die Hosts im Cluster erstellt. Sie können einer Baseline jeweils maximal 10 Treiber zuordnen. Baselining von Treibern wird nur auf vSAN-Clustern unterstützt.
5. Klicken Sie auf **WEITER**.
   Es wird die Seite **Cluster zuordnen** angezeigt.
6. Führen Sie auf der Seite **Cluster zuordnen** die folgenden Aufgaben aus:
   a. Wählen Sie eine Instanz eines registrierten vCenter-Servers aus.
   b. Klicken Sie auf **DURCHSUCHEN**, um die Cluster zuzuordnen.
   c. Wählen Sie den Cluster aus, für den Sie die Baseline erstellen möchten.

d. Klicken Sie auf **OK**.
Der/die ausgewählte(n) Cluster wird/werden auf der Seite **Cluster zuordnen** angezeigt.
e. Klicken Sie auf **WEITER**.

7. Wählen Sie auf der Seite **Abweichungserkennung planen** das Datum und die Uhrzeit aus, und klicken Sie dann auf **WEITER**.
Die **Zusammenfassung**-Seite wird angezeigt. Diese Seite enthält die Informationen zum Cluster-Profil.
8. Klicken Sie auf **FERTIGSTELLEN**.
Der Abweichungserkennungsjob wird sofort nach dem Speichern des Clusterprofils sowie später zur geplanten Zeit durchgeführt. Zeigen Sie den Fertigstellungs-Status des Jobs auf der Seite „Jobs“ an.

ANMERKUNG: Wenn die Anzahl der Nodes, die von OMIVV verwaltet werden, nach der Erstellung des Clusterprofils für ein Cluster geändert wird, wird die Erfassungsgröße automatisch während der nachfolgenden Abweichungserkennungs-Jobs aktualisiert.

Clusterprofil bearbeiten

Durch ein Bearbeiten von Cluster-Profilen wird die Baseline geändert, was dazu führen kann, dass die Compliance-Stufe neu berechnet wird.

Wenn das zugehörige Treiber-Repository oder Firmware-Repository oder das Systemprofil geändert wird und Sie die neuesten Änderungen für das Clusterprofil verwenden möchten, wählen Sie ein Clusterprofil aus, klicken Sie auf **BEARBEITEN**, klicken Sie im Assistenten auf **Weiter** und klicken Sie dann auf **Fertigstellen**.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Profile** > **Cluster-Profile**.
2. Wählen Sie ein Cluster-Profil aus und klicken Sie auf **BEARBEITEN**.
3. Bearbeiten Sie auf der Seite **Profilname und -beschreibung** die Beschreibung und klicken Sie dann auf **WEITER**.
4. Auf der Seite **Profil(e) zuordnen** können Sie die Profilkombinationen ändern.
5. Auf der Seite **Cluster zuordnen** können Sie die vCenter-Instanz und die zugehörigen Cluster ändern.
6. Auf der Seite **Abweichungserkennung planen** können Sie den Zeitplan für die Abweichungserkennung ändern.
7. Überprüfen Sie die aktualisierten Informationen auf der Seite **Zusammenfassung** und klicken Sie dann auf **FERTIGSTELLEN**.
Der Abweichungserkennungsjob wird sofort nach dem Speichern des Clusterprofils sowie später zur geplanten Zeit durchgeführt.

Clusterprofil anzeigen

1. Klicken Sie auf der OMIVV-Seite auf **Compliance und Bereitstellung** > **Profile** > **Clusterprofil**.
Eine Tabelle zeigt alle Clusterprofile zusammen mit den folgenden Informationen an:

   - **Profilname**: Der Name des Clusterprofils
   - **Beschreibung**: Die Beschreibung des Profils
   - **Zugehöriges Systemprofil**: Der zugehörige Systemprofilname. Für grundlegende und erweiterte Systemprofiltypen wird der Systemprofilname im folgenden Format angezeigt: Grundlegend_<Systemprofilname>, Erweitert_<Systemprofilname>
   - **Zugeordnetes Firmware-Repository-Profil**: Der Name des zugeordneten Firmware-Repository-Profils
   - **Zugeordnetes Treiber-Repository-Profil**: Der Name des zugeordneten Treiber-Repository-Profils

     ANMERKUNG: Bei einem PowerEdge MX-Host, der mit einem Gehäuse-Zugangsdatenprofil verwaltet wird, wird die Konfigurationsabweichung nicht berechnet.
   - **vCenter**: Die mit dem Clusterprofil verknüpfte vCenter-Instanz
   - **Letzte erfolgreiche Aktualisierung**: Datum und Uhrzeit, zu dem/der ein Repository-Profil aktualisiert wurde.

   ANMERKUNG: Wenn das zugehörige Repository-Profil (Firmware oder Treiber) oder Systemprofil aktualisiert wird, wird ein Warnsymbol beim Profilnamen angezeigt. Das Clusterprofil muss aktualisiert werden, nachdem ein Repository oder Systemprofil geändert wurde, um die Änderungen in der Baseline zu aktualisieren. Weitere Informationen zur Aktualisierung des Clusterprofils finden Sie unter Clusterprofil aktualisieren auf Seite 54.
2. Wenn Sie die Spaltennamen aus dem Assistenten entfernen oder hinzufügen möchten, klicken Sie auf .
3. Um die Cluster-Profilinformationen zu exportieren, klicken Sie auf das .

Clusterprofil aktualisieren

Wenn Sie das Repository-Profil (Firmware oder Treiber) und das Systemprofil aktualisieren, wird auf der Seite „Clusterprofil“ ein Warnsymbol mit dem Profilnamen angezeigt. Das Aktualisieren der Profile wirkt sich möglicherweise auf die Konfigurations-Compliance der zugehörigen Cluster im Clusterprofil und Firmware-Compliance-Status in vSphere Lifecycle Manager aus. Sie können die Funktion **Profile aktualisieren** für die Aktualisierung oder das Baselining des Clusterprofils verwenden.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Profile** > **Clusterprofile**.
2. Wählen Sie ein Clusterprofil mit Warnsymbol beim Profilnamen aus.
3. Klicken Sie auf **PROFILE AKTUALISIEREN**.
4. Um die zugehörigen Profile auf die neueste Version zu aktualisieren, klicken Sie auf **OK**.

   Nach dem Aktualisieren der Profile kann die Baseline nicht zurückgesetzt werden.

   Das Warnsymbol wird nicht mehr angezeigt, wenn das Clusterprofil mit den aktualisierten Repository-Profilen oder dem Systemprofil synchronisiert wird.

Clusterprofil löschen

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Profile** > **Cluster-Profile**.
2. Wählen Sie ein Clusterprofil aus und klicken Sie dann auf **LÖSCHEN**.
3. Klicken Sie im Dialogfeld zur Bestätigung des Löschvorgangs auf **LÖSCHEN**.
   Wenn das Clusterprofil gelöscht wird, wird auch der entsprechende Treiber-Erkennungsjob gelöscht.

8

Bare-Metal-Server verwalten

Bare-Metal-Server anzeigen

Auf der Seite **Bare-Metal-Server** können Sie Folgendes tun:

- Die Bare-Metal-Server anzeigen, die mithilfe der automatischen und der manuellen Ermittlung erkannt wurden.

  Die Informationen wie z. B. **Service-Tag-Nummer**, **Modellname**, **iDRAC-IP**, **Server-Status**, **Systemsperrmodus**, **Compliance-Status** und **iDRAC-Lizenzstatus** werden angezeigt.

  Im Folgenden werden die verschiedenen Status der Bare-Metal-Server aufgeführt:

  - **Nicht konfiguriert**: Der Server wird zu OMIVV hinzugefügt und wartet auf die Konfiguration.
  - **Konfiguriert**: Der Server wurde mit allen Hardwareinformationen konfiguriert, die für eine erforderliche Betriebssystem-Bereitstellung erforderlich sind.
  - **In Quarantäne**: Die Server können keine Aufgaben wie Betriebssystem-Bereitstellung und Firmwareaktualisierung durchführen, da die Server von den OMIVV-Aktionen ausgeschlossen sind.
- Zeigen Sie den Compliance-Status der Bare-Metal-Server an.

  Ein Bare-Metal-Server ist nicht konform, wenn:

  - Er kein unterstützter Server ist.
  - Er nicht über eine unterstützte iDRAC-Lizenz verfügt (iDRAC Express ist die Mindestanforderung).
  - Auf ihm keine unterstützten Versionen von iDRAC, BIOS oder LC installiert sind.
  - LOM oder NIC nicht vorhanden ist.
  - Der Systemsperrmodus ist eingeschaltet.
- Um weitere Informationen zum Compliance-Problem anzuzeigen, klicken Sie im unteren horizontalen Bereich auf **DETAILS**.

Auf der Seite **Bare-Metal Server** können Sie auch folgende Aufgaben ausführen:

- Manuelle Ermittlung von Bare-Metal-Servern
- Bare-Metal-Server entfernen
- Bereitstellung eines Systemprofils und ISO-Profils
- Bare-Metal-Server aktualisieren
- iDRAC-Lizenz erwerben oder erneuern

Geräteerkennung

Die „Erkennung“ ist der Prozess zum Hinzufügen unterstützter Bare-Metal-Server. Nachdem ein Server erkannt wurde, können Sie ihn zur Bereitstellung das Systemprofils und des ISO-Profils verwenden. Weitere Informationen zur Liste der unterstützten Server finden Sie in der *OpenManage Integration for VMware vCenter Compatibility Matrix* (OpenManage Integration for VMware vCenter-Kompatibilitätsmatrix).

Voraussetzungen:

- Es ist eine Netzwerkverbindung vom iDRAC des Bare-Metal-Servers zur virtuellen OMIVV-Maschine erforderlich.
- Hosts mit bereits vorhandenem Betriebssystem sollten nicht in OMIVV erkannt, sondern zum vCenter hinzugefügt werden. Fügen Sie sie einem Host-Zugangsdatenprofil hinzu.
- Stellen Sie zur Bereitstellung des Betriebssystems auf der SD-Karte und zur Verwendung von Systemprofil-Funktionen in 12G und 13G PowerEdge-Servern sicher, dass iDRAC 2.50.50.50 oder höher installiert ist.

Auto-Ermittlung

Automatische Ermittlung ist der Prozess zum Hinzufügen von Bare-Metal-Servern. Wenn ein Server ermittelt wurde, verwenden Sie ihn zur Bereitstellung von Betriebssystem und Hardware. Die automatische Erkennung ist eine iDRAC-Funktion, die das manuelle Ermitteln von Bare-Metal-Servern über OMIVV unnötig macht.

Voraussetzungen für Auto Discovery (Automatische Ermittlung)

Bevor Sie versuchen, PowerEdge Bare-Metal-Server zu erkennen, stellen Sie sicher, dass OMIVV installiert ist. PowerEdge-Server mit iDRAC Express oder iDRAC Enterprise können in Bare-Metal-Serverpools aufgenommen werden. Stellen Sie sicher, dass eine Netzwerkverbindung vom iDRAC des Dell EMC Bare-Metal-Servers zum OMIVV-Gerät besteht.

ANMERKUNG: Die Hosts mit vorhandenen Betriebssystemen sollten nicht unter Verwendung von OMIVV ermittelt werden, stattdessen fügen Sie das Betriebssystem zu einem Host-Zugangsdatenprofil hinzu.

Damit eine automatische Ermittlung stattfinden kann, müssen die folgenden Voraussetzungen erfüllt sein:

- Strom – Schließen Sie den Server an die Stromversorgung an. Der Server muss nicht eingeschaltet werden.
- Netzwerkverbindung – Stellen Sie sicher, dass der iDRAC des Servers über eine Netzwerkverbindung verfügt und mit dem Bereitstellungsserver über Port 4433 kommuniziert. Sie erhalten die IP-Adresse des Bereitstellungsservers, indem Sie einen DHCP-Server verwenden oder diese manuell im iDRAC-Konfigurationshilfsprogramm angeben.
- Zusätzliche Netzwerkeinstellungen – Zum Auflösen des DNS-Namens aktivieren Sie „DNS-Server-Adresse anfordern“ in „DHCP-Einstellungen“.
- Speicherort des Bereitstellungsdienstes – Dem iDRAC muss die IP-Adresse oder der Hostname des Servers mit dem Bereitstellungsdienst bekannt sein. Siehe Speicherort des Bereitstellungsdienstes.
- Kontozugriff deaktiviert – Wenn iDRAC-Konten mit Administratorrechten vorhanden sind, deaktivieren Sie diese zunächst über die iDRAC-Webkonsole. Nachdem die automatische Ermittlung erfolgreich abgeschlossen wurde, wird das Administrator-iDRAC-Konto mit Anmeldeinformationen für die Bereitstellung, die auf der Seite **Einstellungen** eingegeben wurden, erneut aktiviert. Weitere Informationen zu den Bereitstellungs-Anmeldeinformationen finden Sie unter Konfigurieren von Anmeldeinformationen für die Bereitstellung auf Seite 86.
- Autom. Ermittlung aktiviert – Auf dem iDRAC des Servers muss die Funktion für die automatische Ermittlung aktiviert sein, damit die automatische Ermittlung starten kann. Weitere Informationen finden Sie unter Verwaltungskonten auf iDRAC aktivieren und deaktivieren auf Seite 56.

Bereitstellen von Dienstidentifizierung

Verwenden Sie die folgenden Optionen zum Abrufen des Speicherorts des Bereitstellungsdienstes vom iDRAC während der automatischen Ermittlung:

- Manuell im iDRAC angegeben – Geben Sie manuell den Speicherort in das iDRAC-Konfigurationsdienstprogramm unter LAN-Nutzerkonfiguration, Bereitstellungsserver an.
- DHCP-Bereichsoption – Geben Sie den Speicherort unter Verwendung einer DHCP-Bereichsoption an.
- DNS-Diensteintrag – Geben Sie den Speicherort durch Verwendung eines DNS-Diensteintrags an.
- DNS-bekannter Name – DNS-Server gibt die IP-Adresse für einen Server mit dem bekannten Namen DCIMCredentialServer an.

Wenn der Wert des Bereitstellungsdienstes nicht manuell im iDRAC-Konfigurationsdienstprogramm angegeben wird, versucht der iDRAC, den Wert der DHCP-Bereichsoption zu verwenden. Wenn die DHCP-Bereichsoption nicht vorhanden ist, versucht der iDRAC, den Wert des DNS-Diensteintrags zu verwenden.

Ausführliche Informationen zum Konfigurieren der DHCP-Bereichsoption und des DNS-Leistungssatzes finden Sie im Dokument „Dell Auto-Discovery Network Setup Specification“ unter https://www.dell.com/support.

Verwaltungskonten auf iDRAC aktivieren und deaktivieren

Deaktivieren Sie vor dem Einrichten der AutoErmittlung alle iDRAC-Konten, mit Ausnahme eines Kontos, das nicht über Administratorzugriff verfügt. Nach der AutoErmittlung können Sie alle Konten außer dem Root-Konto aktivieren.

ANMERKUNG: Vor der Deaktivierung der Administratorberechtigung wird empfohlen, in iDRAC ein Nicht-Administrator-Nutzerkonto zu erstellen.

1. Geben Sie die **iDRAC-IP-Adresse** in einen Browser ein.
2. Melden Sie sich an der **GUI von Integrated Dell Remote Access Controller** an.
3. Führen Sie einen der folgenden Schritte aus:
   - Bei iDRAC7: Wählen Sie im linken Fenster die Registerkarte **iDRAC Einstellungen** > **Nutzer-Authentifizierung** > **Nutzer**.
   - Bei iDRAC8: Wählen Sie im linken Fenster die Registerkarte **iDRAC Einstellungen** > **Nutzer-Authentifizierung** > **Nutzer**.
   - Für iDRAC9: gehen Sie zu **iDRAC Einstellungen** > **Nutzer** > **Lokale Nutzer**.
4. Machen Sie im Register **Lokale Nutzer** alle Verwaltungskonten ausfindig, bei denen es sich nicht um das Stammkonto handelt.
5. Wählen Sie zum Deaktivieren eines Kontos unter „Nutzer-ID“ die entsprechende **ID** aus.
6. Klicken Sie auf **Weiter**.
7. Heben Sie auf der Seite **Benutzerkonfiguration** unter **Allgemein** die Markierung des Kontrollkästchens **Nutzer aktivieren** auf.
8. Klicken Sie auf **Anwenden**.
9. Nachdem Sie die AutoErmittlung erfolgreich eingerichtet haben, müssen Sie die einzelnen Konten wieder aktivieren. Wiederholen Sie dazu die Schritte 1 bis 8, wobei Sie jedoch diesmal das Kontrollkästchen **Nutzer aktivieren** markieren und anschließend auf **Anwenden** klicken.

PowerEdge-Server manuell für die automatische Ermittlung konfigurieren

Stellen Sie sicher, dass Sie über eine iDRAC-Adresse verfügen.

Bei der Bestellung von Dell EMC Servern können Sie darum bitten, dass die Funktion zum automatischen Erkennen auf den Servern aktiviert wird, nachdem Sie die IP-Adresse des Bereitstellungsservers übermittelt haben. Die IP-Adresse des Bereitstellungsserver muss die IP-Adresse des OMIVV sein. Die Server werden nach der Lieferung von Dell EMC und Montage und Verbindung des iDRAC-Kabels beim ersten Einschalten automatisch erkannt und auf der Seite **Bare-Metal-Server** angezeigt.

ANMERKUNG: Für automatisch erkannte Server werden die Anmeldeinformationen unter **Einstellungen** > **Geräteeinstellungen** > **Anmeldeinformationen für die Bereitstellung** als Administrator-Anmeldeinformationen gesetzt und zur weiteren Kommunikation mit dem Server verwendet, bis die Bereitstellung des Betriebssystems abgeschlossen ist. Nach einer erfolgreichen Bereitstellung des Betriebssystems werden die im zugehörigen Host-Zugangsdatenprofil bereitgestellten iDRAC-Anmeldeinformationen festgeschrieben.

Um die automatische Ermittlung manuell auf dem Ziel-Computer zu aktivieren, führen Sie die folgenden Schritte für Server der 12. Generation und später durch:

1. Drücken Sie auf dem Zielsystem während des anfänglichen Starts die Taste F2.
2. Gehen Sie zu **iDRAC-Einstellungen** > **Benutzerkonfiguration**, und deaktivieren Sie den Root-Nutzer. Stellen Sie bei der Deaktivierung des Root-Benutzers sicher, dass keine anderen Nutzer mit aktiven Administratorrechten auf der iDRAC-Adresse vorhanden sind.
3. Klicken Sie auf **Zurück** und dann auf **Remote-Aktivierung**.
4. Stellen Sie **Auto-Ermittlung aktivieren** auf **Aktiviert**, und legen Sie den **Provisioning Server** als IP-Adresse der OMIVV fest.
5. Speichern Sie die Einstellungen.
   Der Server wird beim nächsten Serverstart automatisch erkannt. Nach der erfolgreichen automatischen Ermittlung wird der Root-Nutzer aktiviert, und das Kontrollkästchen **Auto-Ermittlung aktivieren** wird automatisch deaktiviert.

Manuelle Ermittlung von Bare-Metal-Servern

Stellen Sie sicher, dass für die Ermittlung ein iDRAC Nutzer mit Administratorberechtigungen verwendet wird.

OMIVV ermöglicht es Ihnen, die Server basierend auf einem IPv4-Bereich manuell zu ermitteln. Sie können eine einzelne IP-Adresse oder eine Gruppe von IPs mithilfe der IPv4-basierten Bereiche ermitteln.

Nachdem der Bare-Metal-Server hinzugefügt wurde, wird er in der Liste der Server auf der Seite **Bare-Metal-Server** angezeigt.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Bereitstellung** > **ERMITTELN**.
   Die Seite **Bare-Metal-Server ermitteln** wird angezeigt.

2. Führen Sie auf der Seite **Bare-Metal-Server ermitteln** die folgenden Aufgaben aus:
   a. Geben Sie in das Feld **Jobname ermitteln** einen Jobnamen ein.
   b. Geben Sie eine Beschreibung ein (optional).
   c. Um IP-Bereiche einzugeben, klicken Sie auf **BEREICHSDATEN HINZUFÜGEN**.

      In jedem Ermittlungs-Job können mehrere Bereiche angegeben werden. Es werden maximal 1024 IPs unterstützt. Die maximale Anzahl von IP-Adressen, die in einem Bereich konfiguriert werden können, ist 256.

      Die eingeschlossenen IPs haben Vorrang, wenn Sie bestimmte IP-Adressen in die Ausschlussliste eines Bereichs hinzufügen und dann die gleichen IPs in der Einschlussliste eines anderen Bereichs hinzufügen.
   d. Geben Sie die **Start-IP** ein.

      Die Start-IP-Adresse muss das Format einer IPv4-Adresse aufweisen.
   e. Geben Sie die **End-IP** ein.

      Die End-IP-Adresse muss das letzte Oktett der IP und größer als die Start-IP-Adresse sein.
   f. Geben Sie die **Ausschlussliste** ein.

      Die Ausschlussliste ist die Liste der IP-Adressen, die Sie aus der Liste ausschließen möchten.

      Der in der **Ausschlussliste** eingegebene Wert muss zwischen den **Start-IP** und **End-IP** Bereichen liegen. Die Werte müssen durch Kommas getrennt werden. Jeder Wert kann ein letzter Oktett-Wert sein oder ein Bereich der letzten Oktett-Werte getrennt durch –.

      Beispiel:

      Um alle IPS von 100.100.100.1 bis 100.100.100.50 außer IPS von 100.100.100.25 bis 100.100.100.30 und von 100.100.100.40 bis 100.100.100.45 zu ermitteln, geben Sie Folgendes in **Start-IP**, **End-IP** und **Ausschlussliste** ein.

      Start-IP: 100.100.100.1

      End-IP: 50

      Ausschlussliste: 25 bis 30, 40 bis 45
   g. Um die iDRAC Anmeldeinformationen zu verwenden, die auf der Seite **Bereitstellungs-Zugangsdaten** eingegeben wurden, markieren Sie das Kontrollkästchen **Bereitstellungs-Zugangsdaten verwenden**.

      Weitere Informationen zu den Bereitstellungs-Anmeldeinformationen finden Sie unter Konfigurieren von Anmeldeinformationen für die Bereitstellung auf Seite 86.
   h. Geben Sie den Nutzernamen und das Kennwort ein, wenn keine Zugangsdaten festgelegt sind.

      Standardmäßig sind die Zugangsdaten für die Bereitstellung festgelegt. Geben Sie den iDRAC-Nutzernamen und das Kennwort ein, wenn Sie andere als die Zugangsdaten für die Bereitstellung verwenden möchten. Sie können separate Zugangsdaten für jeden Bereich haben.

      Der Nutzername muss zwischen 1 und 16 Zeichen lang sein. Die Sonderzeichen /, \, ~ und ' werden nicht unterstützt.

      Kennwörter dürfen aus maximal 42 Zeichen bestehen.
3. Wählen Sie aus den folgenden Optionen aus:
   - **JETZT AUSFÜHREN**: Durch die Ausführung des Jobs werden jetzt alle IPs, die innerhalb des angegebenen Bereichs liegen, ermittelt.
   - **SPÄTER AUSFÜHREN**: Durch das Planen des Jobs zur späteren Ausführung werden dann die IPs innerhalb des angegebenen Bereichs ermittelt.
4. Klicken Sie auf **ANWENDEN**.
   Der Status des Ermittlungs-Jobs wird auf der Seite **Ermittlungs-Jobs** angezeigt. Weitere Informationen finden Sie unter Ermittlungs-Jobs auf Seite 77.

Bare-Metal-Server entfernen

Sie können einen Server manuell entfernen, der automatisch ermittelt oder manuell hinzugefügt wurde.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Bereitstellung** > **LÖSCHEN**.
2. Wählen Sie einen Bare-Metal-Server aus und klicken Sie dann auf **OK**.

Bare-Metal-Server aktualisieren

Der Aktualisierungsvorgang ermittelt die Bare-Metal-Server erneut, indem er eine Verbindung zu iDRAC herstellt und die grundlegende Bestandsaufnahme erfasst.

ANMERKUNG: Wenn Sie den Aktualisierungsvorgang auf den „konfigurierten“ Bare-Metal-Servern durchführen, ändert sich der Status des Servers in den Status „Nicht konfiguriert“, da der Aktualisierungsvorgang den Server erneut erkennt.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Profile** > **AKTUALISIEREN**.
2. Wählen Sie auf der Seite **Bare-Metal-Server aktualisieren** einen Server aus und klicken Sie auf **OK**.
   Die Aktualisierung von Bare-Metal-Server-Daten dauert u. U. einige Minuten. Während der Vorgang ausgeführt wird, können Sie die Seite **Bare-Metal-Server aktualisieren** schließen; der erneute Ermittlungsprozess wird im Hintergrund fortgesetzt. Der neu ermittelte Server wird auf der Seite **Bare-Metal-Server** angezeigt.

iDRAC-Lizenz erwerben oder erneuern

Der Status der Bare-Metal-Server wird als nicht konform angezeigt, wenn Sie nicht über eine kompatible iDRAC-Lizenz verfügen. Eine Tabelle zeigt den Status der iDRAC-Lizenz an. Wählen Sie einen nicht konformen Bare-Metal-Server aus, um weitere Informationen über die iDRAC-Lizenz anzuzeigen.

1. Um die iDRAC-Lizenz zu erneuern, klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Bereitstellung**.
2. Wählen Sie einen Bare-Metal-Server aus, dessen iDRAC-Lizenz nicht konform ist, und klicken Sie auf **IDRAC-LIZENZ ERNEUERN/ ERWERBEN**.
3. Melden Sie sich bei Dell Digital Locker an, und aktualisieren oder erwerben Sie eine neue iDRAC-Lizenz.
4. Nachdem Sie eine iDRAC-Lizenz installiert haben, klicken Sie auf **AKTUALISIEREN**.

9

Bereitstellungsprofile verwalten

Systemprofil

Das Systemprofil erfasst die Einstellungen und Konfigurationen von iDRAC, BIOS, RAID, Ereignisfiltern, FC und NICs auf Komponentenebene. Diese Konfigurationen können während einer Betriebssystem-Bereitstellung auf Bare-Metal-Servern auf andere identische Server angewendet werden. Das Systemprofil kann im Clusterprofil verwendet werden, um die Baseline für die Konfiguration beizubehalten.

Voraussetzungen

Bevor Sie das Systemprofil erstellen oder bearbeiten, stellen Sie Folgendes sicher:

- Die CSIOR-Funktion ist auf dem Referenzserver aktiviert. Der Referenzserver muss nach der Aktivierung von CSIOR neu gestartet werden, damit die von iDRAC zurückgegebenen Daten auf dem neuesten Stand sind.
- Die Bestandsaufnahme ist für jeden Referenz-Host erfolgreich, der von vCenter gemanagt wird.
- Auf Bare-Metal-Servern sind die erforderlichen BIOS- und Firmware-Mindestversion installiert. Weitere Informationen finden Sie in der *OMIVV-Kompatibilitätsmatrix*, die auf der Support-Website verfügbar ist.
- Der Referenzserver und die Zielserver sind homogen (dasselbe Modell, dieselbe Hardwarekonfiguration und dieselbe Firmwareebene).
- Die Hardware (z. B. FC, NIC und RAID-Controller) ist in den identischen Steckplätzen des Referenzservers und der Zielserver vorhanden.
- Bevor Sie ein Attribut in die Standardauswahl aufnehmen oder ausschließen, halten Sie den Mauszeiger über den Attributnamen, um die Details des Attributs zu verstehen.
- Der iDRAC-Nutzer, der zur Ermittlung des iDRAC verwendet wird, wird bei der Konfiguration der iDRAC-Nutzer im Systemprofil ausgewählt.

  ANMERKUNG: Deaktivieren Sie nicht die Attribute, die mit dem iDRAC-Nutzer verknüpft sind, der zur Ermittlung des Bare-Metal-Servers verwendet wird, andernfalls schlägt der Bereitstellungsjob für das Systemprofil fehl.
- Sie können den Nutzernamen des iDRAC-Benutzers, der zur Ermittlung des iDRAC verwendet wird, nicht ändern. Dies führt zu Verbindungsproblemen mit iDRAC, der Bereitstellungsjob des Systemprofils schlägt fehl, ohne Attribute anzuwenden.

Bevor Sie das Systemprofil erstellen, wird empfohlen, dass Sie Attribut und Wert des Referenzservers nach Bedarf konfigurieren. Wenden Sie Referenzattribut und -wert auf alle erforderlichen Zielhosts an.

Die Systemprofile suchen nach der genauen Instanz (FQDD) bei der Anwendung des Profils. Dies funktioniert auf Rack-Servern (identisch), hat jedoch evtl. bei modularen Servern einige Einschränkungen. Beim FC640 können beispielsweise die von einem modularen Server erstellten Systemprofile aufgrund von NIC-Level-Einschränkungen nicht auf anderen modularen Servern im selben FX-Gehäuse angewendet werden. In diesem Fall empfiehlt sich die Nutzung eines Referenzsystemprofils für jeden Steckplatz des Gehäuses. Wenden Sie diese Systemprofile nur für die entsprechenden Steckplätze des Gehäuses an.

ANMERKUNG: Ein Systemprofil unterstützt das Aktivieren bzw. Deaktivieren der Startoptionen nicht.

ANMERKUNG:

- Bei Verwendung des Systemprofils schlägt der Export eines Systemprofils mit einer Unternehmenslizenz und Import des gleichen Systemprofils auf Servern mit Express-Lizenz fehl.
- Systemprofile können nicht mit einer Express-Lizenz der iDRAC9 Firmware 3.00.00.00 importiert werden. Sie benötigen hierzu eine Enterprise-Lizenz.

Systemprofil erstellen

Es wird empfohlen, Google Chrome zu verwenden, um Systemprofile zu erstellen oder zu bearbeiten.

Die PowerEdge-Server R6515, R7515, R65125, R7525 und C6515, die über ein Slimline-Kabel mit HBA, BOSS und PERC verbunden sind. Das Systemprofil, das in OMIVV mit einer iDRAC-Version vor 4.30.30.30 erstellt wurde, kann nicht für iDRAC 4.30.30.30 und neuere Versionen verwendet werden. Erstellen Sie ein neues Systemprofil mit iDRAC 4.30.30.30 oder höher, und verwenden Sie es bei Bedarf.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Profile** > **Systemprofil** > **NEUES PROFIL ERSTELLEN**.
2. Lesen Sie auf der Seite **Systemprofil erstellen** des Assistenten die Anweisungen durch und klicken Sie dann auf **ERSTE SCHRITTE**.
3. Führen Sie auf der Seite **Name und Beschreibung** folgende Schritte aus:
   a. Geben Sie den Profilnamen und eine Beschreibung an. Die Beschreibungsfeld ist ein optionales Feld.
   b. Wählen Sie einen der folgenden Systemprofiltypen aus:
      - **Basis**: Zeigt den minimalen Satz von Attributen für iDRAC, BIOS, RAID, NIC und FC an.
      - **Erweitert**: Zeigt alle Attribute für iDRAC, BIOS, RAID, NIC, FC und EventFilters an.
4. Klicken Sie zum Auswählen eines Referenzservers, der entweder ein Host- oder ein Bare-Metal-Server ist, auf der Seite **Referenzserver** auf **AUSWÄHLEN**.

   Die Serverauswahl ist möglicherweise aus einem der folgenden Gründe deaktiviert:

   - Der Server ist entweder ein nicht konformer Host oder Bare-Metal-Server.
   - Ein Bereitstellungs-Job ist entweder geplant oder läuft auf dem Server.
   - Der Server wird mit dem Gehäuse-Zugangsdatenprofil verwaltet.

   Das Dialogfeld **Bestätigung extrahieren** wird angezeigt.
5. Um die Systemkonfiguration vom Referenzserver zu extrahieren, klicken Sie auf **OK**.
   Das Extrahieren der Systemkonfiguration vom Referenzserver kann einige Minuten dauern.
6. Überprüfen Sie die Referenzserverdetails und klicken Sie auf **WEITER**.
   - Um den Referenz-Server auf der Seite **Referenzserver auswählen** zu ändern, klicken Sie auf **DURCHSUCHEN**.

     Wenn der Referenzserver ein Bare-Metal-Server ist, wird nur seine iDRAC-IP-Adresse angezeigt. Wenn der Referenzserver hingegen selbst ein Hostserver ist, werden sowohl die iDRAC- als auch die Host-(FQDN-)IPs angezeigt.

   Die Seite **Profileinstellungen** wird angezeigt.
7. Auf der Seite **Profileinstellungen** können Sie die Profileinstellungen für Komponenten wie iDRAC, BIOS, RAID, NIC, CNA, FCoE und EvenFilters basierend auf der Konfiguration des Referenzservers einsehen und ändern.

   Standardmäßig werden plattformspezifische und schreibgeschützte Attribute nicht aufgelistet. Weitere Informationen zu plattformspezifischen Attributen finden Sie unter Systemspezifische Attribute auf Seite 174.

   Im Systemprofil werden keine Pseudoattribute angezeigt. Weitere Informationen finden Sie im Dokument Serverkonfigurations-XML-Datei.

   Bevor Sie Attribute neben den standardmäßig ausgewählten Attributen auswählen, überprüfen Sie die Beschaffenheit von Attributen, Abhängigkeiten und anderen Details.

   Wenn Sie Attribute neben den standardmäßig ausgewählten Attributen auswählen, wird die folgende Meldung angezeigt:

   Diese Attribute können sich auf andere abhängige Attribute auswirken oder sie sind destruktiv oder lösen die Serveridentität auf oder beeinträchtigen die Sicherheit der Zielserver.

   ANMERKUNG: Bei PowerEdge-Servern der 12. und 13. Generation können einige Attribute die Abhängigkeit in OMIVV nicht korrekt zuordnen. Beispiel: Die Komponente „Speicherbetriebsspannung“ des BIOS ist schreibgeschützt, es sei denn, das Systemprofil ist in den **System-BIOS-Einstellungen** auf **Benutzerdefiniert** gesetzt.

   a. Erweitern Sie die einzelnen Komponenten zum Anzeigen der Einstellungsoptionen wie **Instanz**, **Attributname**, **Wert**, **Destruktiv**, **Abhängigkeit** und **Gruppe**.

      Wenn der Abhängigkeitstext nicht verfügbar ist, ist das Textfeld leer.

      ANMERKUNG: Sie können das **Suchfeld** verwenden, um Daten zu filtern, die für alle Spalten außer **Wert** spezifisch sind.

   b. Die Werte für Attribute, die mit einem roten Ausrufezeichen gekennzeichnet sind, müssen festgelegt werden. Diese Option ist nur für den für iDRAC aktivierten Nutzer mit einem gültigen Nutzernamen verfügbar.
8. Klicken Sie auf **WEITER**.
   Die Seite **Zusammenfassung** zeigt Informationen zu den Profildetails und die Attributstatistiken der Systemkonfigurationen an.

   Die Attributstatistik zeigt die jeweilige Gesamtanzahl der Attribute, der aktivierten Attribute und der destruktiven Attribute an.
9. Klicken Sie auf **FERTIGSTELLEN**.
   Das gespeicherte Profil wird auf der Seite **Systemprofil** angezeigt.

Einige Attribute des Systemprofils werden überschrieben, damit OMIVV funktioniert. Weitere Informationen zu nutzerdefinierten Attributen finden Sie unter Anpassungsattribute auf Seite 179. Weitere Informationen über die Systemprofil-Konfigurationsvorlage, über Attribute und Workflow finden Sie unter Weitere Informationen auf Seite 178.

Systemprofil bearbeiten

Es wird empfohlen, Google Chrome zu verwenden, um Systemprofile zu erstellen oder zu bearbeiten.

1. Wählen Sie auf der Seite **Systemprofil erstellen** ein Systemprofil aus und klicken Sie dann auf **BEARBEITEN**.
2. Ändern Sie auf der Seite **Name und Beschreibung** den Profilnamen und die Beschreibung. Die Beschreibung ist optional.

   ANMERKUNG: Nach der Erstellung des Basis- oder erweiterten Systemprofils können Sie die Profile nicht mehr ändern.

3. Klicken Sie zum Ändern des Referenzservers, der entweder ein Host- oder ein Bare-Metal-Server ist, auf der Seite **Referenzserver** auf **AUSWÄHLEN**.

   Die Serverauswahl ist möglicherweise aus einem der folgenden Gründe deaktiviert:

   - Der Server ist entweder ein nicht konformer Host oder Bare-Metal-Server.
   - Ein Bereitstellungs-Job ist entweder geplant oder läuft auf dem Server.
   - Der Server wird mit dem Gehäuse-Zugangsdatenprofil verwaltet.

   Das Dialogfeld **Bestätigung extrahieren** wird angezeigt.
4. Um die Systemkonfiguration vom Referenzserver zu extrahieren, klicken Sie auf **OK**.
   Das Extrahieren der Systemkonfiguration vom Referenzserver kann einige Minuten dauern.
5. Überprüfen Sie die Referenzserverdetails und klicken Sie auf **WEITER**.

   - Um den Referenz-Server auf der Seite **Referenzserver auswählen** zu ändern, klicken Sie auf **DURCHSUCHEN**. Wenn der Referenzserver ein Bare-Metal-Server ist, wird nur seine iDRAC-IP-Adresse angezeigt. Wenn der Referenzserver hingegen selbst ein Hostserver ist, werden sowohl die iDRAC- als auch die Host-(FQDN-)IPs angezeigt.

   Die Seite **Profileinstellungen** wird angezeigt.
6. Auf der Seite **Profileinstellungen** können Sie die Profileinstellungen für Komponenten wie iDRAC, BIOS, RAID, NIC, CNA, FCoE und EvenFilters basierend auf der Konfiguration des Referenzservers einsehen und ändern.

   Standardmäßig werden plattformspezifische und schreibgeschützte Attribute nicht aufgelistet. Weitere Informationen zu plattformspezifischen Attributen finden Sie unter Systemspezifische Attribute auf Seite 174.

   Wenn Sie versuchen, einige Attribute zu ändern, wird die folgende Warnmeldung angezeigt:

   Diese Attribute können sich auf andere abhängige Attribute auswirken oder sie sind destruktiv oder lösen die Serveridentität auf oder beeinträchtigen die Sicherheit der Zielserver.

   ANMERKUNG: Nachdem Sie das Systemprofil bearbeitet haben, wird das Kennwort für iDRAC-Nutzer, das zur Ermittlung des Bare-Metal-Servers verwendet wird, geändert und das aktualisierte Kennwort ignoriert. Das aktualisierte Kennwort wird durch das Kennwort ersetzt, das zur Ermittlung der Bare-Metal-Server verwendet wird.

   a. Erweitern Sie die einzelnen Komponenten zum Anzeigen der Einstellungsoptionen wie Instanz, Attributname, Wert, Destruktiv, Abhängigkeit und Gruppe.

      Wenn der Abhängigkeitstext nicht verfügbar ist, ist das Textfeld leer.

   b. Die Werte für Attribute, die mit einem roten Ausrufezeichen gekennzeichnet sind, müssen festgelegt werden. Diese Option ist nur für den für iDRAC aktivierten Nutzer mit einem gültigen Nutzernamen verfügbar.
7. Klicken Sie auf **WEITER**.
   Die Seite **Zusammenfassung** zeigt Informationen zu den Profildetails und die Attributstatistiken der Systemkonfigurationen an.

   Die Attributstatistik zeigt die jeweilige Gesamtanzahl der Attribute, der aktivierten Attribute und der destruktiven Attribute an.
8. Klicken Sie auf **FERTIGSTELLEN**.
   Das gespeicherte Profil wird auf der Seite **Systemprofil** angezeigt.

Einige Attribute des Systemprofils werden überschrieben, damit OMIVV funktioniert. Weitere Informationen zu nutzerdefinierten Attributen finden Sie unter Anpassungsattribute auf Seite 179. Weitere Informationen über die Systemprofil-Konfigurationsvorlage, über Attribute und Workflow finden Sie unter Weitere Informationen auf Seite 178.

Systemprofil anzeigen

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Systemprofil**.
   Eine Tabelle zeigt alle Systemprofile zusammen mit den folgenden Informationen an:
   - **Profilname**: Der Name des Systemprofils
   - **Beschreibung**: Die Beschreibung des Profils
   - **Referenzserver**: Die iDRAC-IP, aus der die Systemkonfigurationsdaten extrahiert werden.
   - **Servermodell**: Der Modellname des Referenzservers
2. Wenn Sie die Spaltennamen aus dem Assistenten entfernen oder hinzufügen möchten, klicken Sie auf .
3. Um die Systemprofilinformationen zu exportieren, klicken Sie auf das .

Systemprofil löschen

Das Löschen eines Systemprofils, das Teil einer laufenden Bereitstellungsaufgabe ist, kann dazu führen, dass der Job fehlschlägt.

1. Wählen Sie auf der Seite **Systemprofil** ein Systemprofil aus und klicken Sie dann auf **LÖSCHEN**.
2. Klicken Sie im Dialogfeld zur Bestätigung des Löschvorgangs auf **LÖSCHEN**.

ISO-Profil

Ein ISO-Profil enthält den Ordnerpfad für die benutzerdefinierte Dell EMC ESXi ISO-Image-Datei, die im NFS- oder CIFS-Ordner gespeichert wurde. Ein ISO-Profil wird im Bereitstellungsassistenten verwendet.

ISO-Profil erstellen

Für ein ISO-Profil ist ein von Dell EMC angepasster ISO-Dateipfad auf einem NFS- oder CIFS-Dateisystem erforderlich.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Profile** > **ISO-Profil** > **NEUES PROFIL ERSTELLEN**.
2. Lesen Sie auf der Seite **ISO-Profil** des Assistenten die Anweisungen und klicken Sie dann auf **ERSTE SCHRITTE**.
3. Geben Sie auf der Seite **Profilname und -beschreibung** den Profilnamen und die Beschreibung ein. Die Beschreibung ist ein optionales Feld.
4. Geben Sie im Feld **Installationsquelle (ISO)** den Speicherort der ISO-Datei (NFS oder CIFS) ein.
   OMIVV unterstützt nur Server Message Block(SMB)-Version 1.0- und SMB-Version 2.0-basierte CIFS-Freigaben.
   a. Geben Sie bei Verwendung von CIFS die Zugangsdaten ein.
5. Wählen Sie in der Dropdownliste **ESXi-Version** eine ESXi-Version aus.
   Wählen Sie die richtige ESXi-Version aus, damit das entsprechende Installations-Startskript verwendet wird. Wenn Sie eine falsche ESXi-Version bereitstellen, kann die Bereitstellung fehlschlagen.
6. Klicken Sie zum Überprüfen der Zugänglichkeit und der Anmeldeinformationen des ISO-Dateipfads auf **TEST STARTEN**.
   Die Testergebnisse werden angezeigt.
7. Klicken Sie auf **FERTIGSTELLEN**.

ISO-Profil bearbeiten

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Profile** > **ISO-Profil**.
2. Wählen Sie ein ISO-Profil aus und klicken Sie auf **BEARBEITEN**.
3. Bearbeiten Sie auf der Seite **Profilname und -beschreibung** den Profilnamen und die Beschreibung. Die Beschreibung ist ein optionales Feld.
4. Ändern Sie im Feld **Installationsquelle (ISO)** den Speicherort der ISO-Datei (NFS oder CIFS).
   OMIVV unterstützt nur Server Message Block(SMB)-Version 1.0- und SMB-Version 2.0-basierte CIFS-Freigaben.

a. Geben Sie bei Verwendung von CIFS die Zugangsdaten ein.

5. Wählen Sie in der Dropdownliste **ESXi-Version** eine ESXi-Version aus.

   Wählen Sie die richtige ESXi-Version aus, damit das entsprechende Installations-Startskript verwendet wird. Wenn Sie eine falsche ESXi-Version auswählen, kann die Bereitstellung fehlschlagen.

6. Klicken Sie zum Überprüfen des ISO-Dateipfads und der Authentifizierung auf **TEST STARTEN**.
   Die Testergebnisse werden angezeigt.
7. Klicken Sie auf **FERTIGSTELLEN**.

Ein ISO-Profil anzeigen

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **ISO-Profil**.
   Eine Tabelle zeigt alle ISO-Profile zusammen mit den folgenden Informationen an:
   - **Profilname**: Der Name des Profils
   - **Beschreibung**: Die Beschreibung des Profils
   - **Installationsquelle**: Der Speicherort der ISO-Datei (NFS oder CIFS)
   - **ESXi-Basisversion**: Die ESXi-Basisversion
2. Wenn Sie die Spaltennamen aus dem Assistenten entfernen oder hinzufügen möchten, klicken Sie auf .
3. Um ISO-Profilinformationen zu exportieren, klicken Sie auf das .

ISO-Profil löschen

Das Löschen eines ISO-Profils, das Teil einer laufenden Bereitstellungsaufgabe ist, führt dazu, dass die Aufgabe fehlschlägt.

1. Wählen Sie auf der OMIVV-Startseite **Compliance und Bereitstellung** > **Profile** > **ISO-Profil**.
2. Wählen Sie ein ISO-Profil aus und klicken Sie auf **LÖSCHEN**.
3. Klicken Sie im Bestätigungsdialogfeld auf **LÖSCHEN**.

Benutzerdefinierte Dell EMC ISO-Images herunterladen

Benutzerdefinierte ESXi-Images, die alle Dell EMC Treiber enthalten, sind für die Bereitstellung erforderlich.

1. Öffnen Sie einen Browser und navigieren Sie zu **support.dell.com**.
2. Klicken Sie auf **Alle Produkte durchsuchen** > **Server** > **PowerEdge**.
3. Klicken Sie auf ein PowerEdge-Servermodell.
4. Klicken Sie auf die Seite **Treiber und Downloads** des Server-Modells.
5. Wählen Sie aus der Dropdown-Liste **Betriebssystem** die ESXi-Version aus.
6. Wählen Sie im Dropdown-Menü **Kategorie** die Option **Enterprise-Lösungen**. aus.
7. Wählen Sie in der Liste **Enterprise-Lösungen** die Version des erforderlichen ISO aus, und klicken Sie dann auf **Herunterladen**.

10

Bereitstellung eines Systemprofils und ISO-Profils

Stellen Sie sicher, dass alle Server die folgenden Anforderungen in Ihrer Umgebung erfüllen, um das Systemprofil und das ISO-Profil bereitzustellen:

- Alle Server werden im Assistenten für die **Bereitstellung eines Systemprofils und ISO-Profils** angezeigt.
- Spezifische Hardware-Supportinformationen, die in der *OpenManage Integration for VMware vCenter-Kompatibilitätsmatrix* aufgeführt sind.
- Erforderliche Mindestversionen der iDRAC-Firmware und des BIOS sind verfügbar.

  Spezifische Firmware-Supportinformationen sind in der *OpenManage Integration for VMware vCenter-Kompatibilitätsmatrix* verfügbar.

- Die IDSDM-Speicherspezifikationen sind verfügbar.

  Die Speicheranforderungen des IDSDM finden Sie in der VMware-Dokumentation.

- Das IDSDM wird über das BIOS vor dem Bereitstellen eines Betriebssystems mit OMIVV aktiviert.

  OMIVV ermöglicht die Bereitstellung auf IDSDM, auf lokalen Festplatten oder auf der BOSS-Karte.

- Es besteht eine Route zwischen den vCenter-, OMIVV- und den iDRAC-Netzwerken, wenn vCenter, OMIVV und iDRAC sich in verschiedenen Netzwerken befinden.

  Dies gilt nur, wenn die OMIVV-Appliance nicht mit zwei Netzwerkschnittstellen-Controllern konfiguriert ist.

- Die Funktion „Systembestandsaufnahme beim Neustart erfassen“ (CSIOR) ist aktiviert.
- Die abgerufenen Daten sind auf dem neuesten Stand, indem Sie einen harten Neustart auf dem Server durchführen, bevor Sie die automatische oder manuelle Ermittlung starten.
- Für die AutoErmittlung von Bare-Metal-Servern bestellen Sie entweder die Dell EMC Server mit automatischer Ermittlung oder Handshake-Optionen, die werksseitig vorkonfiguriert sind. Ist ein Server nicht mit diesen Optionen vorkonfiguriert, müssen Sie die OMIVV IP-Adresse manuell eingeben oder Ihr lokales Netzwerk zur Bereitstellung dieser Informationen konfigurieren.
- Stellen Sie sicher, dass die folgenden Bedingungen vor einer Betriebssystem-Bereitstellung erfüllt sind, wenn OMIVV nicht für die Hardwarekonfiguration verwendet wird:
  - Aktivieren Sie die Virtualization Technology (VT) Kennzeichnung im BIOS.
  - Der virtuelle Treiber, IDSDM und BOSS sind auf die erste Startfestplatte eingestellt.
- Stellen Sie sicher, dass die BIOS-Einstellung für VT automatisch aktiviert ist, auch wenn die BIOS-Konfiguration kein Teil des Systemprofils ist, wenn OMIVV zur Hardwarekonfiguration verwendet wird. Wenn ein virtuelles Laufwerk auf dem Zielsystem nicht konfiguriert ist, ist eine Express- oder Clone-RAID-Konfiguration erforderlich.
- Die nutzerdefinierten ESXi-Images, die alle Dell EMC Treiber enthalten, sind für die Bereitstellung vorhanden.

  Laden Sie die richtigen Images im Abschnitt **Treiber & Downloads** herunter, die auf **support.dell.com** verfügbar sind. Weitere Informationen zum Herunterladen der benutzerdefinierten Dell EMC ISO-Images finden Sie unter Benutzerdefinierte Dell EMC ISO-Images herunterladen auf Seite 64.

- Speichern Sie die nutzerdefinierten Images an einem freigegebenen CIFS- oder NFS-Speicherort, auf den OMIVV während des Bereitstellungsprozesses zugreifen kann.

  Eine aktuelle Liste mit allen unterstützten ESXi-Versionen für dieses Release finden Sie in der *OpenManage Integration for VMware vCenter-Kompatibilitätsmatrix*.

  Folgendes gilt für die Bereitstellung von Hosts mit doppelten NICs:

- Der Host kann iDRAC- und vCenter Management-NIC im gleichen Netzwerk oder in den zwei unterschiedlichen Netzwerken haben.
- Das ISO-Image kann in einem beliebigen Netzwerk gespeichert werden.
- Stellen Sie sicher, dass Sie das richtige vCenter-Netzwerk und OMIVV-Netzwerk auf die Umgebung anwenden. Der BS-Bereitstellungsassistent zeigt beide OMIVV-Netzwerke an.

Bereitstellungsprüfliste

Stellen Sie vor der Bereitstellung von Systemprofil und ISO-Profil sicher, dass Folgendes verfügbar ist:

- Host-Zugangsdatenprofil

  Um ein neues Host-Zugangsdatenprofil zu erstellen, klicken Sie auf **ERSTELLEN**. Weitere Informationen zum Erstellen eines Host-Zugangsdatenprofils finden Sie unter Host-Anmeldeinformationenprofil erstellen auf Seite 39.

- Bare-Metal-Server

  Um einen Bare-Metal-Server zu ermitteln, klicken Sie auf **ERMITTELN**. Weitere Informationen zum Ermitteln von Bare-Metal-Servern finden Sie unter Manuelle Ermittlung von Bare-Metal-Servern auf Seite 57.

- Systemprofil

  Klicken Sie zum Erstellen eines Systemprofils auf **ERSTELLEN**. Weitere Informationen zum Erstellen eines Systemprofils finden Sie unter Systemprofil erstellen auf Seite 60.

- ISO-Profil

  Klicken Sie zum Erstellen eines ISO-Profils auf **ERSTELLEN**. Weitere Informationen zum Erstellen eines ISO-Profils finden Sie unter ISO-Profil erstellen auf Seite 63.

Mithilfe des Assistenten **Systemprofil- und ISO-Profil-Bereitstellung** können Sie Folgendes ausführen:

- Bereitstellung eines Systemprofils

  Weitere Informationen finden Sie unter Systemprofil bereitstellen (Konfiguration der Hardware) auf Seite 66.

- Bereitstellung eines ISO-Profils

  Weitere Informationen finden Sie unter ISO-Profil bereitstellen (ESXi Installation) auf Seite 67.

- Bereitstellung eines Systemprofils und ISO-Profils

  Weitere Informationen finden Sie unter Systemprofil und ISO-Profil bereitstellen auf Seite 69.

Systemprofil bereitstellen (Konfiguration der Hardware)

1. Zum Starten des Bereitstellungsassistenten gehen Sie zu **Compliance & Bereitstellung** > **Bereitstellung** > **Bereitstellen**.
2. Überprüfen Sie auf der Seite **Checkliste für Bereitstellung eines Systemprofils und ISO-Profils** im Bereitstellungsassistenten die Bereitstellungs-Checkliste und klicken Sie dann auf **ERSTE SCHRITTE**.

   Sie können die Bereitstellung nur auf konformen Bare-Metal-Servern durchführen. Weitere Informationen finden Sie unter Bare-Metal-Server anzeigen auf Seite 55.
3. Wählen Sie auf der Seite **Server auswählen** einen oder mehrere Server aus.
   Daraufhin wird die Seite **Bereitstellungsoptionen auswählen** angezeigt.
4. Wählen Sie auf der Seite **Bereitstellungsoptionen auswählen** die Option **Systemprofil (Konfiguration der Hardware)** aus.
5. Wählen Sie aus dem Drop-Down-Menü **Systemprofil** ein entsprechendes Systemprofil aus und klicken Sie dann auf **WEITER**.

   Für grundlegende und erweiterte Systemprofiltypen wird der Systemprofilname im folgenden Format angezeigt: Grundlegend_<Systemprofilname>, Erweitert_<Systemprofilname>.

   Der Job für die **Konfigurationsvorschau** versucht, die Kompatibilität des ausgewählten Systemprofils mit dem ausgewählten Host zu vergleichen oder zu überprüfen.
6. Um einen Vorschau-Job auf iDRAC zu erstellen, wählen Sie auf der Seite **Konfigurationsvorschau** eine iDRAC-IP aus und klicken Sie dann auf **VORSCHAU**. Die Konfigurationsvorschau ist eine optionale Aufgabe.
   Der Systemprofil-Vorschauvorgang kann einige Minuten in Anspruch nehmen. Der Vergleichsstatus wird in der Spalte **Ergebnis** angezeigt.

   Im Folgenden finden Sie die Vergleichsergebnisse:

   - **Abgeschlossen**: Der Vorschau-Job wurde erfolgreich ausgeführt. Um weitere Informationen zu den Vergleichsergebnissen zu erhalten, klicken Sie in der Spalte **Details** auf **Details anzeigen**.

- **Nicht abgeschlossen**: Der Vorschau-Job wurde auf dem iDRAC nicht erfolgreich ausgeführt. Stellen Sie sicher, dass auf iDRAC zugegriffen werden kann, und setzen Sie bei Bedarf den iDRAC zurück. Weitere Informationen über den Job finden Sie in den OMIVV-Protokollen und den Protokollen unter der iDRAC-Konsole.

7. Führen Sie auf der Seite **Bereitstellungs-Job planen** Folgendes aus:
   a. Geben Sie den Namen und die Beschreibung des Bereitstellungs-Jobs an. Die Beschreibung ist ein optionales Feld.
   b. Um den Bereitstellungs-Job jetzt auszuführen, klicken Sie auf **Jetzt ausführen**.
   c. Um den Job zu einem späteren Zeitpunkt zu planen, klicken Sie auf **Später planen** und wählen Sie dann das gewünschte Datum und die Uhrzeit aus.
   d. Aktivieren Sie das Kontrollkästchen **Zu der Job-Warteschlange gehen, nachdem der Job gestartet wurde**.
   Sie können den Status des Jobs auf der Seite **Jobs** nachverfolgen. Weitere Informationen finden Sie unter Bereitstellungs-Jobs auf Seite 76.
8. Klicken Sie auf **FERTIGSTELLEN**.

