OpenManage Integration for VMware vCenter Version 4.2

Benutzerhandbuch Web Client

April 2018
Rev. A00

Anmerkungen, Vorsichtshinweise und Warnungen

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

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

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

Inhaltsverzeichnis

1

Einführung

IT-Administratoren verwenden VMware vCenter als primäre Konsole zur Verwaltung und Überwachung von VMware vSphere-ESX/ESXi-Hosts. OpenManage Integration for VMware vCenter (OMIVV) ermöglicht eine bessere Verwaltung der Dell Hosts auf den VMware Web-Clients, denn es stehen erweiterte Funktionen für die Bereitstellung, Verwaltung, Überwachung und Aktualisierung zur Verfügung.

Themen:

Neues in dieser Version

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

- Vorhandenes Cluster Aware Update wurde verbessert und unterstützt jetzt vSAN Cluster. Unterstützt Treiber und Firmware-Aktualisierungen.
- Möglichkeit für Baseline vSAN Cluster für Treiber-, Firmware- und Hardwarekonfiguration und Abweichungserkennung
- Möglichkeit zum Einschließen/Ausschließen von Attributen für Systemprofile
- Unterstützung für Plattformen der 14. Generation
- Unterstützung für SMB2 CIFS-Shares
- Unterstützung für OMSA 9.1
- Unterstützung für vSphere 6.7

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 Speichermenge und -typ, NIC, PSU, Prozessoren, RAC, Serviceinformationen, Ansicht auf Server-, Cluster- und Rechenzentrumsebene ● Gehäusedetails, z. B. Informationen zum Gehäuse-Verwaltungscontroller, Gehäusenetzteil, KVM-Status, Lüfter-/Wärmeinformationen, Serviceinformationen, Informationen zu Leere Switches/Server.
Überwachen und Senden von Warnungen	Die Überwachung und die Warnmeldungen umfassen folgende Funktionalitäten: ● 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, Alarmen zur Diagnose von Serverproblemen. ● Unterstützung für die Funktion VMware HA ProActive.

Tabelle 1. OMIVV-Funktionen (fortgesetzt)

Funktionen	Beschreibung
Firmware-Aktualisierungen	Die Firmware-Aktualisierung umfasst Folgendes: ● Aktualisieren der Dell EMC Hardware auf die aktuellste Version des BIOS und der Firmware. ● Die aktuelle clusterfähige Aktualisierungsfunktion wurde erweitert, um vSAN Cluster zu unterstützen, wenn die DRS-Option aktiviert ist. Die erweiterte Funktion unterstützt auch die Aktualisierung des Treibers und der Firmware von vSAN Clustern.
Bereitstellung	Erstellen von Hardwareprofilen (11. bis 13. Generation von PowerEdge Servern), Systemprofilen (14. Generation von Servern), Hypervisor-Profilen und Remote-Bereitstellung des BS auf PowerEdge Bare-Metal-Servern mit dem VMware vCenter, ohne Einsatz 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 Servern der 14. Generation.

ANMERKUNG: Ab OMIVV 4.0 wird nur der VMware vSphere Web-Client unterstützt, und der vSphere Desktop-Client wird nicht unterstützt.

ANMERKUNG: Für vCenter 6.5 und höher ist die OMIVV-Appliance nur für die Flash-Version verfügbar. Die OMIVV-Appliance ist nicht verfügbar für die HTML5-Version.

2

Informationen zur Verwaltungskonsole

Sie können die Verwaltung von OpenManage Integration for VMware vCenter und seiner virtuellen Umgebung ausführen, indem Sie die folgenden zwei Administrationsportale nutzen:

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

Themen:

Verwendung des Administration-Portal

Sie können mit dem Administrator-Portal folgende Aufgaben ausführen:

- Einen vCenter-Server registrieren. Informationen dazu finden Sie unter Registrieren eines vCenter-Servers.
- vCenter-Anmeldeinformationen modifizieren. Informationen dazu finden Sie unter Modifizieren der vCenter-Anmeldeinformationen.
- SSL-Zertifikate aktualisieren. Informationen dazu finden Sie unter Aktualisieren der SSL-Zertifikate für registrierte vCenter-Server.
- Eine Lizenz hochladen oder erwerben. Wenn Sie eine Testlizenz verwenden, wird der Link **Software kaufen** angezeigt. Durch Anklicken dieses Links können Sie eine vollständige Produktversion erwerben, um mehrere Hosts zu verwalten. Informationen dazu finden Sie unter Hochladen einer Lizenz auf die Verwaltungskonsole.
- OMIVV aktualisieren. Informationen dazu finden Sie unter Aktualisieren des Repository-Speicherorts des virtuellen Geräts und des virtuellen Geräts auf Seite 16.
- Fehlerbehebungspaket erstellen. Informationen dazu finden Sie unter Fehlerbehebungspaket herunterladen auf Seite 29.
- OMIVV neu starten. Informationen dazu finden Sie unter Virtuelles Gerät neu starten auf Seite 16.
- Sichern und wiederherstellen. Informationen dazu finden Sie unter Aktualisieren des Geräts durch Sichern und Wiederherstellen auf Seite 18.
- Warnungen konfigurieren. Informationen dazu finden Sie unter Einrichten globaler Alarme auf Seite 20.
- Informationen zum Konfigurieren des Bereitstellungsmodus finden Sie unter Bereitstellungsmodus konfigurieren auf Seite 19.

Registrieren von vCenter Server durch Nicht-Administratorbenutzer

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

Zum Aktivieren eines Nicht-Administratorbenutzers mit den erforderlichen Berechtigungen zum Registrieren eines vCenter Servers führen Sie die folgenden Schritte aus:

1. Zum Ändern der für eine Rolle ausgewählten Berechtigungen fügen Sie die Rolle hinzu und wählen Sie die erforderlichen Berechtigungen für die Rolle aus oder ändern Sie eine vorhandene Rolle.

   In der VMware vSphere-Dokumentation finden Sie die erforderlichen Schritte zum Erstellen/Ändern einer Rolle und zur Auswahl von Berechtigungen im vSphere Webclient. Details zur Auswahl aller erforderlichen Berechtigungen für die Rolle finden Sie unter Erforderliche Berechtigungen für Nicht-Administrator-Benutzer.

   ANMERKUNG: Der vCenter Administrator muss eine Rolle hinzufügen oder ändern.

2. Weisen Sie einen Benutzer zu der neu erstellten Rolle zu, nachdem Sie eine Rolle definiert und Berechtigungen für die Rolle ausgewählt haben.

   In der VMware vSphere Dokumentation finden Sie weitere Informationen über das Zuweisen von Berechtigungen im vSphere Webclient.

   ANMERKUNG: Der vCenter Administrator muss im vSphere Client Berechtigungen zuweisen.

   Ein Benutzer des vCenter Servers mit den erforderlichen Berechtigungen kann sich jetzt registrieren und oder die vCenter Registrierung aufheben, Anmeldeinformationen ändern oder das Zertifikat aktualisieren.

3. Registrieren Sie einen vCenter Server mit einem Nicht-Administrator-Benutzer mit den erforderlichen Berechtigungen. Siehe Registrieren eines vCenter Servers durch einen Nicht-Administratorbenutzer mit den erforderlichen Berechtigungen.
4. Weisen Sie der in Schritt 1 erstellten oder bearbeiteten Rolle Dell-Berechtigungen zu. Siehe Zuweisen von Dell Berechtigungen zur Rolle im vSphere Webclient.

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

Erforderliche Berechtigungen für Nicht-Administrator-Benutzer

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

ANMERKUNG: Beim Registrieren eines vCenter Servers mit OMIVV durch einen Nicht-Administrator-Benutzer wird eine Fehlermeldung 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

    ANMERKUNG: Weisen Sie die folgenden Berechtigungen für die Funktionszustandsaktualisierung zu, wenn Sie VMware vCenter 6.5 verwenden oder auf vCenter 6.5 oder höher aktualisieren:
- Funktionszustand-Update-Anbieter
  - Registrieren
  - Registrierung aufheben
  - Aktualisierung
- Host
  - CIM
    - CIM-Interaktion
  - Konfiguration
    - Erweiterte Einstellungen
    - Verbindung
    - Wartung
    - Netzwerkkonfiguration
    - Abfragen von Patches
    - Sicherheitsprofil und Firewall

      ANMERKUNG: Weisen Sie die folgenden Berechtigungen zu, wenn Sie VMware vCenter 6.5 verwenden oder auf vCenter 6.5 oder höher aktualisieren:
      - Host-Konfig.
        - Erweiterte Einstellungen
        - Verbindung
        - Wartung
        - Netzwerkkonfiguration
        - Abfragen von Patches
        - Sicherheitsprofil und Firewall
  - Bestandsaufnahme
    - Hinzufügen von Hosts zu einem Cluster
    - Hinzufügen von eigenständigen Hosts
    - Cluster ändern

ANMERKUNG: Stellen Sie sicher, dass Sie die Berechtigung zum Ändern des Clusters zuweisen, wenn Sie vCenter 6.5 verwenden oder eine Aktualisierung auf vCenter 6.5 oder höher durchführen.

- Hostprofil
  - Bearbeiten
  - Ansicht
- Berechtigungen
  - Ändern von Berechtigungen
  - Ändern einer Rolle
- Sitzungen
  - Validieren einer Sitzung
- Task
  - Erstellen von Tasks
  - Aktualisieren von Tasks

ANMERKUNG: Wenn ein Nicht-Administratorbenutzer versucht, einen vCenter Server zu registrieren, ist es zwingend erforderlich, Dell Berechtigungen zu der vorhandenen Rolle hinzuzufügen. Weitere Informationen über das Zuweisen von Dell Berechtigungen finden Sie unter Dell Berechtigungen vorhandener Rolle zuweisen auf Seite 13.

Registrieren eines vCenter Servers mit einem Nicht-Administrator-Benutzer mit erforderlichen Berechtigungen

Sie können vCenter-Server für das OMIVV-Gerät mit einem Nicht-Administrator-Benutzer mit den erforderlichen Berechtigungen registrieren. Weitere Informationen zum Registrieren eines vCenter-Servers über einen Nicht-Administrator-Benutzer oder als Administrator finden Sie unter Registrieren eines vCenter-Servers auf Seite 14 for information about registering a vCenter server through a nonadministrator user or as an administrator.

Dell Berechtigungen vorhandener Rolle zuweisen

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

ANMERKUNG: Stellen Sie sicher, dass Sie als Benutzer mit Administratorrechten angemeldet sind.

1. Melden Sie sich mit Administratorrechten beim vSphere Web Client an.
2. Klicken Sie im vSphere Web-Client im linken Fensterbereich auf **Verwaltung → Rollen**.
3. Wählen Sie ein vCenter Serversystem aus der Dropdownliste **Rollenanbieter** aus.
4. Wählen Sie die Rolle aus der Liste **Rollen** aus und klicken sie auf  .
5. Klicken Sie auf **Berechtigungen**, erweitern Sie **Dell** und wählen Sie die folgenden Dell Berechtigungen für die ausgewählte Rolle aus. Klicken Sie anschließend auf **OK**:
   - Dell.Configuration
   - Dell.Deploy-Provisioning
   - Dell.Inventory
   - Dell.Monitoring
   - Dell.Reporting

   Siehe Sicherheitsrollen und Berechtigungen verfügbar ist, um weitere Informationen über die verfügbaren OMIVV-Rollen innerhalb von vCenter zu erhalten.

Die Änderungen an Berechtigungen und Rollen werden sofort wirksam. Der Benutzer mit erforderlichen Berechtigungen kann nun die OpenManage Integration für VMware vCenter Vorgänge durchführen.

ANMERKUNG: Für alle vCenter Operations verwendet OMIVV die Berechtigungen des registrieren Benutzers und nicht die Berechtigungen des angemeldeten Benutzers.

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

Registrieren eines vCenter-Servers

Sie können die OMIVV-Geräte auch nach der Installation von OpenManage Integration for VMware vCenter registrieren. OpenManage Integration für VMware vCenter verwendet ein Administrator- oder anderes Benutzerkonto mit den erforderlichen Berechtigungen für vCenter Operations. Eine einzelne OMIVV-Geräteinstanz unterstützt bis zu 10 vCenter-Server und bis zu 1000 ESXi-Hosts.

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

1. Öffnen Sie das **Administration-Portal** von einem unterstützten Browser aus.
   Um das Administrationsportal in der Registerkarte **Hilfe und Support** von OpenManage Integration for VMware vCenter zu öffnen, klicken Sie auf den Link unter **Verwaltungskonsole** oder starten Sie einen Web-Browser, und geben Sie `https:\\<ApplianceIP|hostname>` ein.
2. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**, und klicken Sie dann auf **Neuen vCenter-Server registrieren**.
3. Führen Sie im Dialogfeld **NEUES VCENTER REGISTRIEREN** unter **vCenter-Name** die folgenden Schritte aus:
   a. Geben Sie die vCenter-IP-Adresse oder ein FQDN des Hosts in das Textfeld **vCenter-Server-IP-Adresse oder Hostname** ein.

      ANMERKUNG: Dell empfiehlt, OMIVV beim VMware vCenter unter Verwendung eines FQDN (Fully Qualified Domain Name) zu registrieren. In allen Registrierungen sollte 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-Einträge in der Vorwärts- und Rückwärtssuche Ihres DNS-Servers vorhanden sind.

   b. Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein – optional.
4. Unter **vCenter Benutzerkonto** führen Sie die folgenden Schritte aus:
   a. Geben Sie im Textfeld **vCenter Benutzername** den Benutzernamen des Administrators oder eines Nicht-Administrator-Benutzers mit ausreichenden Berechtigungen an.
   b. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
   c. Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
5. Klicken Sie auf **Registrieren**.

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

ANMERKUNG: Für alle vCenter Operations verwendet OMIVV die Berechtigungen des registrieren Benutzers und nicht die Berechtigungen des angemeldeten Benutzers.

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

vCenter-Anmeldeinformationen modifizieren

Die vCenter-Anmeldeinformationen können von einem Benutzer mit Administratorrechten oder einem Nicht-Administrator-Benutzer mit erforderlichen Berechtigungen geändert werden.

1. Um das Administration-Portal in der Registerkarte **Hilfe und Support** von OpenManage Integration for VMware vCenter zu öffnen, klicken Sie auf den Link unter **Verwaltungskonsole** oder starten Sie einen Web-Browser, und geben Sie die URL `https:\\<ApplianceIP|hostname>` ein.
2. Geben Sie im Dialogfeld **Anmeldung** das Kennwort ein und klicken Sie auf **Anmeldung**.
3. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**.
   Die registrierten vCenter Server werden im rechten Bereich des Fensters **VCENTER Serververbindungen verwalten** angezeigt.
   Um das Fenster **Modify USER Acct** unter **Anmeldeinformationen** zu öffnen, klicken Sie für ein registriertes vCenter auf **Ändern**.
4. Geben Sie den vCenter **Benutzernamen** und das **Kennwort** ein, und bestätigen Sie das Kennwort unter **Kennwort bestätigen**; die Kennwörter müssen übereinstimmen.
5. Klicken Sie auf **Anwenden**, um das Kennwort zu ändern, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

ANMERKUNG: Es wird eine Fehlermeldung angezeigt, wenn die angegebenen Benutzer-Anmeldedaten nicht über die notwendigen Berechtigungen verfügen.

SSL-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 OpenManage Integration for VMware vCenter auf dem Webserver SSL für die sichere Datenübertragung.

Wenn das SSL-Zertifikat auf einem vCenter-Server geändert wird, führen Sie die folgenden Schritte durch, um das neue Zertifikat für OpenManage Integration for VMware vCenter zu importieren:

1. Um das Administration-Portal in der Registerkarte **Hilfe und Support** von OpenManage Integration for VMware vCenter zu öffnen, klicken Sie auf den Link unter **Verwaltungskonsole** oder starten Sie einen Web-Browser, und geben Sie die URL `https:\\<ApplianceIP|hostname>` ein.
2. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**.
   Die registrierten vCenter-Server werden im rechten Fenster angezeigt.
3. Zum Aktualisieren des Zertifikats für eine vCenter Server-IP-Adresse oder den Hostnamen klicken Sie auf **Aktualisierung**.

Deinstallieren von Dell OpenManage Integration for VMware vCenter

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

ANMERKUNG: 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.

1. Um das Administration-Portal in der Registerkarte **Hilfe und Support** von OpenManage Integration for VMware vCenter zu öffnen, klicken Sie auf den Link unter **Verwaltungskonsole** oder starten Sie einen Web-Browser, und geben Sie die URL `https:\\<ApplianceIP|hostname>` ein.
2. Klicken Sie auf der Seite **VCENTER REGISTRIERUNG** in der Tabelle **vCenter Server IP- oder Hostname** auf **Registrierung aufheben**.

   ANMERKUNG: Da mehr als ein vCenter vorhanden sein kann, müssen Sie sicherstellen, dass Sie das korrekte vCenter auswählen.

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: 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. So deaktivieren Sie die proaktive HA:

Entfernen Sie im Bildschirm **Proaktive HA-Ausfälle und Antworten** die Markierung aus dem Kontrollkästchen des **Dell Inc** Anbieters.

Hochladen einer Lizenz auf das Administration-Portal

Sie können eine OMIVV-Lizenz hochladen, um die Anzahl der unterstützten gleichzeitig registrierten vCenter Instanzen und verwalteten Hosts zu ändern. Wenn Sie weitere Hosts hinzufügen müssen, können Sie Lizenzen aufstocken. Führen Sie die folgenden Schritte aus:

1. Um das Administration-Portal in der Registerkarte **Hilfe und Support** von OpenManage Integration for VMware vCenter zu öffnen, klicken Sie auf den Link unter **Verwaltungskonsole** oder starten Sie einen Web-Browser, und geben Sie die URL `https:\\<ApplianceIP|hostname>` ein.
2. Geben Sie im **Anmelde**-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**.
   Die registrierten vCenter-Server werden im rechten Fenster 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 die Lizenzdatei geändert oder bearbeitet wird, betrachtet sie das OMIVV-Gerät als beschädigt und die Datei wird nicht akzeptiert.