ISO-Profil bereitstellen (ESXi Installation)

Sie können die Bereitstellung nur auf konformen Bare-Metal-Servern durchführen. Weitere Informationen finden Sie unter Bare-Metal-Server anzeigen auf Seite 55.

1. Zum Starten des Bereitstellungsassistenten gehen Sie zu **Compliance & Bereitstellung** > **Bereitstellung** > **Bereitstellen**.
2. Überprüfen Sie auf der Seite **Checkliste für Bereitstellung eines Systemprofils und ISO-Profils** im Bereitstellungsassistenten die Bereitstellungs-Checkliste und klicken Sie dann auf **ERSTE SCHRITTE**.
3. Wählen Sie auf der Seite **Server auswählen** einen oder mehrere Server aus.
   Daraufhin wird die Seite **Bereitstellungsoptionen auswählen** angezeigt.
4. Wählen Sie auf der Seite **Bereitstellungsoptionen auswählen** die Option **ISO-Profil (ESXi Installation)** aus.
5. Wählen Sie aus dem Drop-Down-Menü **vCenter-Name** eine Instanz von vCenter aus.
6. Um den vCenter-Zielcontainer auszuwählen, klicken Sie auf **DURCHSUCHEN** und wählen Sie ein entsprechendes Rechenzentrum oder einen Cluster aus, auf dem Sie ein Betriebssystem bereitstellen möchten.
7. Wählen Sie im Drop-Down-Menü **ISO-Profil** ein entsprechendes ISO-Profil aus.
8. Wählen Sie unter **Installationsziel** eine der folgenden Optionen aus:

   - **Erstes Startlaufwerk**: Stellt ein Betriebssystem auf der Festplatte, dem Solid-State-Laufwerk (SSD) oder einem von RAID-Controllern erstellten virtuellen Datenträger bereit.
   - **Internes Dual-SD-Modul (IDSDM)**: Stellt ein Betriebssystem auf dem IDSDM bereit. Wenn ein IDSDM auf mindestens einem der ausgewählten Server verfügbar ist, ist die Option Internes Dual-SD-Modul aktiviert. Ist dies nicht der Fall, ist nur die Option **Erstes Startlaufwerk** verfügbar.
     - Wenn einer der ausgewählten Server kein IDSDM- oder Boss-Modul unterstützt oder wenn kein IDSDM oder BOSS während der Bereitstellung auf den Servern installiert ist, wird der Bereitstellungsvorgang auf diesen Servern übersprungen.

       Um das Betriebssystem auf dem ersten Startlaufwerk der Server bereitzustellen, markieren Sie das Kontrollkästchen **Hypervisor auf dem ersten Startlaufwerk für Server bereitstellen, die über kein internes Dual-SD-Modul verfügen**.

     ANMERKUNG: Das Installationsziel „Erstes Startlaufwerk“ stimmt nicht mit dem ersten Eintrag unter BIOS-Festplattenlaufwerk-Sequenz oder UEFI-Startreihenfolge überein. Diese Option stellt das Betriebssystem auf dem ersten Laufwerk bereit, welches von der ESXi-Vorbetriebssystemumgebung identifiziert wird. Dazu müssen Sie sicherstellen, dass die Option „Festplatten-Failover“ oder „Wiederholung der Startreihenfolge“ aktiviert ist, wenn die Option **Erstes Startlaufwerk** ausgewählt wurde.
   - **BOSS**: Stellt ein Betriebssystem auf der BOSS-Karte bereit. Wenn ein BOSS auf mindestens einem der ausgewählten Server verfügbar ist, ist die Option BOSS aktiviert. Ist dies nicht der Fall, ist nur die Option **Erstes Startlaufwerk** verfügbar.

     Wenn Sie OMIVV verwenden, um ein Betriebssystem auf dem BOSS-Controller bereitzustellen, stellen Sie sicher, dass das Systemprofil vom Referenzserver zusammen mit der BOSS-Konfiguration für virtuelle Laufwerke erfasst wird und der Zielserver einen BOSS mit ähnlicher Konfiguration hat. Weitere Informationen zum Erstellen eines virtuellen Laufwerks finden Sie im *Benutzerhandbuch zu Dell EMC Boot Optimized Server Storage-S1* unter www.dell.com/support.

9. Auf der Seite **Host-Zugangsdatenprofil auswählen** führen Sie die folgenden Aufgaben aus:
   a. Um dasselbe Host-Zugangsdatenprofil für alle Hosts zu verwenden, klicken Sie auf **JA** und führen dann Folgendes durch:
      i. Wählen Sie das Zugangsdatenprofil aus dem Dropdown-Menü aus.
      ii. Geben Sie das Kennwort ein.

Folgendes gilt für Root-Nutzer bei der Bereitstellung:

- Bei ESXi 6.5 und früheren Versionen wird das im Host-Zugangsdatenprofil eingegebene Kennwort verwendet.
- Für ESXi 6.7 und höhere Versionen wird das im Bereitstellungsassistenten eingegebene Kennwort verwendet.
- Für ESXi 6.5 und frühere Versionen: Wenn das Kennwort nicht im Host-Zugangsdatenprofil eingegeben wurde, wird das im Bereitstellungsassistenten eingegebene Kennwort verwendet. Aktualisieren Sie die ESXi-Anmeldeinformationen im Host-Anmeldeinformationenprofil, um sicherzustellen, dass die Bestandsaufnahme nach der Betriebssystembereitstellung erfolgreich ausgeführt wird.

b. Um das individuelle Host-Zugangsdatenprofil für jeden Server auszuwählen, klicken Sie auf **NEIN** und führen dann Folgendes durch:

i. Wählen Sie das Zugangsdatenprofil aus dem Dropdown-Menü aus.
ii. Geben Sie das Root-Kennwort ein. Zum Anzeigen des aktuellen Kennworts klicken Sie auf das Augensymbol.

Stellen Sie sicher, dass Sie das richtige Kennwort eingeben, da die Option „Kennwort bestätigen“ nicht verfügbar ist.

ANMERKUNG: Wenn AD-Anmeldeinformationen für iDRAC oder ESXi im Host-Zugangsdatenprofil verwendet werden, werden diese Profile für eine Betriebssystembereitstellung nicht berücksichtigt.

ANMERKUNG: Im Host-Zugangsdatenprofil wird empfohlen, den Nutzer zu verknüpfen, der zur Ermittlung des Bare-Metal-Servers verwendet wird, andernfalls wird der ermittelte Nutzer in iDRAC nach der Betriebssystembereitstellung deaktiviert.

10. Führen Sie auf der Seite **Netzwerkeinstellungen konfigurieren** folgende Aufgaben aus:

a. Geben Sie einen vollständig qualifizierten Hostnamen (FQDN) für den Server ein. Ein vollständig qualifizierter Domänenname für den Hostnamen ist obligatorisch. Die Verwendung von *localhost* für den vollständig qualifizierten Domänennamen (FQDN) wird nicht unterstützt. Der FQDN wird verwendet, wenn ein Host zu vCenter hinzugefügt wird. Erstellen Sie einen DNS-Datensatz, der die IP-Adresse mit dem vollständig qualifizierten Domänennamen (FQDN) auflöst Konfigurieren Sie den DNS-Server so, dass er umgekehrte Suchanfragen unterstützt. Die DHCP-Reservierungen und DNS-Hostnamen müssen vorhanden sein und überprüft werden, bevor die Ausführung des Bereitstellungs-Jobs geplant wird.

ANMERKUNG: Wenn vCenter mit FQDN bei OMIVV registriert ist, stellen Sie sicher, dass der ESXi-Host die FQDN mithilfe der DNS-Auflösung auflösen kann.

b. Wählen Sie den NIC aus, der für das Managementnetzwerk verwendet wird. Stellen Sie sicher, dass sich der NIC im verbundenen Zustand befindet.

ANMERKUNG: Stellen Sie sicher, dass Sie die Verwaltungs-NICs basierend auf der Netzwerkverbindung mit dem OMIVV auswählen. Die Option **EINSTELLUNG AUF ALLE SERVER ANWENDEN** gilt nicht für die Verwaltungs-NIC-Auswahl.

c. Wählen Sie die OMIVV-Netzwerkinstanz, die Zugriff auf vCenter hat. Weitere Informationen finden Sie unter Bereitstellung eines Systemprofils und ISO-Profils auf Seite 65.

d. Wählen Sie einen der folgenden Netzwerkoptionen aus:

- Geben Sie für „Statisch“ den bevorzugten DNS-Server, alternativen DNS-Server, die IP-Adresse, Subnetzmaske und das Standard-Gateway ein.
- **VLAN verwenden**: Wenn eine VLAN-ID bereitgestellt wird, wird sie für die Verwaltungsschnittstelle eines Betriebssystems während der Bereitstellung angewendet und sie markiert den ganzen Datenverkehr mit der VLAN-ID. Mit der Server-Identifikation werden den bereitgestellten Servern neue Namen und eine Netzwerkidentifikation zugewiesen Weitere Informationen finden Sie unter VLAN-Support auf Seite 69.
- **DHCP verwenden**: Die DHCP zugewiesene IP-Adresse wird beim Hinzufügen des Hosts zu vCenter verwendet. Bei der Verwendung von DHCP wird empfohlen, eine Reservierung für ausgewählte NIC-MAC-Adressen zu verwenden.

11. Führen Sie auf der Seite **Bereitstellungs-Job planen** Folgendes aus:

a. Geben Sie den Namen und die Beschreibung des Bereitstellungs-Jobs an.
b. Um den Bereitstellungs-Job jetzt auszuführen, klicken Sie auf **Jetzt ausführen**.
c. Um den Job zu einem späteren Zeitpunkt zu planen, klicken Sie auf **Später planen** und wählen Sie dann das gewünschte Datum und die Uhrzeit aus.
d. Aktivieren Sie das Kontrollkästchen **Zu der Job-Warteschlange gehen, nachdem der Job gestartet wurde**.
Sie können den Status des Jobs auf der Seite **Jobs** nachverfolgen. Weitere Informationen finden Sie unter Bereitstellungs-Jobs auf Seite 76.

12. Klicken Sie auf **FERTIGSTELLEN**.

ANMERKUNG: Nach dem Ausführen einer Betriebssystembereitstellung auf Bare-Metal-Servern löscht OMIVV alle iDRAC-Jobs.

Der Job zur Bereitstellung des ISO-Profils, der mit einer älteren Version von OMIVV geplant ist, ist in der neuesten Version von OMIVV nicht gültig. Brechen Sie den geplanten Job ab und erstellen Sie einen Bereitstellungs-Job nach Bedarf.

Der Bereitstellungs-Job schlägt fehl, wenn der geplante Job nicht abgebrochen wird. In diesem Fall müssen Sie den Server als Bare-Metal- und ISO-Profil-Bereitstellungs-Job erstellen.

Systemprofil und ISO-Profil bereitstellen

Sie können die Bereitstellung nur auf konformen Bare-Metal-Servern durchführen. Weitere Informationen finden Sie unter Bare-Metal-Server anzeigen auf Seite 55.

1. Zum Starten des Bereitstellungsassistenten gehen Sie zu **Compliance & Bereitstellung** > **Bereitstellung** > **Bereitstellen**.
2. Überprüfen Sie auf der Seite **Checkliste für Bereitstellung eines Systemprofils und ISO-Profils** im Bereitstellungsassistenten die Bereitstellungs-Checkliste und klicken Sie dann auf **ERSTE SCHRITTE**.
3. Wählen Sie auf der Seite **Server auswählen** einen oder mehrere Server aus.
   Daraufhin wird die Seite **Bereitstellungsoptionen auswählen** angezeigt.
4. Wählen Sie auf der Seite **Bereitstellungsoptionen auswählen** die Optionen **Systemprofil (Konfiguration der Hardware)** und **ISO-Profil (ESXi-Installation)**aus.
5. Wählen Sie aus dem Drop-Down-Menü **vCenter-Name** eine Instanz von vCenter aus.
6. Um den vCenter-Zielcontainer auszuwählen, klicken Sie auf **DURCHSUCHEN** und wählen Sie ein entsprechendes Rechenzentrum oder einen Cluster aus, auf dem Sie ein Betriebssystem bereitstellen möchten.
7. Klicken Sie auf **Bestätigen**, um das mit dem Clusterprofil verknüpfte Systemprofil zu verwenden, das dem ausgewählten Cluster zugeordnet ist.
   - Um ein anderes Systemprofil auszuwählen, klicken Sie auf **Anderes auswählen**. Es wird empfohlen, das mit dem Cluster verknüpfte Systemprofil auszuwählen, um eine Konfigurations-Compliance-Abweichung zu vermeiden.
8. Wählen Sie aus dem Drop-Down-Menü **ISO-Profil** ein entsprechendes ISO-Profil aus und klicken Sie dann auf **WEITER**.
9. Um einen Vorschau-Job auf iDRAC zu erstellen, wählen Sie auf der Seite **Konfigurationsvorschau** eine iDRAC-IP aus und klicken Sie dann auf **VORSCHAU**. Die Konfigurationsvorschau ist eine optionale Aufgabe.
   Der Systemprofil-Vorschauvorgang kann einige Minuten in Anspruch nehmen. Der Vergleichsstatus wird in der Spalte **Ergebnis** angezeigt.

   Im Folgenden finden Sie die Vergleichsergebnisse:
   - **Abgeschlossen**: Der Vorschau-Job wurde erfolgreich ausgeführt. Um weitere Informationen zu den Vergleichsergebnissen zu erhalten, klicken Sie in der Spalte **Details** auf **Details anzeigen**.
   - **Nicht abgeschlossen**: Der Vorschau-Job wurde auf dem iDRAC nicht erfolgreich ausgeführt. Stellen Sie sicher, dass auf iDRAC zugegriffen werden kann, und setzen Sie bei Bedarf den iDRAC zurück. Weitere Informationen über den Job finden Sie in den OMIVV-Protokollen und den Protokollen unter der iDRAC-Konsole.
10. Führen Sie die im Thema ISO-Profil bereitstellen (ESXi Installation) auf Seite 67 aufgeführten Aufgaben 7 bis 10 aus.

VLAN-Support

OMIVV unterstützt die Betriebssystem-Bereitstellung auf einem routingfähigen VLAN, und Sie können VLAN-Unterstützung im Bereitstellungsassistenten konfigurieren. In diesem Teil des Bereitstellungsassistenten steht eine Option zur Angabe von VLANs mithilfe der VLAN-ID zur Verfügung. Wenn eine VLAN-ID bereitgestellt wird, wird sie für die Verwaltungsschnittstelle eines Betriebssystems während der Bereitstellung angewendet und sie markiert den ganzen Datenverkehr mit der VLAN-ID.

Stellen Sie sicher, dass das während der Bereitstellung bereitgestellte VLAN mit dem OMIVV-Gerät und dem vCenter Server kommuniziert. Die Bereitstellung eines Betriebssystems für ein VLAN, das nicht mit einem oder beiden dieser Ziele kommunizieren kann, führt dazu, dass die Bereitstellung fehlschlägt.

Falls Sie mehrere Bare-Metal-Server in einem einzelnen Bereitstellungsjob ausgewählt haben und dieselbe VLAN-ID auf alle Server anwenden möchten, dann verwenden Sie im Serveridentifizierungsteil des Bereitstellungsassistenten **EINSTELLUNGEN AUF ALLE SERVER ANWENDEN**. Diese Option ermöglicht Ihnen die Anwendung derselben VLAN-ID zusammen mit den anderen Netzwerkeinstellungen auf alle Server im betreffenden Bereitstellungs-Job.

ANMERKUNG: Stellen Sie sicher, dass Sie die Verwaltungs-NICs basierend auf der Netzwerkverbindung mit dem OMIVV auswählen. Die Option **EINSTELLUNG AUF ALLE SERVER ANWENDEN** gilt nicht für die Verwaltungs-NIC-Auswahl.

Festlegen der Zeit für den Bereitstellungs-Job

Die Bereitstellung des Systemprofils und ISO-Profils kann zwischen 30 Minuten und mehreren Stunden dauern, abhängig von mehreren Faktoren. Beim Starten eines Bereitstellungs-Jobs sollten Sie die Bereitstellungszeit entsprechend der aufgeführten Richtlinien planen. Die erforderliche Zeit für eine vollständige Bereitstellung des Systemprofils und ISO-Profils hängt von Bereitstellungstyp, der Komplexität und der Anzahl gleichzeitig ausgeführter Bereitstellungs-Jobs ab. Die Bereitstellungs-Jobs werden in Batches von bis zu fünf gleichzeitigen Servern ausgeführt, um die Zeit für den gesamten Bereitstellungs-Job zu verbessern. Die genaue Anzahl gleichzeitiger Jobs hängt von den verfügbaren Ressourcen ab.

Die folgende Tabelle gibt den Durchschnittswert an. Dieser kann je nach Faktoren wie Konfiguration des Servers, Servergeneration und Anzahl der für die Bereitstellung geplanten Bare-Metal-Server variieren.

Tabelle 3. Ungefähre Bereitstellungszeit für einen einzelnen Server

Bereitstellungstyp	Ungefähre Zeit pro Bereitstellung
Nur ISO-Profil	Zwischen 30 und 130
Nur Systemprofil	5–6 Minuten
Systemprofil und ISO-Profil	30-130 Minuten

Server-Status innerhalb der Bereitstellungssequenz

Die Server, die während der AutoErmittlung oder manuell erkannt werden, werden in unterschiedlichen Zuständen klassifiziert, um feststellen zu können, ob der Server neu zum Rechenzentrum hinzugefügt wurde oder ob ein ausstehender Bereitstellungs-Job geplant ist. Die Administratoren können diese Status verwenden, um den Status der Hardwarekonfiguration zu überprüfen.

Tabelle 4. Server-Status innerhalb der Bereitstellungssequenz

Serverstatus	Beschreibung
Nicht konfiguriert	Der Server wurde zu OMIVV hinzugefügt und wartet auf die Konfiguration.
Konfiguriert	Der Server wurde mit allen Hardwareinformationen konfiguriert, die für eine erfolgreiche Betriebssystem-Bereitstellung erforderlich sind.

11

Konformität

Verwaltungs-Compliance

Zum Anzeigen und Verwalten von Hosts in OMIVV muss jeder Host bestimmte Kriterien erfüllen. Wenn die Hosts die Compliance-Kriterien nicht erfüllen, überwacht und verwaltet OMIVV sie nicht. OMIVV zeigt Details über den nicht konformen Host an und ermöglicht, die Nichteinhaltung zu korrigieren, sofern zutreffend.

Der Host ist nicht konform, wenn:

- der Host keinem Host-Anmeldeinformationenprofil zugeordnet ist.
- die Funktion „Collect System Inventory on Reboot“ (CSIOR) deaktiviert ist oder nicht ausgeführt wurde. Hierzu ist ein manueller Neustart erforderlich.

  ANMERKUNG: Der CSIOR-Status wird nicht bestimmt, wenn Hosts über ein Gehäuse verwaltet werden.
- Das SNMP-Trap-Ziel des Host ist nicht auf die IP-Adresse des OMIVV-Geräts konfiguriert. Der Fehler bei der Einstellung des SNMP-Trap-Ziels kann auftreten, wenn iDRAC- oder Host-Anmeldeinformationen, die in Verbindung mit einem Profil bereitgestellt werden, ungültig sind. Oder der iDRAC verfügt über keine freien Steckplätze oder der iDRAC-Sperrmodus ist aktiviert (nur bei iDRAC9-basierten Servern). Eine Liste der iDRAC9-basierten Server finden Sie in der Compliance-Matrix.
- OMIVV aktiviert den WBEM-Dienst auf Hosts, auf denen ESXi 6.5 und höher läuft, nicht.
- Die iDRAC-Firmwareversion ist früher als 2.50.50.50. Die iDRAC-Version 2.50.50.50 oder höher ist nur erforderlich, um die Systemprofil-Funktion zu verwenden.
- Die iDRAC-Lizenz ist nicht kompatibel (iDRAC Express ist die Mindestanforderung). Die Server ohne eine kompatible iDRAC-Lizenz können nicht für die Überwachung und Aktualisierung der Firmware verwendet werden.

VORSICHT: Selbst wenn sie nicht konform sind, werden die Hosts im Sperrmodus bei den Compliance-Tests nicht angezeigt. Überprüfen Sie die Compliance-Stufe manuell. Bei manueller Überprüfung wird eine Meldung angezeigt. Ignorieren Sie diese Meldung. Sie werden nicht angezeigt, weil ihr Compliance-Status nicht ermittelt werden kann. Stellen Sie sicher, dass Sie die Compliance dieser Systeme manuell überprüfen. In einem solchen Szenario wird eine Warnmeldung angezeigt.

Auf der Seite **Verwaltungs-Compliance** können Sie die folgenden Aufgaben ausführen:

- Compliance korrigieren. Weitere Informationen finden Sie unter Nicht konformen Host reparieren auf Seite 72.
- Führen Sie eine Bestandsaufnahme aus. Der Link zum Ausführen eines Bestandsaufnahme-Jobs ist aktiv, wenn der iDRAC-Status für einen beliebigen, einem Host-Zugangsdatenprofil zugeordneten Host **Nicht konform** oder **Unbekannt** ist.
- Erneuern Sie die iDRAC Lizenz. Informationen hierzu finden Sie unter iDRAC-Lizenz-Compliance korrigieren auf Seite 73.
- Fügen Sie OEM-Hosts hinzu. Weitere Informationen über das Hinzufügen von OEM-Hosts finden Sie unter OEM-Hosts hinzufügen auf Seite 73.

Nicht konforme Hosts anzeigen

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Verwaltungs-Compliance**.

Eine Tabelle zeigt alle nicht konformen Hosts zusammen mit den folgenden Informationen an:

- **Host**: FQDN oder IP-Adresse des Hosts
- **Modell**: Der Modellname des Servers
- **Anmeldeinformationen-Profil**: Der Name des Host-Anmeldeinformationenprofils
- **CSIOR-Status**: Der CSIOR-Status (**EIN** oder **AUS**). Der CSIOR-Status zeigt **Unbestimmt** für Hosts an, die über Gehäuse verwaltet werden.
- **SNMP-Trap-Status**: Der SNMP-Trap-Status (**Konfiguriert** oder **Nicht konfiguriert**).
- **Hypervisor**: Hypervisor-Name und -Version

- **WBEM-Status**: Der WBEM-Status (**Konform** oder **Nicht konform**). Der CSIOR-Status zeigt **Nicht zutreffend** für Hosts an, die über Gehäuse verwaltet werden.
- **iDRAC-Firmware-Version**: Die iDRAC-Firmwareversion
- **iDRAC-Lizenz-Status**: Der iDRAC-Lizenz Status (**Konform** oder **Nicht konform**).

  ANMERKUNG: Wenn ein PowerEdge MX-Host über ein Gehäuse-Anmeldeinformationenprofil verwaltet wird, wird die iDRAC-Firmwareversion auf der Seite **Verwaltungs-Compliance** als **Nicht zutreffend** angezeigt. Der Grund dafür ist, dass die iDRAC-Firmware-Compliance für iDRAC9-basierte Server nicht anwendbar ist. Eine Liste der iDRAC9-basierten Server finden Sie in der Compliance-Matrix.

Nicht konformen Host reparieren

Der Host ist nicht konform, wenn:

- der Host keinem Host-Anmeldeinformationenprofil zugeordnet ist.
- die Funktion „Collect System Inventory on Reboot“ (CSIOR) deaktiviert ist oder nicht ausgeführt wurde. Hierzu ist ein manueller Neustart erforderlich.

  ANMERKUNG: Der CSIOR-Status wird nicht bestimmt, wenn Hosts über ein Gehäuse verwaltet werden.
- Das SNMP-Trap-Ziel des Host ist nicht auf die IP-Adresse des OMIVV-Geräts konfiguriert. Der Fehler bei der Einstellung des SNMP-Trap-Ziels kann auftreten, wenn iDRAC- oder Host-Anmeldeinformationen, die in Verbindung mit einem Profil bereitgestellt werden, ungültig sind. Oder der iDRAC verfügt über keine freien Steckplätze oder der iDRAC-Sperrmodus ist aktiviert (nur bei iDRAC9-basierten Servern). Eine Liste der iDRAC9-basierten Server finden Sie in der Compliance-Matrix.
- OMIVV aktiviert den WBEM-Dienst auf Hosts, auf denen ESXi 6.5 und höher läuft, nicht.
- Die iDRAC-Firmwareversion ist früher als 2.50.50.50. Die iDRAC-Version 2.50.50.50 oder höher ist nur erforderlich, um die Systemprofil-Funktion zu verwenden.
- Die iDRAC-Lizenz ist nicht kompatibel (iDRAC Express ist die Mindestanforderung). Die Server ohne eine kompatible iDRAC-Lizenz können nicht für die Überwachung und Aktualisierung der Firmware verwendet werden.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Verwaltungs-Compliance**.
2. Wählen Sie einen nicht konformen Host aus und klicken Sie auf **Compliance korrigieren**.
3. Lesen Sie auf der Begrüßungsseite des Assistenten die Anweisungen und klicken Sie dann auf **ERSTE SCHRITTE**.
4. Wählen Sie auf der Seite **Hosts auswählen** einen oder mehrere nicht konforme Hosts aus und klicken Sie auf **WEITER**.
   - Wenn die Hosts keinem Host-Zugangsdatenprofil zugeordnet sind, wird die folgende Warnmeldung angezeigt:

     Es sind ausgewählte Hosts vorhanden, die keinem Host-Zugangsdatenprofil zugewiesen sind. Um OMIVV die Ausführung einer Compliance-Überprüfung zu erlauben, müssen Sie diese Hosts zu einem Host-Zugangsdatenprofil hinzufügen.

     Um die Hosts auszuschließen, die nicht dem Host-Zugangsdatenprofil zugewiesen sind, klicken Sie auf **WEITER**.

     Klicken Sie auf **Abbrechen**, um die Hosts zu einer Seite „Host-Zugangsdatenprofil“ hinzuzufügen und zur Seite „Host-Zugangsdatenprofil“ zu navigieren. Weitere Informationen zum Erstellen eines Host-Zugangsdatenprofils finden Sie unter Host-Anmeldeinformationenprofil erstellen auf Seite 39.

     Hosts in einem MX-Gehäuse mit deaktiviertem iDRAC IPv4 müssen über ein Gehäuse-Zugangsdatenprofil verwaltet werden. Um diese Hosts dem Gehäuse-Zugangsdatenprofil zuzuordnen, müssen Sie das Gehäuse mithilfe von „MX-Gehäuse hinzufügen“ auf der Seite **Dell EMC-Gehäuse** hinzufügen und das Gehäuse einem Gehäuse-Zugangsdatenprofil zuordnen.

   So aktualisieren Sie iDRAC-Firmware und BIOS-Version:

   a. Wählen Sie auf der Seite **iDRAC-Firmware und BIOS-Version aktualisieren** einen oder mehrere Hosts aus, auf denen Sie die Firmware-Version aktualisieren möchten.
   b. Klicken Sie auf **WEITER**.
   c. Zeigen Sie auf der Seite **Hosts neustarten** die ESXi-Hosts an, die neu gestartet werden müssen.
   d. Wenn Sie Hosts automatisch in den Wartungsmodus versetzen und bei Bedarf neu starten möchten, aktivieren Sie das Kontrollkästchen und klicken Sie dann auf **WEITER**.
   e. Überprüfen Sie die Zusammenfassung Ihrer Einstellungen auf der Seite **Zusammenfassung** und klicken Sie auf **FERTIGSTELLEN**.

   So aktivieren Sie CSIOR:

   a. Wählen Sie auf der Seite **Hosts auswählen** einen oder mehrere nicht konforme Hosts aus und klicken Sie auf **WEITER**.
   b. Wählen Sie auf der Seite **CSIOR einschalten** einen oder mehrere Hosts aus, für die Sie CSIOR einschalten möchten, und klicken Sie auf **WEITER**.

c. Überprüfen Sie die Zusammenfassung Ihrer Einstellungen auf der Seite **Zusammenfassung** und klicken Sie auf **FERTIGSTELLEN**.

Der Assistent konfiguriert den Status des SNMP-Trap-Ziels nach der Reparatur der iDRAC- oder Host-Zugangsdaten durch die Bereitstellung gültiger Informationen im Host-Zugangsdatenprofil oder sobald einer der ersten vier Steckplätze im iDRAC-Trap-Ziel verfügbar wird oder wenn der Systemsperrmodus in iDRAC deaktiviert wird auf **Konfiguriert**.

ANMERKUNG: Der Systemsperrmodus ist nur für iDRAC9-basierte Server relevant.

Sind nicht WBEM-konforme Hosts vorhanden, so müssen Sie die Elemente dieser Hosts, die zum Fehlschlagen der Aktivierung des WBEM-Dienstes führten, manuell berichtigen. Sie können die Fehlerbedingungen beheben, indem Sie sie in den Nutzerprotokollen anzeigen. Aktivieren Sie OMIVV, um den WBEM-Service für diese Hosts während der Bestandsaufnahme zu aktivieren.

iDRAC-Lizenz-Compliance korrigieren

Eine kompatible iDRAC-Lizenz ist eine der Compliance-Kriterien für Hosts. Wenn Hosts keine kompatible iDRAC-Lizenz haben, werden diese Hosts auf der Seite **Verwaltungs-Compliance** als nicht konforme Hosts aufgeführt.

Sie können auf einen nicht konformen Host klicken, um Details anzuzeigen, wie z. B. iDRAC-Ablaufdatum, Lizenztyp und Lizenzbeschreibung. **BESTANDSAUFNAHME AUSFÜHREN** ist aktiv, wenn der iDRAC-Compliance-Status für einen beliebigen, einem Host-Zugangsdatenprofil zugeordneten Host **Nicht konform** oder **Unbekannt** ist.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Compliance** > **Verwaltungs-Compliance**, um die iDRAC-Lizenz-Compliance zu korrigieren.
2. Wählen Sie einen Host aus, dessen iDRAC-Lizenz nicht konform ist, und klicken Sie auf **IDRAC-LIZENZ ERNEUERN**.
3. Melden Sie sich bei Dell Digital Locker an, und aktualisieren oder erwerben Sie eine neue iDRAC-Lizenz.
   Nachdem Sie eine iDRAC-Lizenz installiert haben, führen Sie die Aufgabe zum Erstellen einer Bestandsaufnahme für den Host aus und kehren zu dieser Seite zurück, nachdem die Aufgabe zum Erstellen der Bestandsaufnahme erfolgreich abgeschlossen wurde.

Support für OEM-Server

OEM-Server werden von Dell EMC Partnern bereitgestellt, die ähnliche Funktionen oder Portfolios wie PowerEdge-Server anbieten.

- Ab OMIVV 4.3 werden OEM-Rack-Server unterstützt.
- OEM-Server lassen sich mithilfe des Assistenten **OEM-Hosts hinzufügen** eingliedern. Weitere Informationen über das Hinzufügen von OEM-Hosts finden Sie unter OEM-Hosts hinzufügen auf Seite 73.
  ANMERKUNG: Wenn der WBEM-Dienst auf den OEM-Hosts bereits aktiviert ist und zu vCenter hinzugefügt wird, fügt OMIVV diese OEM-Server standardmäßig der von OMIVV verwalteten Liste hinzu. Ordnen Sie die Hosts dem Host-Zugangsdatenprofil zu, um diese Server zu verwalten. Weitere Informationen zum Erstellen eines Host-Zugangsdatenprofils finden Sie unter Host-Anmeldeinformationenprofil erstellen auf Seite 39.
- Nach dem Eingliedern von OEM-Servern laufen alle Hostmanagementprozesse ähnlich wie beim Management von Dell EMC PowerEdge-Servern ab.
- Bare-Metal- und Bereitstellungsfunktionen werden mithilfe von iDRAC auch auf OEM-Servern unterstützt.

OEM-Hosts hinzufügen

Neben Dell EMC PowerEdge-Servern unterstützt OMIVV auch umbenannte Server anderer Marken(hersteller) bzw. Server mit Debranding. Weitere Informationen über OEM finden Sie unter https://www.dellemc.com.

Wenn der WBEM-Dienst bereits aktiviert ist, bestimmt OMIVV die iDRAC-Konnektivität des Hosts. Wenn die Verbindung verfügbar ist, fügt OMIVV den Host zur verwalteten Liste hinzu.

Wenn OMIVV die Konnektivität nicht bestimmen kann, müssen Sie den Host im Assistenten **OEM-Hosts hinzufügen** auswählen, sodass der Host zur durch OMIVV verwalteten Liste hinzugefügt wird.

Wenn der WBEM-Dienst deaktiviert ist oder der iDRAC nicht erreichbar ist, verwenden Sie den Assistenten **OEM-Hosts hinzufügen**, damit der Host der von OMIVV verwalteten Liste hinzugefügt wird.

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Compliance** > **Verwaltungs-Compliance** > **OEM-Hosts hinzufügen**.
2. Wählen Sie im Fenster **OEM-Hosts hinzufügen** aus der Dropdown-Liste **vCenter-Instanz** ein vCenter aus.
3. Wählen Sie aus der Dropdown-Liste **Host-Zugangsdatenprofil** ein entsprechendes Host-Zugangsdatenprofil aus.

4. Zum Hinzufügen oder Entfernen der zugeordneten Hosts klicken Sie auf **HOST HINZUFÜGEN**.
   Das Fenster **Hosts auswählen** wird angezeigt.
5. Wählen Sie im Fenster **Hosts auswählen** die Hosts aus und klicken Sie auf **JA**.

   ANMERKUNG: Es werden nur die Hosts im Fenster **Hosts auswählen** angezeigt, die nicht von OMIVV gehostet werden.

   OMIVV testet die Verbindung automatisch und die Ergebnisse der Testverbindungen werden unter **OEM-Hosts hinzufügen** angezeigt.

   Die Spalten **iDRAC-Test** und **Host-Test** zeigen die Ergebnisse der Testverbindungen für **iDRAC-Anmeldeinformationen** und **Host-Anmeldeinformationen** an.

   Um alle Testverbindungen zu beenden, klicken Sie auf **TEST ABBRECHEN**.
6. Klicken Sie auf **OK**.
   Die ausgewählten Hosts werden dem ausgewählten Host-Zugangsdatenprofil hinzugefügt und die Bestandsaufnahme wird ausgelöst.

Konfigurations-Compliance

Die Seite **Konfigurations-Compliance** zeigt den Status der Compliance basierend auf der Abweichungserkennung für alle Cluster an, die zum Clusterprofil gehören. In der PSC-Umgebung mit mehreren vCenter Servern listet die Seite „Konfigurations-Compliance“" alle Cluster aus allen vCenters auf, die dem gleichen PSC angehören, der mit derselben Appliance registriert ist.

- Hardwarekonfigurations-Compliance: Zeigt die Abweichung zwischen Attributen des im Clusterprofil verwendeten Systemprofils und den zugehörigen Hosts an, die Teil des Clusters sind.
- Firmware-Compliance: Zeigt die Abweichung der Firmware-Version zwischen dem im Clusterprofil verwendeten Firmware-Repository-Profil und den zugehörigen Hosts an, die Teil des Clusters sind.
- Treiber-Compliance: Zeigt die Abweichung der Treiberversion zwischen dem im Clusterprofil verwendeten Treiber-Repository-Profil und den zugehörigen vSAN-Hosts an, die Teil des Clusterprofils sind.

Konfigurations-Compliance anzeigen

1. Hosts and Clusters **Compliance und Bereitstellung** > **Compliance** > **Konfigurations-Compliance**.
   Eine Tabelle zeigt Cluster mit zugehörigem Clusterprofil, Systemprofil, Firmware-Repository-Profil und Treiber-Repository-Profil an.

   Für grundlegende und erweiterte Systemprofiltypen wird der Systemprofilname im folgenden Format angezeigt: Grundlegend_<Systemprofilname>, Erweitert_<Systemprofilname>.
2. Wählen Sie auf der Seite **Konfigurations-Compliance** ein Cluster aus.
   Die Konfigurations-Compliance-Informationen und der Compliance-Status werden angezeigt.

   Die folgenden Informationen werden im Abschnitt **Konfigurations-Compliance** angezeigt:

   - **Cluster-Name**: Der Name des Clusters
   - **WBEM-Status**: Zeigt den WBEM-Status an (Konform oder Nicht konform). Wenn einer der Hosts im Cluster nicht konform ist, wird der Status als „Nicht konform“ angezeigt.
   - **Anzahl der Hosts**: Die Gesamtzahl der Hosts, die im Cluster vorhanden sind
   - **Zeitplan**: Datum und Uhrzeit, zu dem/der der nächste Abweichungserkennungs-Job geplant ist.
   - **Zeitpunkt der letzten Abweichungserkennung**: Datum und Uhrzeit, zu dem/der der letzte Abweichungserkennungs-Job ausgeführt wurde.

   Im Abschnitt **Compliance-Status** wird der Compliance-Zustand der Hardware-, Firmware- und Treiberkomponenten angezeigt. Die verschiedenen Compliance-Zustände sind:

   - **Konform**: Zeigt die Anzahl der Hosts an, die mit den zugehörigen Hardware-, Firmware- und Treiberkomponenten kompatibel sind.
   - **Nicht konform**: Zeigt die Anzahl der Hosts an, die mit den zugehörigen Hardware-, Firmware- und Treiberkomponenten nicht konform sind.
   - **Nicht zutreffend**: Zeigt die Anzahl der nicht verfügbaren Hosts an.

     Hardwareabweichung gilt nicht für Hosts, die über das Gehäuse-Zugangsdatenprofil verwaltet werden.

     Die Treiberabweichung gilt nicht für die Hosts, die Teil von vSphere-Cluster sind.

     Wenn das Clusterprofil mithilfe des Online-Katalogs erstellt wird, gilt die Firmware-Compliance nicht für vSAN-Cluster.

3. Klicken Sie zum Anzeigen der Abweichungsdetails auf **Abweichungsbericht anzeigen**. Dieser Link ist nur für nicht konforme Cluster aktiviert. Weitere Informationen zum Anzeigen des Abweichungsberichts finden Sie unter Abweichungsbericht anzeigen auf Seite 75.

Abweichungsbericht anzeigen

Auf der Seite **Konfigurations-Compliance-Bericht** werden die Abweichungsdetails der Hardware-, Firmware- und Treiberkomponenten angezeigt.

Der Status des Abweichungserkennungs-Jobs wird im Abschnitt **Zusammenfassung** angezeigt.

Für Hardware:

- Hostname oder IP: Zeigt die Host-IP-Adresse oder den Hostnamen an.
- Service-Tag: Zeigt die Service-Tag-Nummer des Hosts an.
- Abweichungsstatus: Zeigt den Abweichungsstatus an (nicht konform oder fehlgeschlagen).
- Instanz: Zeigt den Hardware-Komponentennamen an.
- Gruppe: Zeigt den Gruppennamen der Attribute an.
- Attributname: Zeigt den Attributnamen an.
- Aktueller Wert: Zeigt den aktuellen Wert des Attributs auf dem Host an.
- Baseline-Wert: zeigt den Wert der Baseline an.
- Abweichungstyp/Fehler: Zeigt den Grund für die Nicht-Compliance an. Weitere Informationen zum Abweichungstyp finden Sie unter Vergleich von Komponenten- und Baseline-Version - Matrix auf Seite 180.

ANMERKUNG: Der Abweichungserkennungsjob schlägt nur dann fehl, wenn der Host oder iDRAC nicht erreichbar ist. Wenn der Host oder iDRAC erfolgreich inventarisiert wurde, wird der Abweichungserkennungs-Job als erfolgreich angezeigt. Informationen zum Überprüfen von anderen Ursachen für das Fehlschlagen der Abweichungserkennung finden Sie in der Spalte **Abweichungstyp/ Fehler** im Abweichungsbericht.

Für Firmware und Treiber:

- Hostname oder IP: Zeigt die Host-IP-Adresse oder den Hostnamen an.
- Service-Tag: Zeigt die Service-Tag-Nummer des Hosts an.
- Abweichungsstatus: Zeigt den Abweichungsstatus an.
- Komponentenname: zeigt den Namen der Komponente an.
- Aktueller Wert: Zeigt den aktuellen Wert des Attributs auf dem Host an.
- Baseline-Wert: zeigt den Wert der Baseline an.
- Abweichungstyp/Fehler: Zeigt den Grund für die Nicht-Compliance an. Weitere Informationen zum Abweichungstyp finden Sie unter Vergleich von Komponenten- und Baseline-Version - Matrix auf Seite 180.
- Dringlichkeit (bei Firmware): Zeigt die Prioritätsstufe für die Aktualisierung der Version einer identifizierten Komponente an.
- Empfehlung (für Treiber): Gibt die Aktualisierungsempfehlung einer Treiberkomponente an.

ANMERKUNG: Wenn mehr als eine Version der Firmware verfügbar ist, wird immer die neueste Firmware-Version für den Compliance-Vergleich verwendet.

Sie können die Filteroption verwenden, um die Abweichungsdetails basierend auf dem Abweichungsstatus anzuzeigen.

ANMERKUNG: Das 32-Bit-Firmware-Bundle wird in 5.x nicht unterstützt. Wenn das Clusterprofil in der 4.x-Version mit einem 32-Bit-Firmware-Bundle verknüpft ist, wird der Abweichungsstatus als fehlgeschlagen angezeigt, wenn Sie die Sicherung und Wiederherstellung von 4.x auf 5.x durchführen. Verwenden Sie das 64-Bit-Firmware-Bundle mit Clusterprofil und führen Sie den Abweichungserkennungs-Job erneut aus.

ANMERKUNG: Möglicherweise stellen Sie eine Abweichung zwischen dem OMIVV- und vSphere Lifecycle Manager-Abweichungsbericht fest. Der Grund dafür ist, dass der vSphere Lifecycle Manager immer einen Live Abweichungsbericht anzeigt und OMIVV den Abweichungsbericht, der auf dem geplanten Zeitpunkt und dem geplanten Zeitpunkt basiert. Wenn Sie eine Abweichung zwischen den Abweichungsberichten feststellen, führen Sie den Abweichungserkennungsjob nach Bedarf auf der Seite **Abweichungserkennungsjobs** aus.

12

OMIVV-Jobs verwalten

Auf der Seite **Jobs** werden folgende Jobs angezeigt:

- Bereitstellung
- Ermittlung
- Firmware-Updates
- Systemsperrmodus
- Abweichungserkennung
- Bestandsaufnahme
- Gewährleistung

OMIVV löscht ältere Jobs, wenn die Gesamtzahl der Jobs 500 erreicht. Diese Zahl umfasst vom Nutzer erstellte Jobs (z. b. Bereitstellungs-Jobs) sowie durch OMIVV erstellte Jobs (z. b. Job zum Erstellen von Integritätskennzahlen). Wenn die Anzahl der Jobs 500 überschreitet, werden die älteren 500 Jobs gelöscht.

Bereitstellungs-Jobs

Nachdem die Bereitstellungsaufgaben abgeschlossen sind, können Sie den Bereitstellungs-Job-Status auf der Seite **Bereitstellungs-Jobs** nachverfolgen.

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Bereitstellungs-Jobs**.
   Eine Tabelle zeigt alle Bereitstellungs-Jobs zusammen mit den folgenden Informationen an:
   - **Name**: Der Name des Bereitstellungs-Jobs
   - **Beschreibung**: Die Beschreibung des Jobs
   - **Geplante Zeit**: Datum und Uhrzeit, zu dem/der der Job geplant ist.
   - **Status**: Der Status des Bereitstellungs-Jobs.
   - **Erfassungsgröße**: Die Anzahl der Server im Bereitstellungs-Job.
   - **Fortschrittszusammenfassung**: Die Fortschrittsdetails des Bereitstellungs-Jobs.
2. Um weitere Informationen zu den Servern im Bereitstellungs-Job anzuzeigen, wählen Sie einen Bereitstellungs-Job aus.
   Die folgenden Informationen werden im unteren Fensterbereich angezeigt:
   - **Service-Tag**
   - **iDRAC-IP**
   - **Status**
   - **Warnungen**
   - **Einzelheiten**
   - **Startdatum und -uhrzeit**
   - **Enddatum und -zeit**
   - **Weitere Details**

   a. Um weitere Informationen über einen Bereitstellungs-Job anzuzeigen, wählen Sie einen Job aus und halten Sie den Mauszeiger über die Spalte **Details**.
   b. Für weitere Informationen zum Fehlschlagen von Systemprofil-basierten Jobs klicken Sie auf **Weitere Details**.
   Die folgenden Informationen werden angezeigt:
   - FQDD für die Komponente
   - Wert des Attributs
   - Alter Wert
   - Neuer Wert
   - Meldung und Meldungs-ID zu dem Fehler (wird für einige Arten von Fehlern nicht angezeigt)

   Bei einigen Attributen, die in **Attributname** unter **Systemprofil anwenden – Fehler-Details** angezeigt werden, ist das Fenster nicht identisch zum Attributnamen des Systemprofils beim Klicken auf **Weitere Details**.

3. Klicken Sie auf **ABBRECHEN**, um den Bereitstellungs-Job abzubrechen.
4. Um die Bereitstellungs-Jobs zu löschen, klicken Sie auf **ABGESCHLOSSENE LÖSCHEN**, wählen Sie dann **Älter als Datum und Jobstatus** und klicken Sie dann auf **Anwenden**.
   Die ausgewählten Jobs werden von der Seite **Bereitstellungs-Jobs** gelöscht.

Ermittlungs-Jobs

Nachdem der Ermittlungs-Tasks erstellt wurde, können Sie den Job-Status auf der Seite **Ermittlungs-Jobs** nachverfolgen.

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Ermittlungs-Jobs**.
   Eine Tabelle zeigt alle Ermittlungs-Jobs zusammen mit den folgenden Informationen an:
   - **Name**: Der Name des Ermittlungs-Jobs
   - **Beschreibung**: Die Beschreibung des Jobs
   - **Geplante Zeit**: Datum und Uhrzeit, zu dem/der der Job geplant ist.
   - **Status**: Der Status des Ermittlungs-Jobs

     Der Job-Status zeigt den Erfolg an, wenn der Server erfolgreich ermittelt wurde.

     Wenn ein Job fehlschlägt, wird der Grund für den Fehler angezeigt.
   - **Erfassungsgröße**: Die Anzahl der Server im Ermittlungs-Job
   - **Fortschrittszusammenfassung**: Die Fortschrittsdetails des Ermittlungs-Jobs
2. Wählen Sie einen spezifischen Ermittlungs-Job aus, um weitere Informationen anzeigen zu lassen.
   Die folgenden Informationen werden im unteren Fensterbereich angezeigt:
   - **iDRAC-IP**
   - **Status**
   - **Einzelheiten**
   - **Startdatum und -uhrzeit**
   - **Enddatum und -zeit**
3. Um die Ermittlungs-Job-Warteschlange zu löschen, klicken Sie auf **ABGESCHLOSSENE LÖSCHEN**.
   a. Wählen Sie das gewünschte Datum aus.
      Der Job vor dem ausgewählten Tag wird gelöscht.
   b. Wählen Sie den Status des Jobs aus.
   c. Klicken Sie auf **Anwenden**.

Gehäuse-Firmwareupdates-Jobs

Sobald die Gehäuse-Firmwareupdatesaufgaben abgeschlossen sind, können Sie den Status der Firmwareupdates-Jobs auf der Seite **Gehäuse-Firmwareupdates-Jobs** anzeigen.

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Firmwareupdate** > **Gehäuse-Firmwareupdate**.
2. Zum Anzeigen der aktuellen Protokollinformationen klicken Sie auf das Aktualisierungssymbol.
   Eine Tabelle zeigt alle Gehäuse-Firmwareupdates-Jobs zusammen mit den folgenden Informationen an:
   - **Status**: Der Status des Firmwareupdates-Jobs
   - **Geplante Zeit**: Die für den Firmwareupdates-Job geplante Zeit
   - **Name**: Der Name des Jobs
   - **Beschreibung**: Die Beschreibung des Firmwareupdates-Jobs
   - **vCenter**: Der Name des vCenter.
   - **Erfassungsgröße**: Die Anzahl der Gehäuse, die im Firmwareupdates-Job enthalten sind.

     Die Gesamtzahl der Gehäuse umfasst nur Haupt- und Standalone-Gehäuse. Das Mitgliedsgehäuse nimmt keine Rolle ein.
   - **Fortschrittszusammenfassung**: Details zum Fortschritt der Firmwareupdates-Jobs
3. Um weitere Informationen zu einem bestimmten Job anzuzeigen, wählen Sie einen Job aus.
   Die folgenden Informationen werden im unteren Fensterbereich angezeigt:
   - **Gehäuse-Service-Tag-Nummer**: Die Service-Tag-Nummer des Gehäuses
   - **Status**: Der Status des Jobs

- **Startzeit**: Die Startzeit des Firmwareupdates-Jobs
- **Endzeit**: Die Endzeit des Firmwareupdates-Jobs

4. Wenn Sie ein geplantes Firmwareupdate, das nicht ausgeführt wird, abbrechen möchten, wählen Sie den entsprechenden Job, und klicken Sie auf **STOPP**.

   WARNUNG: Wenn Sie einen Firmwareupdatesjob abbrechen möchten, der bereits an das MX-Gehäuse übermittelt wurde, wird die Firmware möglicherweise trotzdem auf dem Host aktualisiert. OMIVV meldet den Job als abgebrochen.

5. Wenn Sie frühere Firmwareupdate-Jobs oder geplante Firmwareupdates bereinigen möchten, klicken Sie auf **ABGESCHLOSSENE LÖSCHEN**.
   Das Dialogfeld **Firmwareupdates-Jobs säubern** wird angezeigt. Sie können Jobs nur bereinigen, die abgebrochen wurden, erfolgreich abgeschlossen oder fehlgeschlagen sind. Geplante oder aktive Jobs können Sie nicht bereinigen.
6. Wählen Sie im Dialogfeld **Firmwareupdates-Jobs bereinigenÄlter als Datum und Job-Status** aus und klicken Sie auf **OK**.
   Die ausgewählten Jobs werden dann aus der Liste der **Gehäuse-Firmwareupdates-Jobs** gelöscht.

Host-Firmwareupdates-Jobs

Sobald die Gehäuse-Firmwareupdatesaufgaben abgeschlossen sind, können Sie den Status der Firmwareupdates-Jobs auf der Seite **Host-Firmwareupdates-Jobs** anzeigen.

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Firmwareaktualisierung** > **Host-Firmwareupdate**.
2. Zum Anzeigen der aktuellen Protokollinformationen klicken Sie auf das Aktualisierungssymbol.
   Eine Tabelle zeigt alle Host-Firmwareupdates-Jobs zusammen mit den folgenden Informationen an:

   - **Status**: Der Status des Firmwareupdates-Jobs
   - **Geplante Zeit**: Die für den Firmwareupdates-Job geplante Zeit
   - **Name**: Der Name des Jobs
   - **Beschreibung**: Die Beschreibung des Firmwareupdates-Jobs
   - **vCenter**: Der Name des vCenter.
   - **Erfassungsgröße**: Die Anzahl der Server im Firmwareupdates-Job
   - **Fortschrittszusammenfassung**: Details zum Fortschritt der Firmwareupdates-Jobs

3. Um weitere Informationen zu einem bestimmten Job anzuzeigen, wählen Sie einen Job aus.
   Die folgenden Informationen werden im unteren Fensterbereich angezeigt:

   - **Hostname**: Die Service-Tag-Nummer des Hosts
   - **Status**: Der Status des Jobs
   - **Startzeit**: Die Startzeit des Firmwareupdates-Jobs
   - **Endzeit**: Die Endzeit des Firmwareupdates-Jobs

   ANMERKUNG: Wenn der Firmwareupdates-Job mit mehreren Dell Update Packages geplant ist und OMIVV einige der ausgewählten Aktualisierungspakete nicht herunterladen kann, aktualisiert OMIVV weiterhin die erfolgreich heruntergeladenen Pakete. Auf der Jobs-Seite wird der Status der heruntergeladenen Pakete angezeigt.

4. Wenn Sie ein geplantes Firmwareupdate, das nicht ausgeführt wird, abbrechen möchten, wählen Sie den entsprechenden Job und klicken Sie auf **STOPP**.

   WARNUNG: Wenn Sie einen Firmwareupdates-Job abbrechen möchten, der bereits an iDRAC übermittelt wurde, wird die Firmware möglicherweise trotzdem auf dem Host aktualisiert. OMIVV meldet den Job als abgebrochen.

5. Wenn Sie frühere Firmwareupdate-Jobs oder geplante Firmwareupdates bereinigen möchten, klicken Sie auf **ABGESCHLOSSENE LÖSCHEN**.
   Das Dialogfeld **Firmwareupdates-Jobs säubern** wird angezeigt. Sie können Jobs nur bereinigen, die abgebrochen wurden, erfolgreich abgeschlossen oder fehlgeschlagen sind. Geplante oder aktive Jobs können Sie nicht bereinigen.
6. Wählen Sie im Dialogfeld **Firmwareupdates-Jobs bereinigenÄlter als Datum und Job-Status** aus und klicken Sie auf **OK**.
   Die ausgewählten Jobs werden dann aus der Liste der **Host-Firmwareupdates-Jobs** gelöscht.

Systemsperrmodus-Jobs

Die Einstellung für den Systemsperrmodus wird nur für iDRAC9-basierte Server unterstützt. Aktiviert sperrt die Einstellung die Systemkonfiguration, einschließlich Firmwareupdates. Diese Einstellung dient ausschließlich zum Schutz des Systems vor unbeabsichtigten Änderungen. Sie können den Systemsperrmodus für verwaltete Hosts mithilfe des OMIVV-Geräts oder über die iDRAC-

Konsole ein- oder ausschalten. Ab der OMIVV-Version 4.1 können Sie den Sperrmodus von iDRAC auf Servern konfigurieren und überwachen. Außerdem muss der iDRAC über eine Enterprise-Lizenz verfügen, um den Lockdown-Modus zu aktivieren.

ANMERKUNG: Sie können den Systemsperrmodus nicht für Hosts ändern, die vom Gehäuse-Zugangsdatenprofil verwaltet werden.

Sobald die Konfiguration der Systemsperre abgeschlossen ist, können Sie den aktualisierten Status des Sperrmodus auf der Seite **Systemsperrmodus-Jobs** einsehen.

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Systemsperrmodus**.
   Eine Tabelle zeigt alle Systemsperrmodus-Jobs zusammen mit den folgenden Informationen an:
   - **Name**: Der Name des Systemsperrmodus-Jobs.
   - **Beschreibung**: Die Beschreibung des Jobs
   - **Geplante Zeit**: Datum und Uhrzeit, zu dem/der der Systemsperrmodus-Job geplant ist.
   - **vCenter**: Der Name des vCenter.
   - **Status**: Der Status des Systemsperrmodus-Jobs.
   - **Erfassungsgröße**: Die Anzahl der Server, die im Systemsperrmodus-Job enthalten sind.
   - **Fortschrittszusammenfassung**: Die Fortschrittsdetails des Systemsperrmodus-Jobs.
2. Um weitere Informationen zu den Servern im Systemsperrmodus-Job anzuzeigen, wählen Sie einen Systemsperrmodus-Job aus.
   Die folgenden Informationen werden im unteren Fensterbereich angezeigt:
   - **Service-Tag**
   - **iDRAC-IP**
   - **Hostname**
   - **Status**
   - **Einzelheiten**
   - **Startdatum und -uhrzeit**
   - **Enddatum und -zeit**

   Um weitere Informationen über einen Systemsperrmodus-Job anzuzeigen, wählen Sie einen Job aus und halten Sie den Mauszeiger über die Spalte **Details**.
3. Um die Systemsperrmodus-Jobs zu löschen, klicken Sie auf **ABGESCHLOSSENE LÖSCHEN**, wählen Sie **Älter als Datum und Jobstatus** aus, und klicken Sie auf **ANWENDEN**.
   Die ausgewählten Jobs werden aus der Seite **Systemsperrmodus-Jobs** gelöscht.

Abweichungserkennungsjob

Ein Abweichungserkennungsjob wird zum Vergleich zwischen der geprüften Baseline und der Serverkonfiguration ausgeführt, einschließlich Hardwarekonfiguration, Firmware- und Treiberversionen.

ANMERKUNG: Der Abweichungserkennungsjob schlägt nur dann fehl, wenn der Host oder iDRAC nicht erreichbar ist. Wenn der Host oder iDRAC erfolgreich inventarisiert wurde, wird der Abweichungserkennungsjob erfolgreich ausgeführt und Sie können die Abweichungsdetails im Abweichungsbericht anzeigen. Weitere Informationen zum Abweichungsbericht finden Sie unter Abweichungsbericht anzeigen auf Seite 75.

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Abweichungserkennung**.
   Eine Tabelle zeigt alle Abweichungserkennungs-Jobs zusammen mit den folgenden Informationen an:
   - **Name**: Der Name des Abweichungserkennungsjobs.
   - **Letzte Ausführung**: Datum und Uhrzeit, zu dem/der der letzte Abweichungserkennungs-Job ausgeführt wurde.
   - **Nächste Ausführung**: Datum und Uhrzeit, zu dem/der der nächste Abweichungserkennungs-Job geplant ist.
   - **Status**: Der Status des Abweichungserkennungsjobs.
   - **Erfassungsgröße**: Die Anzahl der Server im Abweichungserkennungsjob.
   - **Fortschrittszusammenfassung**: Die Fortschrittsdetails des Abweichungserkennungsjobs.
2. Um die aktualisierten Details des Abweichungserkennungs-Jobs aufzurufen, klicken Sie auf **Aktualisieren**.
3. Um weitere Informationen zu den Servern im Abweichungserkennungsjob anzuzeigen, wählen Sie einen Abweichungserkennungsjob aus. Die folgenden Informationen werden angezeigt:
   - Service-Tag
   - iDRAC-IP
   - Hostname
   - Cluster
   - vCenter

- Status
- Startdatum und -uhrzeit
- Enddatum und -zeit

4. Klicken Sie zum bedarfsgerechten Durchführen eines **Abweichungserkennungs-Jobs** auf die Schaltfläche **JETZT AUSFÜHREN**.

   In einem Baseline-Cluster wird der Abweichungserkennungsjob nach dem Hinzufügen eines Hosts zum Host- oder Gehäuse-Zugangsdatenprofil für einen neu hinzugefügten Host automatisch ausgeführt.

Host-Bestandsaufnahme-Job anzeigen

Die Seite **Host-Bestandsaufnahme** zeigt Informationen über den letzten Bestandaufnahme-Job an, der auf einem Host ausgeführt wird, das einem Host-Zugangsdatenprofil zugeordnet ist.

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Bestand** > **Host-Bestand**.
2. Wählen Sie ein vCenter aus, um alle zugehörigen Hosts-Bestandsaufnahmeinformationen anzuzeigen.

   - **vCenter**: FQDN oder IP-Adresse des vCenter.
   - **Bestandene Hosts**: Die Anzahl der Hosts, für die die Bestandsaufnahme erfolgreich ist
   - **Letzte Bestandsaufnahme**: Datum und Uhrzeit, zu dem/der die letzte Bestandsaufnahme ausgeführt wurde
   - **Nächste Bestandsaufnahme**: Datum und Uhrzeit, zu dem/der die nächste Bestandsaufnahme geplant ist

   Die Details der zugeordneten Hosts werden im unteren Bereich angezeigt.

   - **Host**: FQDN oder IP-Adresse der Hosts.
   - **Status**: Der Bestandsaufnahmestatus der Hosts. Die Optionen umfassen:
     - **Erfolgreich**
     - **Fehlgeschlagen**
     - **Wird durchgeführt**
   - **Dauer (MM:SS)**: Die Dauer des Bestandsaufnahme-Jobs in Minuten und Sekunden.
   - **Startdatum/Zeit**: Datum und die Uhrzeit, zu dem/der der Bestandsaufnahme-Job gestartet wurde
   - **Enddatum/-zeit**: Die Zeit, zu der der Bestandsaufnahme-Job beendet wurde

Bestandsaufnahme-Job ausführen

Sobald die Erstkonfiguration abgeschlossen ist, wird die Bestandsaufnahme automatisch für alle Hosts, die einem Host-Zugangsdatenprofil hinzugefügt sind, ausgelöst.

1. Um die Bestandsaufnahme nach Bedarf auszuführen, klicken Sie auf **Jobs** > **Bestand** > **Host-Bestand**.
2. Klicken Sie auf **JETZT AUSFÜHREN**.
3. Klicken Sie auf **Aktualisieren**, um den Status des Bestandsaufnahme-Jobs zu aktualisieren.
   Nachdem der Bestandsaufnahmejob abgeschlossen ist, können Sie Host-Informationen auf der Seite **OMIVV-Host-Informationen** anzeigen.
4. Um die OMIVV-Hostinformationen anzuzeigen, erweitern Sie **Menü** und wählen Sie dann **Hosts und Cluster** aus.
5. Wählen Sie im linken Fensterbereich einen Host aus.
6. Wählen Sie im rechten Fensterbereich die Option **Überwachen** und dann **OMIVV Hostinnformation**. aus.
   Die folgenden Informationen werden angezeigt:

   - Hardware-Bestandsaufnahme
   - Speicher
   - Firmware
   - Stromüberwachung
   - Gewährleistung
   - System-Ereignisprotokoll

   Wenn die Hosts unter Verwendung des Gehäuse-Zugangsdatenprofils verwaltet werden, zeigen die Daten zur Firmware-Bestandsaufnahme ein paar zusätzliche Komponenten wie den Lifecycle Controller und Software-RAID an.

   ANMERKUNG: Der Bestandsaufnahme-Job für Hosts, die die Lizenzbegrenzung überschreiten, wird übersprungen und als fehlgeschlagen markiert.

7. Auf der Seite **Zusammenfassung** im Abschnitt **OMIVV Hostinformation** können Sie auch die folgenden Aktionen ausführen:
   - Remote-Zugriffskonsole (iDRAC) starten
   - Server-LED-Anzeige blinken lassen
   - Systemsperrmodus konfigurieren

     Wenn die Hosts über Gehäuse verwaltet werden, wird das Konfigurieren des Systemsperrmodus nicht unterstützt.
   - Firmware-Assistent ausführen

Host-Bestandsaufnahme-Job ändern

Nachdem Sie Hosts einem Host-Zugangsdatenprofil zugeordnet haben, müssen Sie eine regelmäßige Bestandsaufnahme planen, um sicherzustellen, dass die Inventarinformationen der Hosts aktuell sind. „Bestandsaufnahme-Jobs“ zeigt den Status der auf den Hosts ausgeführten Bestandsaufnahme-Jobs an.

Sie können den Bestandsaufnahme-Zeitplan auch auf der Seite **Einstellungen** > **Zeitplan für Datenabruf** > **Bestandsaufnahme Abruf** ändern.

1. Wählen Sie auf der Seite **Jobs** eine vCenter-Instanz aus, und klicken Sie auf **ZEITPLAN ÄNDERN**.
   Das Dialogfeld **Abruf von Bestandsaufnahmedaten bearbeiten** wird angezeigt.
2. Führen Sie im Bereich **Bestandsaufnahmedaten** die folgenden Schritte aus:
   a. Aktivieren Sie das Kontrollkästchen **Abruf von Bestandsaufnahmedaten aktivieren (empfohlen)**.
   b. Wählen Sie den Tag und die Uhrzeit für den Abruf von Bestandsaufnahmedaten aus und klicken Sie auf **ANWENDEN**.
   c. Um die Einstellungen zurückzusetzen, klicken Sie auf **LÖSCHEN**.
   d. Um den Bestandaufnahme-Job sofort auszuführen, klicken Sie auf der Seite **Jobs** auf **JETZT AUSFÜHREN**.

   ANMERKUNG: Für Server, die keine iDRAC Express oder Enterprise-Lizenz haben, schlägt die Inventarisierung fehl, da das Lizenz-Upgrade für den iDRAC erforderlich ist.

   ANMERKUNG: Beim Ausführen einer modularen Host-Bestandsaufnahme werden entsprechende Gehäuse automatisch erkannt. Wenn das Gehäuse Teil eines Gehäuse-Zugangsdatenprofils ist, wird die Gehäuse-Bestandsaufnahme automatisch nach der Host-Bestandsaufnahme ausgeführt.

Gehäuse-Bestandsaufnahme-Job anzeigen

Die Seite **Gehäuse-Bestandsaufnahme** zeigt Informationen über den letzten Bestandsaufnahme-Job an, der auf einem Gehäuse ausgeführt wurde, das einem Gehäuse-Anmeldeinformationenprofil zugeordnet ist.

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Bestand** > **Gehäuse-Bestand**.
2. Um die Informationen zur Gehäuse-Bestandsaufnahme anzuzeigen, wählen Sie ein Gehäuse aus.
   - **Gehäuse-IP-Adresse/Hostname**: Die IP-Adresse des Gehäuses.
   - **Service Tag**: Zeigt die Service-Tag-Nummer des Gehäuses an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer im Falle von Fragen und Wartungsdiensten.
   - **Status**: Der Status des Gehäuses
   - **Dauer (MM:SS)**: Die Dauer des Bestandsaufnahme-Jobs in Minuten und Sekunden
   - **Startdatum/Zeit**: Das Datum und die Uhrzeit, zu der der Bestandsaufnahme-Job gestartet wurde.
   - **Enddatum/-zeit**: Die Zeit, zu der der Bestandsaufnahme-Job beendet wurde

   In einer MCM-Gruppe wird die Bestandsaufnahme nur auf dem Lead-Gehäuse ausgeführt. Die Bestandsinformation stellt Daten zu Lead- und Mitglieds-Gehäusen bereit.

   ANMERKUNG: Der Gehäusebestandsaufnahme-Job wird auf den folgenden PowerEdge-Servern nicht unterstützt: C6320P, C6320, C4130 und C6420.

   ANMERKUNG: MX-Gehäuse-Blade-Server werden nur mit ESXi-Version 6.5U2 oder höher unterstützt. Wenn frühere ESXi-Versionen auf diesen Hosts bereitgestellt werden, schlägt der Bestandaufnahme-Job in OMIVV fehl.

Gehäuse-Bestandsaufnahme-Job ausführen

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Gehäuse-Bestand**.
2. Wählen Sie ein Gehäuse aus, und klicken Sie auf **JETZT AUSFÜHREN**.

   Sobald die Gehäuse-Bestandsaufnahme abgeschlossen ist, können Sie die Gehäuseinformationen auf der Seite **Hosts & Gehäuse** > **Gehäuse** anzeigen.
3. Um die Gehäuseinformationen anzuzeigen, wählen Sie auf der Seite **Gehäuse** ein Gehäuse aus und klicken Sie dann auf **ANZEIGEN**.

   ANMERKUNG: Während der Bestandsaufnahme werden das Trap-Ziel und Warnungsrichtlinien durch OMIVV auf dem Lead-Gehäuse in einer MCM-Gruppe konfiguriert.

   ANMERKUNG: Wenn die Hosts über Gehäuse verwaltet werden, löst die laufende Gehäuse-Bestandsaufnahme auch die Host-Bestandsaufnahme für die Hosts aus. Außerdem löst das Ausführen der Host-Bestandsaufnahme die Gehäuse-Bestandsaufnahme aus.

Host-Gewährleistung anzeigen

Ein Service-Job ist ein geplanter Job zum Abrufen von Serviceinformationen auf allen Systemen von www.dell.com/support. Das OMIVV-Gerät benötigt eine Internetverbindung, um Serviceinformationen zu extrahieren. Je nach Netzwerkeinstellungen benötigt OMIVV möglicherweise Proxy-Informationen, um über das Internet erreichbar zu sein und Serviceinformationen abzurufen. Die Proxy-Daten können in der Administratorkonsole aktualisiert werden.

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Service** > **Host-Gewährleistung**.
2. Wählen Sie ein vCenter aus, um alle zugehörigen Host-Informationen anzuzeigen.

   - **vCenter**: Die Liste der vCenter.
   - **Bestandene Hosts**: Die Anzahl der vCenter-Hosts, die bestanden haben
   - **Letzter Service**: Datum und Uhrzeit, zu dem/der der letzte Servicejob ausgeführt wurde.
   - **Nächster Service**: Datum und Uhrzeit, zu dem/der der nächste Servicejob geplant ist.

   Die zugehörigen Hostinformationen werden im unteren Bereich angezeigt.

   - **Host**: Die Host-IP-Adresse.
   - **Status**: Der Status des Service-Jobs, der folgende Optionen umfasst:
     - Erfolgreich
     - Fehlgeschlagen
     - Wird durchgeführt
     - Geplant
   - **Dauer (MM:SS)**: Die Dauer des Service-Jobs in MM:SS.
   - **Startdatum/Zeit**: Datum und die Uhrzeit, zu dem/der der Service-Job gestartet wurde
   - **Enddatum/Zeit**: Datum und Uhrzeit, zu dem/der der Service-Job beendet wurde
3. Um die Host-Gewährleistung nach Bedarf auszuführen, klicken Sie auf **JETZT AUSFÜHREN**.

Host Service-Job ändern

Die Service-Jobs werden ursprünglich im **Erstkonfigurationsassistenten** konfiguriert. Sie können die Service-Jobzeitpläne auch auf der Seite **Einstellungen** > **Servicedaten Abruf** > **Service-Abruf** ändern.

1. Erweitern Sie auf der Seite **Jobs** die Option **Service** und wählen Sie dann **Host-Gewährleistung** aus.
2. Wählen Sie ein vCenter aus, und klicken Sie auf **ZEITPLAN ÄNDERN**.
3. Führen Sie im Bereich **Servicedaten** die folgenden Schritte aus:
   a. Aktivieren Sie das Kontrollkästchen **Abruf von Servicedaten aktivieren (empfohlen)**.
   b. Wählen Sie den Tag und die Uhrzeit für den Abruf von Servicedaten aus und klicken Sie auf **ANWENDEN**.
   c. Um die Einstellungen zurückzusetzen, klicken Sie auf **LÖSCHEN**.

Gehäuseservice anzeigen

Ein Gewährleistungs-Job ist ein geplanter Task zum Abrufen von Serviceinformationen auf allen Systemen von support.dell.com. Das OMIVV-Gerät benötigt eine Internetverbindung, um Serviceinformationen zu extrahieren. Stellen Sie sicher, dass das OMIVV-Gerät über eine Internetverbindung verfügt. Je nach Netzwerkeinstellungen benötigt OMIVV möglicherweise Proxy-Informationen, um über das Internet erreichbar zu sein und Serviceinformationen abzurufen. Die Proxy-Daten können in der Administratorkonsole aktualisiert werden.

1. Klicken Sie auf der OMIVV-Startseite auf **Jobs** > **Service** > **Gehäuse-Service**.

   In einer Tabelle werden alle Informationen zum Gehäuseservice-Job angezeigt.

   - **Gehäuse-IP/Hostname**: Die Host-IP-Adresse
   - **Service-Tag-Nummer**: Die Service-Tag-Nummer des Gehäuses
   - **Status**: Der Status des Service-Jobs, der folgende Optionen umfasst:
     - Erfolgreich
     - Fehlgeschlagen
     - Wird durchgeführt
     - Geplant
   - **Dauer (MM:SS)**: Die Dauer des Service-Jobs in MM:SS.
   - **Startdatum/Zeit**: Das Datum und die Uhrzeit, zu der der Service-Job gestartet wurde.
   - **Enddatum/Zeit**: Die Zeit, zu der der Service-Job beendet wurde.

2. Um den Gehäuse-Service-Job nach Bedarf auszuführen, klicken Sie auf **JETZT AUSFÜHREN**.

13

Protokolle verwalten

Protokollverlauf anzeigen

1. Klicken Sie auf der Seite **OpenManage Integration für VMware vCenter** auf **Protokolle**, um alle Protokolle anzuzeigen.
   Der OMIVV-Protokollabrufprozess ruft alle Protokolle aus der Datenbank ab. Dies kann einige Sekunden dauern, basierend auf der Protokollgröße.

   - Um die Protokolldaten zu exportieren, klicken Sie auf das  .
   - Klicken Sie auf die Spaltenüberschrift, um die Daten in der Tabelle zu sortieren.
   - Um zwischen den Seiten zu navigieren, klicken Sie auf die Symbole für „Zurück“ und „Weiter“.
   - Um die Protokolle zu aktualisieren, klicken Sie auf das Aktualisierungssymbol in der oberen linken Ecke.

2. Klicken Sie auf das ▼ zum Filtern der Protokolle anhand der folgenden Kategorien und/oder Datumsbereiche:
   Kategorien

   - **Alle Kategorien**
   - **Informationen**
   - **Warnung**
   - **Fehler**

   Datum:

   - **Letzte Woche**
   - **Letzten Monat**
   - **Letztes Jahr**
   - **Benutzerdefinierter Bereich**: Wenn Sie diese Option auswählen, geben Sie das Start- und Enddatum durch Klicken auf das Kalendersymbol an.

3. Klicken Sie nach Auswahl der gewünschten Kategorie und des Datums auf **ANWENDEN**.
   Sie können die Protokolle anzeigen, die in Beziehung zur ausgewählten Kategorie und/oder den Datumsbereich stehen. Die Protokolldatentabelle zeigt 100 Protokolle pro Seite an.
4. Klicken Sie zum Löschen der gefilterten Daten auf **FILTER LÖSCHEN**.

14

OMIVV-Geräteeinstellungen verwalten

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

- Konfigurieren Sie die Serviceablaufbenachrichtigungseinstellungen. Weitere Informationen finden Sie unter Serviceablaufbenachrichtigung einrichten auf Seite 85.
- Konfigurieren Sie die Benachrichtigung zur aktuellen Geräteversion. Weitere Informationen finden Sie unter Benachrichtigung über aktuelle Geräteversion konfigurieren auf Seite 86.
- Überschreiben Sie den Schweregrad für proaktive HA-Warnmeldungen. Weitere Informationen finden Sie unter Schweregrad der Funktionszustands-Aktualisierungsbenachrichtigung überschreiben auf Seite 90.
- Erstkonfiguration. Weitere Informationen finden Sie unter . Erstkonfiguration auf Seite 90
- Konfigurieren Sie Ereignisse und Alarme und zeigen Sie sie an. Weitere Informationen finden Sie unter Konfigurieren von Ereignissen und Alarmen auf Seite 96.
- Planen oder ändern Sie die Datenabrufzeitpläne für Bestandsaufnahme und Service an. Weitere Informationen finden Sie unter Einen Bestandsaufnahme-Job planen auf Seite 108 und Serviceabfrage-Jobs planen auf Seite 109.

Mehrere Geräte verwalten

Wenn mehrere vCenter-Instanzen denselben PSC gemeinsam nutzen und bei mehr als einer Instanz eines OMIVV-Geräts registriert sind, können Sie mit diesem Assistenten zwischen den verschiedenen Instanzen von OMIVV wechseln.

Die aktuelle Instanz von OMIVV sehen Sie auf der Startseite.

1. Klicken sie auf der Startseite von **OMIVV** auf **ÄNDERN**.
   - **IP/Name**: FQDN oder IP-Adresse des OMIVV-Geräts.
   - **Version**: Die aktuelle Version des OMIVV-Geräts.
   - **Konformitätsstatus**: Der Status (**Konform** oder **Nicht konform**) des OMIVV-Geräts, je nach Version.
   - **Verfügbarkeitsstatus**: Der Verfügbarkeitsstatus des OMIVV-Geräts, abhängig davon, ob die OMIVV-Dienste ausgeführt werden oder nicht. **OK** oder **FEHLER** wird angezeigt, um den Betriebszustand von OMIVV anzuzeigen.
   - **Registrierte vCenter Server**: FQDN oder IP des registrierten vCenter-Servers.
   - **Aktionen**: Der Aktionsname (**AUSWÄHLEN** oder **AUSGEWÄHLT**).
2. Klicken Sie auf der Seite **OMIVV-Gerät wechseln** auf **AUSWÄHLEN**.
3. Um zu bestätigen, klicken Sie auf **JA**.
   Sie können die Änderung der Geräte-IP auf der Startseite sehen.

Serviceablaufbenachrichtigung einrichten

Aktivieren Sie die Benachrichtigung zum Ablauf des Service, um benachrichtigt zu werden, wenn die Services für einen der Hosts kurz vor dem Ablauf stehen.

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **Benachrichtigungen** > **Serviceablaufbenachrichtigung**.
2. Wählen Sie **Gewährleistungsablaufbenachrichtigung für Hosts aktivieren**.
3. Wählen Sie aus, wie viele Tage vor Ablauf des Service Sie benachrichtigt werden möchten.
4. Klicken Sie auf **ANWENDEN**.

Benachrichtigung über aktuelle Geräteversion konfigurieren

Um über die Verfügbarkeit einer neuen OMIVV-Version informiert zu werden, markieren Sie das Kontrollkästchen **Benachrichtigung zur aktuellen Version aktivieren (empfohlen)**. Es empfiehlt sich, dies wöchentlich zu überprüfen. Um die neuesten Funktionen der Geräteversionsbenachrichtigung von OMIVV zu verwenden, müssen Sie über eine Internetverbindung verfügen. Wenn Ihre Umgebung einen Proxy für die Verbindung mit dem Internet benötigt, stellen Sie sicher, dass Sie die Proxy-Einstellungen auf dem Admin-Portal konfigurieren.

Zum Empfangen regelmäßiger Benachrichtigungen zur Verfügbarkeit der aktuellen Version (RPM, OVF, RPM/OVF) von OMIVV führen Sie die folgenden Schritte aus, um die Benachrichtigung zur aktuellen Version zu konfigurieren:

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **Anwendungseinstellungen** > **Benachrichtigungen** > **Benachrichtigung zur aktuellen Version**.
2. Aktivieren Sie das Kontrollkästchen **Benachrichtigung zur aktuellen Version aktivieren**.
3. Um Benachrichtigung zur aktuellen Geräteversion zu erhalten, wählen Sie Datum und Uhrzeit aus.
4. Klicken Sie auf **ANWENDEN**.

Konfigurieren von Anmeldeinformationen für die Bereitstellung

OMIVV fungiert als Bereitstellungsserver. Die Anmeldeinformationen für die Bereitstellung ermöglichen Ihnen, mit dem iDRAC zu kommunizieren, der das OMIVV-Plug-in als Bereitstellungsserver im Prozess der automatischen Ermittlung verwendet. Mit den Bereitstellungs-Anmeldeinformationen können Sie iDRAC-Anmeldedaten einrichten, um bis zum Abschluss des Betriebssystem-Bereitstellungsprozesses sicher mit einem Bare-Metal-Server zu kommunizieren, das über die automatische Erkennung erkannt wird.

Nach erfolgreichem Abschluss des Betriebssystem-Bereitstellungsprozesses ändert OMIVV die iDRAC-Anmeldeinformationen wie im Host-Zugangsdatenprofil angegeben. Wenn Sie die Bereitstellungs-Anmeldeinformationen ändern, werden alle neu erkannten Systeme ab diesem Zeitpunkt mit den neuen iDRAC-Anmeldeinformationen bereitgestellt. Die Anmeldeinformationen auf Servern, die vor der Änderung der Bereitstellungs-Anmeldeinformationen erkannt wurden, sind jedoch von dieser Änderung nicht betroffen.

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **Appliance-Einstellungen** > **Anmeldeinformationen für die Bereitstellung**.
2. Geben Sie den Nutzernamen und das Kennwort ein. Der Standard-Nutzername lautet **root** und das Kennwort **calvin**.
   Stellen Sie sicher, dass Sie das Kennwort basierend auf der iDRAC-Nutzerkennwort-Richtlinie eingeben, die in iDRAC festgelegt ist. Stellen Sie außerdem sicher, dass Sie von iDRAC unterstützte Zeichen verwenden.
3. Klicken Sie auf **ANWENDEN**.

Funktionszustand der Hardware-Komponentenredundanz – Proaktive HA

Die proaktive HA ist eine Funktion von vCenter, die mit OMIVV funktioniert. Wenn Sie die proaktive HA aktivieren, schützt die Funktion Ihre Arbeitslasten mittels proaktiver Maßnahmen basierend auf der Verschlechterung des Redundanz-Funktionszustands der unterstützten Komponenten in einem Host.

Nach Prüfung des Redundanz-Funktionszustands der unterstützten Hostkomponenten aktualisiert das OMIVV-Gerät die Funktionszustandsänderung auf dem vCenter-Server. Die möglichen Redundanz-Funktionszustände für die unterstützten Komponenten (Netzteil, Lüfter und IDSDM) sind:

- Fehlerfrei (Informationen): Komponente arbeitet normal
- Warnung (Mäßig herabgesetzt) – Komponente weist einen nichtkritischen Fehler auf. Die mäßig herabgesetzten Zustände werden als *Warnung* in der Spalte **Typ** auf der Seite **Ereignisse** angezeigt.
- Kritisch (Stark herabgesetzt) – Komponente weist einen kritischen Fehler auf.

ANMERKUNG: Ein *unbekannter* Funktionszustand gibt die Nichtverfügbarkeit von Funktionszustandaktualisierungen der proaktiven HA bei den Dell Inc Providern an. Ein unbekannter Funktionszustand kann in folgenden Situationen auftreten:

- Alle Hosts, die zu einem proaktiven HA-Cluster hinzugefügt wurden, können möglicherweise noch einige Minuten im unbekannten Zustand bleiben, bis OMIVV sie mit ihren entsprechenden Zuständen initialisiert.
- Die Hosts können bei einem Neustart eines vCenter-Servers in einem proaktiven HA-Cluster in einen unbekannten Zustand versetzt werden, bis OMIVV sie mit ihren entsprechenden Zuständen erneut initialisiert.

Wenn OMIVV eine Änderung beim Redundanz-Funktionszustand der unterstützten Komponenten erkennt (entweder über Traps oder eine Abfrage), wird die Benachrichtigung über die Funktionszustandaktualisierung für die Komponente an den vCenter-Server gesendet. Die Abfrage wird pro Stunde ausgeführt und steht als Ausfallsicherung für die Abdeckung eines Trap-Datenverlusts zur Verfügung.

ANMERKUNG:

- Bei der Konfiguration von Ereignissen wird empfohlen, die Option „Alle Ereignisse senden“ als Ereignisanzeigeebene auszuwählen. Weitere Informationen zum Konfigurieren von Ereignissen finden Sie unter Konfigurieren von Ereignissen und Alarmen auf Seite 96.
- Die proaktive HA steht nur auf den Plattformen zur Verfügung, die Redundanz auf Netzteil, Lüfter und IDSDM unterstützen.
- Die proaktive Hochverfügbarkeit wird für diejenigen Netzteile nicht unterstützt, für die keine Redundanz konfiguriert werden kann (zum Beispiel Netzteile mit Kabel).

Proaktive HA-Ereignisse

Basierend auf den von VMware unterstützten Komponenten für die proaktive HA werden die folgenden Ereignisse vom Dell Inc Provider während seiner Registrierung bei vCenter registriert.

Tabelle 5. Proaktive HA-Ereignisse

Dell Inc. Provider Ereignis	Komponententyp	Beschreibung
DellFanRedundancy	Lüfter	Lüfterredundanz-Ereignis
DellPowerRedundancy	Netzteil (PSU)	Stromredundanz-Ereignis
DellIDSDMRedundancy	Speicher	IDSDM-Redundanz-Ereignis **ANMERKUNG:** Wenn die Hosts dem Proactive HA-fähigen Cluster hinzugefügt werden und wenn IDSDM-Komponenten vorhanden sind, stellen Sie sicher, dass die interne SD-Karten-Redundanz in den iDRAC-Einstellungen als **Spiegelung** konfiguriert ist.

Für einen Host mit proaktiver HA werden die folgenden Traps von OMIVV als Auslöser zur Bestimmung des redundanten Zustands der Komponenten verwendet:

Tabelle 6. Proaktive HA-Ereignisse

Name des Ereignisses	Beschreibung	Schweregrad
Lüfter-Informationen	Lüfter-Informationen	Info
Lüfterwarnung	Lüfterwarnung	Warnung
Lüfterfehler	Lüfterfehler	Kritisch
Netzteil normal	Netzteil auf Normalwert zurückgekehrt	Info
Netzteilwarnung	Netzteil hat eine Warnung erkannt	Warnung
Netzteilfehler	Beim Netzteil ist ein Fehler aufgetreten	Kritisch
Netzteil nicht vorhanden	Netzteil ist nicht vorhanden.	Kritisch
Redundanzinformationen	Redundanzinformationen	Info
Redundanz herabgesetzt	Redundanz herabgesetzt	Warnung
Redundanzverlust	Redundanzverlust	Kritisch

Tabelle 6. Proaktive HA-Ereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad
Es liegen Informationen zum integrierten Dual SD-Modul vor.	Es liegen Informationen zum integrierten Dual SD-Moduls vor.	Info
Es liegt eine Warnung für das integrierte Dual SD-Modul vor.	Es liegt eine Warnung für das integrierte Dual SD-Modul vor.	Warnung
Es liegt ein Fehler am integrierten Dual SD-Modul vor.	Es liegt ein Fehler am integrierten Dual SD-Modul vor.	Kritisch
Das integrierte Dual SD-Modul ist nicht vorhanden.	Das integrierte Dual SD-Modul ist nicht vorhanden.	Kritisch
Es liegen Informationen zur Redundanz des integrierten Dual SD-Moduls vor.	Es liegen Informationen zur Redundanz des integrierten Dual SD-Moduls vor.	Info
Die Redundanz des integrierten Dual SD-Moduls ist herabgesetzt.	Die Redundanz des integrierten Dual SD-Moduls ist herabgesetzt.	Warnung
Die Redundanz des integrierten Dual SD-Moduls ist nicht mehr vorhanden.	Die Redundanz des integrierten Dual SD-Moduls ist nicht mehr vorhanden.	Kritisch
Gehäuseereignisse		
Lüfter-Informationen	Lüfter-Informationen	Info
Lüfterwarnung	Lüfterwarnung	Warnung
Lüfterfehler	Lüfterfehler	Kritisch
Netzteil normal	Netzteil auf Normalwert zurückgekehrt	Info
Netzteilwarnung	Netzteil hat eine Warnung erkannt	Warnung
Netzteilfehler	Beim Netzteil ist ein Fehler aufgetreten	Kritisch
Redundanzinformationen	Redundanzinformationen	Info
Redundanz herabgesetzt	Redundanz herabgesetzt	Warnung
Redundanzverlust	Redundanzverlust	Kritisch

Proactive HA für Rack- und Tower-Server konfigurieren

Stellen Sie sicher, dass alle Hosts für die Redundanz der drei unterstützten redundanten Komponenten (Netzteil, Lüfter und IDSDM) konfiguriert sind.

1. Erstellen Sie ein Host-Anmeldeinformationenprofil und ordnen Sie Hosts einem Host-Anmeldeinformationenprofil zu. Informationen dazu finden Sie unter Host-Anmeldeinformationenprofil erstellen auf Seite 39.
2. Stellen Sie sicher, dass die Host-Bestandsaufnahme erfolgreich abgeschlossen wurde. Informationen dazu finden Sie unter Host-Bestandsaufnahme-Job anzeigen auf Seite 80.
3. Stellen Sie sicher, dass das SNMP Trap-Ziel unter iDRAC als die IP-Adresse des OMIVV-Geräts eingestellt ist.
   ANMERKUNG: Stellen Sie sicher, dass Sie die Verfügbarkeit eines Hosts für einen Proactive HA-Cluster aus den Protokolldaten bestätigen.
4. Aktivieren Sie die proaktive HA auf einem Cluster. Siehe Aktivieren von proaktiver HA auf einem Cluster.

Proactive HA für modulare Server konfigurieren

Vor dem Konfigurieren der proaktiven HA auf modularen Servern vergewissern Sie sich, dass die folgenden Bedingungen erfüllt sind:

- Alle Hosts für die Redundanz der drei unterstützten redundanten Komponenten (Netzteil, Lüfter und IDSDM) sind richtig konfiguriert.
- Host- und Gehäusebestandsaufnahme wurden erfolgreich abgeschlossen.

ANMERKUNG: Es wird empfohlen, dass sich alle modularen Hosts in einen proaktiven HA-Cluster nicht im gleichen Gehäuse befinden, denn ein Ausfall der Gehäusekomponenten (PSU und Lüfter) Auswirkungen auf alle zugehörigen Server hat.

1. Erstellen Sie ein Host-Anmeldeinformationenprofil und ordnen Sie Hosts dem Host-Anmeldeinformationenprofil zu. Informationen dazu finden Sie unter Host-Anmeldeinformationenprofil erstellen auf Seite 39.
2. Stellen Sie sicher, dass die Host-Bestandsaufnahme erfolgreich abgeschlossen wurde. Informationen dazu finden Sie unter Host-Bestandsaufnahme-Job anzeigen auf Seite 80.
   ANMERKUNG: Stellen Sie sicher, dass Sie die Verfügbarkeit eines Hosts für einen Proactive HA-Cluster aus den Protokolldaten bestätigen.
3. Erstellen Sie ein Gehäuse-Anmeldeinformationenprofil für die zugeordneten Gehäuse. Informationen dazu finden Sie unter Gehäuse-Zugangsdatenprofil erstellen auf Seite 44.
4. Stellen Sie sicher, dass die Gehäuse-Bestandsaufnahme erfolgreich abgeschlossen wurde. Informationen dazu finden Sie unter Gehäuse-Bestandsaufnahme-Job anzeigen auf Seite 81.
5. Starten Sie den CMC oder OME-Modular und überprüfen Sie, ob das Trap-Ziel für das Gehäuse als IP-Adresse des OMIVV-Geräts eingestellt wurde. Weitere Informationen zur Konfiguration von Traps finden Sie im CMC- und OME-Modular-Benutzerhandbuch unter **dell.com/Support**.
6. Aktivieren Sie die proaktive HA auf einem Cluster. Siehe Aktivieren von proaktiver HA auf einem Cluster.

Proactive HA auf Clustern aktivieren

Vor dem Aktivieren von Proactive HA auf Clustern vergewissern Sie sich, dass die folgenden Bedingungen erfüllt sind:

- Ein Cluster mit aktiviertem DRS wird in der vCenter-Konsole erstellt und konfiguriert. Informationen zum Aktivieren von DRS auf einem Cluster finden Sie in der VMware-Dokumentation.
- Alle Hosts, die Teil des Clusters sind, sollten Teil eines Host-Zugangsdatenprofils und erfolgreich inventarisiert sein.
- Bei einem modularen Server muss das entsprechende Gehäuse zum Gehäuse-Zugangsdatenprofil hinzugefügt und erfolgreich inventarisiert werden.

1. Blenden Sie in vSphere Client **Menü** ein und wählen Sie dann **Hosts und Cluster** aus.
   Alle Hosts und Cluster werden im linken Fensterbereich angezeigt.
2. Wählen Sie ein Cluster aus und klicken Sie im rechten Fensterbereich auf **vSphere DRS** > **BEARBEITEN**.
3. Wählen Sie **vSphere DRS** aus, wenn diese Option nicht ausgewählt ist.
4. Wählen Sie **Konfigurieren** > **vSphere Verfügbarkeit** > **Proaktive HA** > **Bearbeiten** aus.
   Das Fenster **Cluster-Einstellungen bearbeiten** wird angezeigt.
5. Wählen Sie auf der Seite **Cluster-Einstellungen bearbeiten** die Option **Proactive HA**aus.
6. Wählen Sie im Abschnitt **Ausfälle und Antworten** im Dropdown-Menü die **Manuelle** oder **Automatische** Automatisierungsebene aus.
7. Für **Fehlerbehebung** wählen Sie Quarantäne-Modus, Wartungsmodus oder eine Kombination aus Quarantäne- und Wartungsmodus basierend auf dem Schweregrad-Status (gemischter Modus). Weitere Informationen hierzu finden Sie in der VMware-Dokumentation.
8. Klicken Sie auf **Anbieter** und wählen Sie **Dell Inc** als Anbieter für das Cluster aus.
9. Klicken Sie auf **SPEICHERN**.

Sobald Proactive HA auf einem Cluster aktiviert ist, initialisiert OMIVV den Proactive HA-Zustands- und Redundanzstatus und meldet diese an vCenter. Basierend auf der Benachrichtigung zur Funktionszustandaktualisierung von OMIVV führt der vCenter-Server die manuelle oder automatische Aktion durch, die Sie für **Fehlerbehebung** ausgewählt haben.

Informationen zum Überschreiben des vorhandenen Schweregrads finden Sie unter Schweregrad der Funktionszustands-Aktualisierungsbenachrichtigung überschreiben auf Seite 90.

Alle Anpassungen, die auf dem eingetragenen Dell Funktionszustand-Update-Anbieter für PHA-Cluster durchgeführt werden, werden nach dem RPM-Upgrade- und Backup- und Wiederherstellungsvorgang auf die Standardwerte wiederhergestellt.

Schweregrad der Funktionszustands-Aktualisierungsbenachrichtigung überschreiben

Sie können einstellen, dass der vorhandene Schweregrad der proaktiven Dell HA-Ereignisse für den Dell EMC Host und seine Komponenten mit dem benutzerdefiniertem Schweregrad überschrieben wird, der auf Ihre Umgebung ausgerichtet ist.

Im Folgenden werden die Schweregrade aufgeführt, die für jedes der proaktiven HA-Ereignisse gelten:

- **Info**
- **Mäßig herabgesetzt**
- **Stark herabgesetzt**

ANMERKUNG: Sie können den Schweregrad der proaktiven HA-Komponenten mit dem Schweregrad **Info** anpassen.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Einstellungen** > **Schweregrad für proaktiven HA überschreiben**. Das Datenraster zeigt alle unterstützten proaktiven Hochverfügbarkeitsereignisse an. Zu den Spalten des Datenrasters gehören Spalten wie Ereignis-IDs, Ereignisbeschreibung, Komponententyp, Standardschweregrad und die Spalte „Schweregrad überschreiben“ für die Anpassung des Schweregrads des Hosts und den dazugehörigen Komponenten.
2. Um den Schweregrad eines Hosts oder seiner Komponente zu ändern, wählen Sie in der Spalte **Schweregrad überschreiben** den erforderlichen Status aus der Dropdownliste aus.
   Diese Richtlinie gilt für alle proaktiven HA-Hosts auf alle vCenter-Servern, die bei OMIVV registriert sind.
3. Wiederholen Sie Schritt 2 für alle Ereignisse, die angepasst werden sollen.
4. Führen Sie eine der folgenden Aktionen aus:
   a. Zum Speichern der Anpassung klicken Sie auf **ANWENDEN**.
   b. Klicken Sie auf **ABBRECHEN**, um die Einstellungen zum Überschreiben des Schweregrads abzubrechen.

   Klicken Sie auf **AUF STANDARDEINSTELLUNG ZURÜCKSETZEN**, um die Einstellungen zum Überschreiben des Schweregrads auf die Standardeinstellungen zurückzusetzen.

Erstkonfiguration

Nachdem Sie die grundlegende Installation von OMIVV und die Registrierung der vCenter abgeschlossen haben, wird automatisch erstmals der Erstkonfigurationsassistent angezeigt, wenn Sie auf das OMIVV-Symbol klicken.

Wenn Sie den Assistenten für die Erstkonfiguration später starten möchten, navigieren Sie zu:

- **Einstellungen** > **Erstkonfigurationsassistent** > **ERSTKONFIGURATIONSASSISTENT STARTEN**
- **Dashboard** > **Schnellverweise** > **ERSTKONFIGURATIONSASSISTENT STARTEN**

1. Lesen Sie auf der **Willkommen**-Seite die Anweisungen und klicken Sie dann auf **ERSTE SCHRITTE**.
2. Wählen Sie auf der Seite **vCenter auswählen** im Drop-Down-Menü **vCenter** ein bestimmtes vCenter oder **Alle registrierten vCenter** aus und klicken Sie dann auf **WEITER**.
   ANMERKUNG: Wenn mehrere vCenter-Server als Bestandteil des gleichen PSC vorhanden sind und mit derselben OMIVV registriert sind und Sie die Konfiguration eines einzelnen vCenters ausgewählt haben, müssen Sie Schritt 2 wiederholen, bis Sie jedes vCenter konfiguriert haben.
3. Klicken Sie auf der Seite **Host-Zugangsdatenprofil erstellen** auf **HOST-ZUGANGSDATENPROFIL ERSTELLEN**.
   Weitere Informationen zum Erstellen eines Host-Zugangsdatenprofils finden Sie unter Host-Anmeldeinformationenprofil erstellen auf Seite 39.

   Nachdem Hosts zu einem Host-Zugangsdatenprofil hinzugefügt wurden, wird die IP-Adresse von OMIVV automatisch als SNMP-Trap-Ziel für den iDRAC des Hosts festgelegt. OMIVV aktiviert den WBEM-Service und deaktiviert ihn dann nach dem Abrufen der iDRAC-IP-Adresse für Hosts, auf denen ESXi 6.5 und höher ausgeführt wird.

   OMIVV verwendet den WBEM-Service, um den ESXi-Host und die iDRAC-Beziehungen ordnungsgemäß zu synchronisieren. Wenn die Konfiguration des SNMP-Trap-Ziels und/oder das Aktivieren des WBEM-Service für bestimmte Hosts fehlschlägt, werden diese Hosts als „nicht konform“ geführt. Informationen zum Anzeigen und Beheben der Nichtübereinstimmung finden Sie im Abschnitt Nicht konformen Host reparieren auf Seite 72 .
4. Führen Sie auf der Seite **Zusätzlichen Einstellungen konfigurieren** die folgenden Schritte aus:
   a. Planen Sie Bestandsaufnahme-Jobs. Weitere Informationen zum Planen von Bestandsaufnahme-Jobs finden Sie unter Einen Bestandsaufnahme-Job planen auf Seite 108.
   b. Serviceabfrage-Job planen Weitere Informationen zum Planen von Serviceabfrage-Jobs finden Sie unter Serviceabfrage-Jobs planen auf Seite 109.

Wenn Sie den Zeitplan für die Bestandsaufnahme ändern möchten, navigieren Sie zu **Einstellungen** > **vCenter Einstellungen** > **Zeitplan Datenabruf** > **Bestandsaufnahme-Abruf** oder **Jobs** > **Bestand** > **Hosts-Bestandaufnahme**.

Wenn Sie den Zeitplan für den Gewährleistungsabruf ändern möchten, navigieren Sie zu **Einstellungen** > **vCenter Einstellungen** > **Zeitplan Datenabruf** > **Gewährleistungsabruf** oder **Jobs** > **Gewährleistung**.

c. Konfigurieren von Ereignissen und Alarmen. Informationen zum Konfigurieren von Ereignissen und Alarmen finden Sie unter Konfigurieren von Ereignissen und Alarmen auf Seite 96.

d. Um einzelne Einstellungen anzuwenden, klicken Sie separat auf die Schaltfläche **Anwenden** und klicken Sie dann auf **Weiter**.

Es wird dringend empfohlen, alle zusätzlichen Einstellungen zu aktivieren. Wenn keine der zusätzlichen Einstellungen angewendet werden, wird eine Meldung angezeigt, die darauf hinweist, dass alle zusätzlichen Einstellungen obligatorisch sind.

5. Lesen Sie auf der Seite **Weitere Schritte** die Anweisungen und klicken Sie dann auf **BEENDEN**.

Es wird empfohlen, Ihre OMIVV-Hosts mit einer Konfigurations-Baseline zu verknüpfen, da Ihnen dies ermöglicht, die Konfigurationsänderungen in Hosts und zugehörigen Clustern aufmerksam zu überwachen. Die Konfigurations-Baseline kann für jedes Cluster erstellt werden, sobald die Hosts erfolgreich von OMIVV verwaltet werden. Gehen Sie wie folgt vor, um eine Konfigurations-Baseline zu erstellen:

- Repository-Profil für Firmware und Treiber erstellen: Auf diese Weise können Sie Baseline-Firmware- und Treiberversionen definieren.
- Systemprofil erstellen: Hier können Sie Baseline-Hardwarekonfigurationen für Hosts definieren.
- Clusterprofil erstellen: Um eine erfolgreiche Baseline zu erstellen, wählen Sie Cluster aus und ordnen Sie Firmware, Treiber und Hardwarekonfigurationen zu.
- Die in einem PowerEdge MX-Gehäuse mit einem deaktivierten iDRAC IPv4 vorhandenen Hosts müssen über ein Gehäuse-Anmeldeinformationsprofil verwaltet werden.

Status der Erstkonfiguration anzeigen

Auf der Seite „Assistent für die Erstkonfiguration“ können Sie die folgenden Aufgaben ausführen:

- Status der Erstkonfiguration anzeigen

  Der erste Konfigurationsstatus wird nur dann als abgeschlossen angezeigt, wenn alle vCenter mit Host-Anmeldeinformationen-Profil, Ereignissen und Alarmen, Bestandsaufnahme und Service-Jobs konfiguriert sind.

- Assistent für die Erstkonfiguration starten

Einstellungen für die Firmware-Update

Wenn Sie das Kontrollkästchen **iDRAC Jobs löschen und iDRAC zurücksetzen** aktivieren, werden alle in der **Job-Warteschlange** vorhandenen iDRAC-Jobs gelöscht, gefolgt von der iDRAC-Zurücksetzung vor der Aktualisierung der Firmware auf dem Host.

Die Einstellung **iDRAC-Jobs löschen und iDRAC zurücksetzen** wird bei der Durchführung folgender Vorgänge verwendet:

- Firmware-Update unter Verwendung von OMIVV

  Diese Einstellung kann während der Aktualisierung der Firmware unter Verwendung von OMIVV überschrieben werden. Das Überschreiben der Einstellung hat jedoch keine Auswirkungen auf die Einstellungen, die auf der Seite **Firmware-Aktualisierungseinstellungen** vorgenommen werden.

- Firmware-Korrektur mithilfe von vSphere Lifecycle Manager

  Diese Einstellung kann nicht überschrieben werden, während Firmware-Korrekturen durchgeführt werden.

1. Aktivieren Sie das Kontrollkästchen **iDRAC Jobs löschen und iDRAC zurücksetzen**.
2. Klicken Sie auf **ANWENDEN**.

Lizenzinformationen anzeigen

Beim Installieren der OMIVV-Lizenz wird die Anzahl der unterstützten Hosts und vCenter Server in dieser Registerkarte angezeigt.

Um eine Softwarelizenz zu kaufen, klicken Sie neben **Softwarelizenz** auf **Lizenz kaufen**. Weitere Informationen finden Sie unter Eine Softwarelizenz erwerben auf Seite 93.

Die folgenden Informationen werden auf der Seite **Lizenzierung** angezeigt:

Lizenztyp	Beschreibung
Hostlizenzen	• Verfügbare Lizenzen Zeigt die Anzahl der verfügbaren Lizenzen an • In Verwendung befindliche Lizenzen Zeigt die Anzahl der in Verwendung befindlichen Lizenzen an
vCenter-Lizenzen	• Verfügbare Lizenzen Zeigt die Anzahl der verfügbaren Lizenzen an • In Verwendung befindliche Lizenzen Zeigt die Anzahl der in Verwendung befindlichen Lizenzen an

Im Abschnitt **Lizenzverwaltung** werden folgende Links angezeigt:

- Produktlizenzierungsportal (Digital Locker)
- Admin-Konsole

OpenManage Integration for VMware vCenter-Lizenzierung (OMIVV)

OMIVV verfügt über zwei Arten von Lizenzen:

- Evaluierungslizenz – Wenn die OMIVV Appliance zum ersten Mal hochgefahren wird, wird automatisch eine Evaluierungslizenz installiert. Die Testversion beinhaltet eine Test-Lizenz für fünf Hosts (Server), die durch OMIVV verwaltet werden. Diese 90-Tage-Testversion ist die Standardlizenz, die mitgeliefert wird.
- Standard Lizenz – Sie können eine beliebige Anzahl von Host-Lizenzen erwerben, die von OMIVV verwaltet werden. Diese Lizenz umfasst Produktunterstützung und Updates der OMIVV-Appliance. Die Standard Lizenz ist für drei oder fünf Jahre verfügbar. Jede zusätzliche erworbene Lizenz verlängert den Zeitraum der bestehenden Lizenz.

Die Lizenzdauer für einen einzelnen XML-Schlüssel wird basierend auf dem Verkaufstermin der ursprünglichen Bestellung berechnet. Alle hochgeladenen neuen Lizenzen werden nach Ablauf der Toleranzperiode von 90 Tagen in der Zählung für eine vorab ablaufende Lizenzierung angezeigt.

Der OMIVV unterstützt bis zu 15 vCenter-Instanzen. Wenn Sie eine Testlizenz auf eine vollwertige Standardlizenz hochstufen, erhalten Sie eine Bestellbestätigung per E-Mail und können die Lizenzdatei im Dell Digital Locker herunterladen. Speichern Sie die XML-Lizenzdatei auf Ihrem lokalen System und laden Sie die neue Lizenzdatei mithilfe der **Verwaltungskonsole** hoch.

Wenn Sie die Lizenzdatei kaufen, können Sie die XML-Datei (Lizenzschlüssel) über Dell Digital Locker unter **https://www.dell.com/support** herunterladen. Wenn Sie einen Lizenzschlüssel nicht herunterladen können, finden Sie unter **Bestellsupport kontaktieren** auf der Seite **https://www.dell.com/support** die Telefonnummer für das regionale Dell Supportteam für Ihr Produkt.

Die Lizenzierung enthält die folgenden Informationen in der OMIVV-Verwaltungskonsole:

- Höchstzahl der vCenter-Verbindungslizenzen – bis zu 15 registrierte und verwendete vCenter-Verbindungen sind aktiviert.
- Höchstzahl der Host-Verbindungslizenzen – die Anzahl der erworbenen Hostverbindungen (mit maximal 2000 Hosts, die für eine einzige OMIVV-Instanz unterstützt werden).
- In Verwendung – die Anzahl an Lizenzen für vCenter-Verbindungen oder Hostverbindungen. Bei Hostverbindungen steht diese Zahl für die Anzahl an Hosts (oder Servern), die in die Bestandsliste aufgenommen wurden.
- Verfügbar – die Anzahl von Lizenzen für vCenter-Verbindungen oder Hostverbindungen, die für die Nutzung zur Verfügung stehen.

Beim Versuch, einen Host zu einem Host-Zugangsdatenprofil hinzuzufügen, wird verhindert, dass weitere Hosts hinzugefügt werden, wenn die Anzahl der lizenzierten Servern über die Lizenzanzahl hinausgeht. OMIVV bietet keine Unterstützung für die Verwaltung einer Anzahl von Hosts, die die Anzahl der verfügbaren Hostlizenzen übersteigt.

ANMERKUNG: Jede aktive Lizenz kann für OMIVV 5.x-Versionen verwendet werden. Lizenzen, die von vorherigen Instanzen von OMIVV gesichert oder erneut von Digital Locker heruntergeladen wurden, können für aktuelle Instanzen von OMIVV verwendet werden.

Eine Softwarelizenz erwerben

1. Navigieren Sie zu **Einstellungen** > **Lizenzierung** > **Lizenz kaufen**, oder **Dashboard** > **Lizenz kaufen** oder **Admin Portal** > **vCenter Registrierung** > **Lizenzierung** > **JETZT KAUFEN**.
   Die Supportseite von DellEMC wird angezeigt.
2. Laden Sie die Lizenzdatei herunter und speichern Sie Sie an einem bekannten Speicherort.
   Möglicherweise erhalten Sie die Lizenzdatei als gepackte ZIP-Datei. Stellen Sie sicher, dass Sie die Zip-Datei entpacken und laden Sie nur die XML-Lizenzdatei hoch. Die Lizenzdatei wird wahrscheinlich auf Grundlage Ihrer Auftragsnummer benannt (wie beispielsweise 123456789.xml).

Auf Support-Informationen zugreifen

Tabelle 7. Informationen auf der Seite „Support“

Name	Beschreibung
Dokumentations-Support	Stellt folgende Dokumentations-Links bereit: • PowerEdge-Server • OMIVV-Handbücher • iDRAC mit Lifecycle Controller
Verwaltungskonsole	Stellt einen Link zur Verwaltungskonsole bereit
Allgemeine Hilfe	Stellt einen Link zur Dell EMC Support-Website bereit.
iDRAC zurücksetzen	Stellt einen Link für eine Zurücksetzung des iDRAC bereit, der verwendet werden kann, wenn iDRAC nicht reagiert. Diese Zurücksetzung führt einen normalen Neustart des iDRAC aus. Weitere Informationen zum Zurücksetzen des iDRAC finden Sie unter iDRAC zurücksetzen auf Seite 94.
Bevor Sie den technischen Support anrufen	Bietet Tipps an, wie Sie Dell EMC Support kontaktieren und Anrufe richtig weiterleiten.
Fehlerbehebungsdatei	Stellt einen Link zum Erstellen und Herunterladen der Fehlerbehebungsdatei bereit. Sie können diese Datei bereitstellen oder anzeigen, wenn Sie den technischen Support kontaktieren. Weitere Informationen finden Sie unter Fehlerbehebungsbundle erstellen und herunterladen auf Seite 93.
Empfehlungen von Dell EMC	Stellt einen Link zur Dell EMC Dell Repository Manager (DRM)-Support-Seite bereit. Der DRM wird zum Erstellen eines nutzerdefinierten Katalogs verwendet, der zur Aktualisierung der Firmware- und Abweichungserkennung verwendet werden kann.

Fehlerbehebungsbundle erstellen und herunterladen

Um das Fehlerbehebungspaket zu erzeugen, stellen Sie sicher, dass Sie sich beim Administratorportal anmelden.

Das Fehlerbehebungspaket enthält Informationen zur Protokollierung von OMIVV-Geräten, die verwendet werden können, um Probleme zu lösen oder an den technischen Support zu senden. OMIVV protokolliert keine sensiblen Nutzerdaten.

1. Klicken Sie auf der Seite **Support** auf **Fehlerbehebungsdatei erstellen und herunterladen**.
   Das Dialogfeld **Fehlerbehebungsdatei** wird angezeigt.
2. Klicken Sie im Dialogfeld **Fehlerbehebungsdatei** auf **ERSTELLEN**.
   Je nach Größe der Protokolle kann die Erstellung der Datei einige Zeit dauern.
3. Klicken Sie auf **DOWNLOAD**, um die Datei zu speichern.

iDRAC zurücksetzen

Das Reset des iDRAC führt einen normalen iDRAC-Neustart durch. Nach dem Zurücksetzen von iDRAC wird der iDRAC normalerweise neu gestartet, aber nicht der Host. Nach dem Zurücksetzen kann der iDRAC erst nach wenigen Minuten verwendet werden. Setzen Sie einen iDRAC nur dann zurück, wenn er auf einem OMIVV-Gerät nicht reagiert.