Verwalten des virtuellen Geräts

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

- Das virtuelle Gerät neustarten. Siehe Neustarten des virtuellen Geräts.
- Das virtuelle Gerät aktualisieren und einen Speicherort für die Repository-Aktualisierung konfigurieren. Aktualisieren des Repository-Speicherorts des virtuellen Geräts und des virtuellen Geräts.
- Den NTP-Server einrichten. Siehe Einrichten des Network Time Protocol-Servers.
- HTTPS-Zertifikate hochladen. Siehe Hochladen eines HTTPS-Zertifikats.

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

1. Um das Administration-Portal in der Registerkarte **Hilfe und Support** von OpenManage Integration for VMware vCenter zu öffnen, klicken Sie auf den Link unter **Verwaltungskonsole** oder starten Sie einen Web-Browser, und geben Sie die URL `https:\\<ApplianceIP|hostname>` ein.
2. Geben Sie im **Anmelde**-Dialogfeld Ihr Kennwort ein.
3. Für die Konfiguration des Geräts klicken Sie im Managementabschnitt im linken Fensterbereich auf **GERÄTEVERWALTUNG**.

Virtuelles Gerät neu starten

1. Klicken Sie zum **Neustarten des virtuellen Geräts** auf **GERÄTE-MANAGEMENT**.
2. Klicken Sie zum Neustarten des virtuellen Geräts im Dialogfeld **Virtuelles Gerät neu starten** auf **Anwenden** oder zum Abbrechen auf **Abbrechen**.

Ändern der Hostnamen des virtuellen Geräts

Gehen Sie hierzu wie folgt vor:

1. Klicken Sie auf der Seite **Gerätemanagement** auf **Hostnamen ändern**.
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 Sie kehren zum Hauptmenü zurück.
4. Um das Gerät neu zu starten, klicken Sie auf **Neustart des Geräts**.

ANMERKUNG: Wenn Sie irgendwelche vCenter-Server beim Gerät registriert hatten, heben Sie die Registrierung auf und registrieren Sie alle vCenter-Instanzen erneut.

ANMERKUNG: Stellen Sie sicher, dass Sie alle Referenzen auf das virtuelle Gerät in Ihrer Umgebung manuell aktualisieren, wie z. B. Bereitstellungsserver in iDRAC, DRM.

Aktualisieren des Repository-Speicherorts des virtuellen Geräts und des virtuellen Geräts

Um sicherzustellen, dass alle Daten geschützt sind, führen Sie eine Sicherung der OMIVV-Datenbank vor dem Aktualisieren des virtuellen Geräts aus. SieheVerwalten von Backups und Wiederherstellungen auf Seite 21.

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

   ANMERKUNG: 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. Abhängig von Ihren Netzwerkeinstellungen müssen Sie Proxy aktivieren und Proxy-Einstellungen bereitstellen, wenn Ihr Netzwerk Proxy benötigt. Siehe Einrichten des HTTP-Proxy.

   ANMERKUNG: Stellen Sie sicher, dass **Repository-Pfad aktualisieren** gültig ist.

Für die verfügbare Version des virtuellen Geräts werden entsprechenden RPM- und OVF-Aktualisierungsmechanismen mit einem Häkchen angezeigt. Im folgenden werden die möglichen Optionen des Aktualisierungsmechanismus dargestellt und Sie können eine dieser Optionen für den Aktualisierungsmechanismus durchführen:

- Wenn ein Häkchen neben RPM angezeigt wird, können Sie eine RPM-Aktualisierung von der vorhandenen Version auf die neueste verfügbare Version durchführen. Siehe Durchführen einer Aktualisierung von einer vorhandenen Version auf die neueste Version.
- 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. Siehe Aktualisieren des Geräts durch Sichern und Wiederherstellen.
- 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 virtuellen Geräts führen Sie die genannten Aufgaben den Upgrade-Mechanismen durch, je nach Version von OMIVV.

   ANMERKUNG: Stellen Sie sicher, dass Sie sich von allen Webclient-Sitzungen an den registrierten vCenter-Servern abmelden.

   ANMERKUNG: Stellen Sie vor der Anmeldung an einem registrierten vCenter-Server sicher, dass Sie alle Geräte gleichzeitig unter dem gleichen Plattform Service Controller (PSC) aktualisieren. Andernfalls werden möglicherweise inkonsistente Informationen in den OMIVV-Instanzen angezeigt.

3. Klicken Sie auf **GERÄTEMANAGEMENT** und überprüfen Sie die Aktualisierungsmechanismen.

OMIVV aus vorhandener Version auf aktuelle Version aktualisieren

1. Aktivieren Sie auf der Seite **GERÄTEMANAGEMENT** die Option „Proxy“ entsprechend Ihren Netzwerkeinstellungen und richten Sie die „Proxy-Einstellungen“ ein, wenn Ihr Netzwerk Proxy benötigt. Siehe Einrichten des HTTP-Proxy.
2. Zur Aktualisierung des OpenManage Integration Plug-ins von einer vorhandenen Version auf die aktuelle 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: http://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 http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ zu ändern. Klicken Sie zum Speichern auf **Anwenden**.
   - Zur Aktualisierung der neuesten heruntergeladenen RPM-Ordner oder -Dateien, wenn keine Internetverbindung vorhanden ist, laden Sie alle Dateien und Ordner über den Pfad http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ herunter und kopieren Sie sie auf eine HTTP-Freigabe. Klicken Sie im Fenster **Geräteverwaltung** im Bereich **Geräteaktualisierung** auf **Bearbeiten** und fügen Sie dann im Textfeld **Repository-Pfad aktualisieren** den Pfad für die Offline-HTTP-Freigabe ein und klicken Sie auf **Anwenden**.
3. Vergleichen Sie die verfügbare virtuelle Geräteversion und die aktuelle virtuelle Geräteversion und stellen Sie sicher, dass die verfügbare virtuelle Geräteversion größer ist als die aktuelle virtuelle Geräteversion.
4. Klicken Sie unter **Geräteeinstellungen** auf **Virtuelles Gerät aktualisieren**, um die Aktualisierung des virtuellen 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.

ANMERKUNG: Während des Upgrade-Vorgangs wird das Gerät ein- oder zweimal neu gestartet.

ANMERKUNG: Sobald das Gerät RPM-aktualisiert ist, führen Sie Folgendes aus:

- Leeren Sie den Browser-Cache bevor Sie sich beim Dell Administratorportal anmelden.
- Installieren Sie die VMware-Tools neu.

  Für die Neuinstallation der VMware-Tools:

  1. Klicken Sie mit der rechten Maustaste auf das OMIVV-Gerät.
  2. Bewegen Sie den Mauszeiger über **Gast** und klicken Sie dann auf **VMware-Tools installieren/aktualisieren**.
  3. Klicken Sie im Dialogfeld **VMware-Tools installieren/aktualisieren** auf **Automatische Tool-Aktualisierung** und klicken Sie dann auf **OK**.

     Sie können den Installationsstatus in **Letzte Aufgaben** sehen.

ANMERKUNG: Nach Abschluss der RPM-Aktualisierung wird der Anmeldebildschirm in der OMIVV Konsole angezeigt. Öffnen Sie einen Browser, geben Sie den Link*https:\\<ApplianceIP|Hostname>* ein und navigieren Sie zum Bereich **GERÄTEAKTUALISIERUNG**. Prüfen Sie, ob die Versionen der verfügbaren und aktuellen virtuellen Geräte gleich sind. Wenn Sie die proaktive HA auf Clustern aktiviert haben, hebt OMIVV die Registrierung des Dell Inc. Providers für diese Cluster auf und registriert den Dell Inc. Provider nach dem Aktualisieren erneut. Das heißt, Funktionszustandaktualisierungen für Dell EMC Hosts stehen erst dann zur Verfügung, wenn die Aktualisierung abgeschlossen ist.

Aktualisieren des Geräts durch Sichern und Wiederherstellen

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

1. Sichern Sie die Datenbank für die ältere Version.
2. Deaktivieren Sie das ältere OMIVV-Gerät im vCenter.

   ANMERKUNG: Heben Sie die Registrierung des OMIVV-Plug-ins von vCenter nicht auf. Das Aufheben der Registrierung des Plug-ins in vCenter entfernt alle durch das OMIVV-Plug-in auf vCenter registrierten Alarme und alle Anpassungen an den Alarmen, wie Maßnahmen usw.

3. Stellen Sie das neue OpenManage Integration-Gerät OVF bereit.
4. Starten Sie das neue OpenManage Integration-Gerät.
5. Richten Sie für das neue Gerät das Netzwerk, die Zeitzone usw. ein.

   ANMERKUNG: Stellen Sie sicher, dass die neue OpenManage Integration Version dieselbe IP-Adresse, wie das alte Gerät hat.

   ANMERKUNG: Das OMIVV-Plug-in kann möglicherweise nicht richtig ausgeführt werden, wenn die IP-Adresse für das neue Gerät sich von der IP-Adresse des älteren Geräts unterscheidet. In einem solchen Fall müssen Sie die Registrierung aller vCenter-Instanzen rückgängig machen und sie dann neu registrieren.

6. Im Lieferumfang des OMIVV-Geräts ist ein Standardzertifikat enthalten. Wenn Sie ein benutzerdefiniertes Zertifikat für Ihr Gerät möchten, aktualisieren Sie dasselbe. Siehe Erstellen einer Zertifikatsignierungsanforderung auf Seite 20 und HTTPS-Zertifikat hochladen auf Seite 20. 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. Siehe Installationsprüfung im *Installationshandbuch zu OpenManage Integration for VMware vCenter*, das unter Dell.com/support/manuals bereitgestellt wird.
9. Führen Sie die **Bestandsaufnahme** auf allen registrierten vCenter-Servern aus.

   ANMERKUNG: Dell EMC empfiehlt, dass Sie nach der Aktualisierung die Bestandsaufnahme erneut auf allen Hosts durchführen, die vom Plug-in verwaltet werden. Informationen zum Ausführen der Bestandsaufnahme nach Bedarf finden Sie im Planen von Bestandsaufnahme-Jobs.

   ANMERKUNG: Wenn die IP-Adresse der neuen OMIVV-Version y von der OMIVV-Version x geändert wird, konfigurieren Sie das Trap-Ziel für die SNMP-Traps, sodass es auf das neue Gerät verweist. Für Server der 12. Generation und höher wird die IP-Änderung durch Ausführung der Bestandsaufname auf diesen Hosts korrigiert. Während der Ausführung der Bestandsaufnahme auf Hosts der 12. Generation werden diese Hosts, falls die SNMP-Traps nicht auf die neue IP verweisen, als „nicht konform“ aufgelistet. Bei Hosts vor der 12. Generation, die mit früheren Versionen kompatibel waren, wird die IP-Änderung als nicht konform angezeigt und Sie müssen Dell OpenManage Server Administrator (OMSA) konfigurieren. Zum Beheben von Konformitätsproblemen bei vSphere-Hosts lesen Sie Ausführen des Assistenten zum Korrigieren nicht konformer vSphere-Hosts.

Herunterladen des Fehlerbehebungspakets

1. Klicken Sie unter **GERÄTEMANAGEMENT** auf **Fehlerbehebungspaket erstellen**.
2. Klicken Sie auf den Link **Fehlerbehebungspaket herunterladen**.
3. Klicken Sie auf **Schließen**.

Einrichten des HTTP-Proxy

1. Scrollen Sie auf der Seite **GERÄTEVERWALTUNG** bis zu **HTTP-PROXY-EINSTELLUNGEN**, und klicken Sie dann auf **Bearbeiten**.

2. Führen Sie die folgenden Schritte im Bearbeitungsmodus aus:
   a. Wählen Sie **Aktiviert**, um die Verwendung der HTTP-Proxy-Einstellungen zu aktivieren.
   b. Geben Sie die Proxy-Serveradresse in das **Feld Proxy-Serveradresse** ein.
   c. Geben Sie den Proxyserver-Port in **Proxyserver-Port** ein.
   d. Wählen Sie **Ja** aus, um die Proxy-Anmeldeinformationen zu verwenden.
   e. Bei der Verwendung von Proxy-Anmeldeinformationen geben Sie den Benutzernamen in **Benutzername** ein.
   f. Geben Sie das Kennwort in **Kennwort** ein.
   g. Klicken Sie auf **Anwenden**.

Network Time Protocol (NTP)-Server einrichten

Sie können das Network Time Protocol (NTP) zum Synchronisieren der Uhren der virtuellen Geräte mit der Uhr eines NTP-Servers verwenden.

1. Klicken Sie auf der Seite **GERÄTE-MANAGEMENT** auf **Bearbeiten** im Bereich **NTP-Einstellungen**.
2. Wählen Sie **Aktiviert** aus. Geben Sie den Hostnamen oder die IP-Adresse für einen bevorzugten und einen sekundären NTP-Server ein und klicken Sie auf **Anwenden**.

ANMERKUNG: Es kann etwa 10 Minuten dauern, bis die Uhren der virtuellen Geräte mit dem NTP-Server synchronisieren.

Bereitstellungsmodus konfigurieren

Stellen Sie sicher, dass die folgenden Systemvoraussetzungen für die gewünschten Bereitstellungsmodi erfüllt sind:

Tabelle 2. Systemanforderungen für Bereitstellungsmodi

Bereitstellungsmodi	Anzahl der Hosts	Anzahl der CPUs	Speicher in GB	Mindestspeichergröße
Small (Klein)	Bis zu 250	2	8	44 GB
Mittel	Bis 500	4	16	44 GB
Large (Groß)	Bis zu 1000	8	32	44 GB

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

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

1. Scrollen Sie auf der Seite **GERÄTEMANAGEMENT** runter zu **Bereitstellungsmodus**.
   Die Konfigurationswerte des Bereitstellungsmodus wie **Klein**, **Mittel** oder **Groß** werden angezeigt, und der Bereitstellungsmodus ist standardmäßig auf **Klein** gesetzt.
2. Klicken Sie auf **Bearbeiten**, wenn Sie den Bereitstellungsmodus basierend auf die Umgebung aktualisieren möchten.
3. Wählen Sie im Modus **Bearbeiten** den gewünschten Bearbeitungsmodus aus, nachdem sichergestellt wurde, dass die Voraussetzungen erfüllt sind.
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 und überprüft, und eine der folgenden Situationen tritt ein:
   - 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 und mit dem Neustart des OMIVV-Geräts fortfahren, um die Aktualisierung des Bereitstellungsmodus zu ermöglichen.

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 des Anmeldebildschirms gestartet. Zum Starten des

OMIVV-Geräts muss es heruntergefahren, die Systemressourcen auf die vorhandene Einstellung des Bereitstellungsmodus aktualisiert und die Aufgabe Bereitstellungsmodus zurückstufen ausgeführt werden.

Zurückstufen des Bereitstellungsmodus

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

Erstellen einer Zertifikatsignierungsanforderung

Stellen Sie sicher, dass Sie das Zertifikat vor der Registrierung von OMIVV mit dem vCenter hochladen.

Das Erzeugen einer Zertifikatsignierungsanforderung (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. Klicken Sie zum Fortsetzen der Anforderung auf **Weiter** oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.
2. Wenn Sie mit der Anforderung fortfahren, geben Sie im Dialogfeld **ZERTIFIKATSIGNIERUNGSANFORDERUNG ERSTELLEN** den **allgemeinen Namen**, den **Organisationsnamen**, die **Organisationseinheit**, den **Standort**, den **Staatsnamen**, das **Land** und die **E-Mail** für die Anforderung ein. Klicken Sie auf **Weiter**.
3. Klicken Sie auf **Herunterladen**, dann speichern Sie die resultierende Zertifikatsanforderung 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 dem virtuellen Gerät und Hostsystemen verwendet. Um diese sichere Kommunikation einzurichten, muss eine CSR an eine Zertifizierungsstelle gesendet werden, dann wird das resultierende Zertifikat mithilfe der Administration Console hochgeladen. Darüber hinaus gibt es ein selbst-signiertes Standardzertifikat, das für die sichere Kommunikation verwendet werden kann; dieses Zertifikat ist bei jeder Installation einmalig.

ANMERKUNG: Sie können entweder den Microsoft Internet Explorer, Firefox oder Chrome verwenden, um Zertifikate hochzuladen.

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 Auswählen des gewünschten Zertifikats auf **Durchsuchen** und dann auf **Hochladen**.
4. Klicken Sie auf **Abbrechen**, wenn Sie das Hochladen abbrechen möchten.

   ANMERKUNG: Wenn Sie für das Gerät ein benutzerdefiniertes Zertifikat hochgeladen haben, laden Sie vor der vCenter-Registrierung das neue Zertifikat hoch. Wenn Sie das neue benutzerdefinierte Zertifikat nach der vCenter-Registrierung hochladen, werden im Web-Client Kommunikationsfehler angezeigt. Um dieses Problem zu beheben, müssen Sie die Registrierung von vCenter rückgängig machen und sich erneut registrieren.

Wiederherstellen des standardmäßigen HTTPS-Zertifikats

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**.

Einrichten globaler Alarme

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

1. Um das Administration-Portal in der Registerkarte **Hilfe und Support** von OpenManage Integration for VMware vCenter zu öffnen, klicken Sie auf den Link unter **Verwaltungskonsole** oder starten Sie einen Web-Browser, und geben Sie die URL `https:\\<ApplianceIP|hostname>` ein.
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 für die folgenden Felder ein:
   - **Maximale Anzahl an Alarmen**
   - **Anzahl an Tagen, über die Alarme beibehalten werden sollen**
   - **Timeout für duplizierte Alarme (Sekunden)**
5. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern, oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.