- Sie können diese Reset-Aktion nur auf Hosts ausführen, die Teil eines Host-Anmeldeinformationenprofils sind und mindestens einmal Teil einer Bestandsaufnahme waren.
- Dell EMC empfiehlt, den Host in den Wartungsmodus zu versetzen und dann den iDRAC zurückzusetzen.
- Wenn der iDRAC nach dem Zurücksetzen des iDRAC unbrauchbar wird oder nicht mehr reagiert, führen Sie einen Hardware-Reset des iDRAC durch. Informationen zum Hardware-Reset finden Sie im iDRAC Benutzerhandbuch, das unter https://www.Dell.com/Support/verfügbar ist.

Während der Neustart des iDRACs durchgeführt wird, sehen Sie eventuell folgende Meldungen:

- Verzögerung der Kommunikation, während der OMIVV den Host-Funktionsstatus abruft.
- Alle Sitzungen, die derzeit für iDRAC geöffnet sind, werden beendet.
- Eine Änderung der DHCP-Adresse des iDRAC. Wenn iDRAC DHCP zum Erstellen seiner IP-Adresse verwendet, kann sich die iDRAC-IP-Adresse ändern. In diesem Fall führen Sie die Host-Bestandsaufnahme erneut aus, um die neue iDRAC-IP-Adresse in den Bestandsdaten zu erfassen.

1. Klicken Sie auf der Seite **Support** auf **IDRAC ZURÜCKSETZEN**.
2. Geben Sie auf der Seite **iDRAC ZURÜCKSETZEN** den Host-Namen oder die IP-Adresse ein.
3. Um zu bestätigen, dass Sie den iDRAC-Reset-Vorgang verstehen, aktivieren Sie das Kontrollkästchen **Ich verstehe die Auswirkungen des iDRAC-Reset.** Aktivieren Sie das Kontrollkästchen **iDRAC auf dem ausgewählten Host zurücksetzen**.
4. Klicken Sie auf **IDRAC ZURÜCKSETZEN**.

15

vCenter-Einstellungen verwalten

Informationen zu Ereignissen und Alarmen

Auf der Seite **Einstellungen** können Sie die Ereignisse und Alarme für Hosts und Gehäuse aktivieren, die Ereignis-Veröffentlichungsstufe auswählen und Standard-Alarme wiederherstellen. Sie können Ereignisse und Alarme für einzelne vCenter oder für alle registrierten vCenter konfigurieren. Die Ereignisse und Alarme, die einem Gehäuse entsprechen, werden vCenter zugeordnet.

Dies sind die vier Ereignisanzeigeebenen:

Tabelle 8. Ereignisanzeigeebene

Ereignis	Beschreibung
Keine Ereignisse anzeigen	OMIVV kann keine Ereignisse oder Warnmeldungen an die zugehörigen vCenter weiterleiten.
Alle Ereignisse anzeigen	Anzeigen aller Ereignisse, einschließlich informeller Ereignisse, die das OMIVV von den verwalteten Dell EMC Hosts der betroffenen vCenter erhält. Es wird empfohlen, die Option **Alle Ereignisse anzeigen** als Ereignisanzeigeebene auszuwählen.
Nur kritische Ereignisse und Warnungsereignisse anzeigen	Veröffentlicht nur kritische Ereignisse und Warnungen an die zugehörigen vCenter.
Nur kritische Ereignisse und Warnungsereignisse hinsichtlich der Visualisierung anzeigen	Veröffentlichen von virtualisierungsrelevanten Ereignissen, die von Hosts in die entsprechenden vCenter empfangen werden. Virtualisierungsrelevante Ereignisse sind Ereignisse, die Dell für Hosts, die virtuelle Maschinen ausführen, für höchst bedeutend erachtet.

Beim Konfigurieren von Ereignissen und Alarmen führen kritische Hardware-Alarme dazu, dass das OMIVV das Hostsystem in den Wartungsmodus versetzt. Migrieren Sie die virtuellen Maschinen in bestimmten Fällen zu einem anderen Host-System. Die OMIVV leitet die von verwalteten Hosts empfangenen Ereignisse an vCenter weiter und erstellt Alarme für diese Ereignisse. Sie können diese Alarme dazu verwenden, Aktionen des vCenter wie einen Neustart, den Wartungsmodus oder eine Migration zu veranlassen.

Beispiel: Wenn eine Netzversorgung ausfällt und ein Alarm erzeugt wird, versetzt die sich daraus ergebende Aktion den Computer in den Wartungsmodus, was dazu führt, dass Arbeitsauslastungen in einen anderen Host im Cluster migriert werden.

Alle Hosts außerhalb oder innerhalb der Cluster ohne aktiviertes VMware Drs (Distributed Resource Scheduling) können virtuelle Maschinen sehen, die aufgrund eines kritischen Ereignisses heruntergefahren werden. Dell EMC empfiehlt, DRS vor dem Aktivieren der Dell Alarme zu aktivieren. Weitere Informationen finden Sie in der VMware-Dokumentation.

Das DRS überwacht die Nutzung kontinuierlich über einen Ressourcen-Pool und teilt verfügbare Ressourcen gemäß den Geschäftsanforderungen intelligent zwischen den virtuellen Maschinen auf. Um sicherzustellen, dass virtuelle Maschinen bei kritischen Hardware-Ereignissen automatisch migriert werden, verwenden Sie Cluster mit DRS-konfigurierten Dell Alarmen. In den Details der Bildschirmmeldungen werden alle eventuell betroffenen Cluster in der vCenter-Instanz aufgeführt. Prüfen Sie, ob die Cluster betroffen sind, bevor Sie Ereignisse und Alarme aktivieren.

Wenn Sie die standardmäßigen Alarmeinstellungen wiederherstellen möchten, wählen Sie die Option **Alarme wiederherstellen** aus. Über diese Option kann die standardmäßige Alarm-Konfiguration bequem wiederhergestellt werden, ohne dass das Produkt de- und neuinstalliert werden muss. Alle nach der Installation geänderten Dell EMC Alarmkonfigurationen werden über die Option **Alarme wiederherstellen** zurückgesetzt.

ANMERKUNG: Um die Dell Ereignisse zu erhalten, stellen Sie sicher, dass Sie die erforderlichen Ereignisse in iDRAC, CMC und Management Controller aktivieren.

ANMERKUNG: Das OMIVV trifft eine Vorauswahl der erforderlichen virtualisierungsrelevanten Ereignisse, damit Hosts virtuelle Rechner erfolgreich ausführen können. Standardmäßig sind Dell Hostalarme deaktiviert. Sind die Dell EMC Alarme aktiviert, sollten die Cluster DRS verwenden, um sicherzustellen, dass virtuelle Rechner, die kritische Ereignisse senden, automatisch migriert werden.

Konfigurieren von Ereignissen und Alarmen

Zum Empfangen von Ereignissen von den Servern müssen Sie sicherstellen, dass das SNMP-Trap-Ziel in iDRAC festgelegt ist. OMIVV unterstützt SNMP v1- und v2-Warnmeldungen.

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **vCenter-Einstellungen** > **Ereignisse und Alarme**.
2. Um Alarme für alle Hosts und ihr Chassis zu aktivieren, klicken Sie auf **Alarme für alle Hosts und ihre Gehäuse aktivieren**.
   Auf der Seite **Dell EMC Alarmwarnung aktivieren** werden die Cluster und nicht gruppierten Hosts angezeigt, die möglicherweise nach dem Aktivieren der Dell EMC Alarme beeinträchtigt werden.

   ANMERKUNG: Dell EMC Hosts, auf denen Alarme aktiviert sind, die auf einige spezifische kritische Ereignisse reagieren, indem sie in den Wartungsmodus übergehen. Sie können den Alarm bei Bedarf ändern.

   ANMERKUNG: In vCenter 6.7 U1 und 6.7 U2 schlägt die Bearbeitungsoption fehl. Für die Bearbeitung von Alarmdefinitionen wird die Verwendung von Web Client (FLEX) empfohlen.

   ANMERKUNG: BMC-Traps verfügen nicht über Meldungs-IDs. Warnungen enthalten also demzufolge diese Details nicht in OMIVV.
3. Klicken Sie zum Übernehmen der Änderungen auf **WEITER**.
   Die Alarme für alle Hosts und Ihr Gehäuse sind aktiviert.
4. Wählen Sie eine der folgenden Ereignis-Veröffentlichungsstufen:
   - **Keine Ereignisse veröffentlichen**: Es werden keine Ereignisse oder Warnungen an die zugehörigen vCenter weitergeleitet.
   - **Alle Ereignisse veröffentlichen**: Alle Ereignisse, einschließlich informativer Ereignisse, sowie von den verwalteten Hosts und Gehäusen empfangene Ereignisse, werden in den zugehörigen vCentern veröffentlicht. Es wird empfohlen, die Option Alle Ereignisse anzeigen als Ereignisanzeigeebene auszuwählen.
   - **Nur kritische Ereignisse und Warnereignisse veröffentlichen**: Nur die kritischen Ereignisse und Ereignisse auf Warnstufe werden in den zugehörigen vCentern angezeigt.
   - **Nur Ereignisse im Zusammenhang mit Virtualisierung anzeigen**: Die von den Hosts empfangenen virtualisierungsbezogenen Ereignisse werden in den zugehörigen vCentern veröffentlicht. Virtualisierungsbezogene Ereignisse sind solche, die für Hosts, die VMs ausführen, am wichtigsten sind.
5. Klicken Sie auf **ANWENDEN**, um die Änderungen zu speichern.

   Klicken Sie auf **ALARME WIEDERHERSTELLEN**, um die Standardeinstellungen für vCenter-Alarme für alle Hosts und ihre Gehäuse wiederherzustellen. Es kann bis zu einer Minute dauern, bis die Änderung übernommen wird.

   Mit der Option **ALARME WIEDERHERSTELLEN** kann die standardmäßige Alarmkonfiguration wiederhergestellt werden, ohne dass das Produkt de- und neu installiert werden muss. Alle nach der Installation geänderten Dell EMC Alarmkonfigurationen werden durch den Klick auf Option **ALARME WIEDERHERSTELLEN** zurückgesetzt.

   ANMERKUNG: Die Einstellungen für Ereignisse und Alarme werden nach der Wiederherstellung des Geräts nicht aktiviert. Sie können die Einstellungen für Ereignisse und Alarme über die Registerkarte Einstellungen erneut aktivieren.

Gehäuseereignisse anzeigen

1. Blenden Sie in vSphere Client **Menü** ein und wählen Sie dann **Hosts und Cluster** aus.
2. Wählen Sie im linken Fensterbereich eine Instanz von vCenter aus.
3. Klicken Sie im rechten Fensterbereich auf **Überwachen** > **Aufgaben und Ereignisse** > **Ereignisse**.
4. Wählen Sie ein spezifisches Ereignis aus, um weitere Informationen anzeigen zu lassen.

   ANMERKUNG: Bei einem PowerEdge MX-Gehäuse in einer MCM-Konfiguration wird die Quelle des Ereignisses als Lead-Gehäuse angezeigt, in den Details der Benachrichtigung wird jedoch die Service-Tag-Nummer des Mitgliedsgehäuses zur Identifizierung angegeben.

Gehäusealarme anzeigen

1. Blenden Sie in vSphere Client **Menü** ein und wählen Sie dann **Hosts und Cluster** aus.
2. Wählen Sie im linken Fensterbereich eine Instanz von vCenter aus.

3. Klicken Sie im rechten Fensterbereich auf **Überwachen** > **Probleme und Alarme** > **Ausgelöste Alarme**.
4. Klicken Sie unter **Ausgelöste Alarme** auf den Alarmnamen, um die Alarmdefinition anzuzeigen.

Alarm- und Ereigniseinstellungen anzeigen

Sobald Sie Alarme und Ereignisse konfigurieren, können Sie anzeigen lassen, ob die vCenter-Alarme für Hosts aktiviert sind und welche Ereignisanzeigeebene auf der Registerkarte „Einstellungen“ ausgewählt wurde.

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **Ereignisse und Alarme**.
   Es werden die folgenden Details angezeigt:
   - vCenter-Alarme für Dell EMC Hosts – Zeigt entweder **Aktiviert** oder **Deaktiviert** an.
   - Ereignisanzeigeebene
2. Konfigurieren von Ereignissen und Alarmen. Informationen dazu finden Sie unter Konfigurieren von Ereignissen und Alarmen auf Seite 96.

Informationen zum Anzeigen der Ereignisanzeigeebenen finden Sie unter Informationen zu Ereignissen und Alarmen auf Seite 95.

Ereignisse im Zusammenhang mit der Virtualisierung

Die folgende Tabelle enthält die kritischen und Warnungsereignisse im Zusammenhang mit der Virtualisierung, einschließlich Name des Ereignisses, Beschreibung, Schweregrad und empfohlene Maßnahme.

Die Virtualisierungsereignisse werden im folgenden Format angezeigt:

Dell Meldungs-ID:<ID-Nummer>, Meldung:<Beschreibung der Meldung>.

Die Gehäuseereignisse werden im folgenden Format angezeigt:

Dell Meldung:<Beschreibung der Meldung>, Gehäusename:<Gehäusename>, Meldung:<Gehäuse-Service-Tag-Nummer>, Gehäuseposition:<Gehäuseposition>

Tabelle 9. Virtualisierungsereignisse

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Dell-alertHWCAuditWarning	Hardware-Konfigurationswarnung	Warnung	Keine Maßnahme
Dell-alertHWCAuditInformation	Hardware-Konfigurationsinformationen	Info	Keine Maßnahme
Dell-alertLiquidCoolingLeakInformational	Ein kleines Leck, das zuvor auf dem Gerät erkannt wurde, ist jetzt behoben.	Info	Keine Maßnahme
Dell-alertLiquidCoolingLeakWarning	Ein kleines Leck wird auf dem Gerät erkannt.	Warnung	Keine Maßnahme
Dell-alertLiquidCoolingLeakFailure	Es wurde ein großes Leck auf dem Gerät erkannt.	Kritisch	Trennen Sie den Eingangsstrom und wenden Sie sich an Ihren Dienstanbieter.
Dell-alertStorageSoftwareDefinedSubSystemFailure	Software Defined Storage Subsystem-Fehler	Kritisch	Überprüfen Sie den Funktionszustand der in der Meldung angegebenen Festplatte und versuchen Sie es erneut. Um den Funktionszustand der iDRAC GUI zu überprüfen, klicken Sie im iDRAC-Dashboard auf **Storage** > **Physische Festplatten**. Führen Sie folgenden RACADM-Befehl in der Befehlszeilenschnittstelle (CLI) aus: `racadm raid get pdisks -o -p status`

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
			Fügen Sie dem Storage-Pool weitere physische Laufwerke hinzu und versuchen Sie es erneut.
Dell-alertStorageSoftwareDefinedSubSystemWarning	Software Defined Storage Subsystem-Warnung	Warnung	Keine Maßnahme
Dell-alertTemperatureProbeReadWarning	Temperatursensoren können nicht gelesen werden	Warnung	Keine Maßnahme
Dell-alertTemperatureProbeChangeFailure	Fehler beim Erhöhen der Temperatur	Kritisch	Überprüfen Sie das Gehäuse-Ereignisprotokoll auf Lüfterprobleme und beheben Sie etwaige Probleme. Wenn Lüfterprobleme nicht erkannt werden, überprüfen Sie die Umgebungstemperatur des Gehäuses und stellen Sie sicher, dass die Temperatur innerhalb des Betriebsbereichs liegt. Um die Umgebungstemperatur des Gehäuses zu überprüfen, führen Sie den folgenden RACADM-Befehl aus: `racadm getsensorinfo` .
Dell – Stromsensor hat einen Warnungswert festgestellt	Ein Stromsensor im angegebenen System hat seinen Warnungsschwellenwert überschritten	Warnung	Keine Maßnahme
Dell – Stromsensor hat einen Fehlerwert festgestellt	Ein Stromsensor im angegebenen System hat seinen Fehlerschwellenwert überschritten	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Stromsensor hat einen nicht wiederherstellbaren Wert festgestellt	Ein Stromsensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell – Redundanz wiederhergestellt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Redundanz herabgesetzt	Ein Redundanzsensor in dem angegebenen System hat erkannt, dass eine der Komponenten der Redundanzeinheit fehlerhaft ist, die Einheit aber dennoch redundant ist	Warnung	Keine Maßnahme
Dell – Redundanzverlust	Ein Redundanzsensor in dem angegebenen System hat erkannt, dass eine der Komponenten in der Redundanzeinheit	Fehler	Setzen Sie das System in den Wartungsmodus.

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
	getrennt wurde, fehlerhaft oder nicht vorhanden ist		
Dell – Netzteil auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Netzteil hat eine Warnung erkannt	Der Sensormesswert eines Netzteils im angegebenen System hat einen nutzerdefinierbaren Warnungsschwellenwert überschritten	Warnung	Keine Maßnahme
Dell – Netzteil hat einen Fehler erkannt	Ein Netzteil wurde abgetrennt oder ist fehlerhaft	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Netzteilsensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Netzteilsensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann	Fehler	Keine Maßnahme
Dell – Warnung über Status des Speichergeräts	Die Korrekturrate eines Speichergeräts hat den akzeptablen Wert überschritten	Warnung	Keine Maßnahme
Dell – Speichergerätfehler	Die Korrekturrate eines Speichergeräts hat den akzeptablen Wert überschritten, eine Ersatz-Speicherbank wurde aktiviert oder es ist ein Multibit-ECC-Fehler aufgetreten	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Lüftergehäuse in das System eingesetzt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Lüftergehäuse aus dem System entfernt	Ein Lüftergehäuse wurde aus dem angegebenen System entfernt	Warnung	Keine Maßnahme
Dell – Lüftergehäuse für einen längeren Zeitraum aus dem System entfernt	Ein Lüftergehäuse wurde für eine vom Nutzer festgelegte Zeitdauer aus dem angegebenen System entfernt	Fehler	Keine Maßnahme
Dell – Lüftergehäusesensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Lüftergehäusesensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann	Fehler	Keine Maßnahme

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Dell – Netzstrom wurde wiederhergestellt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Warnung über verloren gegangenen Netzstrom	Ein Netzkabel hat seine Leistung verloren, die Redundanz ist jedoch ausreichend, um dies als Warnung zu klassifizieren	Warnung	Keine Maßnahme
Dell – Ein Netzkabel hat seine Leistung verloren	Ein Netzkabel hat seine Leistung verloren und aufgrund fehlender Redundanz muss dies als Fehler klassifiziert werden	Fehler	Keine Maßnahme
Dell – Prozessorsensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Prozessorsensor hat einen Warnungswert erkannt	Ein Prozessorsensor im angegebenen System befindet sich in einem gedrosselten Zustand	Warnung	Keine Maßnahme
Dell – Prozessorsensor hat einen Fehlerwert erkannt	Ein Prozessorsensor im angegebenen System ist deaktiviert oder bei ihm ist ein Konfigurationsfehler bzw. ein thermischer Auslöser aufgetreten	Fehler	Keine Maßnahme
Dell – Prozessorsensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Prozessorsensor im angegebenen System ist fehlerhaft.	Fehler	Keine Maßnahme
Dell – Gerätekonfigurationsfehler	Für ein austauschbares Gerät im angegebenen System wurde ein Konfigurationsfehler erkannt	Fehler	Keine Maßnahme
Dell – Batteriesensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Batteriesensor hat einen Warnungswert erkannt	Ein Batteriesensor im festgelegten System hat erkannt, dass sich ein Akku im vorhersehbaren Fehlerzustand befindet	Warnung	Keine Maßnahme
Dell – Batteriesensor hat einen Fehlerwert erkannt	Ein Batteriesensor im festgelegten System hat erkannt, dass ein Akku fehlerhaft ist	Fehler	Keine Maßnahme

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Dell – Batteriesensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Batteriesensor im festgelegten System hat erkannt, dass ein Akku fehlerhaft ist	Fehler	Keine Maßnahme
Dell – Temperaturbedingtes Herunterfahren wurde initiiert	Diese Meldung wird generiert, wenn ein System so konfiguriert wurde, dass es bei einem Fehlerereignis temperaturbedingt herunterfährt. Wenn der Messwert eines Temperatursensors den Fehlerschwellenwert überschreitet, für den das System konfiguriert wurde, fährt das Betriebssystem herunter und das System wird ausgeschaltet. Bei bestimmten Systemen kann dieses Ereignis auch initiiert werden, wenn ein Lüftergehäuse für einen längeren Zeitraum aus dem System entfernt wird	Fehler	Keine Maßnahme
Dell – Temperatursensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Temperatursensor hat einen Warnungswert erkannt	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine, der CPU oder dem Festplattenträger im angegebenen System hat ein Überschreiten des Warnungsschwellenwerts erkannt	Warnung	Keine Maßnahme
Dell – Temperatursensor hat einen Fehlerwert erkannt	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine oder dem Festplattenträger im angegebenen System hat ein Überschreiten des Fehlerschwellenwerts erkannt	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Temperatursensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Temperatursensor auf der Rückwandplatine, der	Fehler	Keine Maßnahme

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
	Systemplatine oder dem Festplattenträger im angegebenen System erkannte einen Fehler, der nicht behoben werden kann		
Dell – Lüftersensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Lüftersensor hat einen Warnungswert erkannt	Ein Lüftersensormesswert in Host <x> hat einen Warnungsschwellenwert überschritten	Warnung	Keine Maßnahme
Dell – Lüftersensor hat einen Fehlerwert erkannt	Ein Lüftersensor im angegebenen System hat den Ausfall eines Lüfters oder mehrerer Lüfter erkannt	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Lüftersensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Lüftersensor hat einen Fehler erkannt, der nicht behoben werden kann	Fehler	Keine Maßnahme
Dell – Spannungssensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Spannungssensor hat einen Warnungswert erkannt	Ein Spannungssensor im angegebenen System hat seinen Warnungsschwellenwert überschritten.	Warnung	Keine Maßnahme
Dell – Spannungssensor hat einen Fehlerwert erkannt	Ein Spannungssensor im angegebenen System hat seinen Fehlerschwellenwert überschritten	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Spannungssensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Spannungssensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann	Fehler	Keine Maßnahme
Dell – Stromsensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Speicher: Fehler bei der Speicherverwaltung	Die Speicherverwaltung hat einen geräteunabhängigen Fehlerzustand erkannt	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Controller-Warnung	Ein Teil der physische Festplatte ist beschädigt.	Warnung	Keine Maßnahme

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Dell – Speicher: Controller-Fehler	Ein Teil der physische Festplatte ist beschädigt.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Kanal-Fehler	Kanal-Fehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Gehäuse-Hardware-Information	Information zur Gehäuse-Hardware	Info	Keine Maßnahme
Dell – Speicher: Gehäuse-Hardware-Warnung	Warnung bezüglich Gehäuse-Hardware	Warnung	Keine Maßnahme
Dell – Speicher: Gehäuse-Hardware-Fehler	Fehler der Gehäuse-Hardware	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Array-Festplattenfehler	Fehler der Array-Festplatte	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: EMM-Fehler	EMM-Fehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Netzteilfehler	Netzteilfehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Temperatursondenwarnung	Temperatursondenwarnung der physischen Festplatte: zu kalt oder zu heiß.	Warnung	Keine Maßnahme
Dell – Speicher: Temperatursondenfehler	Temperatursondenfehler der physischen Festplatte: zu kalt oder zu heiß.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Lüfterfehler	Lüfterfehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Batteriewarnung	Akkuwarnung	Warnung	Keine Maßnahme
Dell – Speicher: Warnung: Virtuelle Festplatte wurde herabgesetzt	Warnung: Herabsetzung einer virtuellen Festplatte	Warnung	Keine Maßnahme
Dell – Speicher: Fehler: Virtuelle Festplatte wurde herabgesetzt	Fehler zur Herabsetzung einer virtuellen Festplatte.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Temperatursondeninformation	Informationen zur Temperatursonde	Info	Keine Maßnahme
Dell – Speicher: Array-Festplattenwarnung	Warnung zum Array-Laufwerk	Warnung	Keine Maßnahme
Dell – Speicher: Array-Festplatteninformation	Informationen zum Array-Laufwerk	Info	Keine Maßnahme
Dell – Speicher: Netzteilwarnung	Netzteilwarnung	Warnung	Keine Maßnahme
Dell – Fluid Cache Laufwerksfehler	Fluid Cache Laufwerksfehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Kabelfehler oder kritisches Ereignis	Kabelfehler oder kritisches Ereignis.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Chassis Management Controller hat eine Warnung erkannt	Gehäuse-Verwaltungscontroller	Warnung	Keine Maßnahme

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
	hat eine Warnung erkannt		
Dell – Chassis Management Controller hat einen Fehler erkannt	Gehäuse-Verwaltungscontroller hat einen Fehler erkannt	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – E/A-Virtualisierungsfehler oder kritisches Ereignis	E/A-Virtualisierungsfehler oder kritisches Ereignis	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Verbindungsstatuswarnung	Verbindungsstatuswarnung	Warnung	Keine Maßnahme
Dell – Linkstatusfehler oder kritisches Ereignis	Verbindungsstatusfehler oder kritisches Ereignis	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Sicherheitswarnung	Sicherheitswarnung	Warnung	Keine Maßnahme
Dell - System: Softwarekonfigurationswarnung	System: Softwarekonfigurationswarnung	Warnung	Keine Maßnahme
Dell - System: Softwarekonfigurationswarnung	System: Softwarekonfigurationsfehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speichersicherheitswarnung	Speichersicherheitswarnung	Warnung	Keine Maßnahme
Dell – Speichersicherheitsfehler oder kritisches Ereignis	Speichersicherheitsfehler oder kritisches Ereignis	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Softwareänderungs-Aktualisierungswarnung	Softwareänderungs-Aktualisierungswarnung.	Warnung	Keine Maßnahme
Dell – Chassis Management Controller Auditwarnung	Überprüfungswarnung zum Gehäuse-Verwaltungscontroller	Warnung	Keine Maßnahme
Dell – Chassis Management Controller Auditfehler oder kritisches Ereignis	Gehäuse-Verwaltungscontroller: Überprüfungsfehler oder kritisches Ereignis	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – PCI-Geräte-Auditwarnung	PCI-Geräte-Überprüfungswarnung	Warnung	Keine Maßnahme
Dell – Netzteil-Auditwarnung	Netzteil-Überprüfungswarnung	Warnung	Keine Maßnahme
Dell – Netzteil-Auditfehler oder kritisches Ereignis	Netzteil-Überprüfungsfehler oder kritisches Ereignis	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Stromverbrauchs-Auditwarnung	Stromverbrauchs-Überprüfungswarnung	Warnung	Keine Maßnahme
Dell – Stromverbrauchs-Auditfehler oder kritisches Ereignis	Stromverbrauchs-Überprüfungsfehler	Fehler	Setzen Sie das System in den Wartungsmodus.

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
	oder kritisches Ereignis		
Dell – Sicherheitskonfigurations-Warnung	Sicherheitskonfigurationswarnung	Warnung	Keine Maßnahme
Dell – Konfiguration: Softwarekonfigurationswarnung	Konfiguration: Softwarekonfigurationswarnung	Warnung	Keine Maßnahme
Dell – Konfiguration: Softwarekonfigurationsfehler	Konfiguration: Softwarekonfigurationsfehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Fehler bei der Partition der virtuellen Festplatte	Fehler bei einer Partition der virtuellen Festplatte	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Warnung zur Partition der virtuellen Festplatte	Warnung zu einer Partition der virtuellen Festplatte	Warnung	Keine Maßnahme
iDRAC-Ereignisse **ANMERKUNG:** Für alle proaktiven HA-aktivierten Hosts, die Teil eines Clusters sind, werden die folgenden Virtualisierungsereignisse den proaktiven HA-Ereignissen zugeordnet, ausgenommen die Ereignisse „Die Lüfter sind nicht redundant“ und „Die Netzteile sind nicht redundant“.			
Die Lüfter sind redundant	Keine	Info	Keine Maßnahme
Lüfterredundanz verloren	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Kritisch	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
Lüfter-Redundanz ist herabgesetzt	Ein oder mehrere Lüfter sind ausgefallen oder wurde entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Warnung	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
Die Lüfter sind nicht redundant	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Info	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
Die Lüfter sind nicht redundant. Keine ausreichenden Ressourcen zur Beibehaltung des normalen Betriebs.	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Kritisch	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Die Netzteile sind redundant	Keine	Info	Keine Maßnahme
Verlust der Netzteilredundanz	Der aktuelle Energie-Betriebsmodus ist nicht-redundant, da ein Netzteilausnahmefehler, eine Netzteil-Bestandsänderung oder eine Systemstrom-Bestandsänderung vorliegt. Das System arbeitete zuvor im redundanten Energie-Betriebsmodus.	Kritisch	Überprüfen Sie das Ereignisprotokoll auf Netzteilfehler. Überprüfen Sie die Systemkonfiguration und den Stromverbrauch.
Netzteilredundanz ist herabgesetzt	Der aktuelle Energie-Betriebsmodus ist nicht-redundant, da ein Netzteilausnahmefehler, eine Netzteil-Bestandsänderung oder eine Systemstrom-Bestandsänderung vorliegt. Das System arbeitete zuvor im redundanten Energie-Betriebsmodus.	Warnung	Überprüfen Sie das Ereignisprotokoll auf Netzteilfehler. Überprüfen Sie die Systemkonfiguration und den Stromverbrauch.
Die Netzteile sind nicht redundant	Die aktuelle Netzteilkonfiguration erfüllt nicht die Plattformanforderungen für eine Aktivierung der Redundanz. Wenn ein Netzteil fehlerhaft ist, fährt das System möglicherweise herunter.	Info	Ist dies nicht beabsichtigt, überprüfen Sie die Systemkonfiguration und den Stromverbrauch und installieren Sie entsprechend Netzteile. Überprüfen Sie den Netzteilstatus auf Fehler.
Die Netzteile sind nicht redundant. Keine ausreichenden Ressourcen zur Beibehaltung des normalen Betriebs.	Das System schaltet sich möglicherweise ab oder arbeitet in einem Zustand mit herabgesetzter Leistung.	Kritisch	Überprüfen Sie das Ereignisprotokoll auf Netzteilfehler. Überprüfen Sie die Systemkonfiguration und den Stromverbrauch und installieren Sie entsprechend Netzteile.
Das interne Dual SD-Modul ist redundant.	Keine	Info	Keine Maßnahme
Verlust der internen Dual-SD-Modulredundanz	Eine der beiden SD-Karten oder beide SD-Karten funktionieren nicht ordnungsgemäß.	Kritisch	Ersetzen Sie die fehlerhafte SD-Karte.
Interne Dual-SD-Modulredundanz ist herabgesetzt	Eine der beiden SD-Karten oder beide SD-Karten funktionieren nicht ordnungsgemäß.	Warnung	Ersetzen Sie die fehlerhafte SD-Karte.

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Das interne Dual SD-Modul ist nicht redundant.	Keine	Info	Installieren Sie eine zusätzliche SD-Karte und konfigurieren Sie sie für Redundanz, falls Redundanz gewünscht wird.
Gehäuseereignisse			
Verlust der Netzteilredundanz	Der aktuelle Energie-Betriebsmodus ist nicht-redundant, da ein Netzteilausnahmefehler, eine Netzteil-Bestandsänderung oder eine Systemstrom-Bestandsänderung vorliegt. Das System arbeitete zuvor im redundanten Energie-Betriebsmodus.	Kritisch	Überprüfen Sie das Ereignisprotokoll auf Netzteilfehler. Überprüfen Sie die Systemkonfiguration und den Stromverbrauch.
Netzteilredundanz ist herabgesetzt	Der aktuelle Energie-Betriebsmodus ist nicht-redundant, da ein Netzteilausnahmefehler, eine Netzteil-Bestandsänderung oder eine Systemstrom-Bestandsänderung vorliegt. Das System arbeitete zuvor im redundanten Energie-Betriebsmodus.	Warnung	Überprüfen Sie das Ereignisprotokoll auf Netzteilfehler. Überprüfen Sie die Systemkonfiguration und den Stromverbrauch.
Die Netzteile sind redundant	Keine	Info	Keine Maßnahme
Die Netzteile sind nicht redundant	Die aktuelle Netzteilkonfiguration erfüllt nicht die Plattformanforderungen für eine Aktivierung der Redundanz. Wenn ein Netzteil fehlerhaft ist, fährt das System möglicherweise herunter.	Info	Ist dies nicht beabsichtigt, überprüfen Sie die Systemkonfiguration und den Stromverbrauch und installieren Sie entsprechend Netzteile. Überprüfen Sie den Netzteilstatus auf Fehler.
Die Netzteile sind nicht redundant. Keine ausreichenden Ressourcen zur Beibehaltung des normalen Betriebs.	Das System schaltet sich möglicherweise ab oder arbeitet in einem Zustand mit herabgesetzter Leistung.	Kritisch	Überprüfen Sie das Ereignisprotokoll auf Netzteilfehler. Überprüfen Sie die Systemkonfiguration und den Stromverbrauch und installieren Sie entsprechend Netzteile.
Lüfterredundanz verloren	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die	Kritisch	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.

Tabelle 9. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
	zusätzliche Lüfter erforderlich macht.		
Lüfter-Redundanz ist herabgesetzt	Ein oder mehrere Lüfter sind ausgefallen oder wurde entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Warnung	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
Die Lüfter sind redundant	Keine	Info	Keine Maßnahme
Die Lüfter sind nicht redundant	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Info	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
Die Lüfter sind nicht redundant. Keine ausreichenden Ressourcen zur Beibehaltung des normalen Betriebs.	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Kritisch	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.

Verwaltung der Zeitpläne für Datenabruf

Einen Bestandsaufnahme-Job planen

Um die neuesten Bestandsdaten auf OMIVV anzuzeigen, müssen Sie einen Bestandsaufnahme-Job regelmäßig planen, um sicherzustellen, dass die Bestandsinformationen der Hosts oder des Gehäuses auf dem neuesten Stand sind. Es wird empfohlen, den Bestandsaufnahme-Job wöchentlich auszuführen.

ANMERKUNG: Das Gehäuse wird im OMIVV-Kontext verwaltet. Es gibt keinen Kontext von vCenter in der Gehäuseverwaltung. Nachdem die geplante Host-Bestandsaufnahme abgeschlossen ist, wird die Gehäuse-Bestandsaufnahme für alle mit OMIVV verwalteten Gehäuse ausgelöst.

ANMERKUNG: Die Einstellungen auf dieser Seite werden jedes Mal auf den Standardwert zurückgesetzt, wenn der Konfigurationsassistent aufgerufen wird. Wenn Sie zuvor schon einen Zeitplan für die Bestandsaufnahme konfiguriert haben, stellen Sie sicher, dass Sie den vorherigen Zeitplan auf dieser Seite vor Abschluss der Assistentenfunktionen replizieren, damit der vorherige Zeitplan nicht durch die Standardeinstellungen außer Kraft gesetzt wird.

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **vCenter Einstellungen** > **Zeitplan Datenabruf** > **Bestandsaufnahme-Abruf**.
2. Aktivieren Sie das Kontrollkästchen **Abruf von Bestandsaufnahmedaten aktivieren (empfohlen)**.

   Wenn in einer PSC-Umgebung mit mehreren vCenter Servern der Zeitplan für einzelne vCenter unterschiedlich ist und Sie die Option **Alle registrierten vCenter** auswählen, um den Bestandsaufnahme-Zeitplan zu aktualisieren, wird auf der Seite „Bestandsaufnahme-Zeitplaneinstellungen“ der Standardzeitplan angezeigt.
3. Wählen Sie den Tag und die Uhrzeit für den Abruf von Bestandsaufnahmedaten aus und klicken Sie auf **ANWENDEN**.

ANMERKUNG: Wenn Sie in einer PSC-Umgebung mit mehreren vCenter-Servern den Bestandsaufnahme-Zeitplan für **Alle registrierten vCenter** aktualisieren, überschreibt die Aktualisierung die Einstellungen für den individuellen vCenter-Bestandsaufnahme-Zeitplan.

Serviceabfrage-Jobs planen

1. Um den Autorisierungsschlüssel zu aktualisieren, stellen Sie sicher, dass Sie Zugriff auf den Index-Katalog (`https://downloads.dell.com/catalog/CatalogIndex.gz`) haben.
2. Um einen Servicebericht zu erhalten, stellen Sie sicher, dass Sie Zugriff auf `https://apigtwb2c.us.dell.com` haben.
3. Stellen Sie sicher, dass die Bestandsaufnahme erfolgreich auf Hosts und Gehäusen ausgeführt wird.
4. Um die Servicefunktionen von OMIVV zu verwenden, müssen Sie über eine Internetverbindung verfügen. Wenn Ihre Umgebung einen Proxy für das Internet benötigt, stellen Sie sicher, dass Sie die Proxyeinstellungen im Admin-Portal konfigurieren.

Hardware-Serviceinformationen werden von Dell Online abgerufen und von OMIVV angezeigt. Nur die Service-Tag-Nummer wird gesendet und nicht von Dell Online gespeichert.

In einer PSC-Umgebung mit mehreren vCenter-Servern wird die Gehäusegewährleistung automatisch bei jedem vCenter ausgeführt, wenn die Gewährleistung für ein beliebiges vCenter ausgeführt wird. Jedoch wird der Service nicht automatisch hinzugefügt, wenn er nicht zum Gehäuse-Zugangsdatenprofil hinzugefügt wird.

ANMERKUNG: Die Einstellungen auf dieser Seite werden jedes Mal auf den Standardwert zurückgesetzt, wenn der Konfigurationsassistent aufgerufen wird. Wenn Sie zuvor schon einen Serviceabfrage-Job konfiguriert haben, stellen Sie sicher, dass Sie den vorherigen Zeitplan auf dieser Seite vor Abschluss der Assistentenfunktionen replizieren, damit der vorherige Zeitplan nicht durch die Standardeinstellungen außer Kraft gesetzt wird.

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **vCenter-Einstellungen** > **Planung für Routinejobs** > **Serviceabfrage**.
2. Aktivieren Sie das Kontrollkästchen **Abruf von Servicedaten aktivieren (empfohlen)**.

   Wenn in einer PSC-Umgebung mit mehreren vCenter Servern der Zeitplan für einzelne vCenter unterschiedlich ist und Sie die Option **Alle registrierten vCenter** auswählen, um den Service-Zeitplan zu aktualisieren, wird auf der Seite „Service-Zeitplaneinstellungen“ der Standardzeitplan angezeigt.
3. Wählen Sie den Tag und die Uhrzeit für den Abruf von Servicedaten aus und klicken Sie auf **ANWENDEN**.

   ANMERKUNG: Wenn Sie in einer PSC-Umgebung mit mehreren vCenter-Servern den Service-Zeitplan für **Alle registrierten vCenter** aktualisieren, überschreibt die Aktualisierung die Einstellungen für den individuellen vCenter Service-Zeitplan.

16

Gehäuseverwaltung

Dell EMC Gehäuseinformationen anzeigen

Sie können die Gehäuseinformationen anzeigen, die mithilfe von OMIVV ermittelt und inventarisiert werden. Dell EMC Gehäuse listet alle von OMIVV verwalteten Gehäuse auf.

1. Klicken Sie auf der OMIVV-Startseite auf **Hosts und Gehäuse** > **Gehäuse** > **Gehäuseliste**.
   Die folgenden Informationen werden angezeigt:

   - **Name**: Zeigt einen IP-Adressen-Link für alle Dell EMC-Gehäuse an.
   - **Funktionszustand**: Zeigt den Funktionszustand des Gehäuses an.

     Um den Funktionszustand der einzelnen Dell EMC Gehäuse zu filtern, klicken Sie auf das Filtersymbol, das in der Suche vorhanden ist.

   - **IP-Adresse/FQDN**: Zeigt die vCenter-IP-Adresse oder FQDN an.
   - **Service-Tag-Nummer**: Zeigt die Service-Tag-Nummer des Gehäuses an.
   - **Gehäuse-URL**: Zeigt die Gehäuse-URL an.
   - **Modell**: Zeigt den Modellnamen an.
   - **Rolle**: Gilt nur für MX-Gehäuse. Zeigt die Rolle des Gehäuses an (Haupt oder Mitglied).
   - **Letzte Inventarisierung**: Zeigt die aktuellen Bestandsinformationen an.
   - **Verfügbare Steckplätze**: Zeigt die verfügbaren Steckplätze im Gehäuse an.
   - **Profilname**: Zeigt den Gehäuseprofilnamen an, unter dem das Gehäuse zugeordnet ist.
   - **Standort**: Zeigt die Position des Gehäuses an.

   Wenn Sie die Bestandsaufnahme nicht ausführen, werden der **Name**, die **letzte Bestandsaufnahme**, die **verfügbaren Steckplätze**, der **Profilname**, der **Standort** und die Gehäuse-Bestandsaufnahme-Informationen nicht angezeigt.

   ANMERKUNG: Bei einem PowerEdge MX-Gehäuse in einer MCM-Konfiguration wird die gesamte MCM-Infrastruktur über das Lead-Gehäuse verwaltet. Wenn die Mitgliedsgehäuse-IP-Adressen und iDRAC-IP-Adressen deaktiviert sind und/oder die Gehäuserolle geändert wird, empfiehlt Dell EMC, das vorhandene Lead-Gehäuse zu entfernen, die neue IP-Adresse des Lead-Gehäuses erneut hinzuzufügen und dann dem Gehäuse-Zugangsdatenprofil zuzuweisen.

2. Wählen Sie ein Gehäuse aus, um die Firmware, den Lizenztyp und die Service-bezogenen Informationen anzuzeigen.
   Wenn Sie die Bestandsaufnahme nicht ausführen, werden **Name**, **Firmware**, **Lizenztyp** und **Service**-Informationen nicht angezeigt.

Gehäuse-Bestandsinformationen anzeigen

1. Wählen Sie auf der Seite **Dell EMC Gehäuse** ein Gehäuse aus oder klicken Sie auf „Service-Tag-Nummer“.
2. Klicken Sie im Abschnitt **Gehäuseinformationen** auf **ANZEIGEN**.
   Die Seite **Übersicht** zeigt den Funktionszustand des Gehäuses, die aktiven Fehler, den Funktionszustand der Komponentenebene des Gehäuses, die Hardwareübersicht und die Gehäusebeziehung (nur für MX-Gehäuse) an.

   ANMERKUNG: Für M1000e Version 4.3 und früher werden die aktiven Fehler nicht angezeigt.

   Das Hauptfenster zeigt den allgemeinen Funktionszustand eines Gehäuses an. Die gültigen Funktionsindikatoren lauten **Funktionsfähig**, **Warnung**, **Kritisch** und **Unbekannt**. In der Rasteransicht Gehäuse-Funktionszustand wird der Zustand der einzelnen Komponenten angezeigt. Die Parameter zum Gehäuse-Funktionszustand sind nur für VRTX-Modelle der Version 1.0 und höher und M1000e Version 4.4 und höher relevant. Bei M1000e-Firmwareversionen vor 4.3 werden nur zwei Funktionsindikatoren angezeigt, z. B. Funktionsfähig und Warnung oder Kritisch.

   Der Gesamtfunktionszustand zeigt den Funktionszustand basierend auf dem Gehäuse mit den schlechtesten Funktionszustandswerten. Wenn zum Beispiel 5 Zeichen für funktionsfähig und 1 Warnzeichen angezeigt werden, wird der Gesamtfunktionszustand als Warnung angezeigt.

Anzeigen von Informationen zur Hardware-Bestandsliste für Gehäuse

Sie können Informationen über den Hardwarebestand für das ausgewählte Gehäuse anzeigen.

1. Klicken Sie auf der OMIVV-Startseite auf **Hosts und Gehäuse** > **Gehäuse** > **Gehäuseliste**.
   Die Seite **Dell EMC Gehäuse** wird angezeigt.
2. Wählen Sie ein Gehäuse aus und klicken Sie auf den Link „Service-Tag“.
   Die Seite **Übersicht** wird angezeigt.
3. Klicken Sie auf der Seite **Übersicht** auf **Hardware**.

Tabelle 10. Hardwarebestandsaufnahmedaten

Hardware-Bestandsliste: Komponente	Navigation durch OMIVV	Informationen
Lüfter	• Klicken Sie auf der Seite **Dell EMC Gehäuse** auf **Gehäuse** > **Gehäuse Liste** und klicken Sie auf den Link „Service-Tag-Nummer“. • Klicken Sie im linken Fensterbereich auf der Seite **Übersicht** auf **Hardware**. • Erweitern Sie im rechten Fensterbereich **Lüfter**. **ODER** • Klicken Sie auf der Seite **Übersicht** auf **Lüfter**.	Informationen über Lüfter: • Name • Vorhanden • Bezeichner (gilt nur für MX-Gehäuse) • Stromzustand • Messwert (RPM) • Warnungsschwellenwert (gilt nicht für MX-Gehäuse) • Kritischer Schwellenwert (gilt nicht für MX-Gehäuse) ○ Minimum ○ Maximal • Pulsweitenmodulation (nur für MX Gehäuse) **ANMERKUNG:** In einem PowerEdge MX Gehäuse wird das Vorhandensein eines Lüfters mit „Ja“ gekennzeichnet, auch dann, wenn der Lüfter aus dem Gehäuse entfernt wurde. Der Lüfterzustand wird jedoch als **Kritisch** auf der Seite **Zusammenfassung** mit aktivem Fehler angezeigt.
Netzteile	• Klicken Sie auf der Seite **Dell EMC Gehäuse** auf **Gehäuse** > **Gehäuse Liste** und klicken Sie auf den Link „Service-Tag-Nummer“. • Klicken Sie im linken Fensterbereich auf der Seite **Übersicht** auf **Hardware**. • Erweitern Sie im rechten Fensterbereich **Netzteile**. **ODER** • Klicken Sie auf der Seite **Übersicht** auf **Netzteile**.	Informationen zu den Netzteilen: • Name • Kapazität • Vorhanden • Stromzustand • Eingangsspannung (nur für PowerEdge MX Gehäuse).
Temperature Sensors (Temperatursensoren)	• Klicken Sie auf der Seite **Dell EMC Gehäuse** auf **Gehäuse** > **Gehäuse Liste** und klicken Sie auf den Link „Service-Tag-Nummer“. • Klicken Sie im linken Fensterbereich auf der Seite **Übersicht** auf **Hardware**.	Informationen zu Temperatursensoren: • Speicherort • Lesen • Warnungsschwelle ○ Maximal ○ Minimum • Kritischer Schwellenwert

Tabelle 10. Hardwarebestandsaufnahmedaten (fortgesetzt)

Hardware-Bestandsliste: Komponente	Navigation durch OMIVV	Informationen
	• Erweitern Sie im rechten Fensterbereich **Temperatursensoren**. **ODER** • Klicken Sie auf der Registerkarte **Übersicht** auf **Temperatursensoren**.	○ Maximal ○ Minimum **ANMERKUNG:** Bei einem PowerEdge M1000e Gehäuse werden Informationen zur Gehäusetemperatur angezeigt. Für andere Gehäuse werden Informationen über Temperatursensoren für Gehäuse und zugehörige modulare Server angezeigt.
E/A-Module	• Klicken Sie auf der Seite **Dell EMC Gehäuse** auf **Gehäuse** > **Gehäuse Liste** und klicken Sie auf den Link „Service-Tag-Nummer“. • Klicken Sie im linken Fensterbereich auf der Seite **Übersicht** auf **Hardware**. • Erweitern Sie im rechten Fensterbereich die Option **E/A-Module**. **ODER** • Klicken Sie auf der Seite **Übersicht** auf **E/A-Module**.	Informationen über E/A-Module: • Einschub/Standort • Vorhanden • Name • Fabric • Service-Tag • Stromstatus • Rolle • Firmware-Version • Hardwareversion • IP-Adresse • Subnetzmaske • Gateway • MAC-Adresse • DHCP aktiviert
Fabric (nur für PowerEdge MX Gehäuse)	• Klicken Sie auf der Seite **Dell EMC Gehäuse** auf **Gehäuse** > **Gehäuse Liste** und klicken Sie auf den Link „Service-Tag-Nummer“. • Klicken Sie im linken Fensterbereich auf der Seite **Übersicht** auf **Hardware**. • Erweitern Sie im rechten Fensterbereich **Fabric**. **ODER** • Klicken Sie auf der Seite **Übersicht** auf **Fabric**.	Informationen über Fabric-Komponenten: • Funktionszustand • Fabric • Beschreibung • Switch-Anzahl • Serverknoten-Anzahl • Uplink-Anzahl Wählen Sie zur Anzeige der Switches, die mit dem Fabric verknüpft sind, eine Fabric-Komponente aus, daraufhin werden die folgenden Informationen in der Tabelle unten angezeigt: • Switch • Gehäuse • Steckplatz • Gehäuserolle • Switch-Modell
PCIe	• Klicken Sie auf der Seite **Dell EMC Gehäuse** auf **Gehäuse** > **Gehäuse Liste** und klicken Sie auf den Link „Service-Tag-Nummer“. • Klicken Sie im linken Fensterbereich auf der Seite **Übersicht** auf **Hardware**. • Erweitern Sie im rechten Fensterbereich **PCIe**. **ODER**	Informationen über PCIe: • PCIe-Steckplatz ○ Steckplatz ○ Name ○ Stromstatus ○ Fabric • Serversteckplatz ○ Name ○ Nummer • Steckplatztyp

Tabelle 10. Hardwarebestandsaufnahmedaten (fortgesetzt)

Hardware-Bestandsliste: Komponente	Navigation durch OMIVV	Informationen
	• Klicken Sie auf der Seite **Übersicht** auf **PCIe**.	• Server-Zuordnung • Zuweisungsstatus • Zugewiesener Steckplatzstrom • PCI-ID • Hersteller-ID **ANMERKUNG:** PCIe-Informationen sind nicht auf das M1000e-Gehäuse anwendbar.
iKVM – nur für PowerEdge M1000e	• Klicken Sie auf der Seite **Dell EMC Gehäuse** auf **Gehäuse** > **Gehäuse Liste** und klicken Sie auf den Link „Service-Tag-Nummer“. • Wählen Sie auf der Seite **Übersicht** im linken Fensterbereich die Option **Hardware** aus. Erweitern Sie im rechten Fensterbereich **iKVM**. **ODER** • Klicken Sie auf der Seite **Übersicht** auf **iKVM**.	Informationen zum iKVM: • iKVM-Name • Vorhanden • Firmware-Version • Frontblenden USB/Video aktiviert • Zugriff auf die CMC-CLI erlauben **ANMERKUNG:** Die iKVM-Registerkarte wird nur dann angezeigt, wenn das Gehäuse ein iKVM-Modul enthält.

Firmwarebestandsinformationen anzeigen

Sie können Informationen über die Firmware für das ausgewählte Gehäuse anzeigen.

1. Klicken Sie auf der OMIVV-Startseite auf **Hosts und Gehäuse** > **Gehäuse** > **Gehäuseliste**.
   Die Seite **Dell EMC Gehäuse** wird angezeigt.
2. Wählen Sie ein Gehäuse aus und klicken Sie auf den Link „Service-Tag“.
   Die Seite **Übersicht** wird angezeigt.
3. Klicken Sie auf der Seite **Übersicht** auf **Firmware**.
   Es werden die folgenden Informationen zur Firmware angezeigt:
   - Komponente
   - Aktuelle Version

   Auf dieser Seite können Sie auch OpenManage Enterprise Modular und CMC starten.

Management Controller-Informationen anzeigen

Sie können die Verwaltungscontroller-bezogenen Informationen für das ausgewählte Gehäuse anzeigen.

1. Klicken Sie auf der OMIVV-Startseite auf **Hosts und Gehäuse** > **Gehäuse** > **Gehäuseliste**.
   Die Seite **Dell EMC Gehäuse** wird angezeigt.
2. Wählen Sie ein Gehäuse aus und klicken Sie auf den Link „Service-Tag“.
   Die Seite **Übersicht** wird angezeigt.
3. Klicken Sie auf der Seite **Übersicht** auf **Management Controller**.
   Die folgenden Informationen über den Management Controller werden angezeigt:
   - Allgemein
     - Name

- Firmware-Version
- Zeitpunkt der letzten Aktualisierung
- Gehäuseposition
- Hardwareversion

- Gemeinsames Netzwerk
  - DNS-Domänenname
  - DHCP für DNS verwenden
  - MAC-Adresse
  - Redundanzmodus
  - Hardwareversion
- IPv4-Informationen
  - IPv4 aktiviert
  - DHCP aktiviert
  - IP-Adresse
  - Subnetzmaske
  - Gateway
  - Bevorzugter DNS-Server
  - Alternativer DNS-Server
- IPv6-Information
  - IPv6 aktiviert
  - DHCP aktiviert
  - IP-Adresse
  - Link-Local-Adresse
  - Gateway
  - Bevorzugter DNS-Server
  - Alternativer DNS-Server
- Remotezugriffskonfiguration
  - Quick Sync-Hardware vorhanden
  - LCD vorhanden
  - LED vorhanden
  - KVM aktiviert

ANMERKUNG: Einige Attribute der netzwerkbezogenen Informationen eines Mitgliedsgehäuses, welches Bestandteil der MCM-Konfiguration ist, werden nicht im Abschnitt **Verwaltungscontroller** angezeigt.

Bestandsinformationen anzeigen

Sie können Speicherinformationen für das ausgewählte Gehäuse anzeigen.

1. Klicken Sie auf der OMIVV-Startseite auf **Hosts und Gehäuse** > **Gehäuse** > **Gehäuseliste**.
   Die Seite **Dell EMC Gehäuse** wird angezeigt.
2. Wählen Sie ein Gehäuse aus und klicken Sie auf den Link „Service-Tag“.
   Die Seite **Übersicht** wird angezeigt.
3. Klicken Sie auf der Seite **Übersicht** auf **Speicher**.

   Die folgenden Informationen zum Speicher werden angezeigt:

   - Virtuelle Festplatten
   - Physische Festplatten
   - Controller
   - Gehäuse
   - Ersatzlaufwerke

   Die folgenden Informationen werden für das MX-Gehäuse angezeigt:

   - Steckplatznummer
   - Steckplatzname

- Modell
- Service-Tag
- Firmware-Version
- Asset Tag
- Stromzustand
- Zuweisungsmodus

Für die Anzeige zu Laufwerken für MX-Gehäuse müssen Sie den Speicherschlitten anklicken. Die folgenden Laufwerkinformationen werden im unteren Fensterbereich angezeigt.

- Funktionszustand
- Zustand
- Steckplatz
- Steckplatzzuweisung
- Festplattenname
- Kapazität
- Busprotokoll
- Medien

Wenn eine Festplatte im PowerEdge MX-Gehäuse nicht zugewiesen ist, wird die Steckplatzzuweisung als **NV**angezeigt.

Wenn Sie bei M1000e-Gehäusen ein Speicher-Modul besitzen, werden die folgenden Speicher-Details in einer Rasteransicht ohne zusätzliche Informationen angezeigt:

- Name
- Modell
- Service-Tag
- IP-Adresse (Link zum Speicher)
- Fabric
- Gruppenname
- Gruppen-IP-Adresse (Link zur Speichergruppe).

ANMERKUNG: Wenn Sie auf einem markierten Link unter „Speicher“ klicken, zeigt die Tabelle **Ansicht** die Details für jedes markierte Objekt an. Wenn Sie in der Ansichtstabelle auf die einzelnen Zeilenobjekte klicken, werden zusätzliche Informationen für jedes markierte Objekt angezeigt.

Serviceinformationen anzeigen

Sie können Serviceinformationen für das ausgewählte Gehäuse anzeigen.