Verwalten von Backups und Wiederherstellungen

Die Verwaltung von Backups und Wiederherstellungen erfolgt über die Verwaltungskonsole. Die folgenden Aufgaben können auf dieser Seite ausgeführt werden:

- Konfigurieren von Backup und Wiederherstellung
- Planen von automatischen Backups
- Durchführen eines sofortigen Backups
- Wiederherstellen der Datenbank aus einem Backup

Führen Sie folgende Schritte in OpenManage Integration for VMware vCenter durch, um die Seite **EINSTELLUNGEN ZU BACKUP UND ZUR WIEDERHERSTELLUNG** über die Administrationskonsole aufzurufen.

1. Um das Administration-Portal in der Registerkarte **Hilfe und Support** von OpenManage Integration for VMware vCenter zu öffnen, klicken Sie auf den Link unter **Verwaltungskonsole** oder starten Sie einen Web-Browser, und geben Sie die URL `https:\\<ApplianceIP|hostname>` ein.
2. Geben Sie im **Anmelde**-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.

Konfigurieren von Backup und Wiederherstellung

Die Backup- und Wiederherstellungsfunktion dient zum Sichern der OMIVV-Datenbank an einem Remote-Speicherort, von dem aus sie später wiederhergestellt werden kann. Die Profile, Vorlagen und Host-Informationen sind beim Backup enthalten. Dell empfiehlt, dass Sie zum Schutz gegen Datenverlust automatische Backups planen.

ANMERKUNG: 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 im Feld **Benutzername** den Benutzernamen ein.
   c. Geben Sie im Feld **Kennwort** das Kennwort ein.
   d. Geben Sie das Verschlüsselungskennwort in das Textfeld **Kennwort für die Verschlüsselung von Backups** ein.
      Das Verschlüsselungskennwort darf alphanumerische Zeichen und Sonderzeichen wie „!@#$%*“ 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.

Planen von automatischen Backups

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 ein Backup 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 **JETZT SICHERN**, um den angezeigten Speicherort und das Verschlüsselungskennwort zu verwenden.
3. Geben Sie die Werte für **Sicherungsverzeichnis**, **Benutzername**, **Kennwort** und **Kennwort für Verschlüsselung** ein.
   Das Verschlüsselungskennwort darf alphanumerische Zeichen und Sonderzeichen wie „"!, @, #, $, %, *" enthalten. Es gibt keine Längenbeschränkung.
4. Klicken Sie auf **Sichern**.

OMIVV-Datenbank aus Backup wiederherstellen

Bei einer Wiederherstellung wird das virtuelle Gerät nach Abschluss der Wiederherstellung neu gestartet wird.

1. Öffnen Sie die Seite **BACKUP- UND WIEDERHERSTELLUNGSEINSTELLUNGEN**. Siehe Backup und Wiederherstellung verwalten.
2. Klicken Sie auf der Seite **EINSTELLUNGEN ZUM BACKUP UND ZUR WIEDERHERSTELLUNG** auf **Jetzt wiederherstellen**.
3. Geben Sie im Dialogfeld **JETZT WIEDERHERSTELLEN** einen Pfad für den **Dateispeicherort** zusammen mit der Datei backup .gz im CIFS/NFS-Format ein.
4. Geben Sie den **Benutzernamen**, das **Kennwort** und das **Verschlüsselungskennwort** für die Backup-Datei ein.
   Das Verschlüsselungskennwort darf alphanumerische Zeichen und Sonderzeichen wie „!, @, #, $, %, *" enthalten. Es gibt keine Längenbeschränkung.
5. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
   Das Gerät wird neu gestartet.

ANMERKUNG: Stellen Sie sicher, dass Sie das OMIVV-Gerät erneut registrieren, wenn das Gerät auf die werkseitigen Einstellungen zurückgesetzt wird.

Informationen zur vSphere Client-Konsole

Die vSphere Client-Konsole befindet sich innerhalb des vSphere-Clients auf einer virtuellen Maschine. Die Konsole arbeitet eng mit der Verwaltungskonsole zusammen. Sie können die Konsole für folgende Tasks verwenden:

- Konfigurieren der Netzwerkeinstellungen
- Ändern des Kennworts des virtuellen Geräts
- Konfigurieren von NTP und der Einstellungen zur lokalen Zeitzone
- Neustart des virtuellen Geräts
- Zurücksetzen des virtuellen Geräts auf die werkseitigen Einstellungen
- Abmelden von der Konsole
- Verwenden der schreibgeschützten Benutzerrolle

Öffnen der Konsole der virtuellen Maschine von OMIVV

1. Wählen sie im vSphere Webclient **Start** aus, und klicken Sie auf **vCenter**.
2. Klicken Sie in **Bestandsaufnahmelisten** auf **Virtuelle Maschinen**, und wählen Sie dann das virtuelle Gerät von OMIVV aus.
3. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie in der Registerkarte **Objekt Aktion → Konsole öffnen** aus.
   - Rechtsklicken Sie die ausgewählte virtuelle Maschine und wählen Sie dann **Konsole öffnen**.

Nach dem Öffnen der Konsole der virtuellen Maschine und der Bereitstellung der Anmeldeinformationen (Benutzername: admin und Kennwort: das Kennwort, das Sie während der Bereitstellung des Geräts eingerichtet haben), können Sie mit der Konfiguration der Konsole beginnen.

Konfigurieren der Netzwerkeinstellungen

Sie können die Netzwerkeinstellungen in der vSphere Client-Konsole ändern.

1. Öffnen Sie die Konsole der virtuellen Maschine. Siehe Öffnen der vSphere Client-Konsole.
2. Wählen Sie im Fenster **Konsole** die Option **Netzwerk konfigurieren**, und drücken Sie die **EINGABETASTE**.
3. Geben Sie die gewünschten Netzwerkeinstellungen unter **Geräte bearbeiten** oder unter **DNS bearbeiten** ein, und klicken Sie auf **Speichern und Beenden**. Klicken Sie auf **Beenden**, um die Änderungen zu verwerfen.

Kennworts des virtuellen Geräts ändern

Sie können das Kennwort des virtuellen Geräts im vSphere-Webclient unter Verwendung der Konsole ändern.

1. Öffnen Sie die Konsole der virtuellen Maschine. Siehe Öffnen der vSphere Client-Konsole.
2. Wählen Sie auf im Fenster **Konsole** die Option **Admin-Kennwort ändern** mit den Pfeiltasten aus, und drücken Sie die **EINGABETASTE**.
3. Geben Sie im Feld **Aktuelles Administratorkennwort** den Wert ein, und drücken Sie die **EINGABETASTE**.

   Das Administratorkennwort sollte mindestens acht Zeichen und mindestens ein Sonderzeichen, eine Zahl, einen Großbuchstaben und einen Kleinbuchstaben enthalten.
4. Geben Sie ein neues Kennwort unter **Neues Admin-Kennwort eingeben** ein und drücken Sie die **EINGABETASTE**.
5. Geben Sie das neue Kennwort erneut in das Textfeld **Admin-Kennwort bestätigen** ein, und drücken Sie die **Eingabetaste**.

Konfigurieren von NTP und der Einstellungen zur lokalen Zeitzone

1. Öffnen Sie die Konsole der virtuellen Maschine. Siehe Öffnen der vSphere Client-Konsole.
2. Zum Konfigurieren der OMIVV-Zeitzoneninformationen klicken Sie auf **Datum/Uhrzeit-Eigenschaften**.
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 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**.

Neustarten des virtuellen Geräts

1. Öffnen Sie die Konsole der virtuellen Maschine. Siehe Öffnen der vSphere Client-Konsole.
2. Klicken Sie auf **Gerät hinzufügen**.
3. Klicken Sie zum Neustarten des Geräts auf **`Ja`**, klicken Sie zum Abbrechen auf **`Nein`**.

Zurücksetzen des virtuellen Geräts auf die Werkseinstellungen

1. Öffnen Sie die Konsole der virtuellen Maschine. Siehe Öffnen der vSphere Client-Konsole.
2. Klicken Sie 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. Klicken Sie zum Zurücksetzen des Geräts auf **`Ja`**, klicken Sie zum Abbrechen auf **`Nein`**.
   Wenn Sie auf „Ja“ klicken, wird das OMIVV-Gerät auf die ursprünglichen Werkseinstellungen zurückgesetzt und alle anderen Einstellungen und vorhandenen Daten gehen verloren.

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

Von Konsole abmelden

Zum Abmelden von der vSphere Konsole klicken Sie auf **Abmelden**.

Schreibgeschützte Benutzerrolle

Es gibt eine Benutzerrolle ohne Berechtigungen („schreibgeschützt“) mit Shell-Zugriff für Diagnosezwecke. Der Benutzer mit schreibgeschützter Rolle verfügt über eingeschränkte Rechte zum Ausführen der Ankoppelung. Das Kennwort des schreibgeschützten Benutzers lautet **readonly**. Das Kennwort des schreibgeschützten Benutzers entspricht ab OMIVV Version 3.0 aus Sicherheitsgründen nicht mehr dem Admin-Kennwort wie in früheren OMIVV Versionen (OMIVV Version 1.0 bis Version 2.3.1).

3

Verwaltung mehrerer Geräte

Sie können mehrere OMIVV Appliances verwalten und überwachen, die Sie bei vCenter Servern registrieren, die zum gleichen Plattform Service Controller (PSC) oder einem anderen PSC gehören. Dell EMC empfiehlt die Verwendung ähnlicher vCenter Versionen.

Dell EMC empfiehlt, dass Sie eine globale Aktualisierung durchführen, wenn die Seite zwischengespeichert wird.

1. Klicken Sie auf der Startseite des VMware vCenters auf das Symbol **OpenManage Integration.**
2. Klicken Sie im **Navigator** unter der Gruppe **Dell EMC** auf **OMIVV-Geräte**.
3. Auf der Registerkarte **OMIVV-Geräte** können Sie die folgenden Informationen anzeigen und Geräte überwachen:

   ANMERKUNG: Auf der Registerkarte „Dell Gerät“ wird die Position der Geräte, die in der Liste aufgeführt sind, festgelegt, das markierte Gerät ist dabei das aktive Gerät.

   - **Name** - Zeigt unter Verwendung der IP-Adresse oder FQDN Links für die einzelnen OMIVV-Geräte an. Zum Anzeigen und Überwachen gerätespezifischer Informationen klicken Sie auf die Namensverknüpfung eines bestimmten Geräts. Ein Klick auf eine Gerätenamensverknüpfung führt Sie zum Hauptinhaltsbereich des OMIVV-Geräts. Sie können OMIVV-Vorgänge verwalten und Hosts, Rechenzentren und Cluster für das jeweilige Gerät überwachen.

     ANMERKUNG: Nach einem Klick auf **Name** wird ein Dialogfeld angezeigt, das Sie auffordert, eine globale Aktualisierung der zwischengespeicherten Seiten durchzuführen, wenn Sie mehrere Geräte verwenden.

     Um herauszufinden, auf welchem Gerät Sie die OMIVV-Vorgänge verwalten, führen Sie die folgenden Schritte aus:

     a. Klicken Sie in OpenManage Integration for VMware vCenter auf das Register **Hilfe und Support**.
     b. Lassen Sie unter Verwaltungskonsole die spezifische OMIVV-Geräte-IP anzeigen.
   - **Version** – zeigt die Version der einzelnen OMIVV-Geräte an.
   - **Kompatibilitätsstatus** – gibt an, ob das Gerät mit dem geladenen Plug-in kompatibel ist.

     ANMERKUNG: Der Kompatibilitätsstatus eines Geräts wird als **nicht kompatibel** angezeigt, wenn das OMIVV-Gerät nicht mit dem Plug-in vorgabenkonform ist, der **Namens**-Link ist dann deaktiviert.
   - **Verfügbarkeitsstatus** – zeigt einen Status an, der angibt, ob Sie das Gerät über das Plug-in erreichen können und ob die erforderlichen Webdienste auf dem OMIVV-Gerät ausgeführt werden.

     ANMERKUNG: Sie können ein Gerät wählen, wenn der Kompatibilitätsstatus des Geräts **kompatibel** ist und der Verfügbarkeitsstatus des Geräts **OK**.
   - **Registrierte vCenter-Server** – Zeigt alle bei Geräten registrierte vCenter, auf die Sie für die angemeldete Sitzung zugreifen können. Wenn Sie ein Gerät bei mehreren vCentern registrieren, werden die vCenter als erweiterbare/reduzierbare Liste angezeigt. Ein Klick auf einen vCenter-Link führt zur Seite **vCenter-Server**, auf der alle vCenter im Navigatorbereich aufgeführt werden.

4

Aufrufen der OpenManage-Integration aus dem Webclient

Wenn Sie sich am VMware vCenter nach der Installation von OMIVV über die Registerkarte **Home** anmelden, finden Sie das Symbol **OpenManage Integration** im Hauptinhaltsbereich unter der Gruppe **Administration**. Sie können über das Symbol **OpenManage Integration** zur Seite **OpenManage Integration for VMware vCenter** navigieren. Die Gruppe **Dell EMC** wird im Bereich **Navigator** angezeigt.

Das VMware vCenter-Layout enthält die folgenden drei Abschnitte:

Tabelle 3. OpenManage Integration for VMware vCenter-Abschnitte

Bereiche	Beschreibung
Navigator	Greift auf verschiedene Ansichten in der Konsole zu. OpenManage Integration for VMware vCenter hat eine spezielle Gruppe unter dem vCenter-Menü, das als primärer Zugriffspunkt für OpenManage Integration for VMware vCenter dient.
Hauptinhalt	Zeigt die im Navigator ausgewählten Ansichten an. Der Hauptinhaltsbereich ist der Bereich, in dem die meisten Inhalte angezeigt werden.
Benachrichtigungen	Zeigt vCenter-Alarme, Aufgaben und laufende Jobs an. OpenManage Integration for VMware vCenter integriert sich in die Alarm-, Ereignis- und Tasksysteme in vCenter, um die Informationen im Benachrichtigungsbereich anzuzeigen.

Themen:

Navigieren im VMware vCenter-Webclient

Das **OpenManage Integration for VMware vCenter** befindet sich in einer speziellen **Dell EMC**-Gruppe innerhalb des VMware vCenters.

1. Melden Sie sich an VMware vCenter an.
2. Klicken Sie auf der Startseite des VMware vCenters auf das Symbol **OpenManage Integration**.

   Hier können Sie Folgendes tun:

   - Verbindungsprofile der OpenManage Integration for VMware vCenter und die Produkteinstellungen verwalten, den Zusammenfassungsbereich anzeigen und Durchführen weiterer Tasks im Hauptinhaltsbereich.
   - Überwachen von Hosts, Rechenzentren und Clustern aus dem Navigatorbereich unter **vCenter Bestandslisten**. Wählen Sie den zu untersuchenden Host, das Rechenzentrum oder Cluster aus, und klicken Sie dann auf der Registerkarte **Objekte** auf das Objekt, das Sie überwachen möchten.

Symbole im Webclient

Die Benutzerschnittstelle des Produkts verwendet viele symbolbasierte Aktionsschaltflächen für die ergriffenen Maßnahmen.

Tabelle 4. Symbolschaltflächen definiert

Symbolschaltflächen	Definition
	Etwas Neues hinzuzufügen oder erstellen
	Hinzufügen eines Servers zu einem Verbindungsprofil, einem Rechenzentrum und einem Cluster
	Abbrechen eines Jobs
	Verkleinern einer Liste
	Erweitern einer Liste
	Löschen eines Objekts
	Ändern eines Zeitplans
	Bearbeiten
	Säubern eines Jobs
	Exportieren einer Datei
	Systemprofil anzeigen
	Filter
	Jetzt ausführen

Softwareversion finden

Die Softwareversion befindet sich auf der Registerkarte für erste Schritte in **OpenManage Integration for VMware vCenter**.

1. Klicken Sie auf der Startseite des VMware vCenters auf das Symbol **OpenManage Integration.**
2. Klicken Sie auf die **Versionsinformationen** auf der Registerkarte für erste Schritte in **OpenManage Integration for VMware vCenter**.
3. Zeigen Sie die Versionsinformationen im Dialogfeld **Versionsinformationen** an.
4. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Aktualisieren des Bildschirminhalts

Sie können den Bildschirm durch Verwendung des VMware vCenter **Aktualisieren**-Symbols aktualisieren.

1. Wählen Sie eine Seite aus, die Sie aktualisieren lassen wollen.
2. Klicken Sie in der VMware vCenter-Titelleiste auf das Symbol für **Aktualisieren (Strg+Alt+R)**.
   Das **Aktualisieren**-Symbol befindet sich rechts neben dem Suchbereich und ähnelt einem dem Uhrzeigersinn folgenden Pfeil.

Anzeigen von Dell EMC Hosts

Wenn Sie schnell nur Dell EMC Hosts ansehen möchten, können Sie dies von innerhalb des Dell OpenManage Integration for VMware vCenter tun, indem Sie im Navigator **Dell EMC Hosts** auswählen.

1. Klicken Sie auf der Startseite von VMware vCenter auf das Symbol **OpenManage Integration**.
2. Klicken Sie im **Navigator** unter **OpenManage Integration** auf **Dell EMC Hosts**.
3. Auf der Registerkarte **Dell EMC Host** können Sie folgende Informationen einsehen:
   - **Host-Name** - Zeigt einen Link unter Verwendung der IP-Adresse für jeden Dell EMC Host an. Zum Anzeigen der Informationen von Dell EMC Hosts klicken Sie auf einen spezifischen Hostlink.
   - **vCenter** – Zeigt die vCenter IP-Adresse für diesen Dell EMC Host an.
   - **Cluster** – Zeigt den Clusternamen an, wenn der Dell EMC Host sich in einem Cluster befindet.
   - **Verbindungsprofil** – Zeigt den Namen des Verbindungsprofils an.