1. Klicken Sie auf der OMIVV-Startseite auf **Hosts und Gehäuse** > **Gehäuse** > **Gehäuseliste**.
   Die Seite **Dell EMC Gehäuse** wird angezeigt.
2. Wählen Sie ein Gehäuse aus und klicken Sie auf den Link „Service-Tag“.
   Die Seite **Übersicht** wird angezeigt.
3. Klicken Sie auf der Seite **Übersicht** auf **Service**.

   Informationen über den Service:

   - Anbieter
   - Beschreibung
   - Status
   - Berechtigungstyp
   - Startdatum
   - Enddatum
   - Verbleibende Tage
   - Letzte Aktualisierung

   ANMERKUNG: Zur Anzeige des Servicestatus müssen Sie einen Service-Job ausführen. Informationen dazu finden Sie unter Serviceabfrage-Jobs planen auf Seite 109.

Zugeordneten Host für Gehäuse anzeigen

Sie können Informationen über den zugeordneten Host für das ausgewählte Gehäuse anzeigen.

1. Klicken Sie auf der OMIVV-Startseite auf **Hosts und Gehäuse** > **Gehäuse** > **Gehäuseliste**.
   Die Seite **Dell EMC Gehäuse** wird angezeigt.
2. Wählen Sie ein Gehäuse aus und klicken Sie auf den Link „Service-Tag".
   Die Seite **Übersicht** wird angezeigt.
3. Klicken Sie auf der Seite **Übersicht** auf **Zugeordnete Hosts**.

   Die folgenden Informationen über den zugeordneten Host werden angezeigt:

   - Hostname
   - Service-Tag
   - Modell
   - iDRAC-IP
   - Speicherort
   - Einschubposition
   - Letzte Bestandsaufnahme

4. Um weitere Informationen zu dem Host anzuzeigen, wählen Sie einen Host aus.

Zugehörige Gehäuseinformationen anzeigen

Im Bereich **Gehäusezuordnung** wird die Beziehung zwischen Gehäuse in einem MX-Gehäuse im MCM-Modus angezeigt.

ANMERKUNG: Zugehörige Gehäuseinformationen gelten nur für PowerEdge MX-Gehäuse, die in einer MCM-Gruppe konfiguriert sind.

1. Klicken Sie auf der OMIVV-Startseite **Hosts und Gehäuse** > **Gehäuse** > **Gehäuseliste**.
   Die Seite **Dell EMC Gehäuse** wird angezeigt.
2. Wählen Sie ein Gehäuse aus und klicken Sie auf den Link „Service-Tag".
   Die Seite **Übersicht** wird angezeigt.

   Auf der Seite **Übersicht** zeigt der Abschnitt **Gehäusezuordnung** Informationen zu allen zugehörigen Gehäusen für Haupt- und Mitgliedsgehäuse an.

PowerEdge MX Gehäuse verwalten

Die Art und Weise der Verwaltung eines MX7000X-Gehäuses unterscheidet sich von der Verwaltung anderer Dell EMC-Gehäuse wie M1000e, VRTX und FX2.

Sie können ein MX-Gehäuse in einem Stand-alone-Modus mit öffentlichen IPs für das Managementmodul und iDRAC-IPs verwalten. Außerdem können Sie ein MX-Gehäuse in einem Modus zur Verwaltung von mehreren Gehäusen mit einem Lead und mehreren Mitgliedern konfigurieren.

Dell OpenManage EMC Enterprise-Modular unterstützt kabelgebundene MCM-Gruppen. In der kabelgebundenen Gruppierung sind die Gehäuse über einen redundanten Port am Managementmodul verkabelt bzw. verkettet. Das von Ihnen für die Erstellung der Gruppe ausgewählte Gehäuse muss mit mindestens einem Gehäuse linear verkabelt sein. Weitere Informationen zum Erstellen der Gehäusegruppe finden Sie unter *Benutzerhandbuch für Dell OpenManage EMC Enterprise-Modular, für PowerEdge MX7000* unter dell.com/support.

Sie haben zwei Möglichkeiten, die Server im MX-Gehäuse zu verwalten:

1. **Verwaltung der Server durch Verwendung des Host-Anmeldeinformationenprofils**: Dies ist die empfohlene Standardmethode zur Verwaltung der Server, mit der alle Funktionen unterstützt werden. In diesem Fall wird das Gehäuse erst erkannt, nachdem die MX-Host-Bestandsaufnahme abgeschlossen ist. Weitere Informationen zum Erstellen eines Host-Zugangsdatenprofils finden Sie unter Host-Anmeldeinformationenprofil erstellen auf Seite 39.
2. **Verwalten der Server mit einem Gehäuse-Anmeldeinformationenprofil**: Wenn Sie Ihre Hosts über das Gehäuse-Anmeldeinformationenprofil verwalten, werden OMIVV-Funktionen wie Inventarisierung, Überwachung, Firmware und Treiber-Updates unterstützt. Weitere Informationen über das Verwalten von Gehäusen und Hosts über das Gehäuse-Anmeldeinformationenprofil finden Sie unter Gehäuse-Zugangsdatenprofil erstellen auf Seite 44.

ANMERKUNG: OMIVV bietet keine Unterstützung für die Verwaltung des PowerEdge MX-Gehäuses mit Konfiguration des Backup-Leads.

ANMERKUNG: Wenn die IPv4-Adresse des iDRAC deaktiviert ist, können Sie den Server mithilfe des Gehäuse-Anmeldeinformationenprofils verwalten. Wenn Sie den Server durch Verwendung des Gehäuse-Anmeldeinformationenprofils verwalten, werden folgende OMIVV-Funktionen nicht unterstützt:

- iDRAC-Sperrmodus
- Möglichkeit zur Verwendung dieses Servers als Referenzserver zur Erfassung des Systemprofils
- BS-Bereitstellung
- Beziehen oder Aktualisieren des CSIOR-Status
- Server-Konfigurationskompatibilität
- Einige Bestandsinformationen

ANMERKUNG: Die Hosts mit einer öffentlichen IPv4-iDRAC-IP können auch über das Gehäuse-Anmeldeinformationenprofil verwaltet werden. Diese Methode wird jedoch nicht empfohlen, da die oben genannten Funktionen nicht unterstützt werden.

Gehäuse- und Host-Management mithilfe der einheitlichen Gehäuse-Management-IP

Wenn eine iDRAC-IPv4 für einen über ein Host-Anmeldeinformationenprofil verwalteten Host deaktiviert ist, schlägt die Hosts-Bestandsaufnahme fehl und das Gehäuse wird nicht erkannt. In solchen Fällen muss das Gehäuse manuell hinzugefügt und mit einem Gehäuse-Anmeldeinformationenprofil verknüpft werden, um das Gehäuse und seine zugehörigen Hosts verwalten zu können.

Wenn Sie Ihre Hosts über die einheitliche Gehäuse-Management-IP verwalten, werden OMIVV-Funktionen wie Inventarisierung, Überwachung, Firmware und Treiber-Updates unterstützt. Im Folgenden finden Sie die allgemeine Beschreibung der Aufgaben zur Verwaltung der Hosts und Gehäuse unter Verwendung der einheitlichen Gehäuse-Management-IP:

1. Fügen Sie ein MX-Gehäuse hinzu.

   Weitere Informationen zum Hinzufügen eines MX Gehäuse finden Sie unter PowerEdge MX Gehäuse hinzufügen auf Seite 117.

2. Erstellen Sie ein Gehäuse-Anmeldeinformationenprofil und ordnen Sie die Hosts zu.

   Weitere Informationen zum Erstellen eines Gehäuse-Anmeldeinformationenprofils finden Sie in Gehäuse-Zugangsdatenprofil erstellen auf Seite 44.

3. Zeigen Sie Jobs für Gehäuse und Host an, die über das Gehäuse-Anmeldeinformationenprofil verwaltet werden.
4. Zeigen Sie die Gehäuse- und Host-Bestandsaufnahme an.

   Weitere Informationen zur Host- und Gehäuse-Bestandsaufnahme finden Sie unter Host-Bestandsaufnahme-Job anzeigen auf Seite 80 und Gehäuse-Bestandsaufnahme-Job anzeigen auf Seite 81.

5. Führen Sie Firmware-Updates auf Hosts durch, die über Gehäuse verwaltet werden.

   Weitere Informationen zur Firmwareaktualisierung finden Sie unter Firmware-Aktualisierung auf Seite 133.

   ANMERKUNG: Bare-Metal-Workflow wird nicht unterstützt, wenn die Hosts über Gehäuse verwaltet werden.

PowerEdge MX Gehäuse hinzufügen

Ein Host mit gültiger IPv4 iDRAC-IP kann zum Host-Anmeldeinformationenprofil hinzugefügt werden und das zugehörige MX-Gehäuse wird während der Host-Bestandsaufnahme automatisch erkannt und auf der Seite **Dell EMC Gehäuse** angezeigt.

Wenn eine iDRAC-IPv4-Adresse für einen Host deaktiviert ist, schlägt die Hosts-Bestandsaufnahme fehl und das Gehäuse wird nicht erkannt. In solchen Fällen muss ein MX-Gehäuse manuell hinzugefügt und mit einem Gehäuse-Anmeldeinformationenprofil verknüpft werden, um das Gehäuse und seine zugehörigen Hosts verwalten zu können.

Um ein MX-Gehäuse manuell hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie auf der **OMIVV**-Startseite auf **Hosts und Gehäuse** > **Gehäuse**.
2. Klicken Sie auf der Seite **Dell EMC Gehäuse** auf **MX-GEHÄUSE HINZUFÜGEN**.
3. Geben Sie eine Managementmodul-IPv4 bzw. einen FQDN oder Hostnamen ein und klicken Sie auf **OK**.

Wenn Sie eine IP eingeben, wird überprüft, ob die IP von OMIVV verwaltet wird.

ANMERKUNG: Bevor Sie ein Gehäuse über Hostname oder FQDN hinzufügen, stellen Sie sicher, dass gültige Forward- und Reverse-Lookup-Einträge im DNS erstellt werden.

ANMERKUNG: Wenn Sie eine FQDN eingeben, wird die Gehäuse-URL mit der FQDN angezeigt.

Das Gehäuse wird auf der Seite **Dell EMC Gehäuse** hinzugefügt.

4. Weisen Sie die Hosts dem Gehäuse-Anmeldeinformationenprofil durch die Erstellung des Gehäuseprofils zu. Weitere Informationen zum Erstellen eines Gehäuse-Anmeldeinformationenprofils finden Sie in Gehäuse-Zugangsdatenprofil erstellen auf Seite 44.

ANMERKUNG: Wenn Sie eine andere IP als die MX-Gehäuse-IP-Adresse eingegeben haben, schlägt die Testverbindung fehl und der ungültige Eintrag verbleibt auf der Seite **Dell EMC Gehäuse**. Nur erfolgreich geprüfte Gehäuse werden dem Gehäuse-Anmeldeinformationenprofil zugeordnet.

ANMERKUNG: Die Testverbindung schlägt fehl, wenn die Hosts nicht in den registrierten vCentern vorhanden sind, die dem hinzugefügten MX-Gehäuse zugeordnet sind.

ANMERKUNG: Bei einem PowerEdge MX-Gehäuse, das in einer MCM-Konfiguration konfiguriert wurde, müssen Haupt- und Mitgliedsgehäuse dieselben Anmeldeinformationen haben.

MX-Gehäuse-Firmwareaktualisierung

Bevor Sie die Firmwareaktualisierung planen, stellen Sie sicher, dass die folgenden Bedingungen in der Umgebung erfüllt sind:

- Stellen Sie sicher, dass das MX-Gehäuse Teil des Gehäuse-Anmeldeinformationenprofils ist und erfolgreich inventarisiert wurde.
- Wenn auf einem der Hosts Firmwareaktualisierungen stattfinden, kann die Gehäuse-Firmware nicht aktualisiert werden.

ANMERKUNG: Durch die Verwendung der MX-Gehäuse-Firmwareaktualisierungsfunktion können Sie nur die Managementmodul-Firmware aktualisieren.

1. Klicken Sie auf der OMIVV-Startseite auf **Hosts & Gehäuse** > **Gehäuse** > **Gehäuseliste** > **MX GEHÄUSE-FIRMWAREAKTUALISIERUNG**.
2. Lesen Sie auf der Seite **Gehäuse-Firmwareaktualisierung** die Anweisungen und klicken Sie dann auf **ERSTE SCHRITTE**.
3. Wählen Sie aus der **MX-Gehäuseliste** ein oder mehrere MX-Gehäuse aus und klicken Sie dann auf **WEITER**.

   Das Gehäuse wird nicht angezeigt, wenn eine der folgenden Bedingungen in der Umgebung nicht erfüllt ist:

   - Die Gehäuse-Firmwareaktualisierung wird von OMIVV durchgeführt.
   - Das Gehäuse-Anmeldeinformationenprofil wird nicht für das Gehäuse erstellt.
   - Die Bestandsaufnahme ist für das Gehäuse nicht erfolgreich.

   Für das PowerEdge MX-Gehäuse mit MCM-Konfiguration können Sie nur das Hauptgehäuse auswählen. Das Mitgliedsgehäuse wird automatisch ausgewählt.

4. Führen Sie auf der Seite **Aktualisierungsquelle auswählen** Folgendes aus:
   a. Wählen Sie ein geeignetes Firmware-Repository-Profil aus dem Drop-Down-Menü aus.
   b. Wählen Sie basierend auf dem Gehäuse- und Firmware-Repository-Profil, das Sie ausgewählt haben, die entsprechenden Pakete aus der identifizierten Systemkategorie aus.
5. Wählen Sie auf der Seite **Firmwarekomponentenauswahl** die Firmwarekomponenten aus, die Sie aktualisieren möchten, und dann klicken Sie auf **Weiter**.

   Die Komponenten, die eine niedrigere Version als die verfügbare Version im Katalog haben, oder sich auf derselben Ebene befinden (aktuell sind), können nicht ausgewählt werden. Um die Komponenten auszuwählen, die im Downgrade-Status aufgelistet sind, klicken Sie auf **Firmware-Downgrade zulassen**.

   In einem PowerEdge MX-Gehäuse, das einer MCM-Konfiguration zugeordnet ist, kann die Firmware-Version zurückgestuft werden, selbst wenn das Kontrollkästchen **Firmware-Downgrade zulassen** nicht aktiviert ist.

   Sie können nicht nur Mitgliedsgehäuse für Aktualisierung oder Downgrade auswählen. Wenn Sie das Hauptgehäuse auswählen, wird automatisch das Mitgliedsgehäuse ausgewählt.

   Um alle Firmware-Komponenten auf allen Seiten auszuwählen, klicken Sie auf .

Um alle Firmware-Komponenten auf allen Seiten zu löschen, klicken Sie auf X.

6. Führen Sie auf der Seite **Job planen** Folgendes aus:
   a. Geben Sie den Namen und die Beschreibung der Firmwareaktualisierung an. Die Beschreibung ist ein optionales Feld.

      Der Name des Firmwareaktualisierungs-Jobs ist obligatorisch. So wird sichergestellt, dass Sie keinen bereits vorhandenen Namen verwenden. Wenn Sie den Namen des Firmwareaktualisierungs-Jobs entfernen, können Sie ihn wiederverwenden.
   b. Wählen Sie eine entsprechende Planungsoption aus, um die Aktualisierungen anzuwenden.
7. Überprüfen Sie die Details zur Firmwareaktualisierung auf der Seite **Zusammenfassung überprüfen** und klicken Sie auf **FERTIGSTELLEN**.

Tabelle 11. Gesamtzahl der gleichzeitigen MX-Gehäuse-Firmwareaktualisierungen, die für jeden Bereitstellungsmodus ausgeführt werden.

Bereitstellungsmodus	Anzahl der gleichzeitigen Gehäuse-Firmwareaktualisierungen
Klein	1
Mittel	1
Groß	2
Extra Large (Extra groß)	2

17

Hostverwaltung

OMIVV-Hosts anzeigen

Sie können alle OMIVV-verwalteten Hosts auf der Seite **OMIVV-Hosts** anzeigen.

1. Klicken Sie auf der OMIVV-Startseite auf **Hosts und Gehäuse** > **Hosts**.
2. Auf der Registerkarte **OMIVV-Hosts** können Sie folgende Informationen einsehen:
   - **Hostname**: Zeigt die IP-Adresse des Hosts an. Um die Hostinformationen anzuzeigen, wählen Sie einen Host aus.
   - **Funktionszustand**: Zeigt den Funktionszustand von Hosts an.

     Um den Integritätsstatus jedes Dell EMC Hosts zu filtern, klicken Sie auf das Filtersymbol, das in der Suche vorhanden ist.
   - **vCenter**: Zeigt die vCenter IP-Adresse des Hosts an.
   - **Cluster** – Zeigt den Clusternamen an, wenn der Dell EMC Host sich in einem Cluster befindet.
   - **Host-Zugangsdatenprofil**: Zeigt den Namen des Host-Zugangsdatenprofils an.

Einen einzelnen Host überwachen

Mit dem OMIVV können Sie detaillierte Informationen zu einem einzelnen Host anzeigen. Sie können alle OMIVV-Hosts auf der Seite **Hosts und Cluster** anzeigen. Um weitere Informationen anzuzeigen, wählen Sie einen bestimmten OMIVV-verwalteten Host aus und gehen Sie dann zu**Überwachen** > **OMIVV Host-Information**.

Anzeigen der Hostzusammenfassungsinformationen

Sie können die Details der Host-Zusammenfassung für einzelne Hosts auf der Seite **Zusammenfassung**, auf der verschiedene Portlets angezeigt werden, einsehen. Zwei der Portlets gelten für OMIVV. Die zwei Portlets sind:

- **OMIVV Hostzustand**
- **OMIVV Hostinformationen**

Sie können diese zwei Portlets auf die gewünschte Position ziehen und ablegen, und Sie können die zwei Portlets wie andere Portlets entsprechend Ihren Anforderungen formatieren und anpassen. So zeigen Sie die Details der Host-Zusammenfassung an:

1. Erweitern Sie auf der OMIVV-Startseite **Menü** und wählen Sie dann **Hosts und Cluster** aus.
2. Wählen Sie im linken Fensterbereich einen spezifischen Host aus.
3. Klicken Sie im rechten Fensterbereich auf **Zusammenfassung**.
4. Führen Sie zur Anzeige des OMIVV-Server-Management-Portlets einen Bildlauf nach unten durch.

   Sie können die folgenden Informationen im Abschnitt **OMIVV-Hostinformationen** und **OMIVV-Hostintegrität** anzeigen:

Tabelle 12. OMIVV Hostinformationen

Informationen	Beschreibung
Service Tag	Zeigt die Service-Tag-Nummer des Servers an. Verwenden Sie diese Nummer, wenn Sie den Support anrufen.
Modellname	Zeigt den Modellnamen des Servers an.
Fault Resilient Memory	Zeigt den Status des BIOS-Attributs an. Das BIOS-Attribut wird im BIOS bei der Ersteinrichtung des Servers aktiviert und zeigt den Speicherbetriebsmodus des Servers an. Starten Sie das System nach dem Ändern des Werts des Speicherbetriebsmodus

Tabelle 12. OMIVV Hostinformationen (fortgesetzt)

Informationen	Beschreibung
	neu. Dies gilt für PowerEdge-Server mit Unterstützung der Option FRM (Fault Resilient Memory), auf denen die ESXi-Version 5.5 oder höher läuft. Die vier verschiedenen Werte des BIOS-Attributs sind: ● Aktiviert und geschützt: Dieser Wert bedeutet, dass das System unterstützt wird und das Betriebssystem-Version ESXi 5.5 oder höher ist sowie, dass der Speicherbetriebsmodus in BIOS auf FRM eingestellt ist. ● NUMA aktiviert und geschützt: Dieser Wert bedeutet, dass das System unterstützt wird und dass die Betriebssystem-Version ESXi 5.5 oder höher ist sowie, dass der Speicherbetriebsmodus in BIOS auf NUMA eingestellt ist. ● Aktiviert und nicht geschützt: Dieser Wert zeigt an, dass Systeme mit Betriebssystem-Versionen niedriger als ESXi 5.5 unterstützt werden. ● Deaktiviert: Dieser Wert zeigt an, dass gültige Systeme mit jeglichen Betriebssystem-Versionen unterstützt werden und der Speicherbetriebsmodus in BIOS nicht auf FRM gesetzt ist. ● Leer: Wenn der Speicherbetriebsmodus in BIOS nicht unterstützt wird, wird das FRM-Attribut nicht angezeigt.
Systemsperrmodus	Zeigt den Status des iDRAC-Sperrmodus für iDRAC-Server 8 und höher an. Ein geschlossenes Vorhängeschloss zeigt an, dass der iDRAC-Sperrmodus aktiv ist; ein geöffnetes Schloss zeigt, dass der iDRAC-Sperrmodus ausgeschaltet ist.
Identifikation	Zeigt die folgenden Optionen an: ● Hostname – Zeigt den Namen des OMIVV-verwalteten Hosts an ● Stromzustand: Zeigt an, ob der Strom ein- oder ausgeschaltet ist ● iDRAC-IP – Zeigt die iDRAC-IP-Adresse an ● Verwaltungs-IP – Zeigt die Verwaltungs-IP-Adresse an ● Host-Anmeldeinformationenprofil: Zeigt den Namen des Host-Anmeldeinformationenprofils für diesen Host an ● Modell – Zeigt das Dell EMC Server-Modell an ● Service-Tag-Nummer: Zeigt die Service-Tag-Nummer des Servers an. ● Systemkennnummer – Zeigt die Systemkennnummer an ● Verbleibende Servicezeit – Zeigt die verbleibende Servicezeit in Tagen an ● Letzter Bestandsaufnahme-Scan – Zeigt das Datum und die Uhrzeit des letzten Bestandsaufnahme-Scans an
Hypervisor und Firmware	Zeigt die folgenden Optionen an: ● Hypervisor – Zeigt die Hypervisor-Version an ● BIOS-Version – Zeigt die BIOS-Version an ● Version der Remotezugriffskarte – Zeigt die Version der Remotezugriffskarte an
Management-Konsolen	Zeigt einen Link zum Starten der Remote-Zugriffskonsole (iDRAC) an.
Hostmaßnahmen	Für ein Blinken in verschiedenen Zeitintervallen muss der physische Server entsprechend eingerichtet werden.

Tabelle 12. OMIVV Hostinformationen (fortgesetzt)

Informationen	Beschreibung
	Informationen dazu finden Sie unter Blinkanzeigelicht einrichten auf Seite 150.

Tabelle 13. OMIVV Hostzustand

Informationen	Beschreibung
OMIVV Hostzustand	Der Zustand der Komponenten ist eine grafische Darstellung des Status der wichtigsten Hostserverkomponenten: Globaler Serverstatus, Server, Stromversorgung, Temperatur, Spannung, Prozessoren, Batterien, Eingriffe, Hardwareprotokoll, Stromverwaltung, Strom und Speicher. Die Parameter zum Gehäuse-Funktionszustand sind nur für VRTX-Modelle der Version 1.0 und höher und M1000e Version 4.4 und höher relevant. Bei Versionen unter 4.3 werden nur zwei Zustandsindikatoren angezeigt: Fehlerfrei und Warnung oder Kritisch (ein invertiertes Dreieck mit einem orangefarbenen Ausrufungszeichen). Der Gesamtfunktionszustand zeigt den Funktionszustand basierend auf dem Gehäuse mit den schlechtesten Funktionszustandswerten. Zu den Optionen zählen: • Funktionsfähig (grünes Häkchen) – Komponente arbeitet normal • Warnung (gelbes Dreieck mit Ausrufezeichen) – Komponente weist einen nichtkritischen Fehler auf. • Kritisch (rotes X) – Komponente weist einen kritischen Fehler auf. • Unbekannt (Fragezeichen) – Status der Komponente ist unbekannt.

Wenn zum Beispiel 5 Zeichen für funktionsfähig und 1 Warnzeichen angezeigt werden, wird der Gesamtfunktionszustand als Warnung angezeigt.

ANMERKUNG: Stromüberwachungsinformationen sind für Hosts mit verkabeltem Netzteil oder für modulare Server nicht verfügbar.

OMIVV Hostinformationen anzeigen

Sie können die Hardware-, Speicher-, Firmware-, Stromüberwachung-, Service- und Systemereignisprotokoll-Informationen über alle OMIVV-verwalteten Hosts auf der Seite **OMIVV-Host-Informationen** anzeigen.

1. Erweitern Sie auf der OMIVV-Startseite **Menü** und wählen Sie dann **Hosts und Cluster** aus.
2. Wählen Sie im linken Fensterbereich einen Host aus und klicken Sie dann auf **Überwachen** > **OMIVV Hostinformationen**.

Hardwareinformationen eines Hosts anzeigen

Tabelle 14. Hardware-Informationen für einen einzigen Host

Hardware: *Komponente*	Informationen
FRU	• **Teilename**: Zeigt den FRU-Teilenamen an. • **Teilenummer**: Zeigt die FRU-Teilenummer an. • **Hersteller**: Zeigt den Herstellernamen an. • **Seriennummer**: Zeigt die Seriennummer des Herstellers an. • **Herstellungsdatum**: Zeigt das Herstellungsdatum an.
Prozessoren	• **Steckplatz**: Zeigt die Steckplatznummer an.

Tabelle 14. Hardware-Informationen für einen einzigen Host (fortgesetzt)

Hardware: *Komponente*	Informationen
	• **Geschwindigkeit**: Zeigt die aktuelle Geschwindigkeit an. • **Marke**: Zeigt die Prozessormarke an. • **Version**: Zeigt die Prozessorversion an. • **Kerne**: Zeigt die Anzahl der Prozessorkerne an.
Netzteile	• **Typ**: Zeigt den Netzteiltyp an. Zu den Netzteiltypen zählen: ○ UNBEKANNT ○ LINEAR ○ SCHALTNETZTEIL ○ BATTERY ○ USV ○ UMWANDLER ○ REGULATOR ○ Wechselstrom (AC) ○ Gleichstrom (DC) ○ VRM • **Standort**: Zeigt den Standort des Netzteils an, z. B. Steckplatz 1. • **Ausgang (Watt)**: Zeigt den Stromausgang in Watt an.
Speicher	• **Speichersteckplätze**: Zeigt die verwendete, gesamte und verfügbare Speicheranzahl an. • **Speicherkapazität**: Zeigt die installierten Speicher, Gesamtspeicherkapazität und verfügbaren Speicher an. • **Steckplatz**: Zeigt den DIMM-Steckplatz an. • **Größe**: Zeigt die Speichergröße an. • **Typ**: Zeigt den Speichertyp an.
NICs	• **Insgesamt**: Zeigt die Gesamtanzahl der verfügbaren Netzwerkschnittstellenkarten an. • **Name**: Zeigt den NIC-Namen an. • **Hersteller**: Zeigt nur den Herstellernamen an. • **MAC-Adresse**: Zeigt die MAC-Adresse der NIC an.
PCI-Steckplätze	• **PCI-Steckplätze**: Zeigt die verwendete, gesamte und verfügbare Anzahl an PCI-Steckplätzen an. • **Steckplatz**: Zeigt den Steckplatz an. • **Hersteller**: Zeigt den Herstellernamen des PCI-Steckplatzes an. • **Beschreibung**: Zeigt die Beschreibung des PCI-Geräts an. • **Typ**: Zeigt den Typ des PCI-Steckplatzes an. • **Breite**: Zeigt die Datenbusbreite an, wenn verfügbar.
Remote-Zugriffskarte	• **IP-Adresse**: Zeigt die IP-Adresse der Remote-Zugriffskarte an. Wenn Sie Hosts über eine vereinheitlichte IP-Adresse verwalten, wird die iDRAC-IP in diesem Abschnitt nicht angezeigt. • **MAC-Adresse**: Zeigt die MAC-Adresse der Remote-Zugriffskarte an. • **RAC-Typ**: Zeigt den Typ der Remote-Zugriffskarte an. • **URL**: Zeigt die verfügbare URL für den iDRAC an, der diesem Host zugeordnet wurde.

Speicherinformationen eines Hosts anzeigen

Sie können die Anzahl der virtuellen Festplatten, Controller, Gehäuse und der zugehörigen physischen Festplatten mit der Anzahl der globalen und dedizierten Hotspares anzeigen. Um weitere Informationen zu den einzelnen Speicherkomponenten anzuzeigen, wählen Sie aus dem Drop-Down-Menü **Ansicht** die jeweilige Komponente aus.

Für Hosts, die über Gehäuse verwaltet werden, werden die vollständigen Speicherinformationen wie Controller, Gehäuse, globales Ersatzlaufwerk und dediziertes Ersatzlaufwerk nicht angezeigt.

ANMERKUNG: Wenn die Hosts unter Verwendung des Gehäuseprofils verwaltet werden, klicken Sie auf **Speicher** und wählen Sie Folgendes aus dem Drop-Down-Menü **Ansicht** aus:

- **Gehäuse**: Die Controller-ID des Speichergehäuses wird als 0 anstelle der korrekten Controller-ID angezeigt.
- **Physische Laufwerke**: Der Medientyp für HDD wird als **Magnetisches Laufwerk** anstelle eines **Festplattenlaufwerks** angezeigt.

Tabelle 15. Speicherdetails für einen einzigen Host

Informationen	Beschreibung
Virtuelle Festplatten	• **Name**: Zeigt den Namen des virtuellen Laufwerks an. • **Geräte-FQDD**: Zeigt FQDD an. • **Physisches Laufwerk**: Zeigt an, auf welcher physischen Festplatte sich das virtuelle Laufwerk befindet. • **Kapazität**: Zeigt die Kapazität des virtuellen Laufwerks an. • **Layout**: Zeigt den Layout-Typ des virtuellen Speichers an. Damit ist der für dieses virtuelle Laufwerk konfigurierte RAID-Typ gemeint. • **Medientyp**: Zeigt entweder SSD oder HDD an. Um Informationen wie die Stripe-Größe, das Bus-Protokoll und die Cache-Richtlinie anzuzeigen, wählen Sie eine virtuelle Festplatte aus. • **Controller-ID**: Zeigt die Controller-ID an. • **Geräte-ID**: Zeigt die Geräte-ID an. • **Stripe-Größe**: Bezieht sich auf die Menge an Speicherplatz, die jeder Stripe auf einer einzelnen Festplatte belegt. • **Bus-Protokoll**: Zeigt die Technologie an, die physischen Festplatten im virtuellen Laufwerk verwenden. Die möglichen Wert sind: ○ SCSI ○ SAS ○ SATA • **Standard-Leserichtlinie**: Zeigt die durch den Controller standardmäßig unterstützte Leserichtlinie an. Zu den Optionen zählen: ○ Vorauslesen ○ Kein Vorauslesen ○ Adaptives Vorauslesen ○ Lese-Cache aktiviert ○ Lese-Cache deaktiviert • **Standard-Schreibrichtlinie**: Zeigt die durch den Controller standardmäßig unterstützte Schreibrichtlinie an. Zu den Optionen zählen: ○ Rückschreiben ○ Rückschreiben erzwingen ○ Rückschreiben aktiviert ○ Durchschreiben ○ Schreib-Cache aktiviert und geschützt. ○ Schreib-Cache deaktiviert • **Cache-Regel**: Wird angezeigt, wenn die Cache-Regeln aktiviert sind.
Physische Festplatten	• **Name**: Zeigt den Namen des physischen Laufwerks an. • **FQDD**: Zeigt Geräte-FQDD an.

Tabelle 15. Speicherdetails für einen einzigen Host (fortgesetzt)

Informationen	Beschreibung
Wenn Sie diese Option aus dem Drop-Down-Menü **Ansicht** auswählen, wird die Dropdown-Liste **Filter** angezeigt. Die folgenden Optionen sind im Filter verfügbar: • **Alle physischen Festplatten** • **Globale Hotspares** • **Dedizierte Ersatzgeräte** • Diese letzte Option zeigt den Namen der virtuellen Laufwerke an.	• **Kapazität**: Zeigt die Kapazität der physischen Festplatte an. • **Festplattenstatus**: Zeigt den Status der physischen Festplatte an. Zu den Optionen zählen: ○ ONLINE ○ BEREIT ○ HERABGESETZT ○ FEHLGESCHLAGEN ○ OFFLINE ○ NEUERSTELLUNG ○ INKOMPATIBEL ○ ENTFERNT ○ GELÖSCHT ○ SMART-WARNUNG FESTGESTELLT ○ UNBEKANNT ○ FREMD ○ NICHT UNTERSTÜTZT • **Konfiguriert**: Zeigt an, ob die Festplatte konfiguriert ist. • **Hotspare -Typ**(gilt nicht für PCIe) – Zeigt den Hotspare-Typ an. Zu den Optionen zählen: ○ Nein – Bedeutet, dass kein Hotspare vorhanden ist. ○ Global – Ein globales Hotspare ist eine nicht verwendete Backup-Festplatte, die ein Teil der Festplattengruppe ist ○ Dediziert – Eine nicht verwendete Backup-Festplatte, die einem einzelnen virtuellen Laufwerk zugewiesen ist. Wenn eine physische Festplatte im virtuellen Laufwerk versagt, wird der Hotspare aktiviert, um die fehlerhafte physische Festplatte ohne Unterbrechung des Systems oder erforderlichen Benutzereingriff zu ersetzen. • **Virtuelle Festplatte**: Zeigt den Namen des virtuellen Laufwerks an. • **Bus-Protokoll**: Zeigt das Bus-Protokoll an. • **Controller-ID**: Zeigt die Controller-ID an. • **Medientyp**: Zeigt entweder SSD oder HDD an. • **Geschätzte verbleibende Schreibdauer**: Zeigt die verbleibende SSD-Schreibdauer an. • **Anschluss-ID**: Zeigt die Anschluss-ID an. • **Gehäuse-ID**: Zeigt die Gehäuse-ID an. • **Geräte-ID**: Zeigt die Geräte-ID an. • **Modell**: Zeigt die Modellnummer des physischen Speicherlaufwerks an. • **Teilenummer**: Zeigt die Speicherteilenummer an. • **Seriennummer**: Zeigt die Speicherseriennummer an. • **Hersteller**: Zeigt den Namen des Speicheranbieters an.
Controller	• **Controller-ID**: Zeigt die Controller-ID an. • **Name**: Zeigt den Namen des Controllers an. • **Geräte-FQDD**: Zeigt FQDD des Geräts an. • **Firmware-Version**: Zeigt die Firmware-Version an. • **Minimal erforderliche Firmware**: Zeigt die minimal erforderliche Firmware an. Diese Spalte wird automatisch befüllt, wenn die Firmware veraltet und eine neuere Version verfügbar ist. • **Treiberversion**: Zeigt die Treiberversion an. • **Patrol Read-Zustand**: Zeigt den Patrol Read-Zustand an. • **Cache-Größe**: Zeigt die Cache-Größe an. **ANMERKUNG:** In diesem Abschnitt werden Informationen zum Chipsatz-Controller angezeigt. Dies wird nicht im Speicher-Controller-Abschnitt der iDRAC-

Tabelle 15. Speicherdetails für einen einzigen Host (fortgesetzt)

Informationen	Beschreibung
	Benutzeroberfläche angezeigt, aber Sie können diese Informationen über die Seite „Bestandsaufnahme“ des iDRAC anzeigen.
Gehäuse	• **Controller-ID**: Zeigt die Controller-ID an. • **Anschluss-ID**: Zeigt die Anschluss-ID an. • **Gehäuse-ID**: Zeigt die Gehäuse-ID an. • **Name**: Zeigt den Namen des Gehäuses an. • **FQDD**: Zeigt Geräte-FQDD an. • **Service-Tag-Nummer**: Zeigt die Service-Tag-Nummer an.

Firmware-Informationen für einen einzigen Host anzeigen

Die folgenden Firmware-bezogenen Informationen werden angezeigt:

- **Name**: Zeigt den Namen von sämtlicher Firmware auf diesem Host an.
- **Typ**: Zeigt den Firmware-Typ an.
- **Version**: Zeigt die Version von sämtlicher Firmware auf diesem Host an.
- **Installationsdatum**: Zeigt das Installationsdatum an.

ANMERKUNG: Wenn die Hosts unter Verwendung des Gehäuse-Anmeldeinformationenprofils verwaltet werden, zeigen die Daten zur Firmware-Bestandsaufnahme ein paar zusätzliche Komponenten wie den Lifecycle-Controller und Software-RAID.

Auf dieser Seite können Sie die Firmwareaktualisierung starten und die Assistenten für den Systemsperrmodus konfigurieren.

Stromüberwachungsinformationen für einen einzigen Host anzeigen

Sie können die Informationen anzeigen, wie z. B. allgemeine Informationen, Schwellenwerte, Stromkapazitätsreserve und Energiestatistik.

- **Allgemeine Informationen**: Zeigt das Strombudget und aktuelle Profilname an.
- **Schwellenwert**: Zeigt die Warnungs- und Fehlerschwellenwerte in Watt an.
- **Stromkapazitätsreserve**: Zeigt die unmittelbare- und Spitzenstromkapazitätsreserve in Watt an.

Energiestatistiken

- **Typ**: Zeigt den Typ der Energiestatistiken an.
- **Startzeit der Messung (Hostzeit)** – Zeigt das Datum und die Uhrzeit an, zu der der Host mit dem Energieverbrauch begonnen hat.
- **Endzeit der Messung (Hostzeit)** – Zeigt das Datum und die Uhrzeit an, zu der der Energieverbrauch des Hosts gestoppt wurde.
- **ANMERKUNG:** Die Hostzeit, wie sie hier verwendet wird, bedeutet die Zeit des Orts, an dem sich der Host befindet.

  Messwert: Zeigt den Durchschnittswert der Messwerte über einen Zeitraum von einer Minute an.
- **Spitzenzeit**: Zeigt das Datum und die Uhrzeit der Spitzen-Ampere des Hosts an.
- **Spitzenmesswert**: Zeigt die Statistiken des Spitzenstroms des Systems an, die aus dem Spitzenstromverbrauch des Systems (in Watt) bestehen.

ANMERKUNG: Stromüberwachungsinformationen sind für Hosts mit verkabeltem Netzteil oder für modulare Server nicht verfügbar.

ANMERKUNG: Für Hosts, die über Gehäuse verwaltet werden, werden keine vollständigen Informationen zur Stromüberwachung angezeigt.

Service-Informationen für einen einzigen Host anzeigen

Um einen Servicestatus anzuzeigen, müssen Sie einen Service-Job ausführen. Informationen dazu finden Sie unter Serviceabfrage-Jobs planen auf Seite 109. Die Seite **Servicestatus** ermöglicht Ihnen die Überwachung des Ablaufdatums des Service. Die Serviceeinstellungen legen fest, wann Serverserviceinformationen von Dell online abgerufen werden. Dazu aktivieren oder deaktivieren Sie den Serviceplan und legen einen Schwellenwert für den Alarm „Minimum (Tage)“ fest.

- **Anbieter**: Zeigt den Namen des Anbieters des Service an.

- **Beschreibung** – Zeigt eine Beschreibung an
- **Status**: Zeigt den Servicestatus des Hosts an. Die Statusoptionen beinhalten:
  - Aktiv – Der Host ist unter Service und hat keinen Schwellenwert überschritten.
  - Warnung – Der Host ist aktiv, hat jedoch den Warnungsschwellenwert überschritten.
  - Kritisch – Entspricht einer Warnung, jedoch für einen kritischen Schwellenwert.
  - Abgelaufen – Der Service für diesen Host ist abgelaufen.
  - Unbekannt – OMIVV kann den Servicestatus nicht abrufen, weil der Service-Job nicht ausgeführt wurde, ein Fehler beim Abrufen der Daten aufgetreten ist oder weil das System keinen Service hat
- **Berechtigungstyp**: Zeigt die folgenden Status an:
  - Einstieg
  - Erweitert
  - Abgelaufen
- **Startdatum**: Zeigt das Startdatum des Service an.
- **Enddatum**: Zeigt das Enddatum des Service an.
- **Verbleibende Zeit**: Zeigt die verbleibende Servicezeit in Tagen an.
- **Zuletzt aktualisiert**: Zeigt das Datum der letzten Aktualisierung des Service an.

Systemereignisprotokoll-Informationen für einen einzigen Host anzeigen

Das Systemereignisprotokoll (SEL) zeigt Statusinformationen für von OMIVV ermittelte Hardware an. Folgende Informationen werden angezeigt:

- **Status**: Es gibt verschiedene Status-Symbole, wie z. B. Informativ (blaues Ausrufezeichen), Warnung (gelbes Dreieck mit Ausrufezeichen), Fehler (rotes X) und Unbekannt (Kästchen mit „?”).

  Die Schweregrade sind definiert als:

  - Info
  - Warnung
  - Fehler

- **Uhrzeit (Serverzeit)**: Gibt die Uhrzeit und das Datum an, an dem das Ereignis aufgetreten ist.

Um alle Systemereignisprotokollen zu löschen, klicken Sie auf **PROTOKOLL LÖSCHEN**. Es wird eine Meldung angezeigt, die darauf hinweist, dass die Protokolldaten nach dem Löschen des Protokolls nicht wiederhergestellt werden können.

Hosts auf Clustern und in Rechenzentren überwachen

Das OMIVV ermöglicht die Anzeige detaillierter Informationen für alle Hosts in einem Rechenzentrum oder Cluster.

OMIVV-Rechenzentrums- und Clusterinformationen anzeigen

Übersicht über Rechenzentren und Cluster anzeigen

Sie können die Informationen, wie z. B. Informationen zum Rechenzentrum oder Cluster, zum Sperrmodus des Systems, Hardwareressourcen und Serviceinformationen anzeigen. Um die Informationen zu dieser Seite anzuzeigen, stellen Sie sicher, dass die Bestandsaufnahme erfolgreich abgeschlossen wurde. Die OMIVV-Rechenzentrums- und Cluster-Ansichten melden Daten direkt aus iDRAC.

1. Erweitern Sie auf der OMIVV-Startseite **Menü** und wählen Sie dann **Hosts und Cluster** aus.
2. Wählen Sie im linken Fensterbereich ein Rechenzentrum oder einen Cluster aus und klicken Sie dann auf **Überwachen** > **OMIVV-Cluster- oder Rechenzentrumsinformationen**.
3. Um weitere Informationen anzuzeigen, wählen Sie einen bestimmten Host aus.

   Die Informationen, wie z. B. IP-Adresse des iDRAC, Gehäuse-URL, CPUs und Speicher, werden im unteren oberen Bereich der Seite angezeigt.

Tabelle 16. Übersicht der Rechenzentren und Cluster

Informationen	Beschreibung
Datacenter-/Cluster-Informationen	Zeigt die folgenden Optionen an: ● Datacenter-/Clustername ● Anzahl verwalteter Hosts ● Gesamtenergieverbrauch
Systemsperrmodus	Zeigt den Status des iDRAC-Sperrmodus an. Die Status des iDRAC-Sperrmodus werden folgendermaßen für alle Hosts angezeigt: ● Eingeschaltet ● Ausgeschaltet ● Nicht zutreffend (Nur für iDRAC9-basierte Server) Eine Liste der iDRAC9-basierten Server finden Sie in der Compliance-Matrix.
Hardware-Ressourcen	Zeigt die folgenden Optionen an: ● Gesamtanzahl der Prozessoren ● Gesamter Speicher ● Kapazität von virtuellen Laufwerken
Garantiezusammenfassung	Zeigt den Servicestatus für den ausgewählten Host an. Die Statusoptionen beinhalten: ● Abgelaufene Garantie ● Aktive Garantie ● Überschreitung des Warnungsschwellenwerts ● Überschreiten des kritischen Schwellenwerts ● Unbekannte Garantie Für jeden Host oder jedes Gehäuse mit mehreren oder unterschiedlichen Gewährleistungen (z. B. Service-Level-Code wie ND und 4DP), berücksichtigt OMIVV den Status des Gewährleistungstyps, der die geringste Anzahl an Gewährleistungstagen hat.
Host	Zeigt den Hostnamen an
Service Tag	Zeigt die Service-Tag-Nummer des Hosts an
Modell	Zeigt das PowerEdge-Modell an
Asset Tag	Zeigt die Systemkennnummer an, wenn konfiguriert
Service-Tag-Nummer des Gehäuses	Zeigt die Gehäuse-Service-Tag-Nummer an, falls verfügbar
Betriebssystemversion	Zeigt die Version des ESXi-Betriebssystems an
Speicherort	Nur Blades: Zeigt die Steckplatzposition an. Für andere wird "Nicht zutreffend“ angezeigt
Systemsperrmodus	Nur für iDRAC9-basierte Power Edge Server: Zeigt den iDRAC-Sperrmodus des Host an: Eingeschaltet, Ausgeschaltet oder Unbekannt. Für Power Edge-Server vor der iDRAC9-basierten Version wird der Systemsperrmodus als **Nicht zutreffend** angezeigt. Eine Liste der iDRAC9-basierten Server finden Sie in der Compliance-Matrix.
iDRAC-IP	Zeigt die IP-Adresse des iDRACs an
Service-Konsolen-IP	Zeigt die Service-Konsolen-IP an

Tabelle 16. Übersicht der Rechenzentren und Cluster (fortgesetzt)

Informationen	Beschreibung
CMC- oder Managementmodul-URL	Zeigt die CMC oder Managementmodul-URL an, die bei modularen Servern der Gehäuse-URL entspricht, sonst wird „Nicht zutreffend“ angezeigt.
CPUs	Zeigt die Anzahl der CPUs an
Speicher	Zeigt den Host-Speicher an
Stromzustand	Zeigt an, ob der Host mit Strom versorgt wird.
Letzte Bestandsaufnahme	Zeigt den Tag, das Datum und die Uhrzeit des letzten Bestandsaufnahme-Jobs an
Host-Zugangsdatenprofil	Zeigt den Namen des Host-Anmeldeinformationenprofils an
Version der Remote-Zugriffskarte	Zeigt die Version der Remote-Zugriffskarte an
BIOS-Firmware-Version	Zeigt die Firmware-Version des BIOS an

Hardwareinformationen zu einem Rechenzentrum und Cluster anzeigen

Tabelle 17. Hardware-Informationen für Rechenzentren und Cluster

Hardware: *Komponente*	Informationen
Hardware: FRU	• **Host**: Zeigt den Hostnamen an. • **Service-Tag**: Zeigt den Service-Tag des Hosts an. • **Teilename**: Zeigt den FRU-Teilenamen an. • **Teilenummer**: Zeigt die FRU-Teilenummer an. • **Hersteller**: Zeigt den Herstellernamen an. • **Seriennummer**: Zeigt die Seriennummer des Herstellers an. • **Herstellungsdatum**: Zeigt das Herstellungsdatum an.
Hardware: Prozessor	• **Host**: Zeigt den Hostnamen an. • **Service-Tag**: Zeigt den Service-Tag des Hosts an. • **Steckplatz**: Zeigt die Steckplatznummer an. • **Geschwindigkeit**: Zeigt die aktuelle Geschwindigkeit an. • **Marke**: Zeigt die Prozessormarke an. • **Version**: Zeigt die Prozessorversion an. • **Kerne**: Zeigt die Anzahl der Prozessorkerne an.

Hardware: Netzteil	• **Host**: Zeigt den Hostnamen an.
	• **Service-Tag**: Zeigt den Service-Tag des Hosts an.
	• **Typ**: Zeigt den Netzteiltyp an. Zu den Netzteiltypen zählen:
	  ○ UNBEKANNT
	  ○ LINEAR
	  ○ SCHALTNETZTEIL
	  ○ BATTERY
	  ○ USV
	  ○ UMWANDLER
	  ○ REGULATOR
	  ○ Wechselstrom (AC)
	  ○ Gleichstrom (DC)
	  ○ VRM
	• **Standort**: Zeigt den Standort des Netzteils an, z. B. Steckplatz 1.
	• **Ausgang (Watt)**: Zeigt den Stromausgang in Watt an.

Tabelle 17. Hardware-Informationen für Rechenzentren und Cluster (fortgesetzt)

Hardware: *Komponente*	Informationen
	• **Status**: Zeigt den aktuellen Status des Netzteils an. Die Statusoptionen beinhalten: ○ ANDERE ○ UNBEKANNT ○ OK ○ KRITISCH ○ NICHT KRITISCH ○ WIEDERHERSTELLBAR ○ NICHT WIEDERHERSTELLBAR ○ HOCH ○ NIEDRIG
Hardware: Speicher	• **Host**: Zeigt den Hostnamen an. • **Service-Tag**: Zeigt den Service-Tag des Hosts an. • **Steckplatz**: Zeigt den DIMM-Steckplatz an. • **Größe**: Zeigt die Speichergröße an. • **Typ**: Zeigt den Speichertyp an.
Hardware: Netzwerkschnittstellenkarten	• **Host**: Zeigt den Hostnamen an. • **Service-Tag**: Zeigt den Service-Tag des Hosts an. • **Name**: Zeigt den NIC-Namen an. • **Hersteller**: Zeigt nur den Herstellernamen an. • **MAC-Adresse**: Zeigt die MAC-Adresse der NIC an.
Hardware: PCI-Steckplätze	• **Host**: Zeigt den Hostnamen an. • **Service-Tag**: Zeigt den Service-Tag des Hosts an. • **Steckplatz**: Zeigt den Steckplatz an. • **Hersteller**: Zeigt den Herstellernamen des PCI-Steckplatzes an. • **Beschreibung**: Zeigt die Beschreibung des PCI-Geräts an. • **Typ**: Zeigt den Typ des PCI-Steckplatzes an. • **Breite**: Zeigt die Datenbusbreite an, wenn verfügbar.
Hardware: Remote-Zugriffskarte	• **Host**: Zeigt den Hostnamen an. • **Service-Tag**: Zeigt den Service-Tag des Hosts an. • **IP-Adresse**: Zeigt die IP-Adresse der Remote-Zugriffskarte an. • **MAC-Adresse**: Zeigt die MAC-Adresse der Remote-Zugriffskarte an. • **RAC-Typ**: Zeigt den Typ der Remote-Zugriffskarte an. • **URL**: Zeigt die verfügbare URL für den iDRAC an, der diesem Host zugeordnet wurde.

Speicherinformationen zu einem Rechenzentrum und Cluster anzeigen

Tabelle 18. Speicherdetails für ein Rechenzentrum und Cluster

Speicher: Festplatten	Beschreibung
Physische Festplatte	• **Host**: Zeigt den Hostnamen an. • **Service-Tag**: Zeigt den Service-Tag des Hosts an. • **Kapazität**: Zeigt die Kapazität der physischen Festplatte an. • **Festplattenstatus**: Zeigt den Status der physischen Festplatte an. Zu den Optionen zählen:

Tabelle 18. Speicherdetails für ein Rechenzentrum und Cluster (fortgesetzt)

Speicher: Festplatten	Beschreibung
	○ ONLINE ○ BEREIT ○ HERABGESETZT ○ FEHLGESCHLAGEN ○ OFFLINE ○ NEUERSTELLUNG ○ INKOMPATIBEL ○ ENTFERNT ○ GELÖSCHT ○ ERKENNUNG VON SMART-WARNUNGEN ○ UNBEKANNT ○ FREMD ○ NICHT UNTERSTÜTZT **ANMERKUNG:** Lesen Sie für weitere Informationen über die Bedeutung dieser Warnungen das Dell EMC OpenManage Server Administrator Storage-Verwaltung Benutzerhandbuch unter `dell.com/support` ● **Modellnummer**: Zeigt die Modellnummer des physischen Speicherlaufwerks an. ● **Letzte Bestandsaufnahme**: Zeigt den Tag, Monat und die Uhrzeit an, zu der die letzte Bestandsaufnahme ausgeführt wurde. ● **Status**: Zeigt den Host-Status an. ● **Controller-ID**: Zeigt die Controller-ID an. ● **Anschluss-ID**: Zeigt die Anschluss-ID an. ● **Gehäuse-ID**: Zeigt die Gehäuse-ID an. ● **Geräte-ID**: Zeigt die Geräte-ID an. ● **Bus-Protokoll**: Zeigt das Bus-Protokoll an. ● **Geschätzte verbleibende Schreibdauer**: Zeigt die verbleibende SSD-Schreibdauer an. ● **Hotspare -Typ**(gilt nicht für PCIe) – Zeigt den Hotspare-Typ an. Zu den Optionen zählen: ○ Nein – Bedeutet, dass kein Hotspare vorhanden ist. ○ Global – Ein globales Hotspare ist eine nicht verwendete Backup-Festplatte, die ein Teil der Festplattengruppe ist ○ Dediziert – Eine nicht verwendete Backup-Festplatte, die einem einzelnen virtuellen Laufwerk zugewiesen ist. Wenn eine physische Festplatte in der virtuellen Festplatte ausfällt, wird der Hotspare aktiviert, um die fehlerhafte physische Festplatte ohne Unterbrechung des Systems oder erforderlichen Benutzereingriff zu ersetzen. ● **Teilenummer**: Zeigt die Speicherteilenummer an. ● **Seriennummer**: Zeigt die Speicherseriennummer an. ● **Herstellername**: Zeigt den Namen des Speicheranbieters an.
Virtuelle Festplatte	● **Host**: Zeigt den Namen des Hosts an. ● **Service-Tag**: Zeigt den Service-Tag des Hosts an. ● **Name**: Zeigt den Namen des virtuellen Laufwerks an. ● **Physisches Laufwerk**: Zeigt an, auf welcher physischen Festplatte sich das virtuelle Laufwerk befindet. ● **Kapazität**: Zeigt die Kapazität des virtuellen Laufwerks an. ● **Layout**: Zeigt den Layout-Typ des virtuellen Speichers an. Das bedeutet, dass dieser RAID-Typ für dieses virtuelle Laufwerk konfiguriert wurde. ● **Letzte Bestandsaufnahme**: Zeigt den Tag, das Datum und die Uhrzeit an, zu dem die Bestandsaufnahme zuletzt durchgeführt wurde. ● **Controller-ID**: Zeigt die Controller-ID an. ● **Geräte-ID**: Zeigt die Geräte-ID an. ● **Medientyp**: Zeigt entweder SSD oder HDD an.

Tabelle 18. Speicherdetails für ein Rechenzentrum und Cluster (fortgesetzt)

Speicher: Festplatten	Beschreibung
	• **Bus-Protokoll**: Zeigt die Technologie an, die physischen Festplatten im virtuellen Laufwerk verwenden. Die möglichen Wert sind: ○ SCSI ○ SAS ○ SATA ○ PCIe • **Stripe-Größe**: Bezieht sich auf die Menge an Speicherplatz, die jeder Stripe auf einer einzelnen Festplatte belegt. • Standard-Leserichtlinie: Zeigt die durch den Controller standardmäßig unterstützte Leserichtlinie an. Zu den Optionen zählen: ○ Vorauslesen ○ Kein Vorauslesen ○ Adaptives Vorauslesen ○ Lese-Cache aktiviert ○ Lese-Cache deaktiviert • **Standard-Schreibrichtlinie**: Zeigt die durch den Controller standardmäßig unterstützte Schreibrichtlinie an. Zu den Optionen zählen: ○ Rückschreiben ○ Rückschreiben erzwingen ○ Rückschreiben aktiviert ○ Durchschreiben ○ Schreib-Cache aktiviert und geschützt. ○ Schreib-Cache deaktiviert • **Festplatten-Cache-Richtlinie**: Zeigt die durch den Controller standardmäßig unterstützte Cache-Richtlinie an. Zu den Optionen zählen: ○ Aktiviert – Cache-E/A ○ Deaktiviert – Direct E/A

Firmware-Informationen für ein Rechenzentrum und Cluster anzeigen

Die folgenden Informationen über jede Firmware-Komponente werden angezeigt:

- **Host**: Zeigt den Namen des Hosts an.
- **Service-Tag**: Zeigt den Service-Tag des Hosts an.
- **Name**: Zeigt den Namen von sämtlicher Firmware auf diesem Host an.
- **Version**: Zeigt die Version von sämtlicher Firmware auf diesem Host an.