Anzeigen der Lizenzregisterkarte OpenManage Integration for VMware vCenter

Wenn Sie die Lizenz für OpenManage Integration for VMware vCenter installieren, wird die Anzahl unterstützter Hosts und vCenter Server in dieser Registerkarte angezeigt. Oben auf der Seite können Sie auch die Version von OpenManage Integration for VMware vCenter anzeigen.

Die Seite unter der Lizenzierung zeigt den Link **Lizenz kaufen** an.

Der Abschnitt **Lizenzverwaltung** zeigt Folgendes an:
- **Produktlizenzierungsportal (Digital Locker)**
- **iDRAC-Lizenzierungsportal**
- **Verwaltungskonsole**

Auf der Registerkarte **Lizenzierung** von OpenManage Integration for VMware vCenter werden die folgenden Informationen angezeigt:

Registerkarte Lizenzierungsinformationen	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

Aufrufen von Hilfe und Support

Um die Informationen bereitzustellen, die Sie über Ihr Produkt brauchen, bietet OpenManage Integration for VMware vCenter die Registerkarte **Hilfe und Support**. Auf dieser Registerkarte können Sie die folgenden Informationen finden:

Tabelle 5. Informationen in der Registerkarte „Hilfe und Support“

Name	Beschreibung
Produkthilfe	Stellt folgende Links bereit: • **Hilfe für OpenManage Integration for VMware vCenter** – Stellt einen Link zur Produkthilfe im Produkt bereit. Verwenden Sie die Inhaltsangabe oder Suche, um die gewünschten Informationen zu finden.

Tabelle 5. Informationen in der Registerkarte „Hilfe und Support“ (fortgesetzt)

Name	Beschreibung
	• **Info** – Dieser Link zeigt das Dialogfeld mit den **Versionsinformationen** an. Hier können Sie die Produktversion anzeigen.
Handbücher für Dell EMC	Stellt Live-Links für Folgendes bereit: • **Server-Handbücher** • **Hilfe für OpenManage Integration for VMware vCenter**
Verwaltungskonsole	Stellt einen Link zur Verwaltungskonsole bereit
Zusätzliche Hilfe und Support	Stellt Live-Links für Folgendes bereit: • **iDRAC mit Lifecycle Controller-Handbücher** • **Dell VMware-Dokumentation** • **Produktseite für OpenManage Integration for VMware vCenter** • **Dell Hilfs- und Supportstartseite** • **Dell TechCenter**
Tipps für Support-Anrufe	Bietet Tipps an, wie Sie Dell Support kontaktieren und Anrufe richtig weiterleiten.
Fehlerbehebungsbündel	Stellt einen Link zum Erstellen und Herunterladen des Fehlerbehebungsbündel bereit. Sie können dieses Bündel bereitstellen oder anzeigen, wenn Sie den technischen Support kontaktieren. Weitere Informationen finden Sie unter Herunterladen des Fehlerbehebungsbündels.
Dell EMC empfiehlt	Stellt einen Link zum EMC Dell Repository Manager (DRM) bereit. Verwenden Sie DRM, um alle Firmware-Aktualisierungen zu suchen und herunterzuladen, die für Ihr System verfügbar sind.
iDRAC-Reset	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.

Fehlerbehebungspaket herunterladen

ANMERKUNG: Um Fehlerbehebungsbündel zu erzeugen, stellen Sie sicher, dass Sie sich beim vSphere Client als Benutzer mit Schreibrechten auf OMIVV anmelden.

Sie können die Informationen des Fehlerbehebungsbündels als Hilfe bei der Störungsbehebung nutzen oder die Informationen an den technischen Support senden. Um Informationen zur Störungsbehebung zu erhalten, führen Sie folgende Schritte durch:

1. Klicken Sie in OpenManage Integration for VMware vCenter auf das Register **Hilfe und Support**.
2. Klicken Sie unter **Fehlerbehebungsbündels** auf **Fehlerbehebungsbündel erstellen und herunterladen**.
3. Klicken Sie auf die Schaltfläche **Erstellen**.
4. Klicken Sie auf **Speichern**, um die Datei zu speichern.
5. Klicken Sie im Dialog **Dateien herunterladen** auf **Speichern**.
6. Wechseln Sie im Dialogfeld **Datei speichern** in das Verzeichnis, in dem die Datei gespeichert werden soll, und klicken Sie auf **Speichern**.
7. Klicken Sie zum Beenden auf **Schließen**.

Durchführen des iDRAC-Resets

Sie finden den Link zum Reset des iDRAC auf der Registerkarte **Hilfe und Support**. Das Reset des iDRAC führt einen normalen iDRAC-Neustart durch. Der iDRAC-Neustart startet den Host nicht neu. Nach dem Reset dauert es bis zu 2 Minuten, bis das Gerät wieder im einsatzfähigen Zustand ist. Verwenden Sie die Reset-Funktion in Fällen, in denen der iDRAC im OpenManage Integration for VMware vCenter nicht reagiert.

ANMERKUNG: Es wird empfohlen, dass Sie den Host in den Wartungsmodus versetzen, bevor Sie den iDRAC-Reset durchführen. Sie können die Reset-Aktion auf Hosts ausführen, die Teil eines Verbindungsprofils sind und mindestens einmal Teil einer Bestandsaufnahme waren. Die Reset-Aktion versetzt den iDRAC nicht unbedingt in einen einsatzfähigen Zustand. In einem solchen Fall ist ein harter Reset erforderlich. Weitere Informationen zum harten Reset finden Sie in der iDRAC-Dokumentation.

Während der Neustart des iDRACs durchgeführt wird, sehen Sie eventuell folgende Meldungen:

- Es ist eine leichte Verzögerung oder ein Kommunikationsfehler aufgetreten, während OpenManage Integration for VMware vCenter seinen Funktionszustand abgerufen hat.
- Alle mit iDRAC geöffneten Sitzungen werden geschlossen.
- Die DHCP-Adresse für iDRAC könnte sich ändern.

  Wenn iDRAC DHCP für seine IP-Adresse verwendet, besteht die Möglichkeit, dass die IP-Adresse sich ändert. Wenn die IP-Adresse sich ändert, führen Sie die Host-Bestandsaufnahme erneut aus, um die neue iDRAC-IP-Adresse in den Bestandsdaten zu erfassen.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf das Register **Hilfe und Support**.
2. Klicken Sie unter iDRAC Reset auf **Reset iDRAC**.
3. Geben Sie im Dialogfeld **iDRAC Reset** unter iDRAC Reset die Host-IP-Adresse/den -Namen ein.
4. Um zu bestätigen, dass Sie den iDRAC-Reset-Vorgang verstehen, wählen Sie **Ich verstehe den iDRAC-Reset. Weiter mit dem iDRAC-Reset**.
5. Klicken Sie auf **Reset iDRAC**.

Öffnen der Online-Hilfe

Sie können die Online-Hilfe vom Register **Hilfe und Support** aus öffnen. Sie können das Dokument nach Informationen über ein Thema oder nach einem Vorgang durchsuchen.

1. klicken Sie in OpenManage Integration for VMware vCenter in **Hilfe und Support** unter **Produkthilfe** auf **OpenManage Integration for VMware vCenter-Hilfe**.
   Der Onlinehilfe-Inhalt wird im Browserfenster angezeigt.
2. Verwenden Sie die Inhaltsangabe im linken Bereich oder suchen Sie nach dem gewünschten Thema.
3. Klicken Sie auf das **X** in der rechten oberen Ecke des Browserfensters, um die Online-Hilfe zu schließen.

Starten der Administrationskonsole

Sie können **OpenManage Integration for VMware vCenter** von innerhalb des VMware vCenter-Webclient starten und die Verwaltungskonsole von der Registerkarte „Hilfe und Support“ aus öffnen.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Hilfe und Support** unter der **Verwaltungskonsole** auf den Link zur Konsole.
2. Verwenden Sie im Anmelde-Dialogfeld **Verwaltungskonsole** das Administrator-Kennwort für die Anmeldung.

   Sie können die folgenden Vorgänge in der Verwaltungskonsole ausführen:
   - Ein vCenter registrieren oder die Registrierung aufheben, Anmeldeinformationen ändern oder ein Zertifikat aktualisieren.
   - Die Lizenz hochladen.
   - Die Zusammenfassung über die Anzahl von registrierten und verfügbaren vCentern und über die Höchstzahl verwendeter und verfügbarer Hostlizenzen anzeigen.
   - Das virtuelle Gerät neustarten.
   - Aktualisierung oder Upgrade auf die aktuelle Version.
   - Anzeigen der Netzwerkeinstellungen (Nur-Lesen-Modus).
   - Konfigurieren der HTTP-Proxy-Einstellungen, die dazu verwendet werden, eine Verbindung mit dem Dell EMC Server für eine Geräte-Aktualisierung oder für die Konnektivität mit `http://downloads.dell.com/published/Pages/index.html` herzustellen.
   - NTP-Einstellungen, mit denen Sie einen NTP-Server aktivieren oder deaktivieren können, und einen bevorzugten und sekundären NTP-Server konfigurieren.
   - Eine Zertifikatsignierungsanforderung (CSR) erstellen, ein Zertifikat hochzuladen oder das Standardzertifikat für HTTPS-Zertifikate wiederherstellen.
   - Konfigurieren der globalen Einstellungen zur Vorgehensweise beim Speichern von Alarmen für alle vCenter-Instanzen. Sie können die maximale Anzahl der zu speichernden Warnungen, für wie viele Tage sie beibehalten werden sollen und die Zeitüberschreitung für duplizierte Warnungen konfigurieren.
   - Konfigurieren der globalen Einstellungen zur Vorgehensweise beim Speichern von Alarmen für alle vCenter-Instanzen.

- Backup oder Wiederherstellung einleiten.
- Den Backup-Standort auf einer Netzwerkfreigabe und das Verschlüsselungskennwort für die gesicherten Dateien konfigurieren (zusammen mit dem Test der Netzwerkverbindung).
- Einen Zeitplan für eine Backupserie festlegen.

Anzeigen des Protokollverlaufs

Die Protokollseite ermöglicht Ihnen die Anzeige der Protokolle, die OMIVV erzeugt.

Sie können den Inhalt auf dieser Seite mithilfe der beiden Drop-down-Menüs filtern und sortieren. Über das erste Drop-down-Menü können Sie die Protokolldetails auf Basis der folgenden Protokolltypen filtern und anzeigen:

- Alle Kategorien
- Info
- Warnung
- Fehler

Die zweite Dropdownliste dient dazu, die Protokolldetails auf der Grundlage der folgenden Zeiträume zu sortieren:

- Letzte Woche
- Letzten Monat
- Letztes Jahr
- Benutzerdefinierter Bereich
  - Wenn Sie die Option **Benutzerdefinierter Bereich** wählen, können Sie das Start- und Enddatum basierend auf dem, was Sie filtern möchten, eingeben und dann auf **Anwenden** klicken.

Die Raster-Tabellendarstellung zeigt die folgenden Informationen an:

- Kategorie – zeigt den Typ der Protokollkategorie an
- Datum und Uhrzeit – Zeigt das Datum und die Uhrzeit der Maßnahme seitens des Benutzers an
- Beschreibung – Zeigt eine Beschreibung der Maßnahme seitens des Benutzers an

Sie können die Datengitterspalten in auf- oder absteigender Reihenfolge sortieren, indem Sie auf die Spaltenüberschrift klicken. Verwenden Sie das Textfeld **Filter**, um in Ihrem Inhalt zu suchen. Unter auf dem Seitenraster werden folgende Informationen angezeigt:

Tabelle 6. Protokollverlauf

Protokollinformationen	Beschreibung
Elemente insgesamt	Zeigt die Gesamtzahl aller Protokollelemente an.
Elemente pro Bildschirm	Zeigt die Anzahl der Protokollelemente auf der angezeigten Seite an. Verwenden Sie das Drop-down-Feld, um die Anzahl der Elemente pro Seite einzustellen.
Seite	Zeigt die Seite, auf der Sie sich befinden, wenn Sie die Protokollinformationen anzeigen. Sie können auch eine Seitennummer im Textfeld eingeben oder die Schaltflächen **Vorherig** und **Nächste** verwenden, um zur gewünschten Seite zu gelangen.
Schaltflächen „Vorherig“ oder „Nächste“	Diese Schaltflächen führen Sie zu den nächsten oder vorherigen Seiten.
Symbol „Alle exportieren“	Exportiert den Protokollinhalt in eine CSV-Datei.

Protokolle anzeigen

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.
2. Zeigen Sie auf der Registerkarte **Protokoll** die Benutzeraktionen-Protokolle für Dell OpenManage Integration for VMware vCenter an. Weitere Informationen zu den angezeigten Protokollen finden Sie unter Protokollverlauf.
3. Klicken Sie auf die Spaltenüberschrift, um die Daten in der Tabelle zu sortieren.
4. Um nach Kategorien oder Zeitblöcken zu sortieren, verwenden Sie die der Tabelle vorhergehenden Dropdown-Listen.
5. Um zwischen den Seiten von Protokollelementen hin und her zu navigieren, verwenden Sie die Schaltflächen **Vorhergehend** und **Weiter**.

Protokolldateien exportieren

OpenManage Integration for VMware vCenter verwendet das CSV-Dateiformat (durch Komma getrennte Werte) für das Exportieren von Informationen aus Datentabellen.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.
2. Um den Protokollinhalt in eine CSV-Datei zu exportieren, klicken Sie in der unteren rechten Ecke des Bildschirms auf das Symbol  .
3. Suchen Sie im Dialogfeld **Speicherort für Download auswählen** den Speicherort zum Speichern der Protokollinformationen.
4. Akzeptieren Sie im Textfeld **Dateiname** entweder den Standardnamen `ExportList.csv`, oder geben Sie Ihren eigenen Dateinamen mit der Erweiterung „.CSV“ ein.
5. Klicken Sie auf **Speichern**.

5

OpenManage Integration for VMware vCenter-Lizenzierung

OpenManage Integration for VMware vCenter verfügt über zwei Arten von Lizenzen:

- Testlizenz: Wenn das OMIVV-Gerät Version 4.x zum ersten Mal gestartet wird, wird automatisch eine Testlizenz installiert. Die Testversion beinhaltet eine Test-Lizenz für fünf Host (Server), die durch OpenManage Integration for VMware vCenter verwaltet werden. Dies gilt nur für die 11. und höhere Generationen der Dell Server und ist eine Standardlizenz, die nur für einen Testzeitraum von 90 Tagen gilt.
- Standardlizenz – Die Produkt-Vollversion enthält eine Standardlizenz für bis zu zehn vCenter-Server und die erworbene Anzahl an Hostverbindungen, die von OMIVV verwaltet werden.

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 **Administration Console** hoch.

Die Lizenzierung enthält die folgenden Informationen:

- Höchstzahl der vCenter-Verbindungslizenzen – bis zu zehn registrierte und verwendete vCenter-Verbindungen sind zulässig.
- Höchstzahl der Host-Verbindungslizenzen – entspricht der Anzahl von erworbenen Lizenzen für Hostverbindungen.
- In Verwendung – die Anzahl an Lizenzen für vCenter-Verbindungen oder Hostverbindungen. Bei Hostverbindungen steht diese Zahl für die Anzahl an Hosts (oder Servern), die erfasst und in die Bestandsliste aufgenommen wurden.
- Verfügbar – die Anzahl von Lizenzen für vCenter-Verbindungen oder Hostverbindungen, die für die Nutzung zur Verfügung stehen.

ANMERKUNG: Der Standardlizenzzeitraum beträgt nur drei oder fünf Jahre und die zusätzlichen Lizenzen werden zu den existierenden Lizenzen hinzugefügt und nicht überschrieben.

Wenn Sie die Lizenzdatei kaufen, können Sie die XML-Datei (Lizenzschlüssel) über das digitale Schließfach von Dell unter http://www.dell.com/support/licensing herunterladen. Wenn Sie den/die Lizenzschlüssel nicht herunterladen können, kontaktieren Sie den Dell Support. Gehen Sie zu www.dell.com/support/incidentsonline/in/en/indhs1/email/order-support, um die Telefonnummer des Dell Supports vor Ort für Ihr Produkt zu ermitteln.

Themen:

Software-Lizenz erwerben und hochladen

Bis zum Upgrade auf eine volle Produktversion führen Sie eine Testversion aus. Verwenden Sie den Link **Lizenz kaufen** des Produkts, um zur Dell Website zu navigieren und eine Lizenz zu erwerben. Laden Sie diese nach dem Kauf unter Verwendung der **Verwaltungskonsole** hoch.

ANMERKUNG: Die Option **Lizenz kaufen** wird nur angezeigt, wenn Sie eine Testlizenz verwenden.

1. Führen Sie in OpenManage Integration for VMware vCenter einen der folgenden Tasks aus:
   - Klicken Sie im Register **Lizenzierung** neben **Software Lizenz** auf **Lizenz kaufen**.
   - Klicken Sie im Register **Erste Schritte** unter **Grundlegende Tasks** auf **Lizenz kaufen**.
2. Speichern Sie die Lizenzdatei, die Sie über den Dell Digital Locker heruntergeladen haben, an einem bekannten Speicherplatz.
3. Geben Sie die Verwaltungskonsolen-URL in einen Web-Browser ein.
   Verwenden Sie das Format: `https://<ApplianceIPAddress>`
4. Geben Sie im Anmeldefenster der **Verwaltungskonsole** das Kennwort ein, und klicken Sie auf **Anmelden**.
5. Klicken Sie auf **Lizenz hochladen**.
6. Klicken Sie zum Suchen der Lizenzdatei im Fenster **Lizenz hochladen** auf **Durchsuchen**.
7. Wählen Sie die Lizenzdatei aus, und klicken Sie auf **Hochladen**.