Stromversorgungs-Überwachungsinformationen für ein Rechenzentrum und Cluster anzeigen

- **Host**: Zeigt den Namen des Hosts an.
- **Service-Tag**: Zeigt den Service-Tag des Hosts an.
- **Aktuelles Profil**: Zeigt das Stromprofil zur Maximierung der Systemleistung und zum Stromsparen an.
- **Energieverbrauch**: Zeigt den Energieverbrauch des Hosts an.
- **Spitzenreservekapazität**: Zeigt die Spitzenstromreservekapazität an.
- **Strombudget**: Zeigt die Stromobergrenze für diesen Host an.
- **Warnungsschwellenwert**: Zeigt den konfigurierten Maximalwert für den Warnungsschwellenwert der Temperatursonden des Systems an.
- **Fehlerschwellenwert**: Zeigt den konfigurierten Maximalwert für den Fehlerschwellenwert der Temperatursonden des Systems an.
- **Sofortige Reservekapazität**: Zeigt die Kapazität des sofortigen Toleranzbereichs des Hosts an.
- **Startdatum des Energieverbrauchs**: Zeigt das Datum und die Uhrzeit an, an dem bzw. zu der der Host mit dem Energieverbrauch begonnen hat.
- **Enddatum des Energieverbrauchs**: Zeigt das Datum und die Uhrzeit an, an dem bzw. zu der der Host angehalten hat, um Strom zu verbrauchen.

- **Spitzenstrom des Systems**: Zeigt die Spitzenleistung des Hosts an.
- **Startdatum der Spitzenleistung des Systems**: Zeigt das Datum und die Uhrzeit an, an dem bzw. zu der die Spitzenleistung des Hosts begonnen hat.
- **Enddatum der Spitzenleistung des Systems**: Zeigt das Datum und die Uhrzeit an, an dem bzw. zu der die Spitzenleistung des Hosts beendet wurde.
- **Spitzen-Ampere-Wert des Systems**: Zeigt den Spitzen-Ampere-Wert des Hosts an.
- **Startdatum des Spitzen-Ampere-Werts des Systems**: Zeigt das Startdatum und die Uhrzeit des Spitzen-Ampere-Werts des Hosts an.
- **Enddatum des Spitzen-Amper-Werts des Systems**: Zeigt das Datum und die Uhrzeit des Spitzen-Ampere-Werts des Hosts an.

Service-Informationen für ein Rechenzentrum und Cluster anzeigen

Um einen Servicestatus anzuzeigen, müssen Sie einen Service-Job ausführen. Informationen dazu finden Sie unter Serviceabfrage-Jobs planen auf Seite 109. Die Seite **Servicezusammenfassung** ermöglicht die Überwachung des Serviceablaufdatums. Die Serviceeinstellungen legen fest, wann Serverserviceinformationen von Dell online abgerufen werden. Dazu aktivieren oder deaktivieren Sie den Serviceplan und legen einen Schwellenwert für den Alarm „Minimum (Tage)“ fest.

- **Servicezusammenfassung**: Die Host-Servicezusammenfassung wird mithilfe von Symbolen angezeigt, um die Anzahl der Hosts in jeder Statuskategorie visuell anzuzeigen.
- **Host**: Zeigt den Hostnamen an.
- **Service-Tag**: Zeigt den Service-Tag des Hosts an.
- **Beschreibung** – Zeigt eine Beschreibung an
- **Servicestatus**: Zeigt den Servicestatus des Hosts an. Die Statusoptionen beinhalten:
  - Aktiv – Der Host ist unter Service und hat keinen Schwellenwert überschritten.
  - Warnung – Der Host ist aktiv, hat jedoch den Warnungsschwellenwert überschritten.
  - Kritisch – Entspricht einer Warnung, jedoch für einen kritischen Schwellenwert.
  - Abgelaufen – Der Service für diesen Host ist abgelaufen.
  - Unbekannt – OpenManage Integration for VMware vCenter kann den Servicestatus nicht abrufen, weil der Service-Job nicht ausgeführt wurde, ein Fehler beim Abrufen der Daten aufgetreten ist oder weil das System keinen Service hat.
- **Verbleibende Tage**: Zeigt die verbleibende Servicezeit in Tagen an.

Firmware-Aktualisierung

Das OMIVV-Gerät ermöglicht Ihnen die Ausführung des BIOS und der Firmwareaktualisierungs-Jobs auf den verwalteten Hosts. Sie können Firmwareaktualisierungs-Jobs auf mehreren Clustern oder nicht gruppierten Hosts gleichzeitig ausführen. Die gleichzeitige Ausführung der Firmware-Aktualisierung auf zwei Hosts desselben Clusters ist nicht zulässig.

ANMERKUNG: Um eine Firmwareaktualisierung auf einem Cluster oder Host durchzuführen, müssen Sie in einer Umgebung mit mehreren Geräten sicherstellen, dass das mit dem Ziel-vCenter registrierte Gerät geladen wird.

Im Folgenden werden die zwei Methoden beschrieben, mit denen Sie Firmwareaktualisierungen ausführen können:

- Einzelnes DUP: führt eine Firmwareaktualisierung für iDRAC und BIOS durch, indem direkt auf den DUP-Speicherort gezeigt wird (entweder CIFS oder NFS). Die Methode des einzelnen DUP kann nur auf Hostebene ausgeführt werden.
- Repository-Profil: Führt Firmware- und Treiberaktualisierungen durch. Diese Methode kann sowohl auf Host-Ebene als auch auf Cluster-Ebene genutzt werden.

  Die folgenden Repository-Profile werden für Firmware- und Treiberaktualisierungen verwendet:

  - Firmware-Repository: Ein Repository-Profil, das den Firmware-Katalog verwendet, um die Firmware-Informationen abzurufen.

    Es gibt folgende zwei Typen von Firmware-Repositorys:

    - Vom Benutzer erstelltes Firmware-Repository
    - Werkseitig erstelltes Firmware-Repository: Die folgenden zwei Typen von Katalogen werden werkseitig erstellt: Werksseitige Kataloge gelten nicht für vSAN-Cluster-Firmware-Aktualisierung und Baselining.
      - Dell Standardkatalog: Ein werkseitig erstelltes Firmware-Repository-Profil, das den Dell EMC Onlinekatalog verwendet, um die neuesten Firmware-Informationen zu beziehen. Wenn das Gerät keine Internetverbindung hat, ändern Sie dieses Repository, um auf eine lokale CIFS- oder NFS- bzw. HTTP- oder HTTPs-basierte Freigabe zu verweisen.

- Validierter Katalog für MX-Stapel: Ein werkseitig erstelltes Firmware-Repository-Profil, das den Dell EMC Onlinekatalog verwendet, um die validierten Firmware-Informationen für MX-Gehäuse und die zugehörigen Schlitten abzurufen.

- Treiber-Repository: Ein Repository-Profil enthält Offline-Pakete, die verwendet werden können, um den Treiber für vSAN-Cluster zu aktualisieren.

Der Assistent zur Aktualisierung der Firmware prüft stets die mindestens erforderlichen Firmware-Versionen für iDRAC und BIOS und versucht, diese auf die mindestens erforderlichen Versionen zu aktualisieren. In der *OpenManage Integration for VMware vCenter Compatibility Matrix* (OpenManage Integration for VMware v Center-Kompatibilitätsmatrix) finden Sie weitere Informationen zu den minimal erforderlichen Firmware-Versionen für iDRAC und BIOS. Wenn die iDRAC- und BIOS-Firmware-Versionen die Mindestanforderungen erfüllen, ermöglicht der Vorgang zur Aktualisierung der Firmware alle Firmware-Versionsaktualisierungen, einschließlich iDRAC, RAID Controller, NIC, BIOS usw.

ANMERKUNG: Zur Aktualisierung eines PowerEdge XR2-Servers verwendet OMIVV R440-Firmware-Komponenten, die im Dell Online-Katalog vorhanden sind. Wenn Sie einen benutzerdefinierten Katalog (mithilfe DRM) erstellen möchten, der für das Offline-Firmware-Repository zur Unterstützung von PowerEdge XR2 verwendet wird, verwenden Sie Firmware-Komponenten, die für PowerEdge R440-Server gelten.

Firmware und Treiber auf vSAN-Host aktualisieren

Bevor Sie die Firmwareaktualisierung auf vSAN-Hosts (Hosts in vSAN-fähigen Cluster) planen, müssen Sie sicherstellen, dass die folgenden Bedingungen in der Umgebung erfüllt sind:

- Vergewissern Sie sich, dass der Host konform ist (CSIOR aktiviert und der Host muss eine unterstützte ESXi-Version aufweisen), mit einem Host-Anmeldeinformationenprofil verknüpft ist und erfolgreich inventarisiert wurde.
- Die folgenden Voraussetzungen werden vor der Planung der Firmwareaktualisierung geprüft:
  - DRS ist aktiviert.
  - Der Host befindet sind nicht bereits im Wartungsmodus.
  - Die vSAN-Datenobjekte sind fehlerfrei.

  Um die obigen Überprüfungen zu überspringen, deaktivieren Sie das Kontrollkästchen **Voraussetzungen überprüfen** auf der Seite **Aktualisierung planen**.
- Für Speicher-Controller-, HDD- und SSD-Komponenten sind die ausgewählten Treiber und Firmware-Versionen in den ausgewählten Repositorys gemäß den VMware vSAN-Richtlinien basierend auf der vSAN-Version konform.
- Für Treiber unterstützt OMIVV nur die Offline-Pakete, die in der VMware-Hardware-Kompatibilitätsliste aufgeführt sind.
- Der Cluster erfüllt die vSAN-Anforderungen für die ausgewählte Datenmigrationsoption. Wenn das vSAN-Cluster nicht die Anforderungen für die ausgewählte Datenmigrationsoption erfüllt, wird die Aktualisierung wegen Zeitüberschreitung abgebrochen.
- Dell EMC empfiehlt, das Baseline-(Clusterprofil)-Firmware- oder Treiber-Repository auszuwählen.
- Stellen Sie sicher, dass keine aktiven Firmwareaktualisierungs-Jobs für Hosts unter dem Cluster vorhanden sind, den Sie aktualisieren.
- Stellen Sie sicher, dass Sie den erforderlichen Timeout-Wert für den Job "Wartungsmodus aktivieren" angeben. Wenn die Wartezeit die angegebene Zeit überschreitet, schlägt der Aktualisierungsjob fehl. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.
- Führen Sie die Bestandsaufnahme nach dem Aktivieren von vSAN erneut aus.

Dell EMC empfiehlt, während des Vorgangs zur Firmwareaktualisierung Folgendes nicht zu löschen oder verschieben:

- Den Host aus vCenter, für den der Job zur Aktualisierung der Firmware gerade ausgeführt wird.
- Das Host-Anmeldeinformationenprofil, für das die Aktualisierung der Firmware gerade ausgeführt wird.
- Die Repositorys in CIFS oder NFS.

OMMIV überprüft die Konformität des Hosts und ob andere Firmwareaktualisierungs-Jobs auf einem Host im gleichen Cluster durchgeführt werden. Nach der Überprüfung wird der Firmwareaktualisierungsassistent angezeigt.

1. Um den Assistenten zum Aktualisieren der Firmware zu starten, klicken Sie auf der OMIVV-Startseite auf **Menü**, wählen Sie **Hosts und Cluster** aus und führen Sie dann eine der folgenden Aktionen aus:
   - Klicken Sie mit der rechten Maustaste, wählen Sie anschließend **OMIVV Host-Aktionen** > **Firmwareaktualisierung** aus.
   - Wählen Sie einen Host aus, und wählen Sie im rechten Fensterbereich **Überwachen** > **OMIVV-Hostinformationen** > **Firmware** > **Firmware-Assistent ausführen** aus.
   - Wählen Sie einen Host aus, wählen Sie im rechten Fensterbereich **Zusammenfassung** aus und gehen Sie dann zu **OMIVV Hostinformationen** > **Host-Aktionen** > **Firmware-Assistenten ausführen**.
2. Überprüfen Sie auf der Seite **Firmwareaktualisierungs-Checkliste** vor dem Planen der Aktualisierung, ob alle Voraussetzungen überprüft wurden, und klicken Sie dann auf **ERSTE SCHRITTE**.

3. Wählen Sie auf der Seite **Aktualisierungsquelle** eine der folgenden Optionen aus:
   - **Repository-Profil**
   - **Einzelnes DUP**
4. Wählen Sie zum Laden einer einzelnen Firmwareaktualisierung aus einer Datei die Option **Einzelnes DUP**.
   a. Ein einzelnes DUP kann in einer CIFS- oder NFS-Freigabe verfügbar sein, auf die das OMIVV-Gerät zugreifen kann: Geben Sie den Dateispeicherort in einem der folgenden Formate ein und fahren Sie mit Schritt 9 fort.
      - NFS – `<host>:/<share_path/FileName.exe`
      - CIFS – `\\<host accessible share path>\<FileName>.exe`

      ANMERKUNG: Stellen Sie sicher, dass der Dateiname der Einzelkomponenten-DUPs keine Leerzeichen enthält.

      Bei der CIFS-Freigabe werden Sie vom OMIVV dazu aufgefordert, einen Benutzernamen und ein Kennwort einzugeben, das auf das Freigabelaufwerk zugreifen kann.
5. Wenn Sie die Option **Repository-Profil** auswählen, wählen Sie die Firmware- und Treiber-Repository-Profile aus.

   Wenn das Clusterprofil mit dem Cluster verbunden ist, in dem der Host vorhanden ist, werden standardmäßig die zugehörigen Firmware- und Treiber-Repository-Profile ausgewählt.

   Wenn Sie die Firmware- oder Treiber-Repository-Profile ändern, wird eine Meldung angezeigt, die darauf hinweist, dass das ausgewählte Repository-Profil nicht der Baseline zugeordnet ist und die Verwendung eines anderen Repository den Baseline-Vergleich beeinträchtigen kann.

   ANMERKUNG: Wenn Sie die Treiber- und Firmware-Repositorys mit dem Clusterprofil verknüpft haben, wird empfohlen, den Treiber und die Firmware gleichzeitig zu aktualisieren.

   Wenn Sie die Firmware oder den Treiber nicht aktualisieren möchten bzw. Firmware oder Treiber aktuell sind, wählen Sie aus dem Drop-Down-Menü **Kein Repository ausgewählt** aus.

   Die Standard-Firmware-Kataloge (Dell EMC Standardkatalog und validierter MX-Stack-Katalog) werden nicht im Option Repository-Profil angezeigt. Um die Repository-Profile zu verwenden, erstellen Sie ein benutzerdefiniertes Repository in OMIVV.

   Führen Sie die folgenden Schritte aus, um ein benutzerdefiniertes Repository-Profil zu erstellen:

   a. Navigieren Sie zu Dell EMC Repository Manager (DRM) und erstellen Sie einen Katalog.

      Weitere Informationen zum Erstellen eines Katalogs mit DRM finden Sie unter Erstellen eines Katalogs in Dell EMC Repository Manager (DRM) unter Verwendung von OMIVV auf Seite 136.
   b. Laden Sie den Katalog und die entsprechenden Dateien herunter.
   c. Erstellen Sie ein Repository-Profil in OMIVV unter Verwendung des heruntergeladenen Katalogs.

      Weitere Informationen zum Erstellen eines Repository-Profils finden Sie in Repository-Profil erstellen auf Seite 48.
6. Wählen Sie basierend auf dem von Ihnen ausgewählten Firmware-Repository-Profil ein entsprechendes Paket aus und klicken Sie dann auf **Weiter**. Nur 64-Bit-Pakete werden unterstützt.
7. Wählen Sie auf der Seite **Treiberkomponentenauswahl** die Treiberkomponenten aus, die Sie aktualisieren möchten, und dann klicken Sie auf **WEITER**. Wenn Sie eine Treiberkomponente für die Aktualisierung auswählen, werden alle Komponenten im Paket ausgewählt.

   Sie können die Filteroption verwenden, um die Daten basierend auf den spezifischen Spaltennamen zu filtern.
8. Wählen Sie auf der Seite **Firmwarekomponentenauswahl** die Firmwarekomponenten aus, die Sie aktualisieren möchten, und dann klicken Sie auf **WEITER**.

   Die Anzahl der Komponenten, die auf dem Dringlichkeitsstatus „Empfohlen“, „Optional“ und „Downgrades“ basieren, wird angezeigt.

   Die Komponenten, die eine niedrigere Version als die verfügbare Version im Katalog haben, oder sich auf derselben Ebene befinden (aktuell sind) oder für eine Aktualisierung geplant ist, können nicht ausgewählt werden. Um die Komponenten auszuwählen, die eine niedrigere Version als die verfügbare Version haben, markieren Sie das Kontrollkästchen **Firmware-Downgrade zulassen**.

   Um alle Firmware-Komponenten auf allen Seiten auszuwählen, klicken Sie auf  .

   Um alle Firmware-Komponenten auf allen Seiten zu löschen, klicken Sie auf  .
9. Geben Sie auf der Seite **Aktualisierungen planen** den Namen und die Beschreibung des Firmwareaktualisierungs-Jobs ein. Die Beschreibung ist ein optionales Feld.

   Der Name des Firmwareaktualisierungs-Jobs ist obligatorisch. Wenn Sie den Namen des Firmwareaktualisierungs-Jobs entfernen, können Sie ihn wiederverwenden.
10. Führen Sie im Bereich **Zusätzliche Einstellungen** die folgenden Schritte aus:
    a. Geben Sie den Zeitüberschreitungswert für den Wartungsmodus zwischen 60 und 1440 Minuten an. Wenn die Wartezeit den angegebenen Wert überschreitet, schlagen die Aktualisierungsjobs fehl und die Wartungsaufgabe wird abgebrochen oder weist

eine Zeitüberschreitung auf. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.

b. Wählen Sie aus dem Drop-Down-Menü **Wartungsmodus-Option aufrufen** eine geeignete Datenmigrationsoption aus. Weitere Informationen zur Datenmigrationsoption finden Sie in der VMware-Dokumentation.

ANMERKUNG: Die Aufgabe „Wartungsmodus aufrufen“ schlägt fehl, wenn die Clusterkonfiguration keine vollständige Datenmigration unterstützt oder die Speicherkapazität nicht ausreicht.

Standardmäßig sind die folgenden Optionen ausgewählt:

- **Wartungsmodus nach Abschluss der Firmwareaktualisierung beenden** – Wenn Sie diese Option deaktivieren, bleibt der Host im Wartungsmodus.
- **Ausgeschaltete und angehaltene virtuelle Maschinen auf andere Hosts im Cluster versschieben** – Durch Deaktivieren dieser Option wird die Verbindung zur VM getrennt, bis das Host-Gerät online ist.

c. Wenn Sie Probleme beim Aktualisieren der Firmware haben, aktivieren Sie das Kontrollkästchen **Job-Warteschlange löschen und iDRAC zurücksetzen**. Dadurch kann der Aktualisierungsvorgang erfolgreich beendet werden. Dies erhöht die gesamte Aktualisierungszeit, die für die Fertigstellung des Jobs benötigt wird, storniert alle ausstehenden Jobs oder Aktivitäten, die auf dem iDRAC geplant sind, und setzt den iDRAC zurück.

Für Hosts, die über das Gehäuse-Anmeldeinformationenprofil verwaltet werden, wird das Löschen der Job-Warteschlange nicht unterstützt.

Standardmäßig ist die Option **Voraussetzungen prüfen** ausgewählt.

11. Wählen Sie im Abschnitt **Aktualisierungszeitplan** eine der folgenden Optionen aus:
    - **Jetzt aktualisieren**
    - **Aktualisierung planen**
    - **Aktualisierungen beim nächsten Neustart anwenden**
12. Überprüfen Sie die Informationen zur Firmwareaktualisierung auf der Seite **Zusammenfassung überprüfen** und klicken Sie auf **FERTIGSTELLEN**.
    Die Firmwareaktualisierungs-Jobs können bis zu mehreren Stunden dauern, je nach den Komponenten und der Anzahl der ausgewählten Server. Sie können den Status der Jobs auf der Seite **Jobs** anzeigen.

    Wenn eine Firmwareaktualisierungsaufgabe abgeschlossen ist, läuft die Bestandsaufnahmeprüfung automatisch auf den ausgewählten Hosts. Die Hosts beenden automatisch den Wartungsmodus basierend auf einer Option, die auf der Seite **Aktualisierungen planen** ausgewählt wurde.

Erstellen eines Katalogs in Dell EMC Repository Manager (DRM) unter Verwendung von OMIVV

Dieser Abschnitt beschreibt das Verfahren zum Erstellen eines Katalogs in DRM Version 3.0 und höher.

1. Navigieren Sie zu DRM herunterladen und laden Sie DRM herunter.
2. Klicken Sie auf der DRM-Startseite auf **Neues Repository hinzufügen**.
   Das Fenster **Repository hinzufügen** wird aufgerufen.
3. Führen Sie im Fenster **Repository hinzufügen** die folgenden Schritte aus:
   a. Geben Sie den **Repository-Namen** und eine **Beschreibung** an.
   b. Wählen Sie im Drop-Down-Menü **Basiskatalog** einen Katalog aus.
   c. Wählen Sie im Drop-Down-Menü **Integration-Typ OpenManage Integration for VMware vCenter** aus.
4. Geben Sie im Fenster **OpenManage Integration for VMware vCenter** die **Virtuelle Appliance-IP**, die **vCenter Server-IP**, den **Benutzernamen** und das **Passwort** ein und klicken Sie auf **Verbinden**.
   Der erstellte Katalog wird auf der Startseite angezeigt.
5. Um den Katalog zu exportieren, wählen Sie einen Katalog aus und klicken Sie auf **Exportieren**.

Firmware und Treiber auf vSAN-Cluster aktualisieren

Bevor Sie die Firmwareaktualisierung planen, stellen Sie sicher, dass die folgenden Bedingungen in der Umgebung erfüllt sind:

- Vergewissern Sie sich, dass der Host konform ist (CSIOR aktiviert und der Host muss eine unterstützte ESXi-Version aufweisen), mit einem Host-Anmeldeinformationenprofil verknüpft ist und erfolgreich inventarisiert wurde. Wenn der Host nicht aufgelistet ist, führen

Sie den Verwaltungs-Compliance-Assistenten für Hosts von OMIVV aus, und verwenden Sie dann den Assistenten zur Firmwareaktualisierung.

- Die folgenden Voraussetzungen werden vor der Planung der Firmwareaktualisierung geprüft:
  - DRS ist aktiviert.
  - Der Host befindet sind nicht bereits im Wartungsmodus.
  - Die vSAN-Datenobjekte sind fehlerfrei.
- Stellen Sie für Speicher-Controller-, HDD- und SSD-Komponenten sicher, dass die ausgewählten Treiber und Firmware-Versionen in den ausgewählten Repositorys gemäß den VMware vSAN-Richtlinien basierend auf der vSAN-Version konform sind.
- Für Treiber unterstützt OMIVV nur die Offline-Pakete, die in der VMware-Hardware-Kompatibilitätsliste aufgeführt sind.
- Der Cluster erfüllt die vSAN-Anforderungen für die ausgewählte Datenmigrationsoption. Wenn das vSAN-Cluster nicht die Anforderungen für die ausgewählte Datenmigrationsoption erfüllt, wird die Aktualisierung wegen Zeitüberschreitung abgebrochen.
- Es wird dringend empfohlen, das Baseline-(Clusterprofil)-Firmware- oder Treiber-Repository auszuwählen.
- Stellen Sie sicher, dass keine aktiven Firmwareaktualisierungs-Jobs für Hosts unter dem Cluster vorhanden sind, den Sie aktualisieren.
- Stellen Sie sicher, dass Sie den erforderlichen Timeout-Wert für den Job "Wartungsmodus aktivieren" angeben. Wenn die Wartezeit die angegebene Zeit überschreitet, schlägt der Aktualisierungsjob fehl. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.
- Stellen Sie sicher, dass Sie die Bestandsaufnahme nach dem Aktivieren von vSAN erneut ausführen.

Dell EMC empfiehlt, während des Vorgangs zur Firmwareaktualisierung Folgendes nicht zu löschen oder verschieben:

- Die Hosts eines Clusters von vCenter, für die der Firmwareaktualisierungs-Job ausgeführt wird.
- Das Host-Anmeldeinformationenprofil, für das die Aktualisierung der Firmware gerade ausgeführt wird.
- Die Repositorys in CIFS oder NFS.

ANMERKUNG: VMware empfiehlt, Cluster mit identischer Server-Hardware aufzubauen.

OMMIV überprüft die Konformität des Hosts und ob andere Firmwareaktualisierungs-Jobs auf einem Host im gleichen Cluster durchgeführt werden. Nach der Überprüfung wird der Firmwareaktualisierungsassistent angezeigt.

1. Um den Assistenten zum Aktualisieren der Firmware zu starten, klicken Sie auf der OMIVV-Startseite auf **Menü**, wählen Sie **Hosts und Cluster** aus und führen Sie dann eine der folgenden Aktionen aus:
   - Klicken Sie mit der rechten Maustaste auf einen Cluster, wählen Sie anschließend **OMIVV Cluster-Aktionen** > **Firmwareaktualisierung** aus.
   - Wählen Sie ein Cluster aus und wählen Sie im rechten Fensterbereich **Überwachen** > **OMIVV-Clusterinformationen** > **Firmware** > **Firmware-Assistent ausführen** aus.
2. Überprüfen Sie auf der Seite **Firmwareaktualisierungs-Checkliste** vor dem Planen der Aktualisierung, ob alle Voraussetzungen überprüft wurden, und klicken Sie dann auf **ERSTE SCHRITTE**.
3. Wählen Sie auf der Seite **Aktualisierungsquelle** die Firmware- und Treiber-Repository-Profile aus.

   Wenn das Clusterprofil mit dem Cluster verbunden ist, in dem der Host vorhanden ist, werden standardmäßig die zugehörigen Firmware- und Treiber-Repository-Profile ausgewählt.

   Wenn Sie die Firmware- oder Treiber-Repository-Profile ändern, wird eine Meldung angezeigt, die darauf hinweist, dass das ausgewählte Repository-Profil nicht der Baseline zugeordnet ist und die Verwendung eines anderen Repository den Baseline-Vergleich beeinträchtigen kann.

   ANMERKUNG: Wenn Sie die Treiber- und Firmware-Repositorys mit dem Clusterprofil verknüpft haben, wird empfohlen, den Treiber und die Firmware gleichzeitig zu aktualisieren.

   Wenn Sie die Firmware oder den Treiber nicht aktualisieren möchten bzw. Firmware oder Treiber aktuell sind, wählen Sie aus dem Drop-Down-Menü **Kein Repository ausgewählt** aus.

   Die Standard-Firmware-Kataloge (Dell EMC Standardkatalog und validierter MX-Stack-Katalog) werden nicht im Option Repository-Profil angezeigt. Um die Repository-Profile zu verwenden, erstellen Sie ein benutzerdefiniertes Repository in OMIVV.

   Führen Sie die folgenden Schritte aus, um ein benutzerdefiniertes Repository-Profil zu erstellen:

   a. Navigieren Sie zu Dell EMC Repository Manager (DRM) und erstellen Sie einen Katalog.

      Weitere Informationen zum Erstellen eines Katalogs mit DRM finden Sie unter Erstellen eines Katalogs in Dell EMC Repository Manager (DRM) unter Verwendung von OMIVV auf Seite 136.

   b. Laden Sie den Katalog und die entsprechenden Dateien herunter.

   c. Erstellen Sie ein Repository-Profil in OMIVV unter Verwendung des heruntergeladenen Katalogs.

      Weitere Informationen zum Erstellen eines Repository-Profils finden Sie in Repository-Profil erstellen auf Seite 48.
4. Wählen Sie basierend auf dem von Ihnen ausgewählten Firmware-Repository-Profil ein entsprechendes Paket aus und klicken Sie dann auf **Weiter**. Nur 64-Bit-Pakete werden unterstützt.

ANMERKUNG: Es kann nur ein Paket für OEM-Server anderer Marken ausgewählt werden, auch wenn es sich um verschiedene Modelle handelt. Selbst wenn das Paket für einen oder mehrere der OEM-Server nicht anwendbar ist, listet die Komponenten-Seite des Assistenten für die Firmwareaktualisierung alle OEM-Server- oder Firmware-Komponentenpaare auf. Wenn die Firmwareaktualisierung für ein bestimmtes Firmware-Komponentenpaar fehlschlägt, versuchen Sie es erneut mit dem alternativen Paket, das für den OEM-Server angezeigt wird.

5. Wählen Sie auf der Seite **Treiberkomponentenauswahl** die Treiberkomponenten aus, die Sie aktualisieren möchten, und dann klicken Sie auf **WEITER**. Wenn Sie eine Treiberkomponente für die Aktualisierung auswählen, werden alle Komponenten im Paket ausgewählt.

   Sie können die Filteroption verwenden, um die Daten basierend auf den spezifischen Spaltennamen zu filtern.

6. Wählen Sie auf der Seite **Firmwarekomponentenauswahl** die Firmwarekomponenten aus, die Sie aktualisieren möchten, und dann klicken Sie auf **WEITER**.

   Die Anzahl der Komponenten, die auf dem Dringlichkeitsstatus „Empfohlen“, „Optional“ und „Downgrades“ basieren, wird angezeigt.

   Sie können die Filteroption verwenden, um die Daten basierend auf den spezifischen Spaltennamen zu filtern.

   Die Komponenten, die eine niedrigere Version als die verfügbare Version im Katalog haben, oder sich auf derselben Ebene befinden (aktuell sind) oder für eine Aktualisierung geplant ist, können nicht ausgewählt werden. Um die Komponenten auszuwählen, die eine niedrigere Version als die verfügbare Version haben, markieren Sie das Kontrollkästchen **Firmware-Downgrade zulassen**.

   Um alle Firmware-Komponenten auf allen Seiten auszuwählen, klicken Sie auf  .

   Um alle Firmware-Komponenten auf allen Seiten zu löschen, klicken Sie auf  .

7. Geben Sie auf der Seite **Aktualisierungen planen** den Namen und die Beschreibung des Firmwareaktualisierungs-Jobs ein. Die Beschreibung ist ein optionales Feld.

   Der Name des Firmwareaktualisierungs-Jobs ist obligatorisch. Wenn Sie den Namen des Firmwareaktualisierungs-Jobs entfernen, können Sie ihn wiederverwenden.

8. Führen Sie im Bereich **Zusätzliche Einstellungen** die folgenden Schritte aus:

   a. Geben Sie den Zeitüberschreitungswert für den Wartungsmodus zwischen 60 und 1440 Minuten an. Wenn die Wartezeit den angegebenen Wert überschreitet, schlägt der Aktualisierungsjob fehl und die Wartungsaufgabe wird abgebrochen oder weist eine Zeitüberschreitung auf. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.

   b. Wählen Sie aus dem Drop-Down-Menü **Wartungsmodus-Option aufrufen** eine geeignete Datenmigrationsoption aus. Weitere Informationen zur Datenmigrationsoption finden Sie in der VMware-Dokumentation.

      ANMERKUNG: Die Aufgabe „Wartungsmodus aufrufen“ schlägt fehl, wenn die Clusterkonfiguration keine vollständige Datenmigration unterstützt oder die Speicherkapazität nicht ausreicht.

      Standardmäßig ist die Option **Ausgeschaltete und angehaltene Maschinen zu anderen Hosts im Cluster verschieben** ausgewählt. Wird diese Option deaktiviert, wird die virtuelle Maschine getrennt, bis das Host-Gerät online ist.

   c. Wenn Sie Probleme beim Aktualisieren der Firmware haben, aktivieren Sie das Kontrollkästchen **Job-Warteschlange löschen und iDRAC zurücksetzen**. Dadurch kann der Aktualisierungsvorgang erfolgreich beendet werden. Dies erhöht die gesamte Aktualisierungszeit, die für die Fertigstellung des Jobs benötigt wird, storniert alle ausstehenden Jobs oder Aktivitäten, die auf dem iDRAC geplant sind, und setzt den iDRAC zurück.

      Für Hosts, die über das Gehäuse-Anmeldeinformationenprofil verwaltet werden, wird das Löschen der Job-Warteschlange nicht unterstützt.

9. Wählen Sie im Abschnitt **Aktualisierungszeitplan** eine der folgenden Optionen aus:

   - **Jetzt aktualisieren**
   - **Aktualisierung planen**

10. Überprüfen Sie die Informationen zur Firmwareaktualisierung auf der Seite **Zusammenfassung überprüfen** und klicken Sie auf **FERTIGSTELLEN**.
    Die Firmwareaktualisierungs-Jobs können bis zu mehreren Stunden dauern, je nach den Komponenten und der Anzahl der ausgewählten Server. Sie können den Status der Jobs auf der Seite **Jobs** anzeigen.

    Wenn eine Firmwareaktualisierungsaufgabe abgeschlossen ist, läuft die Bestandsaufnahmeprüfung automatisch auf den ausgewählten Hosts. Die Hosts beenden automatisch den Wartungsmodus basierend auf einer Option, die auf der Seite **Aktualisierungen planen** ausgewählt wurde.

Firmware auf vSphere-Host aktualisieren

Bevor Sie die Firmwareaktualisierung auf vSphere-Hosts planen (nur ESXi), stellen Sie sicher, dass die folgenden Bedingungen in der Umgebung erfüllt sind:

- Vergewissern Sie sich, dass der Host konform ist (CSIOR aktiviert und der Host muss eine unterstützte ESXi-Version aufweisen), mit einem Host-Anmeldeinformationenprofil verknüpft ist und erfolgreich inventarisiert wurde.
- DRS ist aktiviert.

  ANMERKUNG: Für einen Standalone-Host ist die DRS-Prüfung nicht anwendbar.

  Um die obige Voraussetzungsprüfung zu überspringen, deaktivieren Sie das Kontrollkästchen **Voraussetzungen überprüfen** auf der Seite **Firmwareaktualisierung planen**.

  ANMERKUNG: Treiberaktualisierungen werden auf vSphere Cluster und Host nicht unterstützt.

Dell EMC empfiehlt, während des Vorgangs zur Firmwareaktualisierung Folgendes nicht zu löschen oder verschieben:

- Den Host aus vCenter, für den der Job zur Aktualisierung der Firmware gerade ausgeführt wird.
- Das Host-Anmeldeinformationenprofil, für das die Aktualisierung der Firmware gerade ausgeführt wird.
- Die Repositorys in CIFS oder NFS.

OMMIV überprüft die Konformität des Hosts und ob andere Firmwareaktualisierungs-Jobs auf einem Host im gleichen Cluster durchgeführt werden. Nach der Überprüfung wird der Firmwareaktualisierungsassistent angezeigt.

1. Um den Assistenten zum Aktualisieren der Firmware zu starten, klicken Sie auf der OMIVV-Startseite auf **Menü**, wählen Sie **Hosts und Cluster** aus und führen Sie dann eine der folgenden Aktionen aus:
   - Klicken Sie mit der rechten Maustaste, wählen Sie anschließend **OMIVV Host-Aktionen** > **Firmwareaktualisierung** aus.
   - Wählen Sie einen Host aus, und wählen Sie im rechten Fensterbereich **Überwachen** > **OMIVV-Hostinformationen** > **Firmware** > **Firmware-Assistent ausführen** aus.
   - Wählen Sie einen Host aus, wählen Sie im rechten Fensterbereich **Zusammenfassung** aus und gehen Sie dann zu **OMIVV Hostinformationen** > **Host-Aktionen** > **Firmware-Assistenten ausführen**.
2. Überprüfen Sie auf der Seite **Firmwareaktualisierungs-Checkliste** vor dem Planen der Aktualisierung, ob alle Voraussetzungen überprüft wurden, und klicken Sie dann auf **ERSTE SCHRITTE**.
3. Wählen Sie auf der Seite **Aktualisierungsquelle** eine der folgenden Optionen aus:
   - **Repository-Profil**
   - **Einzelnes DUP**
4. Wählen Sie zum Laden einer einzelnen Firmwareaktualisierung aus einer Datei die Option **Einzelnes DUP**.
   a. Ein einzelnes DUP kann in einer CIFS- oder NFS-Freigabe verfügbar sein, auf die das OMIVV-Gerät zugreifen kann. Geben Sie den Dateispeicherort in einem der nachfolgenden Formate ein und dann fahren Sie mit Schritt 8 fort.
      - NFS – `<host>:/<share_path/FileName.exe`
      - CIFS – `\\<host accessible share path>\<FileName>.exe`

      ANMERKUNG: Stellen Sie sicher, dass der Dateiname der Einzelkomponenten-DUPs keine Leerzeichen enthält.

      Bei der CIFS-Freigabe werden Sie vom OMIVV dazu aufgefordert, einen Benutzernamen und ein Kennwort einzugeben, das auf das Freigabelaufwerk zugreifen kann.
5. Wenn Sie die Option **Repository-Profil** auswählen, wählen Sie das Firmware-Repository-Profil aus.

   Wenn das Clusterprofil mit dem Cluster verbunden ist, in dem der Host vorhanden ist, wird standardmäßig das zugehörige Firmware-Repository ausgewählt. Andernfalls ist **Dell Standardkatalog** ausgewählt.

   Wenn Sie das Firmware-Repository-Profil ändern, wird eine Meldung angezeigt, die darauf hinweist, dass das ausgewählte Repository-Profil nicht der Baseline zugeordnet ist und die Verwendung eines anderen Repository den Baseline-Vergleich beeinträchtigen kann.
6. Wählen Sie basierend auf dem von Ihnen ausgewählten Firmware-Repository-Profil ein entsprechendes Paket aus und klicken Sie dann auf **Weiter**. Nur 64-Bit-Pakete werden unterstützt.
7. Wählen Sie auf der Seite **Firmwarekomponentenauswahl** die Firmwarekomponenten aus, die Sie aktualisieren möchten, und dann klicken Sie auf **WEITER**.

   Die Anzahl der Komponenten, die auf dem Dringlichkeitsstatus „Empfohlen“, „Optional“ und „Downgrades“ basieren, wird angezeigt.

   Sie können die Filteroption verwenden, um die Daten basierend auf den spezifischen Spaltennamen zu filtern.

Die Komponenten, die eine niedrigere Version als die verfügbare Version im Katalog haben, oder sich auf derselben Ebene befinden (aktuell sind) oder für eine Aktualisierung geplant ist, können nicht ausgewählt werden. Um die Komponenten auszuwählen, die eine niedrigere Version als die verfügbare Version haben, markieren Sie das Kontrollkästchen **Firmware-Downgrade zulassen**.

Um alle Firmware-Komponenten auf allen Seiten auszuwählen, klicken Sie auf  .

Um alle Firmware-Komponenten auf allen Seiten zu löschen, klicken Sie auf  .

8. Geben Sie auf der Seite **Aktualisierungen planen** den Namen und die Beschreibung des Firmwareaktualisierungs-Jobs ein. Die Beschreibung ist ein optionales Feld.

   Der Name des Firmwareaktualisierungs-Jobs ist obligatorisch. Wenn Sie den Namen des Firmwareaktualisierungs-Jobs entfernen, können Sie ihn wiederverwenden.

9. Führen Sie im Bereich **Zusätzliche Einstellungen** die folgenden Schritte aus:

   a. Geben Sie den Zeitüberschreitungswert für den Wartungsmodus zwischen 60 und 1440 Minuten an. Wenn die Wartezeit den angegebenen Wert überschreitet, schlägt der Aktualisierungsjob fehl und die Wartungsaufgabe wird abgebrochen oder weist eine Zeitüberschreitung auf. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.

      Standardmäßig sind die folgenden Optionen ausgewählt:

      - **Wartungsmodus nach Abschluss der Firmwareaktualisierung beenden** – Wenn Sie diese Option deaktivieren, bleibt der Host im Wartungsmodus.
      - **Ausgeschaltete und angehaltene virtuelle Maschinen auf andere Hosts im Cluster versschieben** – Durch Deaktivieren dieser Option wird die Verbindung zur VM getrennt, bis das Host-Gerät online ist.

   b. Wenn Sie Probleme beim Aktualisieren der Firmware haben, aktivieren Sie das Kontrollkästchen **Job-Warteschlange löschen und iDRAC zurücksetzen**. Dadurch kann der Aktualisierungsvorgang erfolgreich beendet werden. Dies erhöht die gesamte Aktualisierungszeit, die für die Fertigstellung des Jobs benötigt wird, storniert alle ausstehenden Jobs oder Aktivitäten, die auf dem iDRAC geplant sind, und setzt den iDRAC zurück.

      Für Hosts, die über das Gehäuse-Anmeldeinformationenprofil verwaltet werden, wird das Löschen der Job-Warteschlange nicht unterstützt.

      Standardmäßig ist die Option **Voraussetzungen prüfen** ausgewählt.

10. Wählen Sie im Abschnitt **Aktualisierungszeitplan** eine der folgenden Optionen aus:

    - **Jetzt aktualisieren**
    - **Aktualisierung planen**
    - **Aktualisierungen beim nächsten Neustart anwenden**
    - **Aktualisierungen durchführen und einen Neustart erzwingen, ohne in den Wartungsmodus einzutreten**

11. Überprüfen Sie die Informationen zur Firmwareaktualisierung auf der Seite **Zusammenfassung überprüfen** und klicken Sie auf **FERTIGSTELLEN**.
    Die Firmwareaktualisierungs-Jobs können bis zu mehreren Stunden dauern, je nach den Komponenten und der Anzahl der ausgewählten Server. Sie können den Status der Jobs auf der Seite **Jobs** anzeigen.

    Wenn eine Firmwareaktualisierungsaufgabe abgeschlossen ist, läuft die Bestandsaufnahmeprüfung automatisch auf den ausgewählten Hosts. Die Hosts beenden automatisch den Wartungsmodus basierend auf einer Option, die auf der Seite **Aktualisierungen planen** ausgewählt wurde.

Firmware auf vSphere-Cluster aktualisieren

Bevor Sie die Firmwareaktualisierung planen, stellen Sie sicher, dass die folgenden Bedingungen in der Umgebung erfüllt sind:

- Vergewissern Sie sich, dass der Host konform ist (CSIOR aktiviert und der Host muss eine unterstützte ESXi-Version aufweisen), mit einem Host-Anmeldeinformationenprofil verknüpft ist und erfolgreich inventarisiert wurde. Wenn der Host nicht aufgelistet ist, führen Sie den Verwaltungs-Compliance-Assistenten für Hosts von OMIVV aus, und verwenden Sie dann den Assistenten zur Firmwareaktualisierung.
- DRS ist aktiviert.
- Stellen Sie sicher, dass keine aktiven Firmwareaktualisierungs-Jobs für Hosts unter dem Cluster vorhanden sind, den Sie aktualisieren.
- Stellen Sie sicher, dass Sie den erforderlichen Timeout-Wert für den Job "Wartungsmodus aktivieren" angeben. Wenn die Wartezeit die angegebene Zeit überschreitet, schlägt der Aktualisierungsjob fehl. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.

ANMERKUNG: Treiberaktualisierungen werden auf vSphere Cluster und Host nicht unterstützt.

Dell EMC empfiehlt, während des Vorgangs zur Firmwareaktualisierung Folgendes nicht zu löschen oder verschieben:

- Die Hosts eines Clusters von vCenter, für die der Firmwareaktualisierungs-Job ausgeführt wird.
- Das Host-Anmeldeinformationenprofil, für das die Aktualisierung der Firmware gerade ausgeführt wird.
- Die Repositorys in CIFS oder NFS

ANMERKUNG: VMware empfiehlt, Cluster mit identischer Server-Hardware aufzubauen.

OMMIV überprüft die Konformität des Hosts und ob andere Firmwareaktualisierungs-Jobs auf einem Host im gleichen Cluster durchgeführt werden. Nach der Überprüfung wird der Firmwareaktualisierungsassistent angezeigt.

1. Um den Assistenten zum Aktualisieren der Firmware zu starten, klicken Sie auf der OMIVV-Startseite auf **Menü**, wählen Sie **Hosts undClusters** aus und führen Sie dann eine der folgenden Aktionen aus:
   - Klicken Sie mit der rechten Maustaste auf einen Cluster, wählen Sie anschließend **OMIVV Cluster-Aktionen** > **Firmware-Aktualisierung**.
   - Wählen Sie ein Cluster aus und wählen Sie im rechten Fensterbereich **Überwachen** > **OMIVV Clusterinnformation** > **Firmware** > **Firmware-Assistent ausführen**.
2. Überprüfen Sie auf der Seite **Firmwareaktualisierungs-Checkliste** vor dem Planen der Aktualisierung, ob alle Voraussetzungen überprüft wurden, und klicken Sie dann auf **ERSTE SCHRITTE**.
3. Wenn auf der Seite **Quelle aktualisieren** das Clusterprofil mit dem Cluster verbunden ist, in dem der Host vorhanden ist, wird standardmäßig das zugehörige Firmware-Repository ausgewählt. Andernfalls ist **Dell Standardkatalog** ausgewählt.

   Wenn Sie das Firmware-Repository-Profil ändern, wird eine Meldung angezeigt, die darauf hinweist, dass das ausgewählte Repository-Profil nicht der Baseline zugeordnet ist und die Verwendung eines anderen Repository den Baseline-Vergleich beeinträchtigen kann.
4. Wählen Sie basierend auf dem von Ihnen ausgewählten Firmware-Repository-Profil ein entsprechendes Paket aus und klicken Sie dann auf **Weiter**. Nur 64-Bit-Pakete werden unterstützt.

   ANMERKUNG: Es kann nur ein Paket für OEM-Server anderer Marken ausgewählt werden, auch wenn es sich um verschiedene Modelle handelt. Selbst wenn das Paket für einen oder mehrere der OEM-Server nicht anwendbar ist, listet die Komponenten-Seite des Assistenten für die Firmwareaktualisierung alle OEM-Server- oder Firmware-Komponentenpaare auf. Wenn die Firmwareaktualisierung für ein bestimmtes Firmware-Komponentenpaar fehlschlägt, versuchen Sie es erneut mit dem alternativen Paket, das für den OEM-Server angezeigt wird.
5. Wählen Sie auf der Seite **Firmwarekomponentenauswahl** die Firmwarekomponenten aus, die Sie aktualisieren möchten, und dann klicken Sie auf **WEITER**.

   Die Anzahl der Komponenten, die auf dem Dringlichkeitsstatus „Empfohlen“, „Optional“ und „Downgrades“ basieren, wird angezeigt.

   Die Komponenten, die eine niedrigere Version als die verfügbare Version im Katalog haben, oder sich auf derselben Ebene befinden (aktuell sind) oder für eine Aktualisierung geplant ist, können nicht ausgewählt werden. Um die Komponenten auszuwählen, die eine niedrigere Version als die verfügbare Version haben, markieren Sie das Kontrollkästchen **Firmware-Downgrade zulassen**.

   Sie können die Filteroption verwenden, um die Daten basierend auf den spezifischen Spaltennamen zu filtern.

   Um alle Firmware-Komponenten auf allen Seiten auszuwählen, klicken Sie auf .

   Um alle Firmware-Komponenten auf allen Seiten zu löschen, klicken Sie auf .
6. Geben Sie auf der Seite **Aktualisierungen planen** den Namen und die Beschreibung des Firmwareaktualisierungs-Jobs ein. Die Beschreibung ist ein optionales Feld.

   Der Name des Firmwareaktualisierungs-Jobs ist obligatorisch. Wenn Sie den Namen des Firmwareaktualisierungs-Jobs entfernen, können Sie ihn wiederverwenden.
7. Führen Sie im Bereich **Zusätzliche Einstellungen** die folgenden Schritte aus:
   a. Geben Sie den Zeitüberschreitungswert für den Wartungsmodus zwischen 60 und 1440 Minuten an. Wenn die Wartezeit den angegebenen Wert überschreitet, schlägt der Aktualisierungsjob fehl und die Wartungsaufgabe wird abgebrochen oder weist eine Zeitüberschreitung auf. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.

      Standardmäßig ist die Option **Ausgeschaltete und angehaltene Maschinen zu anderen Hosts im Cluster verschieben** ausgewählt. Wird diese Option deaktiviert, wird die virtuelle Maschine getrennt, bis das Host-Gerät online ist.

   b. Wenn Sie Probleme beim Aktualisieren der Firmware haben, aktivieren Sie das Kontrollkästchen **Job-Warteschlange löschen und iDRAC zurücksetzen**. Dadurch kann der Aktualisierungsvorgang erfolgreich beendet werden. Dies erhöht die gesamte Aktualisierungszeit, die für die Fertigstellung des Jobs benötigt wird, storniert alle ausstehenden Jobs oder Aktivitäten, die auf dem iDRAC geplant sind, und setzt den iDRAC zurück.

      Für Hosts, die über das Gehäuse-Anmeldeinformationenprofil verwaltet werden, wird das Löschen der Job-Warteschlange nicht unterstützt.

8. Wählen Sie im Abschnitt **Aktualisierungszeitplan** eine der folgenden Optionen aus:
   - **Jetzt aktualisieren**
   - **Aktualisierung planen**
9. Überprüfen Sie die Informationen zur Firmwareaktualisierung auf der Seite **Zusammenfassung überprüfen** und klicken Sie auf **FERTIGSTELLEN**.
   Die Firmwareaktualisierungs-Jobs können bis zu mehreren Stunden dauern, je nach den Komponenten und der Anzahl der ausgewählten Server. Sie können den Status der Jobs auf der Seite **Jobs** anzeigen.

   Wenn eine Firmwareaktualisierungsaufgabe abgeschlossen ist, läuft die Bestandsaufnahmeprüfung automatisch auf den ausgewählten Hosts. Die Hosts beenden automatisch den Wartungsmodus basierend auf einer Option, die auf der Seite **Aktualisierungen planen** ausgewählt wurde.

Firmware-Komponenten des gleichen Typs aktualisieren

Im Folgenden sind die wichtigsten Punkte aufgelistet, die bei der Aktualisierung der Firmware-Komponenten des gleichen Typs zu beachten sind:

- Wenn mehrere Komponenten des gleichen Typs mit den gleichen Versionen auf dem Server vorhanden sind, wird nur eine Version der Komponente auf der Seite **Firmware-Komponenten auswählen** angezeigt. Die Aktualisierung wird auf alle Komponenten angewendet und die Abweichungsdetails werden nur für eine Version der Komponente angezeigt.

  Beispiel:

  Tabelle 19. Beispiel für mehrere Komponenten mit dem gleichen Typ, die im Server vorhanden sind

Komponente	Aktuelle Version	Verfügbare Version
HDD1	V1	V3
HDD2	V1	V3
HDD3	V1	V3

  In diesem Fall wird auf der Seite **Firmware-Komponenten auswählen** Folgendes angezeigt:

  Tabelle 20. Beispiel für mehrere Komponenten der gleichen Version, die im Server vorhanden sind

Komponente	Aktuelle Version	Verfügbare Version
HDD1	V1	V3

- Wenn mehrere Komponenten des gleichen Typs mit unterschiedlichen Versionen im Server vorhanden sind, wird für jede eindeutige Version eine einzelne Komponente angezeigt. Wenn Sie in diesem Fall eine Komponente auswählen, wird die Aktualisierung unabhängig von der aktuellen Firmware-Version auf alle Komponenten angewendet. Die Abweichungsdetails werden unabhängig von ihrer aktuellen Firmware-Version für alle Komponenten angezeigt.

  Beispiel:

  Tabelle 21. Beispiel für mehrere Komponenten mit unterschiedlicher Version im Server

Komponente	Aktuelle Version	Verfügbare Version
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3

  In diesem Fall wird auf der Seite **Firmware-Komponenten auswählen** Folgendes angezeigt:

  Tabelle 22. Beispiel für mehrere Komponenten mit unterschiedlicher Version im Server

Komponente	Aktuelle Version	Verfügbare Version
HDD1	V1	V3
HDD2	V2	V3

- Wenn der Katalog mehrere verfügbare Versionen enthält, wird empfohlen, nur eine der verfügbaren Versionen für einen Komponententyp auszuwählen. Die ausgewählte Firmware wird dann unabhängig von ihrer aktuellen Version auf alle anwendbaren Komponenten angewendet.

  Beispiel:

Tabelle 23. Beispiel für mehrere verfügbare Versionen, die im Katalog vorhanden sind

Komponente	Aktuelle Version	Verfügbare Version
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3
HDD1	V1	V4
HDD2	V2	V4
HDD3	V2	V4

In diesem Fall wird auf der Seite **Firmware-Komponenten auswählen** Folgendes angezeigt:

Tabelle 24. Beispiel für mehrere verfügbare Versionen, die im Katalog vorhanden sind

Komponente	Aktuelle Version	Verfügbare Version
HDD1	V1	V3
HDD2	V2	V3
HDD1	V1	V4
HDD2	V2	V4

Überblick über vSphere Lifecycle Manager

Der vSphere Lifecycle Manager ist ein Service, der auf einem vCenter-Server ausgeführt wird (gilt für vCenter 7.0 und neuere Versionen).

vSphere Lifecycle Manager ermöglicht Ihnen die Erstellung eines Baseline-Image, das aus ESXi-Image, -Firmware und -Treiber besteht. Er stellt sicher, dass alle Hosts im Cluster auf das Baseline-Image ausgerichtet sind, indem die Konformitätsprüfung durchgeführt wird. Wenn eine Nichtkonformität vorliegt, bietet er eine Option zum Korrigieren von Clustern.

In vSphere Lifecycle Manager agiert OMIVV als Firmware-Add-on-Anbieter. Weitere Informationen zum vSphere Lifecycle Manager finden Sie in der VMware-Dokumentation.

Um vSphere Lifecycle Manager mit OMIVV zu verwenden, ist die vCenter-Registrierung erforderlich. Weitere Informationen zum Registrieren von vCenter und vSphere Lifecycle Manager finden Sie unter Neuen vCenter-Server registrieren auf Seite 13.

Sie können den vSphere Lifecycle Manager (anwendbar für vCenter 7.0 und höher) in der Dell EMC-Verwaltungskonsole während der vCenter-Registrierung registrieren. Nachdem die vCenter-Registrierung erfolgreich abgeschlossen wurde, können Sie den Registrierungsstatus von vSphere Lifecycle Manager auf der Seite **VCENTER-REGISTRIERUNG** der Dell EMC-Verwaltungskonsole ändern (registrieren oder deregistrieren). Weitere Informationen finden Sie unter Registrieren von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole auf Seite 144 und Aufheben der Registrierung von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole auf Seite 144.

Anzeigen des Status von vSphere Lifecycle Manager in Dell EMC-Verwaltungskonsole

Im Folgenden werden die möglichen vSphere Lifecycle Manager-Status angezeigt, die Sie in der Spalte **vSphere Lifecycle Manager** anzeigen können:

- **Registrieren** (gilt nur für vCenter 7.0 und höher) – wird angezeigt, wenn der vSphere Lifecycle Manager nicht registriert ist.
- **Aufheben der Registrierung** (gilt nur für vCenter 7.0 und höher) – wird angezeigt, wenn vSphere Lifecycle Manager bereits registriert ist.

- **NV** – wird nur angezeigt, wenn der registrierte vCenter älter als Version 7.0 ist. Wenn für das vCenter ein Upgrade auf 7.0 durchgeführt wird, bleibt der Status **NV**. Um den Status widerzuspiegeln, starten Sie die OMIVV-Appliance neu.

Registrieren von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole

Die vCenter Version muss 7.0 oder höher sein.

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.
2. Klicken Sie auf der Seite **VCENTER-REGISTRIERUNG** unter **vSphere Lifecycle Manager** auf **Registrieren**.
   Das Dialogfeld **VSPHERE LIFECYCLE MANAGER REGISTRIEREN** <vCenter Name> wird angezeigt.
3. Klicken Sie auf **vSphere Lifecycle Manager registrieren**.
   Die Bestätigungsmeldung wird angezeigt, die auf die erfolgreiche Registrierung von vSphere Lifecycle Manager hinweist.

Aufheben der Registrierung von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole

Die vCenter Version muss 7.0 oder höher sein.

1. Navigieren Sie zu https://<ApplianceIP/hostname/>.
2. Klicken Sie auf der Seite **VCENTER-REGISTRIERUNG** unter **vSphere Lifecycle Manager** auf **Registrierung aufheben**.
   Das Dialogfeld **VSPHERE LIFECYCLE MANAGER-REGISTRIERUNG AUFHEBEN** <vCenter Name> wird angezeigt.
3. Klicken Sie auf **Registrierung aufheben**.
   Die Bestätigungsmeldung wird angezeigt, die auf die erfolgreiche Deregistrierung von vSphere Lifecycle Manager hinweist. Die **DellEMC-OMIVV** wird aus der Liste **Hardware Support Manager** im vSphere Lifecycle Manager entfernt. Dies hat keine Auswirkungen auf die OMIVV-Funktionalität.

Verwalten von Clustern mithilfe von vSphere Lifecycle Manager

Voraussetzungen:

Stellen Sie vor der Verwaltung der Cluster mit vSphere Lifecycle Manager Folgendes sicher:

- Der vSphere Lifecycle Manager ist in der Dell EMC-Verwaltungskonsole aktiviert. Weitere Informationen finden Sie unter Registrieren von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole auf Seite 144.
- Die Hosts in den Clustern sind verwaltungskonform. Weitere Informationen finden Sie unter Verwaltungs-Compliance auf Seite 71.
- Das Clusterprofil wird für den ausgewählten Cluster erstellt und das Clusterprofil ist dem Firmware-Repository in OMIVV zugeordnet. Weitere Informationen zum Erstellen eines Clusterprofils finden Sie unter Clusterprofil erstellen auf Seite 52.

Sie können die Cluster mithilfe der Benutzeroberfläche oder der vSphere Automation APIs in vSphere Lifecycle Manager verwalten. OMIVV unterstützt die Verwaltung von Clustern über die Benutzeroberfläche wie auch über vSphere Automation APIs.

ANMERKUNG: Sie können die OMIVV-Cluster-Aktionen, wie z. B. die Systemsperrung und Firmware-Aktualisierung, in einem vSphere Lifecycle Manager-gemanagten Cluster verwenden, aber es kann Auswirkungen auf das Baseline-Reporting haben.

Verwenden von OMIVV als Firmware-Add-on-Anbieter in vSphere LifeCycle Manager – Benutzeroberfläche

Sie können OMIVV mit vSphere Lifecycle Manager als Firmware-Add-on-Anbieter verwenden.

Das Clusterprofil wird als HSP (Hardware Support Package) im vSphere Lifecycle Manager-Kontext bezeichnet. Das in OMIVV erstellte Clusterprofil wird als **Firmware- und Treiber-Add-on** in vSphere Lifecycle Manager ausgewählt. Weitere Informationen zum Erstellen eines Clusterprofils finden Sie unter Clusterprofil auf Seite 52.

Um ein Image für ein ausgewähltes Cluster einzurichten und OMIVV als **Firmware-und Treiber-Add-on** zuzuordnen, führen Sie die folgenden Aufgaben aus:

1. Klicken Sie im vSphere Client auf **Hosts und Cluster** und wählen Sie dann einen Cluster aus, den Sie mit einem Image verwalten möchten.
2. Erweitern Sie auf der Seite **Aktualisierungen** im linken Bereich die Option **Hosts** und klicken Sie dann auf **Images**.
3. Um ein Firmware- und Treiber-Add-on auszuwählen, klicken Sie auf das Auswahlsymbol.
   Die Seite **Firmware- und Treiber-Add-on auswählen** wird angezeigt.
4. Wählen Sie im Abschnitt **Hardware-Support-Manager auswählen** die Option **DellEMC-OMIVV** aus.

   Nachdem Sie **DellEMC OMIVV** ausgewählt haben, werden alle Clusterprofile, die dem Firmware-Repository zugeordnet sind und mit einem Cluster im ausgewählten vCenter verknüpft sind, im Abschnitt **Firmware- und Treiber-Add-on auswählen** aufgeführt.
5. Wählen Sie ein Clusterprofil aus, das für den ausgewählten Cluster gilt, und klicken Sie dann auf **AUSWÄHLEN**.

   Informationen zum Identifizieren des Clusterprofils, das dem ausgewählten Cluster zugeordnet ist, finden Sie in der Beschreibung im Clusterprofil.

   ANMERKUNG: Wenn Sie kein Clusterprofil in OMIVV erstellt haben, wird eine leere Liste angezeigt. Weitere Informationen zum Erstellen von Clusterprofilen finden Sie unter Clusterprofil erstellen auf Seite 52.

   - **Add-on-Version**– zeigt die aktuelle Version des Clusterprofils an. Wenn das Clusterprofil geändert oder die Version in OMIVV erhöht wird, stellen Sie sicher, dass Sie die neueste Version des Clusterprofils in vSphere Lifecycle Manager verwenden.

     ANMERKUNG: Manchmal zeigt vSphere Lifecycle Manager die Nichtkonformität der Firmware an. Allerdings ist die nicht konforme Firmware in vSphere Lifecycle Manager nicht aufgeführt. Um dieses Problem zu lösen, korrigieren Sie den Cluster. Die Korrektur des Clusters führt nicht zum Neustart von vSphere Lifecycle Manager.
   - **Unterstützte ESXi-Versionen**: Zeigt die von OMIVV unterstützte ESXi-Version (7.0.0) an.

   Das ausgewählte Clusterprofil wird als Firmware-Add-on auf der Seite **Aktualisierungen** angezeigt.
6. Klicken Sie auf **SPEICHERN**.
   Der vSphere Lifecycle Manager führt eine Cluster-Konformitätsprüfung durch. Die Ergebnisse der Konformitätsprüfung werden im Abschnitt **Image-Konformität** im vSphere Lifecycle Manager angezeigt.

   Die allgemeine Compliance umfasst Software- und Firmware-Compliance. OMIVV verwaltet den Firmware-Konformitätsteil der vSphere Lifecycle Manager-Aufgaben.

Anzeigen des Konformitätsstatus

Im Folgenden sind die möglichen Firmware-Konformitätsstatus für jeden Host aufgeführt:

- **Konform**: Die Firmware-Versionen für alle auf dem Host installierten Firmware-Komponenten sind identisch mit der Firmware-Version, die im Clusterprofil in OMIVV vorhanden ist.
- **Nicht konform**: Eine oder mehrere auf dem Host installierte Firmware-Versionen entsprechen nicht der Firmware-Version, die im Clusterprofil in OMIVV vorhanden ist.

  ANMERKUNG: Nach dem Upgrade der OMIVV-Appliance schlägt die vSphere Lifecycle Manager-Konformitätsüberprüfung für das Image fehl, das mit einer älteren Version von OMIVV erstellt wurde. Um dieses Problem zu beheben, speichern Sie das Image mit der neuesten Version von Hardware Support Package (HSP).
- **Inkompatibel**: wird angezeigt, wenn:
  - Der in vCenter ausgewählte Cluster ist nicht mit dem ausgewählten **Treiber- und Firmware-Add-on** verknüpft (Clusterprofil in OMIVV).
  - Wenn das Firmware-Repository im Clusterprofil nach dem Speichern des vSphere Lifecycle Manager-Image für den ausgewählten Cluster aktualisiert wird.
- **Unbekannt**: Wenn der Host in OMIVV nicht erfolgreich inventarisiert wurde. Weitere Informationen finden Sie unter Host-Zugangsdatenprofil auf Seite 39.

ANMERKUNG: Möglicherweise stellen Sie eine Abweichung zwischen dem OMIVV- und vSphere Lifecycle Manager-Abweichungsbericht fest. Der Grund dafür ist, dass der vSphere Lifecycle Manager immer einen Live Abweichungsbericht anzeigt und OMIVV den Abweichungsbericht, der auf dem geplanten Zeitpunkt und dem geplanten Zeitpunkt basiert. Wenn Sie eine Abweichung zwischen den Abweichungsberichten feststellen, führen Sie den Abweichungserkennungsjob nach Bedarf auf der Seite **Abweichungserkennungsjobs** von OMIVV aus.

Beheben von Konformitätsproblemen im Cluster

1. Wenn der Host-Status **Konform** ist, sind für diesen Host keine weiteren Maßnahmen erforderlich.

2. Wenn der Hoststatus **Nicht konform** ist, fahren Sie mit dem Korrekturvorgang fort. Weitere Informationen finden Sie unter Korrigieren eines Clusters in vSphere Lifecycle Manager auf Seite 146.
3. Wenn der Hoststatus **Inkompatibel** ist:
   a. Stellen Sie sicher, dass der ausgewählte Cluster in vCenter mit einem Clusterprofil verknüpft ist. Wählen Sie dasselbe Clusterprofil wie **Firmware und Treiber-Add-on** in vSphere Lifecycle Manager aus.
   b. Bearbeiten Sie das vSphere Lifecycle Manager-Image, wählen Sie das aktualisierte Clusterprofil (Firmware und Treiber-Add-on) aus und speichern Sie das Image.
4. Wenn der Host-Status **Unbekannt** ist, stellen Sie sicher, dass der Host zu einem Host-Anmeldeinformationenprofil in OMIVV hinzugefügt wurde und die Bestandsaufnahme erfolgreich ausgeführt wird.

Hardware-Kompatibilitätsprüfung

vSphere Lifecycle Manager bietet eine Option zum Durchführen der Hardware-Kompatibilitätsprüfung für vSAN-Cluster vor der Durchführung von Firmware-Korrekturen. Die Hardware-Kompatibilitätsprüfung vergleicht die im Image vorhandenen Firmware und Treiber mit der aufgelisteten Hardware und dem unterstützten Treiber in der vSAN Hardware Compatibility List (HCL). vSphere Lifecycle Manager führt Hardware-Kompatibilitätsprüfungen nur für Speicher-Controller (PCIe-Geräte) durch. Gehen Sie für die Liste der unterstützten Firmware in vSphere Client zu **Überwachung** > **vSAN** > **Skyline-Integrität**.

Klicken Sie zum Durchführen der Hardware-Kompatibilitätsprüfung im Abschnitt **Image-Konformität** auf **KONFORMITÄT ÜBERPRÜFEN**.

Während der Durchführung der Hardware-Kompatibilitätsprüfung gibt OMIVV die Firmware-Versionen zurück, die im Clusterprofil vorhanden sind.

Wenn die Firmware-Version mit der in der Hardware Compatibility List (HCL) aufgeführten Firmware kompatibel ist, zeigt vSphere Lifecycle Manager den Konformitätsstatus als **Kompatibel** an. Weitere Informationen zum Konformitätsstatus finden Sie in der VMware-Dokumentation.

Die Ergebnisse der Hardware-Kompatibilitätsprüfung werden auf der Seite **Hardwarekompatibilität** angezeigt.

Durchführen einer Korrektur-Vorabprüfung

Der Vorabprüfungsvorgang führt verschiedene Prüfungen für jeden Host in einem Cluster durch, um die Cluster-Bereitschaft für die Firmware-Korrektur zu gewährleisten.

Die Vorabprüfung ist eine optionale Aufgabe, die auf Host- oder Cluster-Ebene ausgeführt werden kann.

Sie können den Vorabprüfungsvorgang überspringen, der vSphere Lifecycle Manager führt während der Korrektur eine Vorprüfung durch.

Im Rahmen einer Vorabprüfung führt OMIVV die Überprüfung der Voraussetzungen durch, die für die Firmware-Korrektur erforderlich sind:

- iDRAC-Erreichbarkeit
- iDRAC-Sperrmodus
- Status des Firmwareupdate-Jobs (sofern vorhanden), der von OMIVV für alle Hosts für den ausgewählten Cluster ausgelöst wurde
- Aktivierung von Systembestandsaufnahme beim Neustart erfassen (CSIOR)
- Konnektivität zum Firmware-Repository und zu den erforderlichen Firmware-Komponenten

Um die Voraussetzungen für die Firmware-Korrektur zu überprüfen, klicken Sie auf **VORABPRÜFUNG**.
Der Status der Vorabprüfung und die Ergebnisse werden im Abschnitt **Image-Konformität** angezeigt.

Wenn die Vorabprüfung für einen Host fehlschlägt, beheben Sie das Problem und führen Sie eine erneute Vorabprüfung durch oder fahren Sie mit der Korrekturaufgabe fort.

Korrigieren eines Clusters in vSphere Lifecycle Manager

Im Abschnitt **Image-Konformität** können Sie einen einzelnen Host oder alle Hosts im Cluster gleichzeitig korrigieren.

a. Um die Korrekturaufgabe für einen einzelnen Host auszuführen, klicken Sie im Abschnitt **Image-Konformität** auf das vertikale Ellipsensymbol neben dem Host und wählen Sie dann **Korrektur**.
b. Um die Korrekturaufgabe für alle Hosts im Cluster durchzuführen, klicken Sie im Abschnitt **Image-Konformität** auf **ALLE KORRIGIEREN**.

   Es wird empfohlen, dass Sie den iDRAC zurücksetzen, bevor Sie das Firmwareupdate ausführen. Das Zurücksetzen des iDRAC reduziert die Ausfallwahrscheinlichkeit.

Um den iDRAC vor der Durchführung des Firmwareupdates mithilfe von vSphere Lifecycle Manager auf jedem Host automatisch zurückzusetzen, aktivieren Sie das Kontrollkästchen **iDRAC-Jobs löschen und iDRAC zurücksetzen** in OMIVV. Weitere Informationen finden Sie unter Einstellungen für die Firmware-Update auf Seite 91.

Sie können den Status der Korrekturaufgabe anzeigen, indem Sie auf der Seite **Updates** auf **MEHR ANZEIGEN** klicken.

Sie können die Protokolle im Zusammenhang mit OMIVV auf der Seite **Protokolle** von OMIVV anzeigen.

Verwenden von OMIVV als Firmware-Add-on-Anbieter in vSphere Lifecycle Manager – vSphere Automation APIs

Stellen Sie vor dem Verwalten von Clustern mithilfe vSphere Automation API sicher, dass Sie die folgenden Aufgaben mithilfe der vSphere Lifecycle Manager-Benutzeroberfläche durchgeführt haben:

- Wählen Sie den Hardware-Support-Manager als Dell EMC OMIVV aus.
- Wählen Sie ein Clusterprofil aus, das für den ausgewählten Cluster gilt, und speichern Sie das Image.

Scannen der Firmware-Compliance

Befehl: POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=scan

```
{
    "spec" : {
      "message": "test commit"
    }
}
```

Beschreibung: Scannt alle Hosts im Cluster mit dem gewünschten Status des Clusters. Das Ergebnis dieses Vorgangs kann abgefragt werden, indem `cis/tasks/{task-id}` aufgerufen wird, wobei die Aufgaben-ID die Antwort dieses Vorgangs ist.

HTTP-Antwortcodes: 200 Eine Liste aller Antwortcodes finden Sie unter Antwortcodes auf Seite 182.

Beispielantwort:

```
{task ID}
```

Abrufen des Status der Compliance-Aufgabe

Befehl: GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

Beschreibung: Gibt Informationen zu einer Aufgabe zurück.

HTTP-Antwortcodes: 200 Eine Liste aller Antwortcodes finden Sie unter Antwortcodes auf Seite 182.

Beispielantwort: Das folgende Beispiel enthält nur die Nichtkonformität der Firmware.

```
"result":
[
{
 "value":
[
{
"value":
{
"hardware_modules":
[
{
 "value":
 {
 "current":
 {
 "version": "25.5.6.0009"
```

```
 },
 "details":
 {
 "component_class": "PCI_DEVICE",
 "description": "PERC H730 Mini"
 } "notifications":
 {
  "info":
 [
 {
 "id": "Different versions.",
 "time": "2020-02-04T10:47:54.422Z",
 "message":
 {
 "args": [],
 "default_message": "Different versions.",
 "id": "Different versions."
  }
  }
 ]
 },
 "status": "NON_COMPLIANT",
 "target": {
 "version": "25.5.5.0005"
  }
  }
 "key": ""
  }
  ],
 "notifications":
 {
 "info":
 [
 {
 "id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/
FQDN>]              The host is non-compliant",
 "time": "2020-02-04T10:47:54.423Z",
 "message":
 {
 "args": [],
 "default_message": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/
FQDN>] The host is non-compliant",
 "id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/FQDN>] The host
is non-compliant"
 }
 }]
 },
"status": "NON_COMPLIANT",
"target": {
"pkg": "<cluster profile name>",
 "version": "0.0.0-0"
 }
 },
 "key": "com.dell.plugin.OpenManager_HWSupportManager"
 }
 ],
```


Durchführen einer Korrektur-Vorabprüfung

Befehl: POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=check

Beschreibung: führt Tests auf dem Cluster aus, bevor der gewünschte Status auf alle Hosts im Cluster angewendet wird. Überprüft, ob alle Hosts im Cluster in einem entsprechenden Zustand sind, damit Sie mit dem gewünschten Status aktualisiert werden können.

HTTP-Antwortcodes: 200 Eine Liste aller Antwortcodes finden Sie unter Antwortcodes auf Seite 182.

Beispielantwort:

```
{task-id}
```

Überprüfen des Aufgabenstatus vor der Korrektur

Befehl: GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

Beschreibung: Gibt Informationen zu einer Aufgabe zurück.

HTTP-Antwortcodes: 200 Eine Liste aller Antwortcodes finden Sie unter Antwortcodes auf Seite 182.

Beispielantwort:


```
{
 "value":
{
"parent": "",
"cancelable": true,
"end_time": "2020-02-12T18:03:59.391Z",
"description":
{
 "args": [],
 "default_message": "Task created by VMware vSphere Lifecycle Manager",
 "id": "com.vmware.vcIntegrity.lifecycle.Task.Description"
  },
 "target":
{
"id": "domain-c8",
 "type": "ClusterComputeResource"
 },
 "result":
{
"start_time": "2020-02-12T17:52:09.264Z",
"commit": "",
"end_time": "2020-02-12T18:03:59.386Z",
 "entity_results":
[
{
"host": "host-47",
"type": "HOST",
"check_statuses": [],
"status": "OK"
 }
 {
"host": "host-41",
"type": "HOST",
"check_statuses": [],
"status": "OK"
 },
 {
 "host": "host-22",
 "type": "HOST",
 "check_statuses": [],
 "status": "OK"
  },
{
  "host": "host-16",
  "type": "HOST",
  "check_statuses": [
{
  "check":
 {
   "name":
  {
  "args": [],
  "default_message": "Host Hardware support check.",
  "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Name"
   },
  "description":
 {
  "args": [],
  "default_message": "Checks if the hardware update can be performed.",
  "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Description"
  },
  "check": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck"
  },
```

```
 "issues": [
 {
 "args": [],
 "default_message": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster:
R6415_vSAN_AllFlash_ESXi7.0RC+][Host: 100.100.10.154][Update PreCheck Task] System Lockdown
Mode is turned On for iDRAC IP, 172.20.5.5; hence Firmware update cannot continue.",
"id": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster: R6415_vSAN_AllFlash_ESXi7.0RC+][Host:
100.100.10.154][Update PreCheck Task] System Lockdown Mode is turned On for iDRAC IP,
172.20.5.5; hence Firmware update cannot continue."
 }
],
"status": "ERROR"
 }
 ],
"status": "ERROR"
 },
 {
 "host": "host-19",
 "type": "HOST",
 "check_statuses": [],
 "status": "OK"
 },
 {
"host": "host-13",
 "type": "HOST",

 "check_statuses": [],
 "status": "OK"
  },
```


Cluster wird korrigiert

Befehl: POST https://{{VC IP/FQDN}/}}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=apply

```
{
 "accept_eula" : true
}
```

Beschreibung: Wendet den gewünschten Status an, der dem angegebenen Cluster für Hosts im Cluster zugeordnet ist.

HTTP-Antwortcodes: 200 Eine Liste aller Antwortcodes finden Sie unter Antwortcodes auf Seite 182.

Beispielantwort:

```
{task-id}
```

Blinkanzeigelicht einrichten

Sie können ein Anzeigelicht an der Frontblende eines physischen Servers in einer großen Rechenzentrums-Umgebung über einen bestimmten Zeitraum blinken lassen, so dass Sie den Server leichter erkennen können.

1. Führen Sie eine der folgenden Aktionen aus, um den **Blinkende Server-LED-Anzeige**-Assistenten zu starten:
   a. Erweitern Sie auf der OMIVV-Startseite **Menü** die Option **Hosts und Cluster**, klicken Sie mit der rechten Maustaste auf einen Host oder Cluster und navigieren Sie zu **Zusammenfassung** > **OMIVV Host-Informationen** > **Host-Aktionen** > **Blinkende Server-LED-Anzeige**.
   b. Klicken Sie mit der rechten Maustaste auf einen Host, gehen Sie zu **OMIVV Host-Aktionen** > **Blinkende Server-LED-Anzeige**.
2. Klicken Sie im rechten Fensterbereich auf „Zusammenfassung“ und gehen Sie dann zu **OMIVV Hostinformationen** > **Host-Aktion** > **Blinkende Server-LED-Anzeige.**
   Das Dialogfeld **Blinkende Server-LED-Anzeige** wird angezeigt.
3. Wählen Sie eine der folgenden Optionen aus:
   a. Um die Server-LED-Anzeige einzuschalten und den Zeitraum festzulegen, klicken Sie auf **Ein**.
   b. Um die Server-LED-Anzeige zu deaktivieren, klicken Sie auf **Aus**.

Systemsperrmodus konfigurieren

Der Systemsperrmodus wird nur für iDRAC9-basierte Server mit einer Enterprise-Lizenz unterstützt. Wenn Sie den Systemsperrmodus einschalten, sperren Sie die Systemkonfiguration, einschließlich der Firmwareaktualisierungen. Die Einstellung für den Systemsperrmodus dient ausschließlich zum Schutz des Systems vor unbeabsichtigten Änderungen. Sie können den Systemsperrmodus für verwaltete Hosts mithilfe des OMIVV-Geräts oder über die iDRAC-Konsole ein- oder ausschalten. Ab der OMIVV-Version 4.1 können Sie den Sperrmodus von iDRAC auf Servern konfigurieren und überwachen. Außerdem muss der iDRAC über eine Enterprise-Lizenz verfügen, um den Lockdown-Modus zu aktivieren.

ANMERKUNG: Sie können den Systemsperrmodus nicht für Hosts ändern, die vom Gehäuse-Anmeldeinformationenprofil verwaltet werden.

Sie können den Systemsperrmodus durch das Sperren oder Entsperren eines Hosts oder Clusters auf Host- oder Cluster-Ebene konfigurieren. Wenn der Systemsperrmodus eingeschaltet ist, unterliegen folgende Funktionen Einschränkungen:

- Alle Konfigurationsaufgaben, z. B. Firmwareaktualisierung, Betriebssystem-Bereitstellung, Löschen der Systemereignisprotokolle, Reset des iDRAC und Konfiguration des iDRAC-Trap-Ziels.

1. Zum Start des Assistenten zur Konfiguration des Systemsperrmodus führen Sie einen der folgenden Aktionen aus:
   a. Erweitern Sie auf der OMIVV-Startseite **Menü** die Option **Hosts und Cluster**, klicken Sie mit der rechten Maustaste auf einen Host oder Cluster und navigieren Sie zu **Zusammenfassung** > **OMIVV Host-Informationen** > **Host-Aktionen** > **Systemsperrmodus konfigurieren**.
   b. Klicken Sie mit der rechten Maustaste auf einen Host oder ein Cluster, gehen Sie zu **OMIVV Host-Aktionen** > **Systemsperrmodus konfigurieren**.
   c. Wählen Sie einen Host oder Cluster aus und navigieren Sie zu **Überwachen** > **OMIVV-Host- oder Clusterinformationen** > **Firmware** > **Systemsperrmodus konfigurieren**.
2. Geben Sie für Cluster Level den Namen und die Beschreibung des Systemsperrmodus-Jobs ein. Die Beschreibung ist ein optionales Feld.
3. Um den Sperrmodus des Systems zu aktivieren, klicken Sie auf **Einschalten**. Diese Option schränkt Änderungen an den Systemkonfigurationen (einschließlich Firmware und BIOS-Version) im System ein.
4. Um den Sperrmodus des Systems zu deaktivieren, klicken Sie auf **Ausschalten**. Mit dieser Option werden Änderungen an den Systemkonfigurationen (einschließlich Firmware und BIOS-Version) im System aktiviert.

   Wenn Sie versuchen, den Sperrmodus für Power Edge-Server der 13. Generation und früher zu konfigurieren, werden Sie durch eine Meldung informiert, dass diese Fukntion nicht auf dieser Platform unterstützt wird.
5. Klicken Sie auf **OK**.
   Ein Job wurde erfolgreich für die Konfiguration des Systemsperrmodus erstellt. Um den Job-Status zu prüfen, navigieren Sie zu **Jobs** > **Systemsperrmodus**. Weitere Informationen zu Systemsperrmodus-Jobs finden Sie unter Systemsperrmodus-Jobs auf Seite 78.

18

Sicherheitsrollen und Berechtigungen

Die OpenManage Integration for VMware vCenter speichert Benutzeranmeldedaten in einem verschlüsselten Format. Es stellt keine Kennwörter für Clientanwendungen bereit, um unsachgemäße Anfragen zu vermeiden. Die Datenbanksicherung ist mithilfe benutzerdefinierter Sicherheitsausdrücke vollständig verschlüsselt, deshalb können Daten nicht missbräuchlich verwendet werden.

Als Standardeinstellung besitzen Benutzer in der Administratorgruppe alle Rechte. Die Administratoren können alle Funktionen der OpenManage Integration for VMware vCenter innerhalb des VMware vSphere Webclients benutzen. Wenn ein Benutzer mit erforderlichen Berechtigungen das Produkt verwalten soll, gehen Sie folgendermaßen vor:

1. Erstellen Sie eine Rolle mit erforderlichen Berechtigungen.
2. Registrieren Sie einen vCenter Server mithilfe des Benutzers.
3. Schließen Sie sowohl die operative Dell Rolle als auch die Dell Infrastrukturbereitstellungsrolle ein.

Datenintegrität

Die Kommunikation zwischen OpenManage Integration for VMware vCenter, der Verwaltungskonsole und vCenter erfolgt über HTTPS. OpenManage Integration for VMware vCenter erzeugt ein Zertifikat, das für die vertrauenswürdige Kommunikation zwischen vCenter und der Appliance verwendet wird. Außerdem überprüft sie das Zertifikat des vCenter-Servers und vertraut ihm vor der Kommunikation und der Registrierung von OpenManage Integration für VMware vCenter.

Bei einer sicheren Verwaltungskonsolen-Sitzung erfolgt nach 15-minütiger Inaktivität ein Timeout und die Sitzung ist nur im aktuellen Browserfenster und/oder in der aktuellen Registerkarte gültig. Wenn Sie versuchen, die Sitzung in einem/einer neuen Fenster oder Registerkarte zu öffnen, wird ein Sicherheitsfehler angezeigt, der nach einer gültigen Sitzung fragt. Diese Aktion verhindert auch, dass der Nutzer auf eine bösartige URL klickt, die die Sitzung der Verwaltungskonsole angreifen kann.

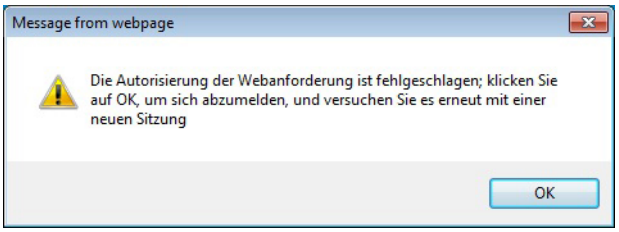


Abbildung 1. Sicherheitsfehlermeldung

Zugriffskontrollauthentifizierung, -autorisierung und -rollen

Um vCenter-Operationen durchzuführen, verwendet OpenManage Integration for VMware vCenter die aktuelle Nutzersitzung des vSphere-Clients und die gespeicherten Administratorzugangsdaten für die OpenManage-Integration. Die OpenManage-Integration für VMware vCenter verwendet das integrierte Rollen- und Berechtigungsmodell des vCenter-Servers, um Benutzeraktionen mit der OpenManage-Integration und den von vCenter verwalteten Objekten (Hosts und Cluster) zu autorisieren.

Dell Vorgangsrolle

Enthält die Berechtigungen/Gruppen zur Ausführung von Geräte- und vCenter Server-Aufgaben einschließlich Firmware-Aktualisierungen, Hardware-Bestandslisten, Neustarten eines Hosts, Versetzen eines Hosts in den Wartungsmodus oder Erstellen einer vCenter Server-Aufgabe.

Diese Rolle umfasst die folgenden Berechtigungsgruppen:

Tabelle 25. Berechtigungsgruppen

Gruppenname	Beschreibung
Berechtigungsgruppe – Dell.Configuration	Ausführen von mit Hosts verknüpften Aufgaben, Ausführen von mit vCenter verknüpften Aufgaben, Konfigurieren von SelLog, Konfigurieren von ConnectionProfile, Konfigurieren von ClearLed, Firmware-Aktualisierung
Berechtigungsgruppe – Dell.Inventory	Konfigurieren der Bestandsaufnahme, Konfigurieren des Serviceabrufs, Konfigurieren von ReadOnly
Berechtigungsgruppe – Dell.Monitoring	Konfigurieren der Überwachung, Überwachung
Berechtigungsgruppe – Dell. Reporting (nicht verwendet)	Erstellen eines Berichts, Ausführen eines Berichts

Dell Infrastrukturbereitstellungsrolle

Diese Rolle umfasst die Berechtigungen, die mit den Hypervisor-Bereitstellungsfunktionen verknüpft sind.

Zu den Berechtigungen dieser Rolle gehören das Konfigurieren des Host-Zugangsdatenprofils, die Identitätszuweisung und die Bereitstellung.

Berechtigungsgruppe – Dell.Deploy- Provisionierung

Konfigurieren des Host-Zugangsdatenprofils, Identitätszuweisung, Bereitstellung.

Informationen zu Berechtigungen

Jede Aktion, die von der OpenManage Integration für VMware vCenter ausgeführt wird, ist einer Berechtigung zugeordnet. In den folgenden Abschnitten sind die verfügbaren Aktionen und die zugehörigen Berechtigungen aufgelistet:

- Dell.Configuration.Perform von mit vCenter verknüpften Aufgaben
  - Beenden und Starten des Wartungsmodus
  - Aufrufen der vCenter-Benutzergruppe zur Abfrage von Berechtigungen
  - Registrieren und Konfigurieren von Alarmen, z. B. Aktivieren/Deaktivieren von Alarmen auf der Seite mit den Ereigniseinstellungen
  - Veröffentlichen von Ereignissen/Warnungen bei vCenter
  - Konfigurieren von Ereigniseinstellungen auf der Seite mit den Ereigniseinstellungen
  - Wiederherstellen von Standardwarnungen auf der Seite mit den Ereigniseinstellungen
  - Überprüfen des DRS-Status auf Clustern während der Konfiguration von Warnungs-/Ereigniseinstellungen
  - Neustarten des Hosts nach Aktualisierungs- oder anderen Konfigurationsmaßnahmen
  - Überwachen des Status/Fortschritts von vCenter-Tasks
  - Erstellen von vCenter-Tasks, z. B. Firmware-Aktualisierungstask, Hostkonfigurationstask und Bestandsaufnahmetask
  - Aktualisieren des Status/Fortschritts von vCenter-Tasks
  - Abrufen von Hostprofilen
  - Hinzufügen von Hosts zu einem Datencenter
  - Hinzufügen von Hosts zu einem Cluster
  - Übernehmen des Profils für einen Host
  - Abrufen von CIM-Anmeldeinformationen
  - Konfigurieren von Hosts für Konformität
  - Abrufen des Status des Konformitätstasks
- Dell.Inventory.Configure ReadOnly
  - Abrufen aller vCenter-Hosts zum Aufbau der vCenter-Struktur während der Konfiguration von Verbindungsprofilen
  - Bei Auswahl der Registerkarte überprüfen, ob der Host ein Dell Server ist
  - Abrufen der Adresse/IP von vCenter
  - Abrufen der Host-IP/Adresse
  - Abrufen des Benutzers der aktuellen vCenter-Sitzung basierend auf der vSphere-Clientsitzungs-ID
  - Abrufen der vCenter-Bestandsaufnahmestruktur, um die vCenter-Bestandsliste in einer Baumstruktur anzuzeigen.
- Dell.Monitoring.Monitor

- Abrufen des Hostnamens für die Veröffentlichung des Ereignisses
- Ausführen von Ereignisprotokollierungsvorgängen, z. B. Aufrufen der Ereignisanzahl oder Ändern der Ereignisprotokolleinstellungen
- Registrieren, Aufheben der Registrierung und Konfigurieren von Ereignissen/Warnungen – Empfangen von SNMP-Traps und Veröffentlichen von Ereignissen

- Dell.Configuration.Firmware Update
  - Ausführen einer Firmware-Aktualisierung
  - Laden von Firmware-Repository- und DUP-Dateninformationen auf der Seite des Assistenten zur Firmware-Aktualisierung
  - Abfragen der Firmware-Bestandsliste
  - Konfigurieren der Firmware-Repository-Einstellungen
  - Konfigurieren des Stagingordners und Ausführen der Aktualisierung unter Verwendung der Stagingfunktion
  - Testen der Netzwerk- und Repository-Verbindungen
- Dell.Deploy-Provisioning Erstellen von Vorlagen
  - HW-Konfigurationsprofil konfigurieren
  - Hypervisor-Bereitstellungsprofil konfigurieren
  - Verbindungsprofil konfigurieren
  - Identität zuweisen
  - Bereitstellen
- Dell.Configuration. Ausführen von mit Hosts verknüpften Tasks
  - LED blinken, LED löschen
  - Starten der iDRAC-Konsole
  - Anzeigen und Löschen des SEL-Protokolls
- Dell.Inventory. Konfigurieren der Bestandsaufnahme
  - Anzeigen der Systembestandsliste auf der Registerkarte zur Dell Serververwaltung
  - Abrufen von Speicherdetails
  - Abrufen von Stromüberwachungsdetails
  - Erstellen, Anzeigen, Bearbeiten, Löschen und Testen von Verbindungsprofilen auf der Seite mit den Verbindungsprofilen
  - Planen, Aktualisieren und Löschen des Bestandsaufnahmezeitplans
  - Ausführen einer Bestandsaufnahme auf Hosts

19

Häufig gestellte Fragen – FAQs

In diesem Abschnitt finden Sie Antworten auf Fragen zur Fehlerbehebung. Dieser Abschnitt umfasst:

- Häufig gestellte Fragen (FAQs)
- Probleme bei der Bare-Metal-Bereitstellung auf Seite 172

Häufig gestellte Fragen – FAQs

In diesem Abschnitt werden einige allgemeine Fragen und Lösungen beschrieben.

iDRAC-Lizenztyp und -Beschreibung werden für nicht konforme vSphere Hosts falsch angezeigt.

Wenn ein Host nicht konform ist, wenn CSIOR deaktiviert ist oder nicht ausgeführt wurde, werden iDRAC-Lizenzinformationen falsch angezeigt, obwohl eine gültige iDRAC-Lizenz verfügbar ist. Daher wird der Host in der Liste der vSphere-Hosts angezeigt, wenn Sie jedoch auf den Host klicken, um Details anzuzeigen, werden die Informationen in **iDRAC-Lizenztyp** als leer angezeigt und unter **iDRAC-Lizenzbeschreibung** wird „Ihre Lizenz muss aktualisiert werden“ angezeigt.

Lösung: Um dieses Problem zu beheben, aktivieren Sie CSIOR auf einem Referenzserver.

Betroffene Version: 4.0 und später

Dell Anbieter wird nicht als Anbieter für Funktionszustandsaktualisierung angezeigt

Wenn Sie einen vCenter-Server bei OMIVV registrieren und dann die Version des vCenter-Servers z. B. von vCenter 6.0 auf vCenter 6.5 aktualisieren, wird der Dell Anbieter in der Liste der **Proaktiven HA-Anbieter** nicht angezeigt.

Lösung: Sie können einen registrierten vCenter für Nicht-Administrator-Nutzer oder Administrator-Nutzer aktualisieren. Wenn Sie ein Upgrade auf die neueste Version des vCenter-Servers durchführen möchten, lesen sie zunächst die VMware-Dokumentation und führen Sie anschließend einen der folgenden Schritte aus:

- Für Nicht-Administratornutzer
  1. Weisen Sie Nicht-Administratornutzern bei Bedarf zusätzliche Berechtigungen zu. Informationen dazu finden Sie unter Erforderliche Berechtigungen für Nicht-Administratornutzer auf Seite 15.
  2. Führen Sie einen Neustart des registrierten OMIVV-Geräts durch.
  3. Melden Sie sich vom vSphere Client ab und melden Sie sich dann erneut an.
- Für Administratornutzer:
  1. Führen Sie einen Neustart des registrierten OMIVV-Geräts durch.
  2. Melden Sie sich vom vSphere Client ab und melden Sie sich dann erneut an.

Der Dell Anbieter ist jetzt in der Liste der **Proaktiven HA-Anbieter** aufgeführt.

Betroffene Version: 4.0 und später

Aufgrund einer ungültigen oder unbekannten iDRAC-IP-Adresse ist die Host-Bestandsaufnahme oder Testverbindung fehlgeschlagen.

Die Host-Bestandsaufnahme oder Testverbindung ist aufgrund einer ungültigen oder unbekannten iDRAC-IP-Adresse fehlgeschlagen, und Sie erhalten Meldungen wie „Netzwerklatenzen oder unerreichbarer Host“, „Verbindung verweigert“, „Zeitüberschreitung bei Vorgang“, „WSMAN“, „Keine Route zum Host“ und „IP-Adresse: null“.

1. Öffnen Sie die virtuelle iDRAC-Konsole.
2. Drücken Sie F2 und navigieren Sie zu **Optionen zur Fehlerbehebung**.
3. Navigieren Sie in **Optionen zur Fehlerbehebung** zu **Verwaltungsagenten neu starten**.
4. Um die Verwaltungsagenten neu zu starten, drücken Sie auf F11.

Nun ist ein gültiger iDRAC-IP verfügbar.

ANMERKUNG: Host-Bestandsaufnahmen können fehlschlagen, wenn OMIVV die WBEM-Services auf Hosts, auf denen ESXi 6.5 läuft, nicht aktivieren können. Weitere Informationen zum WBEM-Dienst finden Sie unter Host-Anmeldeinformationenprofil erstellen auf Seite 39.

Bei der Ausführung eines Fix-Assistenten für nicht konforme vSphere Hosts wird der Status eines spezifischen Hosts als „Unknown“ angezeigt.

Wenn Sie den Fix-Assistenten für nicht konforme vSphere Hosts zum Beheben nicht konformer Hosts ausführen, wird der Status eines spezifischen Hosts als „Unbekannt“ angezeigt. Dieser Status wird angezeigt, wenn iDRAC nicht erreichbar ist.

Lösung: Überprüfen Sie die iDRAC Konnektivität des Hosts und stellen Sie sicher, dass die Bestandsaufnahme erfolgreich ausgeführt wird.

Betroffene Version: 4.0

Dell Berechtigungen, die beim Registrieren des OMIVV-Geräts zugewiesen wurden, werden nach dem Aufheben der Registrierung von OMIVV nicht entfernt

Nach der Registrierung von vCenter mit einem OMIVV-Gerät werden verschiedene Dell Berechtigungen zur Liste der vCenter-Berechtigungen hinzugefügt. Sobald Sie die Registrierung von vCenter von der OMIVV Appliance aufgehoben haben, werden die Dell Rechte nicht entfernt.

ANMERKUNG: Obwohl die Berechtigungen von Dell nicht entfernt werden, entstehen keine Auswirkungen auf OMIVVVorgänge.

Betroffene Version: 3.1 und höher

Wie behebe ich den Fehlercode 2000000, der von der VMware Zertifizierungsstelle – VMCA – verursacht wird?

Wenn Sie den vSphere Certificate Manager ausführen und das Zertifkat für vCenter Server oder Platform Controller Service (PSC) durch ein neues CA-Zertifikat und einen Schlüssel für vCenter 6.0 ersetzen, zeigt OMIVV den Fehlercode 2000000 an und löst eine Ausnahme aus.

Lösung: Zur Lösung der Ausnahme müssen Sie die SSL-Anker für die Dienste aktualisieren. Die SSL-Anker können durch Ausführen des Skripts `ls_update_certs.py` auf PSK aktualisiert werden. Das Skript nutzt einen alten Zertifikat-Fingerabdruck als Eingabeargument und das neue Zertifikat wird installiert. Das alte Zertifikat ist das Zertifikat vor dem Austausch und das neue Zertifikat ist das Zertifikat nach dem Austausch. Weitere Informationen finden Sie unter https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 und https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689.

Betroffene Version: 3.0 und höher, vCenter 6.0 und höher

Ersetzen der Zertifikate einer vCenter Windows Installation

Weitere Informationen finden Sie in https://kb.vmware.com/s/article/2121689.

Ersetzen der Zertifikate auf dem vCenter Server-Gerät

Weitere Informationen finden Sie in https://kb.vmware.com/s/article/2121689.

Abrufen des alten Zertifikats aus dem Managed Object Browser – MOB

Weitere Informationen finden Sie in https://kb.vmware.com/s/article/2121701.

Extrahieren des Fingerabdrucks vom alten Zertifikat

Weitere Informationen finden Sie in https://kb.vmware.com/s/article/2121701.

In der Verwaltungskonsole ist nach dem Zurücksetzen des Geräts auf die werksseitigen Einstellungen Aktualisierungs-Repository-Pfad nicht auf den Standard-Pfad eingestellt.

Nachdem Sie das Gerät zurückgesetzt haben, wechseln Sie zur **Verwaltungskonsole**, und klicken Sie dann auf **Appliance-Verwaltung** im linken Fensterbereich. Auf der Seite **Appliance-Einstellungen** wurde der **Aktualisierungs-Repository-Pfad** nicht auf den Standard-Pfad geändert.

Lösung: Kopieren Sie in der **Verwaltungskonsole** manuell den Pfad im Feld **Standard-Aktualisierungs-Repository** in das Feld **Repository-Aktualisierungspfad**.

Was soll ich tun, wenn ein Web-Kommunikationsfehler im vCenter HTML-5-Client nach dem Ändern der DNS-Einstellungen in OMIVV angezeigt wird?

Wenn irgendeine Art von Web-Kommunikationsfehler in vCenter HTML-5-Client angezeigt wird, während Sie eine oder mehrere Aufgaben im Zusammenhang mit OMIVV durchführen, führen Sie Folgendes durch:

- Löschen Sie den Browser-Cache.
- Melden Sie sich ab und dann über den vSphere Client an.

Das Installationsdatum wird für einige Firmware-Versionen auf der Firmware-Seite als 31.12.1969 angezeigt.

Im vSphere-Client wird das Installationsdatum für einen Host für einige Firmware-Elemente auf der Firmware-Seite als 31.12.1969 angezeigt. Wenn das Firmware-Installationsdatum nicht verfügbar ist, wird das alte Datum angezeigt.

Lösung: Wenn Sie dieses alte Datum für eine Firmware-Komponente sehen, ist das wirkliche Installationsdatum nicht verfügbar.

Betroffene Versionen: 2.2 und höher

Warum wird das OpenManage Integration Symbol im HTML-5 Client nicht angezeigt, selbst wenn die Registrierung des Plug-ins im vCenter erfolgreich war?

Das OpenManage Integration Symbol wird nicht im vSphere-Client angezeigt, außer wenn die vSphere Webclient-Services neu gestartet werden. Bei der Registrierung der OpenManage Integration for VMware vCenter Appliance wird die Appliance beim vSphere-Client registriert. Wenn Sie die Registrierung der Appliance aufheben und dann entweder die gleiche Version oder eine neue Version der Appliance registrieren, wird sie erfolgreich registriert, aber das OMIVV Symbol wird möglicherweise im vSphere-Client nicht angezeigt. Der Grund dafür liegt in einem Zwischenspeicherproblem von VMware. Zum Beheben des Problems stellen Sie sicher, dass Sie den vSphere-Client-Service auf dem vCenter Server neu starten. Dann wird das Plug-in in der UI angezeigt.

Lösung: Starten Sie den vSphere-Client-Service auf dem vCenter Server neu.

Betroffene Version: 2.2 und höher

Warum werden DNS-Konfigurationseinstellungen nach dem Neustart des Geräts auf die ursprünglichen Einstellungen zurückgesetzt, wenn die IP- und DNS-Einstellungen des Geräts mit DHCP-Werten überschrieben werden?

Es gibt einen bekannten Fehler, bei dem statisch zugewiesene DNS-Einstellungen durch DHCP-Werte ersetzt werden. Dies kann vorkommen, wenn DHCP verwendet wird, um IP-Einstellungen abzurufen, und DNS-Werte statisch zugewiesen werden. Wenn die DHCP-Lease erneuert oder das Gerät neu gestartet wird, werden die statisch zugewiesenen DNS-Einstellungen entfernt.

Lösung: Weisen Sie IP-Einstellungen statisch zu, wenn sich die DNS-Servereinstellungen von DHCP unterscheiden.

Betroffene Version: Alle

Wenn die Firmwareaktualisierung ausgeführt wird, wird möglicherweise die Fehlermeldung angezeigt, dass die Firmware-Repository-Datei nicht vorhanden oder ungültig ist.

Während der Ausführung des Assistenten für die Firmwareaktualisierung auf Cluster-Ebene wird möglicherweise folgende Fehlermeldung angezeigt: **Die Firmware-Repository-Datei ist nicht vorhanden oder ungültig**. Ursache dafür kann ein täglicher Hintergrundprozess sein, der die Katalogdatei nicht aus dem Repository herunterladen und im Cache ablegen konnte. Dies geschieht, wenn die Katalogdatei zu dem Zeitpunkt nicht erreichbar ist, zu dem der Hintergrundprozess ausgeführt wird.

Lösung: nach der Behebung von Problemen im Zusammenhang mit der Katalogverbindung können Sie den Hintergrundprozess erneut starten, indem Sie den Speicherort des Firmware-Repositorys ändern und ihn dann wieder auf den ursprünglichen Speicherort zurücksetzen. Warten Sie etwa fünf Minuten, bis der Hintergrundprozess abgeschlossen ist. Stellen Sie sicher, dass die Anmeldeinformationen für CIFS kein @-Zeichen enthalten. Stellen Sie außerdem sicher, dass die DUP-Datei am Freigabespeicherort vorhanden ist.

Betroffene Version: Alle

Die Verwendung von OMIVV zum Aktualisieren einer Intel-Netzwerkkarte mit der Firmwareversion 13.5.2 wird nicht unterstützt.

Es gibt ein bekanntes Problem mit den Dell EMC PowerEdge-Servern und einigen Intel-Netzwerkkarten mit der Firmwareversion 13.5.2. Das Aktualisieren einiger Intel-Netzwerkkarten mit dieser Firmwareversion schlägt fehl, wenn die Firmware-Aktualisierung mithilfe des iDRAC und dem Lifecycle Controller durchgeführt wird. Kunden, die diese Firmwareversion verwenden, müssen die Netzwerktreibersoftware mithilfe eines Betriebssystems aktualisieren. Wenn die Firmwareversion der Intel-Netzwerkkarte eine andere ist als 13.5.2, können Sie die Aktualisierung mithilfe von OMIVV durchführen. Weitere Informationen finden Sie unter http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx.

ANMERKUNG: Wählen Sie bei der Anwendung einer Firmware-Aktualisierung vom Typ 1:n keine Intel-Netzwerkadapter der Version 13.5.2 aus. Anderenfalls schlägt die Aktualisierung fehl und die Aktualisierungsaufgabe für die verbleibenden Server wird gestoppt.

Die Verwendung von OMIVV zum Aktualisieren einer Intel Netzwerkkarte von 14.5 oder 15.0 auf 16.x schlägt aufgrund der Bereitstellungsanforderung von DUP fehl.

Dies ist ein bekanntes Problem bei NIC 14.5 und 15.0. Stellen Sie sicher, dass Sie den benutzerdefinierten Katalog zum Aktualisieren der Firmware auf 15.5.0 vor der Aktualisierung der Firmware auf 16.x verwenden.

Betroffene Version: Alle

Warum zeigt das Administrationsportal einen nicht erreichbaren Aktualisierungs-Repository-Speicherort an?

Wenn Sie einen nicht erreichbaren Aktualisierungs-Repository-Pfad angeben, wird die Fehlermeldung „Fehlgeschlagen: Fehler beim Herstellen einer Verbindung mit der URL“ im oberen Bereich der Geräte-Aktualisierungsansicht angezeigt. Allerdings wird der Aktualisierungs-Repository-Pfad nicht auf den Wert vor der Aktualisierung zurückgesetzt.

Lösung: Gehen Sie von dieser Seite auf eine andere Seite und stellen Sie sicher, dass die Seite aktualisiert wird.

Betroffene Version: Alle

Warum wechselt das System bei der Durchführung einer 1:n-Firmware-Aktualisierung nicht in den Servicemodus?

Bei einigen Firmware-Aktualisierungen muss der Host nicht neu gestartet werden. In diesem Fall wird die Firmware-Aktualisierung durchgeführt, ohne dass der Host in den Wartungsmodus wechselt.

Die globale Gehäuse-Integrität ist immer noch funktionsfähig, obwohl sich einige der Netzteil-Status zu kritisch geändert haben.

Die globale Gehäuse-Integrität für das Netzteil basiert auf den Redundanzrichtlinien und darauf, ob der Gehäuse-Strombedarf von den PSU erfüllt wird, die noch online und funktionsfähig sind. Deshalb kann der gesamte Stromverbrauch des Gehäuses erfüllt werden, obwohl einige der Netzteile nicht mehr funktionieren. Daher ist der globale Funktionszustand des Gehäuses funktionsfähig. Weitere Informationen über die Netzteile und das Energiemanagement finden Sie im Benutzerhandbuch der Firmware des Dell PowerEdge M1000e Chassis Management Controller.

Die Prozessor-Version wird auf der Seite „System-Überblick“ als „Nicht verfügbar“ angezeigt.

In 12G und neueren Servern befindet sich die Prozessorversion in der Spalte „Marke“. In Servern vorheriger Generationen wird die Prozessor-Version in der Spalte **Version** angezeigt.

Unterstützt OMIVV vCenter im verknüpften Modus?

Ja, OMIVV unterstützt bis zu 10 vCenter Server entweder in einem verknüpften Modus oder in einem unverknüpften Modus.

Erforderliche Porteinstellungen für OMIVV

Verwenden Sie die folgende Porteinstellungen für OMIVV:

Tabelle 26. Virtual Appliance

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
53	DNS	TCP	Keine	Ausgang	OMIVV-Gerät zu DNS-Server	DNS-Client	Konnektivität zum DNS-Server oder Auflösen der Hostnamen.
68	DHCP	UDP	Keine	Eingang	DHCP-Server zu OMIVV-Gerät	Dynamische Netzwerkkonfiguration	Um die Netzwerkdetails wie IP, Gateway, Netzmaske und DNS abzurufen.
69	TFTP	UDP	128 Bit	Ausgang	OMIVV auf iDRAC	Trivial File Transfer (Einfache Dateiübertragung)	Wird verwendet, um den Bare-Metal-Server auf die erforderliche Mindestversion der Firmware zu aktualisieren.
123	NTP	UDP	Keine	Eingang	NTP zu OMIVV-Gerät	Zeitsynchronisation	Zum Synchronisieren mit einer bestimmten Zeitzone.
162	SNMP-Agent	UDP	Keine	Eingang	iDRAc oder CMC oder OME-Modular zu OMIVV-Gerät	SNMP-Agent (Server)	Für den Empfang von SNMP-Traps von verwalteten Knoten.
443	HTTP oder HTTPS	TCP	Keine	Ausgang	OMIVV-Gerät zu Internet	Dell Online-Datenzugriff	Konnektivität zu Online-Garantie (Internet), Firmware und aktuellen RPM-Informationen.
443	HTTPS	TCP	128 Bit	Eingang	OMIVV UI zu OMIVV-Gerät	HTTPS-Server	Von OMIVV angebotene Webdienste. Diese Webdienste werden vom vSphere Client und Dell Admin-Portal genutzt.
443	HTTPS	TCP	128 Bit	Eingang	ESXi-Server zu OMIVV-Gerät	HTTPS-Server	Wird im Betriebssystem-Bereitstellungsprozess für Skripts nach der Installation zur Kommunikation mit dem OMIVV-Gerät verwendet.
443	HTTPS	TCP	128 Bit	Eingang	iDRAC zu OMIVV-Gerät	Automatische Ermittlung	Bereitstellungsserver, der für die automatische Ermittlung von verwalteten Knoten verwendet wird.
443	WSMAN	TCP	128 Bit	Ein/Aus	OMIVV-Gerät zu oder von iDRAC	iDRAC-Kommunikation	iDRAC-, CMC- oder OME-Modular-Kommunikation; wird zur Verwaltung und Überwachung der verwalteten Knoten verwendet.
445/139	SMB	TCP	128 Bit	Ausgang	OMIVV-Gerät zu CIFS	CIFS-Kommunikation	Für die Kommunikation mit Windows-Freigaben.
2049 /111	NFS	UDP/TCP	Keine	Ein/Aus	OMIVV-Gerät zu NFS	Öffentliche Freigabe	Öffentliche NFS-Freigabe, die vom OMIVV-Gerät für die verwalteten Knoten verfügbar gemacht und für Firmwareaktualisierungs- und Betriebssystem-Bereitstellungsprozesse verwendet wird.
4001 zu 4004	NFS	UDP/TCP	Keine	Ein/Aus	OMIVV-Gerät zu NFS	Öffentliche Freigabe	Diese Ports müssen offen gehalten werden zur Ausführung der statd, quotd, lockd, und mountd Dienstleistungen durch den V2 und V3-Protokolle der NFS-Server.
Benutzer definierte	beliebig	UDP/TCP	Keine	Ausgang	OMIVV-Gerät zu Proxy-Server	Proxy	Für die Kommunikation mit dem Proxy-Server

Tabelle 27. Verwaltete Knoten (ESXi)

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
162	SNMP	UDP	Keine	Ausgang	ESXi zu OMIVV-Gerät	Hardware-Ereignisse	Asynchrone SNMP-Traps, die von ESXi gesendet werden. Dieser Port muss über ESXi geöffnet werden.
443	WSMAN	TCP	128 Bit	Eingang	OMIVV-Gerät zu ESXi	iDRAC-Kommunikation	Wird verwendet, um Informationen für die Management Station bereitzustellen. Dieser Port muss über ESXi geöffnet werden.
443	HTTPS	TCP	128 Bit	Eingang	OMIVV-Gerät zu ESXi	HTTPS-Server	Wird verwendet, um Informationen für die Management Station bereitzustellen. Dieser Port muss über ESXi geöffnet werden.