ANMERKUNG: 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).

6

Gerätekonfiguration für VMware vCenter

Nachdem Sie die grundlegende Installation von OMIVV und die Registrierung der vCenter abgeschlossen haben, wird der **Erstkonfigurationsassistenten** angezeigt, wenn Sie auf das OMIVV-Symbol anklicken. Sie können mit der Konfiguration des Geräts mithilfe einer der folgenden Methoden fortfahren:

- Konfigurieren des Geräts mit dem **Erstkonfigurationsassistenten**
- Konfigurieren des Geräts über die Registerkarte **Einstellungen** in OMIVV.

Sie können den **Erstkonfigurationsassistenten** zur Konfiguration der Einstellungen des OMIVV-Geräts beim ersten Start konfigurieren. Für Folgeinstanzen verwenden Sie die Registerkarte **Einstellungen**.

ANMERKUNG: Die Benutzeroberfläche ist bei beiden Methoden ähnlich.

Themen:

Konfigurationstasks im Konfigurationsassistenten

ANMERKUNG: Wenn Sie einen Webkommunikationsfehler bei der Durchführung OMIVV-bezogener Aufgaben nach dem Ändern der DNS-Einstellungen erhalten; löschen Sie den Browser-Cache, melden Sie sich vom Webclient ab und melden Sie sich dann erneut an.

Unter Verwendung des Konfigurations-Assistenten können Sie die folgenden Aufgaben anzeigen und ausführen:

- Willkommens-Seite im Konfigurationsassistenten anzeigen.
- Wählen Sie vCenter aus. Siehe Auswählen von vCenters.
- Erstellen Sie ein neues Verbindungsprofil. Siehe Erstellen eines neuen Verbindungsprofils.
- Konfigurieren von Ereignissen und Alarmen. Siehe Konfigurieren von Ereignissen und Alarmen.
- Planen Sie Bestandsaufnahme-Jobs. Siehe Planen von Bestandsaufnahme-Jobs.
- Führen Sie einen Serviceabfrage-Job aus. Siehe Ausführen eines Serviceabfrage-Jobs.

Anzeigen des Begrüßungsdialogs des Konfigurationsassistenten

Um OMIVV nach dem Installieren und Registrieren im vCenter zu konfigurieren, führen Sie folgende Schritte durch, um den **Erstkonfigurationsassistenten** anzuzeigen:

1. Klicken Sie im vSphere Web-Client auf die **Startseite** und dann auf das Symbol **OpenManage Integration.**

   Sie können eine der folgenden Optionen für den Zugriff auf den Erstkonfigurationsassistenten verwenden:

   - Wenn Sie das erste Mal auf das Symbol für **OpenManage Integration** klicken, wird der **Erstkonfigurationsassistent** automatisch angezeigt.
   - Klicken Sie unter **OpenManage Integration** > **Erste Schritte** auf **Erstkonfigurationsassistenten starten**.
2. Überprüfen Sie im Dialogfeld **Willkommen** die Schritte, und klicken Sie dann auf **Weiter**.

Auswählen der vCenter

Im Dialogfeld **vCenter-Auswahl** können Sie die folgenden vCenter konfigurieren:

- Ein spezifisches vCenter
- Alle registrierten vCenter

So zeigen Sie das Dialogfeld **vCenter-Auswahl** an:

1. Klicken Sie im **Erstkonfigurationsassistent** im Dialogfeld **Willkommen** auf **Weiter**.
2. Wählen Sie ein oder alle registrierten vCenter aus der **vCenter**-Dropdown-Liste aus.

Wählen Sie ein vCenter, das noch nicht konfiguriert wurde bzw. wenn Sie der Umgebung ein vCenter hinzugefügt haben. Die vCenter-Auswahlseite ermöglicht Ihnen die Auswahl eines oder mehrerer vCenter zur Konfiguration Ihrer Einstellungen.

3. Klicken Sie im Dialogfeld **Verbindungsprofilbeschreibung** auf **Weiter**.

   ANMERKUNG: Wenn mehrere vCenter-Server als Bestandteil des gleichen SSO vorhanden sind und mit derselben OMIVV-Anwendung registriert sind und Sie die Konfiguration eines einzelnen vCenters ausgewählt haben, müssen Sie die Schritte 1 bis 3 wiederholen, bis Sie jedes vCenter konfiguriert haben.

Verbindungsprofil erstellen

Bevor Sie die Active Directory-Anmeldeinformationen mit einem Verbindungsprofil verwenden, muss Folgendes sichergestellt werden:

- Das Active Directory-Benutzerkonto muss in Active Directory vorhanden sein.
- iDRAC und der Host müssen für die Active Directory-basierte Authentifizierung konfiguriert sein.

Ein Verbindungsprofil speichert die iDRAC- und Host-Anmeldeinformationen, die OMIVV für die Kommunikation mit Dell EMC Servern verwendet. Jeder Dell EMC Server muss einem Verbindungsprofil zugeordnet sein, damit er von OMIVV verwaltet werden kann. Sie können einem einzelnen Verbindungsprofil mehrere Server zuweisen. Sie können ein Verbindungsprofil mithilfe des Konfigurationsassistenten oder über die Registerkarte **OpenManage Integration for VMware vCenter** > **Einstellungen** erstellen. Sie können sich am iDRAC und dem Host mithilfe von Active Directory-Anmeldeinformationen anmelden.

ANMERKUNG: Die Active Directory-Anmeldeinformationen können werden entweder dieselben oder unterschiedlich für den iDRAC und den Host sein.

ANMERKUNG: Sie können ein Verbindungsprofil nicht erstellen, falls die Anzahl an hinzugefügten Hosts das Lizenzlimit zur Erstellung eines Verbindungsprofils überschreitet.

1. Klicken Sie auf das Dialogfeld **Verbindungsprofilbeschreibung** auf **Weiter**.
2. Geben Sie im Dialogfeld **Name und Anmeldeinformationen des Verbindungsprofils** den **Profilnamen** der Verbindung und eine optionale **Beschreibung** des Verbindungsprofils ein.
3. Führen Sie im Dialogfeld **Name und Anmeldeinformationen des Verbindungsprofils** unter **iDRAC-Anmeldeinformationen**, abhängig davon, ob iDRAC mit oder ohne Active Directory konfiguriert werden soll, folgende Schritte aus:

   ANMERKUNG: Das iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware, die Anwendung von Hardwareprofilen sowie von Systemprofilen bei Servern der 14. Generation und die Bereitstellung des Hypervisors.

   - Für iDRAC-IPs, auf denen Sie Active Directory benutzen möchten, und die für Active Directory bereits konfiguriert und aktiviert wurden, wählen Sie **Active Directory verwenden** aus. Anderenfalls scrollen Sie nach unten, um die iDRAC-Anmeldeinformationen zu konfigurieren.
     a. Geben Sie unter Active Directory-**Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: `Domäne\Benutzername` oder benutzername@domäne. Der Benutzername darf maximal 256 Zeichen enthalten.
     b. Geben Sie unter Active Directory-**Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
     c. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
     d. Führen Sie je nach Bedarf einen der folgenden Schritte aus:
        - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
        - Um das iDRAC-Zertifikat nicht zu speichern und dessen Prüfung während allen zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.
   - Zum Konfigurieren der iDRAC-Anmeldeinformationen ohne Active Directory führen Sie die folgenden Tasks aus:
     a. Geben Sie unter **Benutzername** den Benutzernamen ein. Der Benutzername darf maximal 16 Zeichen enthalten. Informationen zur Benutzername-Einschränkungen für Ihre Version von iDRAC finden Sie in der iDRAC-Dokumentation.
     b. Geben Sie im Feld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 20 Zeichen enthalten.
     c. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
     d. Führen Sie eine der folgenden Aktionen aus:
        - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
        - Um das iDRAC-Zertifikat nicht zu speichern und dessen Prüfung während allen zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.
4. Führen Sie unter **Host-Root** einen der folgenden Schritte aus:

- Für Hosts, auf denen Sie Active Directory benutzen möchten, und die für Active Directory bereits konfiguriert und aktiviert wurden, wählen Sie **Active Directory verwenden** aus. Anderenfalls führen Sie folgende Schritte zum Konfigurieren Ihrer Host-Anmeldeinformationen durch:
  a. Geben Sie unter Active Directory-**Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: `Domäne\Benutzername` oder benutzername@domäne. Der Benutzername darf maximal 256 Zeichen enthalten.

  ANMERKUNG: Host-Benutzernamen und Domäne-Einschränkungen finden Sie in den folgenden Informationen:

  Host-Benutzernamen-Anforderungen:

  - Zwischen 1 und 64 Zeichen lang
  - Keine nicht druckbaren Zeichen
  - Keine ungültigen Zeichen wie: " / \ [ ] : ; | = , + * ? < > @

  Host-Domänen-Anforderungen:

  - Zwischen 1 und 64 Zeichen lang
  - Das erste Zeichen muss ein alphabetisches Zeichen sein.
  - Leerzeichen sind nicht zulässig.
  - Keine ungültigen Zeichen wie: " / \ [ ] : ; | = , + * ? < > @

  b. Geben Sie unter Active Directory-**Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
  c. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
  d. Führen Sie eine der folgenden Aktionen aus:
     - Um das Host-Zertifikat herunterzuladen und zu speichern und es während allen zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
     - Um das iDRAC-Zertifikat nicht zu speichern und dessen Prüfung während allen zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.
- Um Host-Anmeldeinformationen ohne Active Directory zu konfigurieren, führen Sie die folgenden Tasks aus:
  a. Im Textfeld **Benutzername** lautet der Benutzername **`root`**. Dies ist der Standardbenutzername und Sie können ihn nicht ändern. Falls Active Directory eingestellt ist, können Sie einen beliebigen Active Directory-Benutzer auswählen, nicht nur root.
  b. Geben Sie im Feld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.

  ANMERKUNG: Die OMSA-Anmeldeinformationen sind die gleichen, die auch für die ESXi-Hosts verwendet werden.

  c. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
  d. Führen Sie eine der folgenden Aktionen aus:
     - Um das Host-Zertifikat herunterzuladen und zu speichern und es während allen zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
     - Um das Host-Zertifikat nicht zu speichern und dessen Prüfung während aller zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.

5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Dem Verbindungsprofil zugewiesene Hosts** die Hosts für das Verbindungsprofil aus und klicken auf **OK**.
7. Um das Verbindungsprofil zu prüfen, wählen Sie einen oder mehrere Hosts aus und klicken Sie auf **Verbindung testen**.

   ANMERKUNG: Dieser Schritt ist optional und überprüft, ob die Host- und iDRAC-Anmeldeinformationen korrekt sind. Der Schritt ist zwar optional, wird jedoch zum Test des Verbindungsprofils empfohlen.

   ANMERKUNG: Die Testverbindung schlägt für alle Hosts fehl, auf denen ESXi 6.5 und/oder höher mit deaktiviertem WBEM-Dienst ausgeführt wird. Für solche Hosts wird der WBEM-Dienst automatisch aktiviert, wenn Sie eine Bestandsaufnahme auf diesen Hosts durchführen. Obwohl die Testverbindung fehlschlägt, wird empfohlen, dass Sie die Aktionen des Verbindungsprofilassistenten abschließen, die Bestandsaufnahme auf den Hosts durchführen und dann das Verbindungsprofil erneut prüfen.

8. Zur Erstellung des Profils klicken Sie auf **Weiter**.
   Nachdem Sie auf „Weiter“ klicken, werden alle Details, die Sie in diesem Assistenten eingeben, gespeichert, und Sie können die Details über den Assistenten nicht mehr ändern. Sie können weitere Verbindungsprofile für dieses vCenter-Detail über die Seite **Profile** > **verwalten Verbindungsprofile** ändern oder erstellen, nachdem Sie die Konfiguration über den Konfigurationsassistenten abgeschlossen haben. Siehe Thema **Ändern von Verbindungsprofilen** in diesem Handbuch..

ANMERKUNG: Bei Servern, die nicht über eine iDRAC Express- oder Enterprise-Karte verfügen, ist das Ergebnis für den iDRAC-Verbindungstest Für dieses System nicht anwendbar.

Wenn Hosts einem Verbindungsprofil hinzugefügt werden, wird die IP-Adresse von OMIVV automatisch auf das SNMP Trap-Ziel des iDRAC des Hosts gesetzt, und OMIVV aktiviert automatisch den WBEM (Web-Based Enterprise Management)-Service für ESXi 6.5-Hosts. 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 nicht konformer Hosts, bei denen das SNMP Trap-Ziel neu konfiguriert werden muss und/oder die WBEM Services aktiviert werden müssen, finden Sie unter Berichterstattung und Festsetzen der Kompatibilität für vSphere Hosts auf Seite 131.

Planen von Bestandsaufnahme-Jobs

Sie können den Bestandsaufnahmen-Zeitplan unter Verwendung des Konfigurationsassistenten oder OpenManage Integration unter der Registerkarte **OpenManage Integration** > **Verwalten** > **Einstellungen** konfigurieren.

ANMERKUNG: Um sicherzustellen, dass OMIVV weiterhin aktualisierte Informationen anzeigt, wird empfohlen, dass Sie einen regelmäßigen Bestandsaufnahme-Job planen. Der Bestandsaufnahme-Job erfordert nur minimale Ressourcen und wirkt sich nicht negativ auf die Hostleistung aus.

ANMERKUNG: Ein Gehäuse wird automatisch erkannt, sobald die Bestandsaufnahme für alle Hosts ausgeführt wurde. Wenn das Gehäuse zu einem Gehäuse-Profil hinzugefügt wird, wird die Bestandsaufnahme automatisch ausgeführt. In einer SSO-Umgebung mit mehreren vCenter-Severn wird die Gehäusebestandsaufnahme automatisch bei jedem vCenter ausgeführt, wenn die Bestandsaufnahme für ein beliebiges vCenter planmäßig ausgeführt wird.

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. Wählen Sie im **Erstkonfigurationsassistenten** im Fenster **Bestandsaufnahme-Zeitplan Bestandsaufnahme-Datenabruf aktivieren** aus, falls dies nicht aktiviert ist. **Abrufen von Bestandsaufnahmedaten** ist standardmäßig aktiviert.
2. Führen Sie unter **Zeitplan für den Abruf von Bestandsaufnahmedaten** folgende Schritte durch:
   a. Aktivieren Sie die Kontrollkästchen neben den Wochentagen, an denen eine Bestandsaufnahme erstellt werden soll. Standardmäßig ist die Option **Auf alle Tage** ausgewählt.
   b. Geben Sie in **Uhrzeit für Bestandsaufnahme-Datenabruf** die Zeit im Format SS:MM ein.

      Bei der von Ihnen eingegebenen Zeit muss es sich um die bei Ihnen geltende Ortszeit handeln. Wenn Sie daher beabsichtigen, die Bestandsaufnahme in der Zeitzone des virtuellen Geräts auszuführen, berechnen Sie den Zeitunterschied zwischen Ihrer Lokalzeit und der Zeitzone des virtuellen Geräts und geben dann die Zeit entsprechend ein.
   c. Klicken Sie auf **Weiter**, um die Änderungen zu übernehmen und fortzufahren.

   Sobald Sie auf "Weiter" klicken, werden alle Details, die Sie in diesem Assistenten angeben, gespeichert. Sie können die Details nicht mithilfe dieses Assistenten ändern. Sie können die Details zum Bestandsaufnahme-Zeitplan der Hosts über die Registerkarte **Verwalten** > **Einstellungen** ändern, nachdem Sie die Konfiguration über den Konfigurationsassistenten abgeschlossen haben. Weitere Informationen finden Sie unter Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme auf Seite 59.

Ausführen von Serviceabfrage-Jobs

Die Konfiguration für Serviceabfrage-Jobs ist in OMIVV unter "Einstellungen" verfügbar. Darüber hinaus können Serviceabfrage-Jobs auch unter **Job-Warteschlange** > **Service** ausgeführt bzw. geplant werden. Die geplanten Jobs werden in der Job-Warteschlange aufgelistet. In einer SSO-Umgebung mit mehreren vCenter-Servern wird die Gehäusegarantie automatisch bei jedem vCenter ausgeführt, wenn die Garantie für ein beliebiges vCenter ausgeführt wird. Jedoch wird der Service nicht automatisch hinzugefügt, wenn er nicht zum Gehäuseprofil 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. Im Dialogfeld **Servicezeitplan** wählen Sie **Serviceabruf aktivieren**.
2. Führen Sie unter **Serviceabrufzeitplan** eine der folgenden Aktionen aus:
   a. Aktivieren Sie das Kontrollkästchen neben den Wochentagen, an denen die Garantie ausgeführt werden soll.
   b. Geben Sie die Uhrzeit in dem Format SS:MM ein.

Bei der von Ihnen eingegebenen Zeit muss es sich um die bei Ihnen geltende Ortszeit handeln. Wenn Sie daher beabsichtigen, die Bestandsaufnahme in der Zeitzone des virtuellen Geräts auszuführen, berechnen Sie den Zeitunterschied zwischen Ihrer Lokalzeit und der Zeitzone des virtuellen Geräts und geben dann die Zeit entsprechend ein.

3. Um die Änderungen anzuwenden und fortzufahren, klicken Sie auf **Weiter** und fahren Sie mit den Einstellungen unter **Alarm und Ereignis** fort.
   Nachdem Sie auf „Weiter“ klicken, werden alle Details, die Sie in diesem Assistenten eingeben, gespeichert, und Sie können die Details über den Assistenten nicht mehr ändern. Sie können die Details zum Serviceabfrage-Zeitplan über die Registerkarte **Einstellungen** ändern, nachdem Sie die Konfiguration über den Konfigurationsassistenten abgeschlossen haben. Weitere Informationen finden Sie unter Ändern von Service-Jobzeitplänen auf Seite 62

Konfigurieren von Ereignissen und Alarmen

Sie können Ereignisse und Alarme unter Verwendung des **Konfigurationsassistenten** oder über die Registerkarte **Einstellungen** für Ereignisse und Alarme einrichten. Zum Empfangen von Ereignissen von Servern wird OMIVV als Trap-Ziel konfiguriert. Bei Hosts der 12. Generation und höher müssen die SNMP-Trap-Ziele in iDRAC festgelegt sein. Bei Hosts vor der 12. Generation müssen die Trap-Ziele in OMSA eingestellt sein.

ANMERKUNG: OMIVV unterstützt SNMP-v1 und v2-Alarme für Hosts der 12. Generation und höher. Bei Hosts vor der 12. Generation unterstützt OMIVV nur SNMP v1-Warnungen.

1. Wählen Sie im **Erstkonfigurationsassistenten** unter **Anzeigeebenen für das Ereignis** eine der folgenden Optionen:
   - Keine Ereignisse übermitteln – Hardware-Ereignisse blockieren
   - Alle Ereignisse übermitteln – Alle Hardware-Ereignisse übermitteln
   - Nur kritische Ereignisse und Warnungsereignisse übermitteln – Nur kritische und Warnungsereignisse der Hardware übermitteln
   - Nur kritische Ereignisse und Warnungsereignisse in Bezug auf Virtualisierung übermitteln – Nur kritische und Warnungsereignisse in Bezug auf Virtualisierung übermitteln ist die Standardeinstellung für die Ereignis-Übermittlung
2. Wählen Sie **Alarme für alle Dell EMC Hosts aktivieren**, um alle Hardware-Alarme und -Ereignisse zu aktivieren.

   ANMERKUNG: Dell EMC Hosts mit aktivierten Alarmen reagieren auf bestimmte kritische Ereignisse, indem sie in den Wartungsmodus übergehen; Sie können den Alarm nach Bedarf ändern.

   Das Dialogfeld **Aktivieren der Dell EMC Alarmwarnung** wird angezeigt.
3. Um die Änderung zu akzeptieren, klicken Sie auf **Fortsetzen** oder, um den Vorgang abzubrechen, klicken Sie auf **Abbrechen**.

   ANMERKUNG: Sie müssen diesen Schritt nur dann abschließen, wenn **Alarme für Dell EMC Hosts aktivieren** ausgewählt wurde.

4. Klicken Sie auf **Standard-Alarme wiederherstellen**, um die standardmäßigen Alarm-Einstellungen für alle Dell EMC Server im vCenter wiederherzustellen.
   Es kann bis zu einer Minute dauern, bis die Änderung übernommen wird.

   ANMERKUNG: Nach dem Wiederherstellen des Geräts sind die Einstellungen für Ereignisse und Alarme nicht aktiviert, selbst wenn die GUI „Aktiviert“ anzeigt. Sie können die Einstellungen **Ereignisse und Alarme** über die Registerkarte **Einstellungen** erneut aktivieren.

   ANMERKUNG: BMC-Traps verfügen nicht über Meldungs-IDs. Warnungen enthalten also demzufolge diese Details nicht in OMIVV.

5. Klicken Sie auf **Anwenden**.

Konfigurationsaufgaben über die Registerkarte Einstellungen

Unter Verwendung der Registerkarte Einstellungen können Sie die folgenden Konfigurationsaufgaben anzeigen und ausführen:

- Aktivieren des OMSA-Links. Siehe Aktivieren des OMSA-Links.
- Konfigurieren der Einstellungen für die Serviceablaufbenachrichtigung. Siehe Konfigurieren der Einstellungen für die Serviceablaufbenachrichtigung.
- Einrichten des Firmware-Aktualisierungs-Repositorys. Siehe Einrichten des Firmware-Aktualisierungs-Repositorys.
- Konfigurieren der Benachrichtigung zur aktuellen Geräteversion. Siehe Konfigurieren der Benachrichtigung zur aktuellen Geräteversion.

- Konfigurieren und Anzeigen von Ereignissen und Alarmen. Siehe Konfigurieren von Ereignissen und Alarmen.
- Anzeigen von Zeitplänen für den Abruf von Daten für Bestandsaufnahmen und Service. Siehe Anzeigen von Zeitplänen für den Abruf von Daten für Bestandsaufnahmen und Service.

Geräteeinstellungen

In diesem Abschnitt konfigurieren Sie das folgende OMIVV-Gerät:

- Garantieablaufbenachrichtigung
- Repository für die Firmware-Aktualisierung
- Benachrichtigung über aktuelle Geräteversion
- Anmeldeinformationen für die Bereitstellung

Konfigurieren von Serviceablaufbenachrichtigungseinstellungen

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Einstellungen** unter **unter Geräteeinstellungen** auf **Serviceablaufbenachrichtigung**.
2. Erweitern Sie **Serviceablaufbenachrichtigung** zur Anzeige folgender Optionen:
   - **Serviceablaufbenachrichtigung** – Zeigt an, ob die Einstellung aktiviert oder deaktiviert ist
   - **Warnung** – Einstellung der Anzahl der Tage bis zur ersten Warnung
   - **Kritisch** – Einstellung der Anzahl der Tage bis zur kritischen Warnung
3. Zur Konfiguration der Serviceablaufschwellenwerte für eine Warnung zum Serviceablauf klicken Sie auf das Symbol  auf der rechten Seite der **Serviceablaufbenachrichtigung**.
4. Verfahren Sie im Dialogfeld **Serviceablaufbenachrichtigung** wie folgt:
   a. Falls Sie diese Einstellung aktivieren möchten, wählen Sie **Serviceablaufbenachrichtigung für Hosts aktivieren** aus. Durch die Auswahl des Kontrollkästchens wird die Serviceablaufbenachrichtigung aktiviert.
   b. Verfahren Sie unter **Mindesttageschwellenwertalarm** wie folgt:
      i. Wählen Sie in der Drop-Down-Liste **Warnung** den zeitlichen Abstand in Tagen aus, mit dem Sie vor Ablauf des Service gewarnt werden wollen.
      ii. Wählen Sie in der Drop-Down-Liste **Kritisch** den zeitlichen Abstand in Tagen aus, mit dem Sie vor Ablauf des Service gewarnt werden wollen.
5. Klicken Sie auf **Anwenden**.

Repository für die Firmwareaktualisierung einrichten

Sie können das Firmware-Aktualisierungs-Repository der Registerkarte **Einstellungen** von OMIVV erstellen.

1. Klicken Sie in OpenManage Integration für VMware vCenter auf der Registerkarte **Verwalten** > **Einstellungen** unter **Geräteeinstellungen** auf der rechten Seite des Repository für die **Firmwareaktualisierung** auf das Symbol  .
2. Wählen Sie im Dialogfeld **Repository für die Firmware-Aktualisierung** eine der folgenden Optionen aus:
   - **Dell Online**: Sie können auf den Speicherort, der das Repository für die Firmware-Aktualisierung von Dell (ftp.dell.com) verwendet, zugreifen. OpenManage Integration for VMware vCenter lädt ausgewählte Firmware-Aktualisierungen vom Dell Repository herunter und aktualisiert die verwalteten Hosts.
     ANMERKUNG: Je nach Art Ihrer Netzwerk-Einstellungen müssen Sie Proxy-Einstellungen aktivieren, wenn Ihr Netzwerk Proxy benötigt.
   - **Freigegebener Netzwerkordner**: Sie können über ein lokales Repository der Firmware in einer CIFS-basierten oder NFS-basierten Netzwerkfreigabe verfügen. Dieses Repository kann ein Abbild der Server Update Utility (SUU), das Dell regelmäßig veröffentlicht, oder ein benutzerdefiniertes Repository sein, das unter Verwendung von DRM erstellt wurde. OMIVV muss auf diese Netzwerkfreigabe zugreifen können.
     ANMERKUNG: Wenn Sie CIFS-Freigabe verwenden, dürfen die Kennwörter für Repositorien nicht mehr als 31 Zeichen umfassen.
     ANMERKUNG: Stellen Sie sicher, dass Sie die neueste DRM-Version (Dell EMC Repository Manager) (3.0) verwenden.
3. Wenn Sie **Freigegebenen Netzwerkordner** ausgewählt haben, dann geben Sie den **Speicherort der Katalogdatei** unter Verwendung des folgenden Formats ein:
   - NFS-Freigabe für xml-Datei – host:/share/filename.xml

- NFS-Freigabe für gz-Datei – host: /share/filename.gz
- CIFS-Freigabe für xml-Datei – \\host\share/filename.xml
- CIFS-Freigabe für gz-Datei – \\host\share/filename.gz

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

ANMERKUNG: Wenn Sie CIFS-Freigabe verwenden, fordert OMIVV Sie dazu auf, den Benutzernamen und das Kennwort einzugeben. Die Zeichen @, % und , werden für die Verwendung in Benutzernamen/Kennwörtern für freigegebene Netzwerkordner nicht unterstützt.

4. Klicken Sie auf **Anwenden**, nachdem das Herunterladen abgeschlossen ist.

ANMERKUNG: Das Lesen des Katalogs von der Quelle und das Aktualisieren der OMIVV-Datenbank kann 60 bis 90 Minuten dauern.

Konfigurieren der Benachrichtigung über aktuelle Geräteversion

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 in OpenManage Integration for VMware vCenter auf die Registerkarte **Verwalten → Einstellungen** unter **Geräteeinstellungen**, rechts neben **Benachrichtigung über aktuelle Geräteversion** auf das Symbol für klicken. Standardmäßig ist die Benachrichtigung zur aktuellen Version deaktiviert.
2. Führen Sie im Dialogfeld **Benachrichtigung zur aktuellen Version und Abrufplan** folgende Schritte aus:
   a. Wenn Sie die Benachrichtigung zur aktuellen Version aktivieren möchten, wählen Sie das Kontrollkästchen **Benachrichtigung zur aktuellen Version aktivieren** aus.
   b. Wählen Sie unter **Letzter Serviceabrufzeitplan** die Wochentage für den Job aus.
   c. Geben Sie bei **Abrufzeit der aktuellen Version** die erforderliche Ortszeit an.
   Die von Ihnen angegebene Zeit entspricht Ihrer Ortszeit. Stellen Sie sicher, dass Sie jeglichen Zeitunterschied zur Ausführung dieser Aufgabe für die Zeit auf dem OMIVV-Gerät einkalkulieren.
3. Klicken Sie zum Speichern der Einstellungen auf **Anwenden**, klicken Sie zum Zurücksetzen der Einstellungen auf **Löschen**, und klicken Sie zum Abbrechen des Vorgangs auf **Abbrechen**.

Konfigurieren von Anmeldeinformationen für die Bereitstellung

Die Anmeldeinformationen für die Bereitstellung ermöglichen Ihnen die Einrichtung der Anmeldeinformationen zur sicheren Kommunikation mit einem Bare-Metal-System, das mithilfe der Auto-Ermittlung erkannt wird, bis die Bereitstellung des Betriebssystems vollständig ist. Zur sicheren Kommunikation mit iDRAC verwendet OMIVV Anmeldeinformationen für die Bereitstellung von der ersten Erfassung bis zum Ende des Bereitstellungsprozesses. Nachdem der BS-Bereitstellungsvorgang erfolgreich abgeschlossen wurde, ändert OMIVV die Anmeldeinformationen von iDRAC wie im Verbindungsprofil angegeben. Wenn Sie die Anmeldeinformationen der Bereitstellung ändern, werden alle neu erkannten Systeme ab diesem Punkt mit den neuen Anmeldeinformationen bereitgestellt. Die Anmeldeinformationen auf Servern, die vor der Änderung der Anmeldeinformationen der Bereitstellung erfasst wurden, sind von dieser Änderung nicht betroffen.

ANMERKUNG: OMIVV fungiert als Bereitstellungsserver. Die Anmeldeinformationen für die Bereitstellung werden benutzt, um mit dem iDRAC zu kommunizieren, der das OMIVV-Plug-in als Provisionierungsserver im Prozess der automatischen Ermittlung verwendet.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Einstellungen** > **Verwalten** unter **Geräteeinstellungen** auf der rechten Seite der **Anmeldeinformationen der Bereitstellung** auf das Symbol für .
2. Geben Sie in **Anmeldeinformationen für die Bereitstellung eines Bare-Metal-Servers** unter **Anmeldeinformationen** die folgenden Werte ein:
   - Geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.

     Der Benutzername darf nicht mehr als 16 (ASCII-druckbare Zeichen) umfassen.
   - Geben Sie das Kennwort in das Textfeld **Kennwort** ein.

     Das Kennwort darf nicht mehr als 20 (ASCII-druckbare Zeichen) umfassen.
   - Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.

     Stellen Sie sicher, dass die Kennwörter übereinstimmen.

3. Zum Speichern der angegebenen Anmeldeinformationen klicken Sie auf **Anwenden**.

vCenter-Einstellungen

In diesem Abschnitt konfigurieren Sie die folgenden vCenter-Einstellungen:

- Aktivieren von OMSA-Links. Siehe Aktivieren des OMSA-Links.
- Ereignisse und Alarme konfigurieren. Siehe Konfigurieren von Ereignissen und Alarmen.
- Konfigurieren von Zeitplänen für den Abruf von Daten für Bestandsaufnahmen und Service. Siehe Konfigurieren von Zeitplänen für den Abruf von Daten für Bestandsaufnahmen und Service.

Aktivieren von OMSA-Link

Installieren und konfigurieren Sie den OMSA Web Server vor dem Aktivieren des OMSA-Links. Anweisungen, wie Sie den Webserver für die verwendete OMSA-Version installieren und konfigurieren finden Sie im Installationshandbuch *Dell OpenManage Server Administrator Installation Guide*.

ANMERKUNG: OMSA wird nur auf PowerEdge-Servern der 11. Generation oder älter benötigt.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Einstellungen** > **Verwalten** unter **vCenter-Einstellungen** rechts neben der URL des OMSA Webservers auf das Symbol für .
2. Geben Sie im Dialogfeld **OMSA-Web-Server-URL** die URL ein.
   Stellen Sie sicher, dass Sie die vollständige URL zusammen mit HTTPS und der Portnummer 1311 angeben.
   https://<OMSA Server-IP oder FQDN>:1311
3. Zur Anwendung der OMSA-URL auf alle vCenter wählen Sie **Diese Einstellungen auf alle vCenter anwenden** aus.

   ANMERKUNG: Wenn Sie das Kontrollkästchen nicht aktivieren, wird die OMSA-URL nur auf ein vCenter angewandt.

4. Um zu überprüfen, ob der OMSA-URL-Link, den Sie bereitgestellt haben, funktioniert, navigieren Sie zur Registerkarte **Zusammenfassung** des Hosts und überprüfen, ob der OMSA-Konsolenlink im Abschnitt **Dell Host-Information** aktiv ist.

Konfigurieren von Ereignissen und Alarmen

Im Dialogfeld „Ereignisse und Alarme“ im Dell EMC Management Center können alle Hardware-Alarme aktiviert oder deaktiviert werden. Der aktuelle Alarm-Status wird auf der Registerkarte „Alarme“ im vCenter angezeigt. Ein kritisches Ereignis deutet auf einen tatsächlichen oder bevorstehenden Datenverlust oder auf einen Systemausfall hin. Ein Warnereignis bedarf nicht unbedingt sofortiger Aufmerksamkeit, kann aber auf ein mögliches zukünftiges Problem hindeuten. Die Ereignisse und Alarme können auch mit dem VMware Alarm Manager aktiviert werden. Die Ereignisse werden auf der Registerkarte „Tasks und Ereignisse“ im vCenter in der Ansicht „Hosts und Cluster“ angezeigt. Um die Ereignisse von den Servern zu empfangen, ist OMIVV als SNMP-Trap-Ziel konfiguriert. Für Hosts der 12. Generation und höher wird das SNMP-Trap-Ziel in iDRAC festgelegt. Bei Hosts vor der 12. Generation wird das Trap-Ziel in OMSA eingestellt.
Sie können die Ereignisse und Alarme im Dell OpenManage Integration for VMware vCenter auf der Registerkarte **Verwaltung** > **Einstellungen** konfigurieren. Erweitern Sie unter den vCenter-**Einstellungen** die Überschrift **Ereignisse und Alarme** zur Anzeige der vCenter-Alarme für Dell EMC Hosts (Aktiviert oder Deaktiviert) und der Ereignisanzeigeebene.

ANMERKUNG: OMIVV unterstützt SNMP v1-Alarme und -v2-Alarme für Hosts der 12. Generation und höher. Bei Hosts vor der 12. Generation unterstützt OMIVV SNMP v1-Alarme.

ANMERKUNG: Um die Dell Ereignisse zu erhalten, müssen Sie Alarme sowie Ereignisse aktivieren.

1. Erweitern Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Einstellungen** unter **vCenter Einstellungen Ereignisse und Alarme**.
   Es werden die aktuellen **vCenter-Alarme für Dell EMC Hosts** (Aktiviert/Deaktiviert) oder alle vCenter-Alarme und die **Ereignisanzeigeebene** angezeigt.
2. Klicken Sie auf das Symbol rechts neben **Ereignisse und Alarme**.
3. Wählen Sie **Alarme für alle Dell EMC Hosts aktivieren**, um alle Hardware-Alarme und -Ereignisse zu aktivieren.

   ANMERKUNG: Die Dell EMC Hosts mit aktivierten Alarmen reagieren auf kritische Ereignisse, indem sie in den Wartungsmodus wechseln; Sie können den Alarm nach Bedarf ändern.