Weitere Informationen über die iDRAC und CMC Portinformationen finden Sie im *Integrated Dell Remote Access Controller-Benutzerhandbuch* und im *Dell Chassis Management Controller Benutzerhandbuch* unter **https://www.dell.com/support**.

Weitere Informationen über die OME Modular Portinformationen finden Sie im *Dell EMC OME-Modular Benutzerhandbuch* unter **https://www.dell.com/support**.

ANMERKUNG: Für iDRAC9-basierte Server bindet iDRAC NFS über TCP am Port 2049 ein. Eine Liste der iDRAC9-basierten Server finden Sie in der Compliance-Matrix.

Das Passwort für den Benutzer, der für die Bare-Metal-Erkennung verwendet wird, wird nach der erfolgreichen Anwendung des Systemprofils nicht geändert, das über den gleichen Benutzer mit neuen geänderten Anmeldeinformationen in der iDRAC-Benutzerliste verfügt.

Das Kennwort des Benutzers, der bei der Erkennung verwendet wird, wird nicht in die neue Berechtigung geändert, wenn nur Systemprofil (Konfiguration der Hardware) für die Bereitstellung ausgewählt ist. Dieses Verhalten ist beabsichtigt, damit das Plug-in mit dem iDRAC kommunizieren kann, und in zukünftigen Bereitstellungen verwendbar ist.

Die auf der Seite vCenter Hosts und Clusters aufgelisteten neuen iDRAC-Versionsdetails können nicht angezeigt werden.

Lösung: Nach der erfolgreichen Fertigstellung einer Firmware-Aktualisierungsaufgabe im vSphere Webclient aktualisieren Sie die Seite **Firmware-Aktualisierung** und überprüfen Sie die Firmware-Versionen. Wenn auf der Seite die alten Versionen angezeigt werden, wechseln Sie zur Seite **Host-Kompatibilität** in OpenManage Integration for VMware vCenter und überprüfen Sie den CSIOR-Status dieses Hosts. Wenn CSIOR nicht aktiviert ist, aktivieren Sie CSIOR und starten Sie den Host neu. Wenn die CSIOR-Funktion bereits aktiviert ist, melden Sie sich in der iDRAC-Konsole an, setzen Sie iDRAC zurück, warten Sie einige Minuten und aktualisieren Sie dann die Seite **Firmware-Aktualisierung**.

Unterstützt OMIVV ESXi mit aktiviertem Sperrmodus?

Ja. Der Sperrmodus wird in dieser Version auf ESXi 6.0 Hosts und höher unterstützt.

Beim Verwenden des Sperrmodus tritt ein Fehler auf

Als ich im Sperrmodus einen Host zum Host-Anmeldeprofil hinzugefügt habe, wurde eine Bestandsaufnahme gestartet, die jedoch mit der Meldung „Es wurde kein Remote Access Controller gefunden, oder auf diesem Host wird keine Bestandsaufnahme unterstützt“ fehlschlug.

Wenn Sie den Host in den Sperrmodus versetzen oder einen Host aus dem Sperrmodus entfernen, müssen Sie 30 Minuten warten, bevor Sie den nächsten Vorgang in OMIVV durchführen.

Versuch schlägt fehl, ESXi bei einem Serverausfall bereitzustellen

1. Stellen Sie sicher, dass der **ISO-Speicherort (NFS-Pfad)** und die **Pfade des Staging-Ordners** korrekt sind.
2. Stellen Sie sicher, dass das virtuelle Gerät während der Zuweisung der Serveridentität Zugriff auf die ausgewählte **NIC** hat.
3. Stellen Sie sicher, dass Sie die Verwaltungs-NICs basierend auf der Netzwerkverbindung mit dem OMIVV auswählen.
4. Stellen Sie bei Verwendung einer **statischen IP-Adresse** sicher, dass die angegebenen Netzwerkinformationen (einschließlich Subnetzmaske und Standard-Gateway) korrekt sind. Stellen Sie außerdem sicher, dass die IP-Adresse im Netzwerk nicht bereits zugewiesen wurde.
5. Stellen Sie sicher, dass mindestens eine virtuelle Festplatte, IDSDM oder BOSS vom System erkannt wird.

Automatisch ermittelte Systeme werden ohne Modellinformationen im Bereitstellungsassistenten angezeigt

Meist bedeutet dies, dass die auf dem System installierte Firmware-Version nicht die empfohlenen Mindestanforderungen erfüllt. In manchen Fällen wurde möglicherweise eine Firmware-Aktualisierung nicht vom System registriert.

Lösung: Durch einen Kalt-Neustart des Systems oder durch erneutes Einsetzen des Blades wird dieses Problem behoben. Das neu aktivierte Konto auf dem iDRAC muss deaktiviert und die automatische Ermittlung neu initiiert werden, um Modellinformationen und NIC-Informationen für OMIVV bereitzustellen.

Die NFS-Freigabe wurde mit dem ESXi-ISO-Image eingerichtet, die Bereitstellung schlägt jedoch mit Fehlern beim Laden des Freigabeortes fehl

Gehen Sie folgendermaßen vor, um die Lösung zu finden:

1. Stellen Sie sicher, dass der iDRAC einen Ping zum Gerät durchführen kann.
2. Stellen Sie sicher, dass Ihr Netzwerk nicht zu langsam ist.
3. Stellen Sie sicher, dass die Ports: 2049, 4001–4004 offen sind und die Firewall entsprechend eingestellt ist.

So wird ein OMIVV-Gerät zwangsweise aus dem vCenter entfernt

1. Gehen Sie zu vSphere Client und deaktivieren Sie das Kontrollkästchen für den Dell Anbieter für alle proaktiven HA-fähigen Cluster.
2. Wechseln Sie zu **https://<vCenter_Server-IP-Adresse>/mob**
3. Geben Sie die VMware vCenter Administrator-Anmeldeinformationen ein.
4. Klicken Sie auf **Startseite** > **Inhalt** > **HealthUpdateManager**.
5. Klicken Sie auf **QueryProviderList** > **Aufrufmethode**.
6. Kopieren Sie den Wert der Anbieter-ID-Zeichenkette und schließen Sie das Fenster.
7. Klicken Sie auf **UnregisterHealthUpdateProvider** und geben Sie den Wert für die kopierte Anbieter-ID ein.
8. Klicken Sie auf **Aufrufmethode**.
9. Gehen Sie zur **Startseite** > **Inhalt**
10. Klicken Sie auf **ExtensionManager**.
11. Klicken Sie auf **UnregisterExtension**.

12. Geben Sie den Erweiterungsschlüssel zur Deregistrierung von com.dell.plugin.openManage_integration_for_VMware_vCenter_WebClient ein und klicken Sie anschließend auf **Methode aufrufen**.
13. Schalten Sie OMIVV im vSphere-Client aus und löschen Sie es. Der Schlüssel zur Aufhebung der Registrierung muss für den vSphere-Client bestimmt sein.
14. Deaktivieren Sie in vCenter Serenity-Einträge und starten Sie den vCenter-Service neu.

Beim Eingeben eines Kennworts im Bildschirm „Jetzt sichern“ wird eine Fehlermeldung angezeigt.

Wenn Sie einen Monitor mit niedriger Auflösung verwenden, wird das Feld „Verschlüsselungskennwort“ nicht im Fenster JETZT SICHERN angezeigt. Scrollen Sie auf der Seite nach unten, um das Verschlüsselungskennwort einzugeben.

Was mache ich, wenn eine Aktualisierung fehlschlägt?

Prüfen Sie in den Protokollen der OMIVV-Appliance, ob bei den Aufgaben eine Zeitüberschreitung aufgetreten ist. Wenn dies der Fall ist, muss iDRAC durch einen Kalt-Neustart zurückgesetzt werden. Nach dem Hochfahren, und sobald das System ausgeführt wird, überprüfen Sie den Erfolg der Aktualisierung entweder durch Durchführen einer Bestandsaufnahme oder durch die Verwendung der Registerkarte **Firmware**.

Was kann ich tun, wenn die vCenter Registrierung fehlgeschlagen ist?

Die vCenter Registrierung kann aufgrund von Kommunikationsproblemen fehlschlagen. Falls diese Probleme auftreten, lassen sie sich durch die Verwendung einer statischen IP-Adresse lösen. Wenn Sie eine statische IP-Adresse verwenden möchten, wählen Sie auf der Registerkarte „Konsole“ des OpenManage Integration for VMware vCenter **Netzwerk konfigurieren** > **Geräte bearbeiten** und geben Sie das richtige **Gateway** und den **FQDN** (Fully Qualified Domain Name) ein. Geben Sie den DNS-Servernamen unter „DNS -Konfiguration bearbeiten“ ein.

ANMERKUNG: Stellen Sie sicher, dass die virtuelle Appliance den eingegebenen DNS-Server auflösen kann.

Die Leistung ist während des Tests der Anmeldeinformationen im Host-Anmeldeprofil langsam oder die Anwendung reagiert nicht.

Der iDRAC auf einem Server hat nur einen Benutzer (z. B. nur *root*) und der Benutzer befindet sich im Status „deaktiviert“, oder alle Benutzer befinden sich im Status „deaktiviert“. Die Kommunikation mit einem Server im deaktivierten Status verursacht Verzögerungen. Um dieses Problem zu beheben, können Sie entweder den deaktivierten Status des Servers aufheben oder den iDRAC auf dem Server zurücksetzen, um den Stammbenutzer erneut mit der Standardeinstellung zu aktivieren.

Gehen Sie wie nachfolgend beschrieben vor, um das Problem mit einem Server in einem deaktivierten Zustand zu beheben:

1. Öffnen Sie die Konsole „Chassis Management Controller“ und wählen Sie den deaktivierten Server aus.
2. Um die iDRAC-Konsole automatisch zu öffnen, klicken Sie auf **iDRAC-GUI starten**.
3. Navigieren Sie in der iDRAC-Konsole zur Benutzerliste, und klicken Sie auf eine der folgenden Optionen:
   - iDRAC7: Wählen Sie die Registerkarten **iDRAC-Einstellungen** > **Benutzer**.
   - iDRAC8: Wählen Sie die Registerkarten **iDRAC-Einstellungen** > **Benutzer**.
   - iDRAC9: Wählen Sie die Registerkarten **iDRAC-Einstellungen** > **Benutzer**.

   Für iDRAC 7 und 8:

   a. Um die Einstellungen zu bearbeiten, klicken Sie in der Spalte „Benutzer-ID“ auf den Link für den Admin-(Stamm-)Benutzer.
   b. Klicken Sie auf **Benutzer konfigurieren** und dann auf **Weiter**.
   c. Aktivieren Sie auf der Seite **Benutzerkonfiguration** für den ausgewählten Benutzer das Kontrollkästchen neben „Benutzer aktivieren“, und klicken Sie dann auf **Anwenden**.

   Für iDRAC9:

a. Wählen Sie den **Root**-Benutzer aus und klicken Sie auf **Aktivieren**.

Unterstützt OMIVV die VMware vCenter Server Appliance?

Ja, OMIVV unterstützt die VMware vCenter Server Appliance ab v2.1.

Ein Server kann als nicht konform mit dem CSIOR-Status „unbekannt“ angezeigt werden

Lösung: ein unbekannter CSIOR-Status zeigt einen nicht reagierenden iDRAC auf dem Host an. Manuelles Zurücksetzen des iDRAC auf dem Host behebt dieses Problem.

Betroffene Version: Alle

Der Firmware-Level wird nicht aktualisiert, obwohl ich eine Firmware-Aktualisierung mit der Option „Beim nächsten Neustart anwenden“ ausgeführt und das System neu gestartet habe.

Um die Firmware zu aktualisieren, führen Sie nach Abschluss des Neustarts eine Bestandsaufnahme auf dem Host aus. Gelegentlich kann es vorkommen, dass das Neustartereignis das Gerät nicht erreicht. Dann wird die Bestandsaufnahme nicht automatisch ausgelöst. In diesem Fall müssen Sie die Bestandsaufnahme manuell erneut ausführen, um die aktualisierten Firmware-Versionen zu ermitteln.

Der Host wird auch nach dem Entfernen des Hosts aus der vCenter Struktur weiterhin unter dem Gehäuse angezeigt.

Die Hosts unter dem Gehäuse werden als Teil des Gehäuseinventars identifiziert. Nach einer erfolgreichen Gehäuse-Bestandsaufnahme wird die Host-Liste unter dem Gehäuse aktualisiert. Der Host wird bis zur nächsten Ausführung der Gehäuse-Bestandsaufnahme unter dem Gehäuse angezeigt, selbst wenn der Host aus der vCenter Struktur entfernt wurde.

Nach der Sicherung und Wiederherstellung von OMIVV wurden die Alarmeinstellungen nicht wiederhergestellt.

Das Wiederherstellen der OMIVV Appliance-Sicherung stellt die Alarmeinstellungen nicht wieder her. In der OpenManage Integration for VMware GUI zeigt das Feld **Alarme und Events** die wiederhergestellten Einstellungen an.

Lösung: Ändern Sie auf der OMIVV-GUI auf der Registerkarte **Einstellungen** manuell die Einstellungen für **Ereignisse und Alarme**.

Die BS-Bereitstellung schlägt fehl, wenn NPAR auf einem Zielknoten aktiviert und im Systemprofil deaktiviert ist

Die BS-Bereitstellung schlägt fehl, wenn ein Systemprofil mit deaktivierter NIC-Partitionierung (NPAR) auf einem Zielrechner angewendet wird. Hierbei wird NPAR am Zielknoten und nur einer der partitionierten NIC aktiviert, außer wenn Partition 1 als NIC über den Bereitstellungs-Assistenten während des Bereitstellungsprozesses für die Verwaltungsaufgaben ausgewählt wird.

Lösung: Wenn Sie den NPAR-Status mithilfe des Systemprofils während der Bereitstellung ändern, stellen Sie sicher, dass Sie nur die erste Partition für das Verwaltungsnetzwerk im Bereitstellungsassistenten auswählen.

Betroffene Version: 4.1 und höher

Die verfügbare OMIVV-Geräteversion zeigt falsche Informationen an, wenn die verfügbare Version niedriger ist als die aktuelle Version.

In der OMIVV Admin-Konsole werden unter **Geräteverwaltung**, **Verfügbare virtuelle Geräteversion** die Modi RPM und OVF als verfügbar angezeigt.

ANMERKUNG: Es wird empfohlen, dass der Aktualisierungs-Repository-Pfad auf die aktuelle Version eingestellt und das Zurückstufen der Version des virtuellen Geräts nicht unterstützt wird.

Ausnahme 267027 wird beim Hinzufügen eines Bare-Metal-Servers der 12. Generation und höher ausgelöst

Während der Bare-Metal-Erkennung wird das Benutzerkonto automatisch ein paar Minuten gesperrt, wenn falsche Anmeldeinformationen eingegeben werden. Während dieses Zeitraums reagiert iDRAC nicht mehr und die Rückkehr zum Normalzustand dauert ein paar Minuten.

Lösung: Warten Sie einige Minuten und geben Sie die Anmeldeinformationen des Benutzers erneut ein.

Während der Bereitstellung schlägt das Anwenden des Systemprofils aufgrund eines iDRAC-Fehlers fehl

Während der Bereitstellung versucht OMIVV, den Konfigurationsaktualisierungs-Job in iDRAC zu erstellen. Die Erstellung dieses Jobs schlägt allerdings manchmal fehl und zeigt eine Meldung an, die angibt, dass der Konfigurationsjob bereits erstellt wurde.

Lösung: Löschen Sie die veralteten Einträge und wiederholen Sie die Bereitstellung. Melden Sie sich bei iDRAC an, um die Jobs zu löschen.

OMIVV RPM-Upgrade schlägt fehl, wenn Proxy mit Domain-Benutzerauthentifizierung konfiguriert ist

Wenn das OMIVV-Gerät für den Zugriff auf das Internet mit Proxy konfiguriert wurde und Proxy mit NTLM-Authentifizierung authentifiziert wird, schlägt die RPM-Aktualisierung aufgrund von Problemen im zugrunde liegenden yum-Tool fehl.

Betroffene Version: OMIVV 4.0 und höher

Lösung/Umgehungslösung: Führen Sie „Sichern und Wiederherstellen“ zum Aktualisieren des OMIVV Appliance aus.

Ein Systemprofil kann nicht angewendet werden, das eine PCIe-Erweiterungskarte im FX-Gehäuse hat.

Die BS-Bereitstellung schlägt auf einem Zielserver fehl, wenn dem Quellserver PCIe-Karteninformationen beim Verwenden eines FX-Gehäuse hat. Die Systemprofile auf dem Quellserver haben eine andere `fc.chassislot ID` als auf dem Zielserver. OMIVV versucht, dieselbe `fc.chassislot ID` auf dem Zielserver bereitzustellen. Dies schlägt jedoch fehl. Die Systemprofile suchen nach der genauen Instanz (FQDD) bei der Anwendung des Profils. Dies funktioniert auf Rack-Servern (identisch), hat jedoch evtl. bei modularen Servern einige Einschränkungen. Beim FC640 können beispielsweise die von einem modularen Server erstellten Systemprofile aufgrund von NIC-Level-Einschränkungen nicht auf anderen modularen Servern im selben FX Gehäuse angewendet werden.

Betroffene Version: 4.1 und höher.

Lösung: Das Systemprofil eines FC640 Servers in Steckplatz 1 eines FX2s Gehäuses kann nur auf einen anderen FC640 Server angewendet werden, der sich auf dem Steckplatz 1 eines anderen FX2s Gehäuses befindet.

Die Abweichungserkennung zeigt nicht kompatible modulare Server an, die im FX-Gehäuse über eine PCIe-Karte verfügen

Die Systemprofile suchen nach der genauen Instanz (FQDD) beim Vergleich mit der Baseline. Dies funktioniert auf Rack-Servern (identisch), hat jedoch evtl. bei modularen Servern einige Einschränkungen. Beim FC640 zeigt beispielsweise das von einem modularen Server erstellten Systemprofil (Baseline) aufgrund von falschen FQDD-Zuordnungen eine Abweichung für andere modulare Server im selben FX Gehäuse.

Betroffene Version: 4.1 und höher.

Lösung: Bei der Erstellung des Systemprofils müssen Sie die FQDDs löschen, die nicht mit den anderen Servern übereinstimmen.

Auf PowerEdge-Servern kann kein Betriebssystem bereitgestellt werden, wenn iDRAC die MAC-Adresse des ausgewählten NIC nicht anzeigt

Auf PowerEdge-Servern schlägt die Bereitstellung des Betriebssystems fehlt, wenn iDRAC die MAC-Adresse des ausgewählten NIC-Ports nicht anzeigt.

Lösung: Aktualisieren Sie die entsprechende NIC-Firmware sowie die iDRAC-Firmware auf die neueste Version und stellen Sie sicher, dass die MAC-Adresse am NIC-Port angezeigt wird.

Betroffene Version: 4.3 und höher

Beim Erstellen eines neuen Host-Anmeldeinformationenprofils für den Host mit ESXi 6.5U1 wird die Service-Tag-Nummer des Hosts nicht auf der Seite der ausgewählten Hosts angezeigt

Wenn OMIVV beim vCenter bezüglich der Service-Tag-Nummer von ESXi anfragt, kann das vCenter die Service-Tag-Nummer nicht ausgeben, weil der Wert der Service-Tag-Nummer Null ist.

Lösung: Aktualisieren Sie die ESXi-Version auf ESXi 6.5U2 oder ESXi 6.7U1.

Betroffene Version: 4.3 und höher

Das Dell EMC Symbol wird nach der Sicherung und Wiederherstellung einer früheren zu einer späteren OMIVV-Version nicht angezeigt.

Nach der Sicherung und Wiederherstellung von einer früheren OMIVV-Version zu einer späteren OMIVV-Version treten die folgenden Probleme auf:

- Das Dell EMC Logo wird in vCenter nicht angezeigt.
- Fehler 2000000
- Fehler 3001

  Auflösung:

  - Starten Sie den vSphere Client auf dem vCenter-Server neu.
  - Wenn das Problem weiterhin besteht:
    - Um zu VMware vCenter Server Appliance zu gelangen, gehen Sie zu `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity` und für Windows vCenter gehen Sie zum `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` Ordner im vCenter Gerät und prüfen Sie, ob die alten Daten vorhanden sind, wie beispielsweise: com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX.
    - Löschen Sie den Ordner für die frühere OMIVV-Version manuell.

Beim Aktualisieren oder Zurückstufen einiger iDRAC-Firmwareversionen über OMIVV meldet OMIVV möglicherweise, dass

der Auftrag fehlgeschlagen ist, obwohl die Firmwareaktualisierung erfolgreich durchgeführt wurde.

Wenn Sie iDRAC-Versionen wie z. B. 3.20.20.20, 3.21.21.21 und 3.21.21.22 während der Firmwareaktualisierung erweitern oder zurückstufen wird der Auftragsstatus als fehlgeschlagen gemeldet, obwohl der Auftrag erfolgreich durchgeführt wurde.

Lösung: Aktualisieren Sie die Bestandsaufnahme nach der Fehlermeldung und führen Sie den Auftrag bei anderen Komponenten neu aus.

Betroffene Version: 4.3

Beim Konfigurieren des Systems im Sperrmodus auf Cluster-Ebene wird gelegentlich die Meldung „Kein Host unter dem Cluster verfügt über eine erfolgreiche Bestandsaufnahme“ angezeigt.

Bei der Konfiguration des System-Sperrmodus auf einer Cluster-Ebene wird manchmal die Meldung „Unter dem Cluster konnte keine erfolgreiche Bestandsaufnahme durchgeführt werden“ angezeigt. Diese Meldung wird angezeigt, auch wenn das Cluster die von OMIVV verwalteten iDRAC9-basierten Servern erfolgreich inventarisiert hat. Eine Liste der iDRAC9-basierten Server finden Sie in der Compliance-Matrix.

Lösung: Starten Sie vCenter neu.

Um vCenter neuzustarten, gehen Sie wie folgt vor:

1. Melden Sie sich bei dem vSphere-Client mit einem vCenter Single Sign-On Administratorkonto an.
2. Gehen Sie auf **Verwaltung** > **Bereitstellung** > **Bereitstellung** > **Systemkonfiguration**.
3. Klicken Sie auf **Knoten**, wählen Sie den vCenter Server Appliance-Knoten, und klicken Sie auf die Registerkarte **Zugehörige Objekte**.
4. Starten Sie den vCenter-Knoten neu.

Manchmal werden bei der nachträglichen RPM-Aktualisierung des OMIVV-Geräts mehrere Einträge in den letzten Aufgaben des vCenter angezeigt.

Manchmal werden nach der RPM-Aktualisierung mehrere Einträge in den Protokollen der letzten Aufgaben des vCenter angezeigt.

Lösung: Starten Sie die Dienste in vCenter neu.

Betroffene Version: 4.3

Nach der Registrierung von vCenter wird das Dell EMC Logo von OMIVV nicht auf der Startseite von VMware angezeigt

Beschreibung: das Dell EMC Logo von OMIVV wird möglicherweise nicht auf der **Startseite** von VMware angezeigt, da VMware vCenter kurz nach Abschluss der Registrierung das Plug-in validieren wird.

Lösung: Führen Sie folgende Schritte aus:

1. Aktualisieren Sie den Browser, leeren Sie den Browser-Cache oder starten Sie die Client-Services für vSphere Client (HTML-5) neu.
2. Melden Sie sich vom vSphere Client ab und melden Sie sich dann erneut an.

Betroffene Version: 5.0

Nicht konforme 11G-PowerEdge-Server werden im OMIVV-Bestand nach der Sicherung und Wiederherstellung beibehalten.

Nach der Durchführung des Sicherungs- und Wiederherstellungsvorgangs in OMIVV sind die nicht konformen und nicht inventarisierten 11G-Hosts weiterhin dem Host-Anmeldeinformationenprofil zugeordnet. Wenn Sie jedoch versuchen, die Konfigurations-Compliance zu beheben und eine neue Bestandsaufnahme auszuführen, schlägt der Job auf den nicht unterstützten 11G-Servern fehl.

Lösung: 11G-Server werden von OMIVV 5.0 nicht unterstützt. Entfernen Sie die nicht unterstützten 11G-Hosts manuell aus dem Host-Anmeldeinformationenprofil.

Betroffene Version: 5.0

VCenter kann nach dem Upgrade des OMIVV-Geräts vom Flex-Client nicht gestartet werden

Lösung: Informationen zur Lösung finden Sie im VMware KB-Artikel: https://kb.vmware.com/s/article/54751.

Betroffene Version: 5.0

Beim Hinzufügen oder Entfernen von Netzwerkadaptern zu OMIVV verschwinden die vorhandenen NIC von der OMIVV-Konsole.

Wenn Sie einen Netzwerkadapter zum OMIVV-Gerät mithilfe des vSphere-Client hinzufügen oder von ihm entfernen, verschwinden die vorhandenen NIC manchmal von der OMIVV-Konsole.

Umgehung: Führen Sie eine der folgenden Aufgaben durch:

1. a. Entfernen Sie alle Arbeitsadapter vom Terminal-Konsolendienstprogramm.
   b. Fahren Sie das Gerät herunter.
   c. Entfernen Sie die Netzwerkadapter vom Gerät.
   d. Führen Sie einen Neustart des OMIVV-Geräts durch.
   e. Fahren Sie das Gerät herunter.
   f. Fügen Sie den/die erforderlichen Netzwerkadapter hinzu und schließen Sie die Konfiguration der Netzwerkadapter ab.
   g. Starten Sie das Gerät neu.
2. a. Sichern Sie OMIVV über das Admin-Portal.
   b. Erstellen Sie ein OMIVV-Gerät.
   c. Fahren Sie das Gerät herunter.
   d. Fügen Sie den/die erforderlichen Netzwerkadapter hinzu und schließen Sie die Konfiguration der Netzwerkadapter ab.
   e. Starten Sie das Gerät neu.
   f. Stellen Sie die neuesten gesicherten Daten wieder her.

Betroffene Version: OMIVV 5.0

Nach dem Hinzufügen oder Entfernen des zweiten NIC werden auf der Seite „Netzwerkkonfiguration“ drei NIC angezeigt.

Nach dem Hinzufügen oder Entfernen eines NIC über das OMIVV-Gerät unter Verwendung des vSphere-Clients zeigt die Seite **Netzwerkkonfiguration** nach dem Starten des OMIVV-Geräts und der Anmeldung bei der OMIVV-Terminalkonsole manchmal eine inkonsistente Anzahl von NIC an.

Lösung: Verwenden Sie die MAC-Adresse, um die korrekten NIC zu vergleichen und zu konfigurieren und verwenden Sie die Schaltfläche **–** , um die zusätzlichen NIC zu entfernen.

Betroffene Version: 5.0

Ein Server mit unbekanntem Status in der älteren Version ist auf der Bare-Metal-Server-Seite nach der Sicherung und Wiederherstellung auf eine neueste OMIVV-Version nicht aufgeführt.

Nach der Wiederherstellung einer Sicherung aus früheren Versionen werden nicht unterstützte Server (11G und früher) aus dem Bare-Metal-Bestand entfernt. Server, deren Generation nicht von der früheren Version vor der Sicherung bestimmt wurde, werden ebenfalls entfernt.

Lösung: Ermitteln Sie den Server erneut. Wenn der fehlende Server unterstützt wird, wird er im Bare-Metal-Bestand aufgeführt.

Betroffene Version: 5.0

Nach der BS-Bereitstellung konnte OMIVV ESXi-Host nicht zu vCenter hinzufügen oder ein Host-Profil konnte nicht hinzugefügt werden oder der Wartungsmodus für den Host ist fehlgeschlagen.

Nach der BS-Bereitstellung veranlasst OMIVV, dass vCenter die Host-Aktionen durchführt (Host hinzufügen, Hostprofil hinzufügen oder in den Wartungsmodus wechseln). Wenn die Abfrage innerhalb von zwei Minuten keine Antwort erhält, liegt eine Zeitüberschreitung für bestimmte Aktion auf vCenter vor und im Aufgabenverlauf wird eine Meldung angezeigt, die darauf hinweist, dass die Kommunikation fehlgeschlagen ist. Allerdings sind die vCenter-Abfragevorgänge manchmal erfolgreich.

Lösung: Nehmen Sie die Host-IP aus dem Aufgabenverlauf und fügen Sie sie manuell hinzu.

Der iDRAC-Lizenzstatus wird auf der Seite „Verwaltungs-Compliance“ als konform angezeigt, wenn die IP-Adresse des iDRAC nicht erreichbar ist.

Wenn der iDRAC nicht erreichbar ist, wird nach der Durchführung einer periodischen Bestandsaufnahme der iDRAC-Lizenzstatus auf der Seite „Verwaltungs-Compliance“ als konform angezeigt.

Lösung: Stellen Sie sicher, dass der iDRAC erreichbar ist und führen Sie die Bestandsaufnahme erneut aus, um die richtigen iDRAC-Lizenzdetails zu erhalten.

ESXi-Host ist nach erfolgreicher BS-Bereitstellung unter Verwendung von OMIVV entweder getrennt oder antwortet nicht

ESXi-Host kann keine Heartbeat-Pakete an vCenter senden, da seine DNS nicht ordnungsgemäß für das Nachschlagen des FQDN des vCenter konfiguriert ist.

Lösung: Führen Sie folgende Schritte aus:

1. Entfernen Sie den ESXi-Host aus dem vCenter-Inventar.
2. Fügen Sie die Hosts mithilfe des Assistenten **Host hinzufügen** hinzu.
3. Erstellen Sie ein Gehäuse-Anmeldeinformationenprofil und führen Sie die Bestandsaufnahme durch.

Zeitüberschreitung bei der Bereitstellung, wenn die Netzwerkschnittstellenkarte (NIC) von OMIVV nicht mit dem ESXi-Host-Netzwerk verbunden ist

Die BS-Bereitstellung hängt von der Auswahl der NIC ab. Wenn nicht die richtige NIC ausgewählt ist, tritt für den OSD-Job eine Zeitüberschreitung auf.

Lösung: Wählen Sie auf der Seite „Host-Einstellungen konfigurieren“ des Bereitstellungsassistenten die entsprechende Option „Mit dem Host verbundene Geräte-NIC“ aus. Diese wird von OMIVV benötigt, um das ESXi-Netzwerk während der BS-Installation zu erreichen.

Service-Job für bestimmte Hosts wird nicht ausgeführt

Wenn Sie in einer PSC-Umgebung mit mehreren vCenter einen Host über FQDN zu einem vCenter und über eine IP-Adresse zu einem anderen vCenter hinzufügen, wird der Service-Job nur für eine Host-Instanz ausgeführt.

Lösung: Entfernen Sie die getrennte Hostinstanz aus dem Host-Anmeldeinformationenprofil und führen Sie den Bestandsaufnahme- und Service-Job aus.

Betroffene Version: 5.0

Die proaktive HA-Initialisierung erfolgt nach der Durchführung von Sicherungen und Wiederherstellungen nicht

Beim Wiederherstellen von OMIVV aus der vorherigen Version, die beim vSphere-Client registriert ist, wird für proaktive-HA-fähige Cluster der Dell Anbieter getrennt.

Lösung: Deaktivieren und aktivieren Sie die proaktive HA für Cluster.

Betroffene Version: 5.0

OMIVV-Seite zeigt ungültige Sitzung oder Zeitüberschreitungs-Ausnahmefehler oder 2-Millionen-Fehler im Firefox-Browser an

Wenn die OMIVV-Seite eine Zeit lang inaktiv ist (5 bis 10 Minuten), wird der ungültige Sitzungs-, Zeitüberschreitungs-Ausnahme- oder 2-Millionen-Fehler angezeigt.

Lösung: Aktualisieren Sie den Browser. `Wenn das Problem weiterhin besteht, melden Sie sich ab und melden Sie sich über vCenter an.`

Um die korrekten Daten in OMIVV zu sehen, stellen Sie sicher, dass Sie die in der Lösung aufgeführte Aufgabe durchführen.

Betroffene Version: 5.0

In vCenter wird im Bereich „Letzte Tasks“ die Spalte „Details“ für einige OMIVV-Task-Benachrichtigungen nicht angezeigt

Lösung: um die Task-Benachrichtigungen anzuzeigen, öffnen Sie die **Task-Konsole** in vCenter.

Betroffene Version: 5.0

Bei Verwendung vCenter 6.5 U2 kann der Fehler 2000002 auf allen Seiten von OMIVV angezeigt werden.

Lösung: Verwenden Sie das neueste Update von VMware für 6.5 U2 oder migrieren Sie auf 6.5 U3 und neuere Versionen.

Betroffene Version: 5.1

Der Fehler 2000002 wird auf allen Seiten von OMIVV nach der Durchführung von RPM-Aktualisierungen oder -Sicherungen und -Wiederherstellungen von einer früheren OMIVV-Version auf eine neuere OMIVV-Version angezeigt.

Wenn Sie eine frühere Version von OMIVV in vCenter Server haben, wird vor der Registrierung der aktuellen Version eine SSL-Handshake-Ausnahme veranlasst, dass die neue Version von OMIVV nicht erreichbar ist, bis vCenter die neuen Plug-ins aktualisiert. Denn das vCenter enthält die Daten aus der früheren Version von OMIVV, die den SSL-Verkehr anders behandelt.

Auflösung:

- Starten Sie den vSphere Client auf dem vCenter-Server neu.
- Wenn das Problem weiterhin besteht:
  - Für VMware vCenter Server Appliance rufen sie den Ordner `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity` und für Windows vCenter den Ordner `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` auf dem vCenter Gerät auf und prüfen Sie, ob die alten Daten vorhanden sind, beispielsweise: com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX.
  - Löschen Sie den Ordner für die frühere OMIVV-Version manuell.
  - Neustart von vSphere Client-Services für vSphere Client (HTML5)

Betroffene Version: 5.0 und später

Manchmal nimmt die Aufhebung der Registrierung des vCenter von OMIVV viel Zeit in Anspruch.

Wenn Sie die Registrierung des vCenter mit einer großen Anzahl von Hosts aufheben (über 300), verbleibt OMIVV für lange Zeit im Ladezustand.

Lösung: Aktualisieren Sie den Browser.

Wenn die Aufhebung der Registrierung von vCenter fehlgeschlagen ist, heben Sie die Registrierung des vCenter erneut auf.

Betroffene Version: 5.1

Nach der Aktualisierung des OMIVV-Zertifikats wird die Fehlermeldung „Verbindung zur OMIVV-Appliance fehlgeschlagen. Das SSL-Zertifikat ist ungültig.“ angezeigt.

Lösung: Starten Sie den Client-Service in vCenter neu.

Betroffene Version: Alle

Bereitstellungs-Job schlägt in OMIVV fehl.

Der Bereitstellungs-Job schlägt fehl, weil der Lifecycle Controller mit ausstehenden oder anderen Jobs beschäftigt ist.

Lösung: Führen Sie folgende Schritte aus:

1. Löschen Sie die iDRAC-Job-Warteschlange in iDRAC [optional].
2. iDRAC zurücksetzen
3. Führen Sie den Bereitstellungs-Job erneut aus.

Betroffene Version: Alle

Testverbindung und Bestandsaufnahme in OMIVV nach der Änderung des vCenter-Kennworts fehlgeschlagen

Für ESXi Version 6.7 und höher ruft OMIVV eine iDRAC-IP-Adresse vom ESXi-Host über das Intelligent Platform Management Interface (IPMI)-Protokoll ab. Dieser Vorgang ist nicht von WBEM abhängig.

Wenn OMIVV eine iDRAC-IP aus irgendeinem Grund nicht abrufen kann, verwendet OMIVV das Common Information Model (CIM)-Protokoll (als Fallback), welches vom WBEM-Status abhängig ist. Wenn das Kennwort für vCenter Nutzer, das für die Registrierung verwendet wird, geändert wird, können Sie ein WBEM-bezogenes Problem beim Ausführen von Testverbindung und -bestand beobachten.

Lösung: Modifizieren Sie nach dem Ändern des vCenter-Kennworts die vCenter-Zugangsdaten in der OMIVV-Verwaltungskonsole, bevor Sie einen Vorgang in vCenter durchführen. Weitere Informationen zur Änderung von Zugangsdaten finden Sie unter vCenter-Anmeldeinformationen ändern auf Seite 16.

Betroffene Version: Alle

Die OMIVV-Instanz wird nach dem Zurücksetzen der OMIVV-Appliance auf die Werkseinstellungen nicht aus vCenter entfernt.

Dieses Problem tritt auf, wenn Sie die Appliance auf die Werkseinstellungen zurücksetzen. Der OMIVV-Geräteeintrag verbleibt im `vsphere-client-serenity` Ordner von vCenter, der die vCenter-Registrierung nach dem Zurücksetzen auf die Werkseinstellungen verhindert.

Lösung: Entfernen Sie den OMIVV-Eintrag aus dem vCenter. Weitere Informationen finden Sie unter So wird ein OMIVV-Gerät zwangsweise aus dem vCenter entfernt auf Seite 162.

Betroffene Version: Alle

OMIVV zeigt nur BIOS- und iDRAC-Attribute auf der Seite für Profileinstellungen des Systemprofils an.

Lösung: Aktualisieren Sie Google Chrome auf die neueste Version.

Betroffene Version: 5.2

Die BS-Bereitstellung wurde mit unbekanntem Fehler abgeschlossen.

Dieses Problem tritt auf, wenn Sie die BS-Bereitstellung mit einem anderen Nutzer als dem Nutzer durchführen, der zur Ermittlung des Servers verwendet wird. Die Fehlermeldung auf der Seite OMIVV **Protokolle** zeigt den Fehler an, dass die Klasse nicht gefunden wurde.

Lösung: Nicht zutreffend. Dieses Problem wirkt sich nicht auf die Funktionalität der OMIVV-Funktionen aus.

Betroffene Version: 5.2

Chassis Management Controller (CMC)-Firmware-Updates schlägt im FX2-Gehäuse fehl

OMIVV ermöglicht Ihnen die Aktualisierung der FX2-Gehäuse -CMC-Firmware über die Server iDRAC. Die CMC-Firmware-Update schlägt fehl, wenn die Option **CMC-Aktualisierungen über BS und Lifecycle Controller zulassen** in iDRAC deaktiviert ist.

Antwort: Führen Sie folgende Schritte in iDRAC aus:

1. Navigieren Sie zu **Einstellungen** > **Update und Rollback**.
2. Setzen Sie die Option **CMC-Aktualisierungen über BS und Lifecycle Controller zulassen** auf **Aktiviert**.

Betroffene Version: 5.2

Die Bereitstellung des ISO-Profils schlägt in OMIVV fehl

Der Job zur Bereitstellung des ISO-Profils, der mit einer älteren Version von OMIVV geplant ist, ist in der neuesten Version von OMIVV nicht gültig.

Lösung: Brechen Sie den geplanten Job ab und erstellen Sie einen Bereitstellungs-Job nach Bedarf.

Der Bereitstellungs-Job schlägt fehl, wenn der geplante Job nicht abgebrochen wird. In diesem Fall müssen Sie den Server als Bare-Metal- und ISO-Profil-Bereitstellungs-Job erstellen.

Betroffene Version: 5.2

Probleme bei der Bare-Metal-Bereitstellung

In diesem Abschnitt werden Probleme behandelt, die während des Bereitstellungsprozesses auftreten könnten.

Voraussetzungen für Auto-Ermittlung und Handshake

- Bevor Sie Auto-Ermittlung und Handshake ausführen können, müssen Sie sicherstellen, dass die Versionen der iDRAC- und Lifecycle-Controller-Firmware sowie des BIOS die Mindestempfehlungen erfüllen.
- CSIOR muss mindestens einmal auf dem System oder iDRAC ausgeführt worden sein.

Hardware-Konfigurationsfehler

- Achten Sie vor der Initialisierung einer Bereitstellungsaufgabe darauf, dass das System CSIOR abgeschlossen hat und nicht gerade neu gestartet wird.
- Die BIOS-Konfiguration sollte im Klonmodus ausgeführt werden, sodass der Referenzserver ein identisches System ist.
- Manche Controller lassen die Erstellung eines RAID 0 Arrays mit nur einem Laufwerk nicht zu. Diese Funktion wird nur auf High-End-Controllern unterstützt und die Anwendung eines solchen Hardwareprofils kann zu Fehlern führen.

Aktivieren der automatischen Ermittlung auf einem neu erworbenen System

Die Funktion für die automatische Ermittlung eines Hostsystems ist nicht standardmäßig aktiviert. Diese Aktivierung muss zum Zeitpunkt des Kaufs angefordert werden. Wenn die Aktivierung der automatischen Ermittlung zum Zeitpunkt des Kaufs angefordert wird, wird DHCP auf dem iDRAC aktiviert und die Administratorkonten werden deaktiviert. Es ist nicht erforderlich, eine statische IP-Adresse für den iDRAC zu konfigurieren. Diese wird von einem DHCP-Server im Netzwerk abgerufen. Um die Funktion für die automatische Ermittlung zu verwenden, muss ein DHCP-Server oder ein DNS-Server (oder beides) zur Unterstützung des Ermittlungsprozesses konfiguriert werden. CSIOR sollte bereits werksseitig ausgeführt worden sein.

Falls die Auto-Ermittlung nicht zum Zeitpunkt des Kaufs angefordert wurde, kann sie wie folgt aktiviert werden:

1. Drücken Sie während des Startvorgangs **Ctrl+E**.
2. Aktivieren Sie im iDRAC-Setupfenster die NIC (nur Blade-Server).
3. Aktivieren Sie die automatische Ermittlung.
4. Aktivieren Sie DHCP.
5. Deaktivieren Sie die Administratorkonten.
6. Aktivieren Sie **DNS-Serveradresse vom DHCP abrufen**.
7. Aktivieren Sie **DNS-Domänenname vom DHCP abrufen**.
8. Geben Sie in das Feld **Bereitstellungsserver** Folgendes ein:

```
<OpenManage Integration virtual appliance IPaddress>:4433
```

A

Systemspezifische Attribute

iDRAC

Tabelle 28. Systemspezifische Attribute – iDRAC

Attributname	Anzeigeattributname	Gruppen-Anzeigename
DNS-RAC-Name	DNS-RAC-Name	NIC-Informationen
DataCenterName	Name des Datenzentrums	Server-Topologie
Name des Gangs	Name des Gangs	Server-Topologie
Rack-Name	Rack-Name	Server-Topologie
Rack-Steckplatz	Rack-Steckplatz	Server-Topologie
RacName	Active Directory-RAC-Name	Active Directory
Adresse	IPv4-Adresse	Statische IPv4-Informationen
Netzwerkmaske	Netzwerkmaske	Statische IPv4-Informationen
Gateway	Gateway	Statische IPv4-Informationen
DNS2	DNS-Server 2	Statische IPv4-Informationen
Adresse 1	IPv6-Adresse 1	Statische IPv6-Informationen
Gateway	IPv6-Gateway	Statische IPv6-Informationen
Präfixlänge	IPV6-Link-Local-Präfixlänge	Statische IPv6-Informationen
DNS1	IPV6-DNS-Server 1	Statische IPv6-Informationen
DNS2	IPv6-DNS-Server 2	Statische IPv6-Informationen
DNSFromDHCP6	DNS-Server aus DHCP6	Statische IPv6-Informationen
HostName	Server-Hostname	Server-Betriebssystem
RoomName	RoomName	Server-Topologie
NodeID	Systemknoten-ID	Server-Informationen

BIOS

Tabelle 29. Systemspezifische Attribute für BIOS

Attributname	Anzeigeattributname	Gruppen-Anzeigename
AssetTag	Asset Tag	Verschiedene Einstellungen
IscsiDev1con1Gateway	Initiator-Gateway	Einstellungen für Verbindung 1
IscsiDev1con1IP-	Initiator IP Address (Initiator-IP-Adresse)	Einstellungen für Verbindung 1
IscsiDev1Con1Mask	Initiator-Subnetzmaske	Einstellungen für Verbindung 1
IscsiDev1Con1TargetIp	Ziel-IP-Adresse	Einstellungen für Verbindung 1

Tabelle 29. Systemspezifische Attribute für BIOS (fortgesetzt)

Attributname	Anzeigeattributname	Gruppen-Anzeigename
IscsiDev1Con1TargetName	Zielname	Einstellungen für Verbindung 1
IscsiDev1Con2Gateway	Initiator-Gateway	Einstellungen für Verbindung 1
IscsiDev1Con2Ip	Initiator-IP-Adresse	Einstellungen für Verbindung 1
IscsiDev1Con2Mask	Initiator-Subnetzmaske	Einstellungen für Verbindung 1
IscsiDev1Con2TargetIp	Ziel-IP-Adresse	Einstellungen für Verbindung 1
IscsiDev1Con2TargetName	Zielname	Einstellungen für Verbindung 1
iscsiInitiatorName	iSCSI Initiator-Name	Netzwerkeinstellungen
Ndc1PcieLink1	PCIe-Link 1 für integrierte Netzwerkkarte 1	Integrierte Geräte
Ndc1PcieLink2	PCIe-Link 2 für integrierte Netzwerkkarte 1	Integrierte Geräte
Ndc1PcieLink3	PCIe-Link 3 für integrierte Netzwerkkarte 1	Integrierte Geräte
UefiBootSeq	UEFI-Startsequenz	UEFI-Starteinstellungen

RAID

Tabelle 30. Systemspezifische Attribute für RAID

Attributname	Anzeigeattributname	Gruppen-Anzeigename
Angeforderter Gehäusekonfigurationsmodus	-	-
Aktueller Gehäusekonfigurationsmodus	-	-

CNA

Tabelle 31. Systemspezifische Attribute für CNA

Attributname	Anzeigeattributname	Gruppen-Anzeigename
ChapMutualAuth	Gegenseitige CHAP-Authentifizierung	Allgemeine iSCSI-Parameter
ConnectFirstTgt	Verbinden	Parameter für erstes iSCSI-Ziel
ConnectSecondTgt	Verbinden	Parameter für zweites iSCSI-Ziel
FirstFCoEBootTargetLUN	Start-LUN	FCoE-Konfiguration
FirstFCoEWWPNTarget	Ziel für World Wide Port Name	FCoE-Konfiguration
FirstTgtBootLun	Start-LUN	Parameter für erstes iSCSI-Ziel
FirstTgtChapId	CHAP-ID	Parameter für erstes iSCSI-Ziel
FirstTgtChapPwd	CHAP-Geheimschlüssel	Parameter für erstes iSCSI-Ziel
FirstTgtIpAddress	IP-Adresse	Parameter für erstes iSCSI-Ziel
FirstTgtIscsiName	iSCSI-Name	Parameter für erstes iSCSI-Ziel
FirstTgtTcpPort	TCP-Anschluss	Parameter für erstes iSCSI-Ziel
IP-Autokonfiguration	IpAutoConfig	Allgemeine iSCSI-Parameter
IscsiInitiatorChapId	CHAP-ID	iSCSI Initiator-Parameter
IscsiInitiatorChapPwd	CHAP-Geheimschlüssel	iSCSI Initiator-Parameter

Tabelle 31. Systemspezifische Attribute für CNA (fortgesetzt)

Attributname	Anzeigeattributname	Gruppen-Anzeigename
IscsiInitiatorGateway	Standard-Gateway	iSCSI Initiator-Parameter
IscsiInitiatorIpAddr	IP-Adresse	iSCSI Initiator-Parameter
IscsiInitiatorIpv4Addr	IPv4-Adresse	iSCSI Initiator-Parameter
IscsiInitiatorIpv4Gateway	IPv4-Standard-Gateway	iSCSI Initiator-Parameter
IscsiInitiatorIpv4PrimDns	IPv4 primäre DNS	iSCSI Initiator-Parameter
IscsiInitiatorIpv4SecDns	IPv4 sekundäre DNS	iSCSI Initiator-Parameter
IscsiInitiatorIpv6Addr	IPv6-Adresse	iSCSI Initiator-Parameter
IscsiInitiatorIpv6Gateway	IPv6-Standard-Gateway	iSCSI Initiator-Parameter
IscsiInitiatorIpv6PrimDns	IPv6 primäre DNS	iSCSI Initiator-Parameter
IscsiInitiatorIpv6SecDns	IPv6 sekundäre DNS	iSCSI Initiator-Parameter
iscsiInitiatorName	iSCSI-Name	iSCSI Initiator-Parameter
IscsiInitiatorPrimDns	Primärer DNS-Server	iSCSI Initiator-Parameter
IscsiInitiatorSecDns	Sekundärer DNS-Server	iSCSI Initiator-Parameter
IscsiInitiatorSubnet	Subnetzmaske	iSCSI Initiator-Parameter
IscsiInitiatorSubnetPrefix	Subnetzmasken-Präfix	iSCSI Initiator-Parameter
SecondaryDeviceMacAddr	MAC-Adresse des sekundären Geräts	Parameter für sekundäres iSCSI-Gerät
SecondTgtBootLun	Start-LUN	Parameter für zweites iSCSI-Ziel
SecondTgtChapPwd	CHAP-Geheimschlüssel	Parameter für zweites iSCSI-Ziel
SecondTgtIpAddress	IP-Adresse	Parameter für zweites iSCSI-Ziel
SecondTgtIscsiName	iSCSI-Name	Parameter für zweites iSCSI-Ziel
SecondTgtTcpPort	TCP-Anschluss	Parameter für zweites iSCSI-Ziel
UseIndTgtName	Unabhängigen Zielnamen verwenden	Parameter für sekundäres iSCSI-Gerät
UseIndTgtPortal	Unabhängiges Zielportal verwenden	Parameter für sekundäres iSCSI-Gerät
VirtFIPMacAddr	Virtuelle FIP-MAC-Adresse	Haupt-Konfigurationsseite
VirtIscsiMacAddr	Virtuelle iSCSI Offload MAC-Adresse	Haupt-Konfigurationsseite
VirtMacAddr	Virtuelle MAC-Adresse	Haupt-Konfigurationsseite
VirtMacAddr[Partition:n]	Virtuelle MAC-Adresse	Konfiguration der Partition n
VirtWWN	Virtueller World Wide Knotenname	Haupt-Konfigurationsseite
VirtWWN[Partition:n]	Virtueller World Wide Knotenname	Konfiguration der Partition n
VirtWWPN	Virtueller World Wide Schnittstellenname	Haupt-Konfigurationsseite
VirtWWPN[Partition:n]	Virtueller World Wide Schnittstellenname	Konfiguration der Partition n
Weltweiter Knotenname	WWN	Haupt-Konfigurationsseite
Weltweiter Knotenname	WWN[Partition:n]	Konfiguration der Partition n

FC

Tabelle 32. Systemspezifische Attribute für FC

Attributname	Anzeigeattributname	Gruppen-Anzeigename
VirtualWWN	Virtueller World Wide Knotenname	Port-Konfigurationsseite
VirtualWWPN	Virtueller World Wide Schnittstellenname	Port-Konfigurationsseite

B

Weitere Informationen

Die folgenden technischen Dell Whitepaper, die unter **www.delltechcenter.com** verfügbar sind, stellen weitere Informationen über die Systemprofil-Konfigurationsvorlage, Attribute und den Workflow bereit:

- *Erstellen von Server-Klonen mit Serverkonfigurationsprofilen*
- *Serverkonfigurations-XML-Datei*
- *Konfiguration-XML-Workflow*
- *Konfigurations-XML-Workflow-Skripte 133*
- *XML-Konfigurationsdateibeispiele*

C

Anpassungsattribute

Tabelle 33. Anpassungsattribute

FQDD	Attribute	Anpassung von OMIVV
BIOS	Virtualisierungstechnologie	Immer aktiviert
iDRAC	Systeminventar beim Neustart erfassen	Immer aktiviert
RAID	IncludedPhysicalDiskID	Wenn der Wert von IncludedPhysicalDiskID auf automatische Auswahl gesetzt ist, entfernen wir diesen Wert
RAID	RAIDPDState	Entfernt
iDRAC	Benutzer-Admin-Kennwort Kennwort	Nur für iDRAC freigeschaltete Benutzer verfügen über einen „Password“-Link zur Eingabe des Kennworts.
PCIeSSD	PCIeSSDSecureErase	Immer deaktiviert

D

Vergleich von Komponenten- und Baseline-Version - Matrix

Tabelle 34. Vergleich von Komponenten- und Baseline-Version - Matrix

Abweichungstyp				
Hardware	**Zugeordneter Basisplan**	**Zielkomponente**	**Szenario**	**Übereinstimmungsstatus**
	Verfügbar	Verfügbar	Die Hardware-Komponente stimmt mit der zugehörigen Baseline überein.	Konform
	Verfügbar	Verfügbar	Die Hardwareattribute der Komponente stimmen nicht mit der zugehörigen Baseline überein.	Nicht konform
	Nicht verfügbar	Verfügbar	Der Vergleichsstatus wird nicht berechnet oder ignoriert.	Konform
	Verfügbar	Nicht verfügbar	Die Hardware-Komponente ist in der zugehörigen Baseline verfügbar, die Komponente oder das Attribut sind jedoch im Host nicht verfügbar.	Nicht konform
	Nicht verfügbar	Nicht verfügbar	Der Vergleichsstatus wird nicht berechnet oder ignoriert.	Konform
Firmware	**Zugeordneter Basisplan**	**Zielkomponente**	**Szenario**	**Übereinstimmungsstatus**
	Verfügbar	Verfügbar	Die Version der Firmware-Komponente stimmt mit der zugehörigen Baseline überein.	Konform
	Verfügbar	Verfügbar	Die Version der Firmware-Komponente stimmt nicht mit der zugehörigen Baseline überein.	Nicht konform
	Nicht verfügbar	Verfügbar	Die Version der Firmware-Komponente ist in der zugehörigen Baseline nicht verfügbar, die Komponente ist jedoch im Host verfügbar. Der Vergleichsstatus wird nicht berechnet oder ignoriert.	Konform
	Verfügbar	Nicht verfügbar	Der Vergleichsstatus wird nicht berechnet oder ignoriert.	Konform
	Nicht verfügbar	Nicht verfügbar	Der Vergleichsstatus wird nicht berechnet oder ignoriert.	Konform
Treiber	**Zugeordneter Basisplan**	**Zielkomponente**	**Szenario**	**Übereinstimmungsstatus**
	Verfügbar	Verfügbar	Die Version der Treiberkomponente stimmt mit der zugehörigen Baseline überein.	Konform

Tabelle 34. Vergleich von Komponenten- und Baseline-Version - Matrix (fortgesetzt)

Abweichungstyp				
	Verfügbar	Verfügbar	Die Version der Treiberkomponente stimmt nicht mit der zugehörigen Baseline überein.	Nicht konform
	Nicht verfügbar	Verfügbar	Der Vergleichsstatus wird nicht berechnet oder ignoriert.	Konform
	Verfügbar	Nicht verfügbar	Die Version der Hardware-Komponente ist in der zugehörigen Baseline verfügbar, die Komponente ist jedoch im Host verfügbar.	Nicht konform
	Nicht verfügbar	Nicht verfügbar	Der Vergleichsstatus wird nicht berechnet oder ignoriert.	Konform

E

Antwortcodes

Tabelle 35. Antwortcodes

Antwortcodes	Beschreibung
200	Erfolgreiche Erzeugung/Rückgabe von Aufgabeninformationen oder Aufgabenliste.
202	Erfolgreicher Start einer Aufgabe.
400	Ungültige Anfrage
401	Unbefugte Anfrage
404	Nicht gefunden
409	Konflikt
500	Interner Serverfehler
503	Dienst nicht verfügbar