4. Klicken Sie auf **Standard-Alarme wiederherstellen**, um die standardmäßigen Alarm-Einstellungen für alle Dell-Server im vCenter wiederherzustellen.
   Es kann bis zu einer Minute dauern, bis die durch diesen Schritt bewirkten Änderung in Kraft treten; er ist nur verfügbar, wenn **Alarme für Dell EMC Hosts aktivieren** ausgewählt ist.
5. Wählen Sie unter **Ereignisanzeigeebene** entweder „Keine Ereignisse veröffentlichen“, „Alle Ereignisse veröffentlichen“, „nur kritische Ereignisse und Warnungsereignisse veröffentlichen“ oder „nur virtualisierungsbezogene kritische Ereignisse und Warnungsereignisse veröffentlichen“ aus. Weitere Informationen finden Sie unter Ereignisse, Alarme und Systemüberwachung.
6. Falls Sie diese Einstellungen auf alle vCenters anwenden möchten, wählen Sie **Diese Einstellungen auf alle vCenters anwenden** aus.

   ANMERKUNG: Die Auswahl der Option überschreibt die vorhandenen Einstellungen für alle vCenters.

   ANMERKUNG: Die Option ist nicht verfügbar, wenn Sie bereits **Alle registrierten vCenter** aus der Dropdown-Liste auf der Registerkarte **Einstellungen** ausgewählt haben.

7. Klicken Sie zum Speichern auf **Anwenden**.

Anzeigen der Datenabrufzeitpläne für Bestandsaufnahme und Service

1. Klicken Sie in OpenManage Integration with VMware vCenter auf die Registerkarte **Verwalten** > **Einstellungen** unter **vCenter-Einstellungen** auf **Zeitplan für den Abruf von Daten**.
   Der „Zeitplan für den Abruf von Daten“ wird bei Anklicken erweitert, um die Zeitpläne für Bestandsaufnahme und Service aufzudecken.
2. Klicken Sie auf das Symbol neben **Bestandslistenabfrage** oder **Serviceabfrage**.
   Im Dialogfeld **Bestandslisten-/Serviceabfrage** können Sie die folgenden Informationen zur Bestandslisten- oder Serviceabfrage anzeigen:
   - Sie sehen, ob die Bestandsaufnahme- und/oder Serviceabfrage aktiviert oder deaktiviert ist.
   - Sie sehen die Wochentage, für die diese Option aktiviert ist.
   - Sie sehen die Tageszeit, zu der sie aktiviert ist.
3. Wenn Sie den Zeitplan für den Abruf von Daten ändern wollen, lesen Sie die Abschnitte Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme oder Ändern eines Service-Jobzeitplans.
4. Klicken Sie erneut auf **Zeitplan für den Abruf von Daten**, um die Pläne der Bestandsaufnahme und den Service zusammenzuführen und in einer einzigen Zeile anzuzeigen.

Konfigurieren einer SNMP-Trap-Communityzeichenfolge

1. Klicken Sie auf der Seite **OpenManage Integration for VMware vCenter** auf der Registerkarte **Verwalten** > **Einstellungen** unter **Geräteeinstellungen** auf das an der **OMSA-SNMP-Trap-Communityzeichenfolge**.
   Das Dialogfeld **Einstellungen zur OMSA-SNMP-Trap-Communityzeichenfolge** wird angezeigt. Standardmäßig wird in der SNMP-Trap-Communityzeichenfolge **public** angezeigt.
2. Passen Sie den **public**-Text an eine beliebige Zeichenfolge an und klicken Sie auf **Anwenden**.

   ANMERKUNG: Die Konfiguration der SNMP-Trap-Communityzeichenfolge für PowerEdge-Server der 11. Generation wird während der Installation oder Aktualisierung von OMSA über OMIVV festgelegt.

7

Verwenden der Registerkarte „Baseline“

Sie können mit der Baseline-Registerkarte ein Repository-Profil und ein Clusterprofil erstellen.

Themen:

Repository-Profil

Ein Repository-Profil ermöglicht es Ihnen, mehrere Treiber- oder Firmware-Repository-Profile zu erstellen oder pflegen. Diese Treiber- oder Firmware-Repository-Profile können für Folgendes verwendet werden:

- Im Baseline-Profile zur Identifizierung von Abweichungen für vSAN-Cluster.
- Zum Aktualisieren von Treibern oder Firmware für vSAN-Cluster oder vSAN-Clusterknoten.

ANMERKUNG:

- Verwenden Sie einen benutzerdefinierten Firmwarekatalog, der speziell für Ihre vSAN-Umgebungen erstellt wurde.
- Ein Treiber-Repository-Profil kann maximal 10 Treiber besitzen.

  ANMERKUNG: Stellen Sie sicher, dass nicht mehr als 10 Offline-Pakete vorhanden sind (.zip-Dateien). Falls weitere Dateien vorhanden sind, ist die Auswahl der Treiber zufällig.
- Für Treiber-Repository-Profile werden nur asynchrone, VIB-formatierte Treiber von Offline-Paketen verwendet (.zip-Dateien).

  ANMERKUNG: Nur die erforderlichen asynchronen VIB-Treiber, die entsprechend den vSAN-Anforderungen validiert sind. Weitere Informationen finden Sie in der VMware Hardware-Kompatibilitätsmatrix.
- Für Treiber-Repository-Profile benötigt OMIVV Schreibzugriff auf die CIFS- oder NFS-Freigabe.
- Bei Treiber-Repository-Profilen werden Dateien in Unterordnern oder Dateien von mehr als 10 MB Größe nicht berücksichtigt.
- Erst nach dem erfolgreichen Parsen stehen die Repository-Profile zur Verwendung im **Baseline-Profil** oder zum Ausführen eines Jobs zum Aktualisieren des vSAN-Treibers oder der Firmware zur Verfügung.
- Wenn mehr als eine Version der Firmware verfügbar ist, wird immer die neueste Firmware-Version für den Kompatibilitätsvergleich verwendet.

Führen Sie zum Starten der Repository-Profilseite die folgende Schritte durch:

1. Klicken Sie auf der Seite **OpenManage Integration für VMware vCenter** auf die Registerkarte **Verwalten** > **Baseline**, erweitern Sie die **Baseline-Info** und klicken Sie dann auf **Repository-Profil**.
   a. Auf der Seite **Repository-Profil** können Sie eine Liste der Repository-Profile sehen, die Sie erstellt haben.

      Es wird eine Tabelle angezeigt, die die Repository-Profile zusammen mit **Profilname**, **Beschreibung**, **Typ**, **Freigabepfad**, **Zeitpunkt der letzten erfolgreichen Aktualisierung** und **Letzter Aktualisierungsstatus** auflistet.

   b. Um weitere Details eines Repository-Profils zu sehen, wählen Sie das gewünschte Repository-Profil aus.

      Sehen Sie sich die angezeigten Repository-Profilinformationen an, z. B. **Profilname**, **Freigabepfad**, **Erstellungsdatum**, **Änderungsdatum** und **Zuletzt geändert von**.

   c. Um die Spalten innerhalb der Datentabelle zu vertauschen, ziehen Sie diese an die gewünschte Stelle.
   d. Um die Inhalte der Datentabelle zu filtern oder zu durchsuchen, geben Sie im Feld **Filtern** die Filterkriterien ein.

e. Um die Details des Repository-Profils in eine .csv-Datei zu exportieren, wählen Sie ein Repository-Profil aus und klicken Sie dann in der rechten Ecke der Datentabelle auf das Symbol  .

Erstellen eines Repository-Profils

1. Klicken Sie auf der Seite **OpenManage Integration für VMware vCenter** auf **Verwalten** > **Baseline**, erweitern Sie **Baseline-Info** und klicken Sie dann auf **Repository-Profil**.
2. Klicken Sie auf  .
3. Lesen Sie sich auf der **Willkommen**-Seite die Anweisungen durch und klicken Sie auf **Weiter**, um weitere Details hinzuzufügen:
   a. Geben Sie im Feld **Profilname** den Repository-Profilnamen ein.
   b. Geben Sie im Feld **Profilbeschreibung** eine Beschreibung ein (dies ist optional).
   c. Klicken Sie auf **Weiter**.
4. Wählen Sie im Dialogfeld **Profileinstellungen** einen der folgenden Repository-Typen aus:
   - Firmware (standardmäßig ist die Option ausgewählt)
   - Treiber

   a. Geben Sie im Feld **Repository-Freigabespeicherort** den Repository-Freigabespeicherort ein (CIFS oder NFS).
   b. Geben Sie für die CIFS-Freigabe den Benutzernamen und das Kennwort ein. Folgende Zeichen sind für das Kennwort nicht erlaubt: &, ! ,@ ,% und <.

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

   c. Klicken Sie zum Validieren des Zugriffs für den angegebenen Repository-Pfad und das Vorhandensein der Katalogdatei für das Firmware- und Treiber-Repository auf **Test starten**. Diese Validierung ist zwingend erforderlich, um fortzufahren.

    : Zeigt an, dass die Testverbindung erfolgreich ist.

    : Zeigt an, dass die Testverbindung fehlgeschlagen ist.

   d. Klicken Sie auf **Next** (Weiter).

   ANMERKUNG: Laden Sie für das Treiber-Repository die Offline-Treiber-.zip-Dateien herunter, speichern Sie sie am Freigabespeicherort und geben Sie den vollständigen Pfad des Freigabespeicherorts an. OMIVV erstellt automatisch den Katalog im Inneren des OMIVV-Geräts. VIB-Treiber-Pakete stehen unter https://my.vmware.com/web/vmware/downloads zur Verfügung.

5. Klicken Sie auf **Next** (Weiter).
   Die Seite **Zusammenfassung** wird angezeigt. Diese Seite zeigt die Informationen zum Repository-Profil an.
6. Klicken Sie auf **Fertigstellen**.
   Nach dem Erstellen des Katalogs, startet der Katalog-Download und das Parsen, außerdem wird der Status auf der Startseite des Repository-Profils angezeigt.

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

Repository-Profil bearbeiten

1. Klicken Sie auf der Seite **OpenManage Integration für VMware vCenter** auf **Verwalten** > **Baseline**, erweitern Sie **Baseline-Info** und klicken Sie dann auf **Repository-Profil**.
2. Wählen Sie ein Repository-Profil aus, das Sie bearbeiten möchten und klicken Sie auf  .
3. Im **Repository-Profil**-Assistenten können Sie **Profilname** und **Beschreibung** bearbeiten (Letzteres ist optional). Klicken Sie dann auf **Weiter**.
4. Führen Sie im Dialogfeld **Profileinstellungen** die folgenden Schritte aus:
   a. Hier können Sie die CIFS-Anmeldeinformationen bearbeiten.
   b. Klicken Sie zum Validieren des Zugriffs für den angegebenen Repository-Pfad und das Vorhandensein der Katalogdatei für das Firmware- und Treiber-Repository auf **Test starten**. Diese Validierung ist zwingend erforderlich, um fortzufahren.

: Zeigt an, dass die Testverbindung erfolgreich ist.

: Zeigt an, dass die Testverbindung fehlgeschlagen ist.

c. Klicken Sie zum Aktualisieren des aktuellen Inhalts am angegebenen Speicherort des Repository auf **Mit Repository-Speicherort synchronisieren**.

ANMERKUNG: Standardmäßig ist die Option ***Mit Repository-Speicherort synchronisieren*** ausgewählt. Stellen Sie sicher, dass diese Option aktiviert ist, wenn Sie den Katalog über den aktuellen Treiber- oder Firmwarekatalog (Freigabespeicherort) neu erstellen möchten.

5. Klicken Sie auf **Weiter**.
   Die Seite **Zusammenfassung** wird angezeigt. Diese Seite zeigt die Informationen zum Repository-Profil an.
6. Klicken Sie auf **Fertigstellen**.

Löschen eines Repository-Profils

Stellen Sie vor dem Löschen des Repository-Profils sicher, dass Sie die Verknüpfung zwischen dem Repository-Profil und den zugehörigen Cluster-Profilen aufheben.

1. Klicken Sie auf der Seite **OpenManage Integration für VMware vCenter** auf **Verwalten** > **Baseline**, erweitern Sie **Baseline-Info** und klicken Sie dann auf **Repository-Profil**.
2. Wählen Sie ein Repository-Profil aus, das Sie löschen möchten, und klicken Sie dann auf .
3. Um das Profil zu löschen, klicken Sie im Bestätigungsdialogfeld auf **Ja** oder zum Abbrechen des Vorgangs auf **Nein**.

Clusterprofil

Mithilfe des Clusterprofils können Sie die Baseline-Konfiguration wie die Hardwarekonfiguration (nur für Server der 14. Generation), Firmware oder Treiberversionen erfassen und den gewünschten Status für vSAN-Cluster beibehalten, indem Sie die Abweichung gegenüber der Baseline identifizieren.

ANMERKUNG:

- Firmware- und Treiberrepository-Profile müssen nach dem Erstellen analysiert werden, bevor sie für die Erstellung eines Clusterprofils verwendet werden können.
- Sobald das Clusterprofil erstellt wird, löst es den Abweichungserkennung-Job aus.
- Wenn ein Cluster mit einem Clusterprofil verknüpft wird, werden vorherige Clusterprofil-Zuordnungen überschrieben.

Führen Sie zum Starten der Seite des Clusterprofils folgende Schritte durch:

1. Klicken Sie auf der Seite **OpenManage Integration für VMware vCenter** auf die Registerkarte **Verwalten** > **Baseline**, erweitern Sie die **Baseline-Info** und klicken Sie dann auf **Clusterprofil**.
   a. Die Seite **Clusterprofile** zeigt die Liste der Clusterprofile, die Sie erstellt haben.

      Es wird eine Tabelle angezeigt, die die Clusterprofile zusammen mit **Profilname**, **Beschreibung**, **Zugeordnetes Systemprofil**, **Zugeordnetes Firmware-Repository-Profil**, **Zugeordnetes Treiber-Repository-Profil**, **Zeitpunkt der letzten erfolgreichen Aktualisierung** auflistet.

      ANMERKUNG: Wenn eine aktuelle Version der Repository-Profile für ein vorhandenes Cluster-Profil verfügbar ist, wird ein Warnsymbol für das zugehörige Firmware- oder Treiber-Profil angezeigt.

   b. Um weitere Details eines Clusterprofils anzuzeigen, wählen Sie das gewünschte Clusterprofil aus.

      Sehen Sie sich die Clusterprofilinformationen an, die Details zu **Profilname**, **Erstellungsdatum**, **Änderungsdatum** und **Zuletzt geändert von** enthalten.

   c. Um die Spalten innerhalb der Datentabelle zu vertauschen, ziehen Sie diese an die gewünschte Stelle.
   d. Um die Inhalte der Datentabelle zu filtern oder zu durchsuchen, verwenden Sie das Feld **Filtern**.
   e. Um die Details des Repository-Profils in eine .csv-Datei zu exportieren, wählen Sie ein Repository-Profil aus und klicken dann in der rechten Ecke der Datentabelle auf .

Clusterprofil erstellen

1. Systemprofil, Repository-Profil für Firmware und Treiber, homogene Servermodelle für das Cluster.
2. vSAN-Cluster muss in vCenter vorhanden sein.
3. Ein Verbindungsprofil muss für mindestens einen Host im vSAN-Cluster erstellt werden und die Bestandsaufnahme muss erfolgreich ausgeführt werden.

ANMERKUNG: Wenn mehrere eigenständige vCenter in OMIVV registriert sind, wird empfohlen, eindeutige Cluster-Profile für die einzelnen vCenter zu erstellen.

ANMERKUNG: Bei der Erstellung des Clusterprofils wird ein aktueller Snapshot des zugehörigen Firmware- und Treiberrepositorys für die Baseline erstellt. Wenn sich die Repositorys ändern, müsste das Clusterprofil erneut aktualisiert werden, um die Änderungen widerzuspiegeln. Andernfalls werden Aktualisierungen, die für die Repositorys durchgeführt werden, nicht im ursprünglichen Clusterprofil-Snapshot aktualisiert.

1. Klicken Sie auf der Seite **OpenManage Integration für VMware vCenter** auf **Verwalten** > **Baseline**, erweitern Sie **Baseline-Info** und klicken Sie dann auf **Clusterprofil**.
2. Klicken Sie auf  .
3. Lesen Sie sich auf der **Willkommen**-Seite die Anweisungen durch und klicken Sie auf **Weiter**, um weitere Details hinzuzufügen:
   a. Geben Sie im Feld **Profilname** den Cluster-Profilnamen ein.
   b. Geben Sie im Feld **Profilbeschreibung** eine Beschreibung des Clusterprofils ein. Die Profilbeschreibung ist optional.
   c. Klicken Sie auf **Weiter**.
4. Führen Sie im Dialogfeld **Profileinstellungen** die folgenden Schritte aus:
   a. Wählen Sie das Systemprofil oder Repository-Profil (Firmware-Repository-Profil oder Treiber-Repository-Profil) oder entsprechende Kombinationen aus.

      ANMERKUNG: Das Systemprofil ist nur für Server der 14. Generation relevant.

      ANMERKUNG: Dell EMC empfiehlt, die Baseline mit Systemprofil, Firmware- und Treiber-Repository zu erstellen.

   b. Klicken Sie auf **Weiter**.
5. Führen Sie im Dialogfeld **Profilzuordnung** die folgenden Schritte aus:
   a. Wählen Sie den registrierten vCenter-Server aus der Drop-Down-Liste aus.
   b. Klicken Sie auf **Durchsuchen**, um die erforderlichen vSAN-Cluster zuzuordnen.
   c. Klicken Sie auf **Weiter**.
6. Wählen Sie im Dialogfeld **Abweichungserkennungszeitplan** Tag und Uhrzeit aus und klicken Sie auf **Weiter**.
   Die **Zusammenfassung**-Seite wird angezeigt. Diese Seite enthält die Informationen zum Cluster-Profil.
7. Klicken Sie auf **Fertigstellen**.
   Das Clusterprofil wird automatisch gespeichert und wird auf der Seite **Clusterprofil** angezeigt.

   ANMERKUNG: Der Abweichungserkennungsjob wird sofort nach dem Speichern des Clusterprofils sowie später zur geplanten Zeit durchgeführt.

Clusterprofil bearbeiten

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

1. Klicken Sie auf der Seite **OpenManage Integration für VMware vCenter** auf **Verwalten** > **Baseline**, erweitern Sie **Baseline-Info** und klicken Sie dann auf **Clusterprofil**.
2. Wählen Sie ein Clusterprofil aus, das Sie bearbeiten möchten und klicken Sie auf  .
3. Auf dem **Clusterprofil**-Assistenten können Sie die **Beschreibung** bearbeiten, die optional ist, und dann auf **Weiter** klicken.

   ANMERKUNG: Sie können den Profilnamen nicht bearbeiten.

4. Im **Profileinstellungen**-Dialogfeld können Sie die Profilkombinationen ändern.

5. Im **Profilzuordnung**-Dialogfeld können Sie die im Clusterprofil erforderlichen Zuordnungen und Konfigurationen ändern.
6. Im **Profilkonfiguration**-Dialogfeld können Sie den **Abweichungserkennungszeitplan** bearbeiten und auf **Weiter** klicken.
   Die Seite **Zusammenfassung** wird angezeigt. Diese Seite zeigt die aktualisierten Informationen zum Clusterprofil.
7. Klicken Sie auf **Fertigstellen**.

   Das aktualisierte Clusterprofil wird automatisch gespeichert und im Clusterprofil-Fenster angezeigt.

   ANMERKUNG: Der Abweichungserkennungsjob wird sofort nach dem Speichern des Clusterprofils sowie später zur geplanten Zeit durchgeführt.

Clusterprofil löschen

1. Klicken Sie auf der Seite **OpenManage Integration für VMware vCenter** auf **Verwalten** > **Baseline**, erweitern Sie **Baseline-Info** und klicken Sie dann auf **Clusterprofil**.
2. Wählen Sie ein Clusterprofil aus, das Sie löschen möchten und klicken Sie auf .
3. Um das Profil zu löschen, klicken Sie im Bestätigungsdialogfeld auf **Ja** oder zum Abbrechen des Vorgangs auf **Nein**.
   Wenn das Clusterprofil gelöscht wird, wird auch der entsprechende Treiber-Erkennungsjob gelöscht.

8

Profile

Anmeldeprofile ermöglichen Ihnen die Verwaltung und Konfiguration von Verbindungsprofilen und der Gehäuseprofile, die **Bereitstellungsvorlage** ermöglicht die Verwaltung und Konfiguration von Hardware- und Hypervisor-Profilen.

Themen:

Informationen zum Verbindungsprofil

Auf der Registerkarte **Verbindungsprofile** können Sie Verbindungsprofile verwalten und konfigurieren, die Anmeldeinformationen enthalten, die das virtuelle Gerät für die Kommunikation mit Dell EMC Servern verwendet. Weisen Sie jeden Dell EMC Server nur einem einzigen Verbindungsprofil zur Verwaltung durch Dell OpenManage Integration for VMware vCenter zu. Sie können einzelnen Verbindungsprofilen mehrere Server zuweisen. Nachdem Sie den **Erstkonfigurationsassistenten** ausgeführt haben, können Sie die Verbindungsprofile vom OpenManage Integration for VMware vCenter über folgende Aktivitäten verwalten:

- Anzeigen von Verbindungsprofilen
- Erstellen eines neuen Verbindungsprofils
- Ändern von Verbindungsprofilen
- Löschen von Verbindungsprofilen
- Testen von Verbindungsprofilen

Verbindungsprofile anzeigen

Bevor ein Verbindungsprofil angezeigt werden kann, muss es erstellt werden und/oder existieren. Nachdem eines oder mehrere Verbindungsprofile erstellt wurden, können diese auf der Seite **Verbindungsprofile** angezeigt werden. OpenManage Integration for VMware vCenter verwendet die in den Profilen angegebenen Anmeldeinformationen für die Kommunikation mit Dell EMC Hosts.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Verwalten**.
2. Klicken Sie auf **Profile**, und klicken Sie dann auf **Anmeldeprofile**.
3. Erweitern Sie **Anmeldeprofile**, und klicken Sie auf die Registerkarte **Verbindungsprofile**.

   Sie können alle Verbindungsprofile anzeigen, die Sie erstellt haben.

Tabelle 7. Informationen zu Verbindungsprofilen

Felder der Verbindungsprofile	Beschreibung
Profilname	Zeigt den Namen des Verbindungsprofils an
Beschreibung	Zeigt eine Beschreibung an, falls vorhanden
vCenter	Zeigt den vollständigen qualifizierten Domänennamen (FQDN) oder den Hostnamen oder aber die IP-Adresse des vCenter entsprechend dem Kontext an
Zugeordnete Hosts	Zeigt die Hosts an, denen ein Verbindungsprofil zugewiesen wurde. Gibt es mehr als einen, können Sie alle über das Erweiterungssymbol anzeigen.
iDRAC-Zertifikatsüberprüfung	Gibt an, ob die iDRAC-Zertifikatsüberprüfung aktiviert oder deaktiviert ist
Host-Stamm-Zertifikatsüberprüfung	Gibt an, ob die Host-Stamm-Zertifikatsüberprüfung aktiviert oder deaktiviert ist
Date Created (Erstellungsdatum)	Zeigt das Datum an, an dem das Verbindungsprofil erstellt wurde

Tabelle 7. Informationen zu Verbindungsprofilen (fortgesetzt)

Felder der Verbindungsprofile	Beschreibung
Date Modified (Geändertes Datum)	Zeigt das Datum an, an dem das Verbindungsprofil geändert wurde
Zuletzt geändert von	Zeigt die Details des Benutzers an, der das Verbindungsprofil geändert hat

Verbindungsprofil erstellen

Sie können einem einzelnen Verbindungsprofil mehrere Hosts zuweisen. Führen Sie die folgenden Schritte durch, um ein Verbindungsprofil zu erstellen:

ANMERKUNG: Die vCenter-Hosts, die während dieses Vorgangs aufgeführt werden, wurden unter Verwendung desselben Single Sign On (SSO) authentifiziert. Falls Sie keinen vCenter-Host sehen, befindet dieser sich evtl. auf einem anderen SSO oder Sie verwenden vielleicht eine VMware vCenter-Version unter 5.5.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Profile** → **Anmeldeprofile** → **Verbindungsprofile** auf ✚.
2. Zeigen Sie die Informationen auf der Seite **Willkommen** an, lesen Sie die Anweisungen, und klicken Sie auf **Weiter**.
3. Geben Sie auf der Seite **Verbindungsprofil** die folgenden Daten ein:
   a. Geben Sie unter **Profil** den **Profilnamen** und optional eine **Beschreibung** ein.
   b. Wählen Sie unter **vCenter** die vCenter-Server aus der Drop-Down-Liste aus, für die das Profil erstellt werden soll. Mit dieser Option können Sie ein eindeutiges Verbindungsprofil für jedes vCenter erstellen.
   c. Führen Sie im Bereich **iDRAC-Anmeldeinformationen** einen der folgenden Tasks aus:

      ANMERKUNG: Das iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware, Anwendung von Hardware-Profilen und die Bereitstellung des Hypervisors.

      - Für iDRAC, auf denen Sie Active Directory benutzen möchten, und die für Active Directory bereits konfiguriert und aktiviert wurden, markieren Sie das Kontrollkästchen **Active Directory verwenden**. Anderenfalls springen Sie zur nächsten Option.
        - Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: `Domäne\Benutzername` oder `domäne@benutzername`. Der Benutzername darf maximal 256 Zeichen enthalten. Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zum Microsoft Active Directory.
        - Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
        - Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
        - Zum Überprüfen des iDRAC-Zertifikats wählen Sie eine der folgenden Optionen aus:
          - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
          - Wenn Sie keine Prüfung ausführen und das Zertifikat nicht speichern möchten, deaktivieren Sie **Zertifikatprüfung aktivieren**.
      - Zum Konfigurieren der iDRAC-Anmeldeinformationen ohne Active Directory führen Sie die folgenden Aktionen aus:
        - Geben Sie den Benutzernamen in das Textfeld **Benutzername** ein. Der Benutzername darf maximal 16 Zeichen enthalten. Informationen zu Einschränkungen in Sachen Benutzername für Ihre Version von iDRAC finden Sie in der iDRAC-Dokumentation.

          ANMERKUNG: Das lokale iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware, Anwendung von Hardware-Profilen und die Bereitstellung des Hypervisors.
        - Geben Sie das Kennwort in das Textfeld **Kennwort** ein. Das Kennwort darf maximal 20 Zeichen enthalten.
        - Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
        - Zum Überprüfen des iDRAC-Zertifikats wählen Sie eine der folgenden Optionen aus:
          - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
          - Wenn Sie keine Prüfung ausführen und das Zertifikat nicht speichern möchten, wählen Sie **Zertifikatprüfung aktivieren** nicht aus.
   d. Führen Sie im **Host-Root**-Bereich eine der folgenden Aktionen aus:

- Für Hosts, die für Active Directory, auf dem Sie Active Directory benutzen möchten, bereits konfiguriert und aktiviert sind, wählen Sie das Kontrollkästchen **Active Directory verwenden** aus. Anderenfalls gehen Sie nach unten, um Ihre Host-Anmeldeinformationen zu konfigurieren.
  - Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: `Domäne\Benutzername` oder `domäne@benutzername`. Der Benutzername darf maximal 256 Zeichen enthalten. Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zum Microsoft Active Directory.
  - Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
  - Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
  - Wählen Sie für die Zertifikatsprüfung eine der folgenden Optionen aus:
    - Um das Host-Zertifikat herunterzuladen und zu speichern und es während allen zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
    - Wenn Sie keine Prüfung ausführen und das Zertifikat nicht speichern möchten, wählen Sie **Zertifikatprüfung aktivieren** nicht aus.

- Um Host-Anmeldeinformationen ohne Active Directory zu konfigurieren, führen Sie die folgenden Aktionen aus:
  - Im Textfeld **Benutzername** heißt der Benutzername root.

    Der Root-Benutzername ist der standardmäßige Benutzername, Sie können diesen nicht ändern.

    ANMERKUNG: Falls das Active Directory eingestellt ist, können Sie einen beliebigen Active Directory-Benutzer auswählen, nicht root.
  - Geben Sie im Textfeld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
  - Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
  - Wählen Sie für die Zertifikatsprüfung eine der folgenden Optionen aus:
    - Um das Host-Zertifikat herunterzuladen und zu speichern und es während allen zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
    - Wenn Sie keine Prüfung ausführen und das Zertifikat nicht speichern möchten, wählen Sie **Zertifikatprüfung aktivieren** nicht aus.

ANMERKUNG: Die OMSA-Anmeldeinformationen sind die gleichen, die auch für die ESXi-Hosts verwendet werden.

4. Klicken Sie auf **Next** (Weiter).
5. Wählen Sie im Dialogfeld **Hosts auswählen** die Hosts für dieses Verbindungsprofil aus und klicken Sie auf **OK**.
6. Wählen Sie bei Bedarf auf der Seite **Zugeordnete Hosts** einen oder mehrere Hosts für das Verbindungsprofil aus.

   Zum Hinzufügen von Hosts klicken Sie auf  , wählen Sie die Hosts aus und klicken Sie dann auf **OK**.
7. Um das Verbindungsprofil zu prüfen, wählen Sie einen oder mehrere Hosts aus und klicken Sie auf das  .

   ANMERKUNG: Dieser Schritt ist optional und überprüft, ob die Host- und iDRAC-Anmeldeinformationen korrekt sind. Dieser Schritt ist optional, aber es wird empfohlen, das Verbindungsprofil zu testen.

   ANMERKUNG: Die Testverbindung schlägt für alle Hosts fehl, auf denen ESXi 6.5 und/oder höher mit deaktiviertem WBEM-Dienst ausgeführt wird. Für solche Hosts wird der WBEM-Dienst automatisch aktiviert, wenn Sie eine Bestandsaufnahme auf diesen Hosts durchführen. Obwohl die Testverbindung fehlschlägt, wird empfohlen, dass Sie die Aktionen des Verbindungsprofilassistenten abschließen, die Bestandsaufnahme auf den Hosts durchführen und dann das Verbindungsprofil erneut prüfen.
8. Klicken Sie auf **Weiter**, um die Profilerstellung abzuschließen.
   Bei Servern, die nicht über eine iDRAC Express- oder Enterprise-Karte verfügen, lautet das Ergebnis für den iDRAC-Verbindungstest **Für dieses System nicht anwendbar**.

Wenn Hosts einem Verbindungsprofil hinzugefügt werden, wird die IP-Adresse von OMIVV automatisch auf das SNMP Trap-Ziel des iDRAC des Hosts gesetzt, und OMIVV aktiviert automatisch den WBEM (Web-Based Enterprise Management)-Service für ESXi 6.5-Hosts. 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. Details zur Anzeige nicht konformer Hosts, für die das SNMP Trap-Ziel neu konfiguriert und/oder der WBEM-Service aktiviert werden muss, finden Sie unter Ausführen des Assistenten zur Reparatur nicht konformer vSphere-Hosts.

Ändern von Verbindungsprofilen

Nachdem Sie ein Verbindungsprofil konfiguriert haben, können Sie den Profilnamen, die Beschreibung, zugeordnete Hosts und iDRAC sowie Host-Anmeldeinformationen bearbeiten.

ANMERKUNG: Die während dieses Vorgangs aufgelisteten **vCenter** wurden unter Verwendung desselben Single Sign On (SSO) authentifiziert. Falls Sie keinen vCenter-Host sehen, befindet dieser sich evtl. auf einem anderen SSO oder Sie verwenden eine VMware vCenter-Version unter 5.5.

ANMERKUNG: Stellen Sie sicher, dass Sie ein Verbindungsprofil nicht aktualisieren, wenn ein Job für die Bestandsaufnahme-/Serviceliste oder ein Bereitstellungsauftrag ausgeführt wird.

ANMERKUNG: Stellen Sie sicher, dass Sie keinen Host, der einem Verbindungsprofil zugeordnet ist, zu einem anderen Verbindungsprofil verschieben oder einen Host aus einem Verbindungsprofil entfernen, wenn eine Bestandsaufnahme, eine Garantie oder ein Bereitstellungsauftrag ausgeführt wird.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Verwalten**.
2. Klicken Sie auf **Profile**, und klicken Sie dann auf **Anmeldeprofile**.
3. Erweitern Sie **Anmeldeprofile** und klicken Sie dann auf **Verbindungsprofile**.
4. Wählen Sie ein Profil aus und klicken Sie auf .
5. Klicken Sie in der **Willkommen**-Registerkarte des Fensters **Verbindungsprofil**, lesen Sie die Informationen, und klicken Sie auf **Weiter**.
6. Führen Sie auf der Registerkarte **Name und Anmeldeinformationen** folgende Schritte aus:
   a. Geben Sie unter **Profil** den **Profilnamen** und eine **Beschreibung** ein, die optional ist.
   b. Zeigen Sie unter **vCenter** die zugeordneten Hosts für dieses Verbindungsprofil an. Beachten Sie den obigen Hinweis dazu, warum Sie die Hosts hier angezeigt sehen.
   c. Führen Sie unter **iDRAC-Anmeldeinformationen** einen der folgenden Schritte aus:
      - Für die iDRAC-Konten, auf denen Sie Active Directory benutzen möchten, und die für Active Directory bereits konfiguriert und aktiviert wurden, markieren Sie das Kontrollkästchen **Active Directory verwenden**.
        - Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: `domain\benutzername`, `domain/benutzernamen` oder `benutzername@domain`. Der Benutzername darf maximal 256 Zeichen enthalten. Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zum Microsoft Active Directory.
        - Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
        - Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
        - Wählen Sie für die Zertifikatsprüfung eine der folgenden Optionen aus:
          - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
          - Wenn Sie keine Prüfung ausführen und das Zertifikat nicht speichern möchten, wählen Sie **Zertifikatprüfung aktivieren** nicht aus.
      - Um die iDRAC-Anmeldeinformationen ohne Active Directory zu konfigurieren, geben Sie Folgendes ein:
        - **Benutzername** – Geben Sie den Benutzernamen in einem dieser Formate ein: `Domäne\Benutzername` oder `domäne@benutzername`.

          Diese Zeichen sind für den Benutzernamen zulässig: `/` (Schrägstrich), `&` (kaufmännisches Und-Zeichen), `\` (umgekehrter Schrägstrich), `.` (Punkt), `"` (Anführungszeichen), `@` (kaufmännisches A), `%` (Prozent) (Begrenzung auf 127 Zeichen).

          Die Domain darf nur alphanumerische Zeichen enthalten, z. B. – (Bindestrich) und `.` (Punkt) (Begrenzung auf 254 Zeichen). Das erste und letzte Zeichen der Domain muss alphanumerisch sein.

        - **Kennwort** – Geben Sie das Kennwort ein.

          Die folgenden Zeichen sind für das Kennwort nicht zulässig: `/` (Schrägstrich), `&` (kaufmännisches Und-Zeichen), `\` (umgekehrter Schrägstrich), `.` (Punkt), `"` (Anführungszeichen).

        - **Kennwort bestätigen** – Geben Sie das Kennwort erneut ein.
        - **Zertifikatprüfung aktivieren** – Standardmäßig ist dieses Kontrollkästchen nicht markiert. Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**. Wenn Sie keine Prüfung ausführen und das Zertifikat nicht speichern möchten, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren** nicht.

          ANMERKUNG: Wenn Sie Active Directory verwenden, wählen Sie **Zertifikatsprüfung aktivieren** aus.

d. Führen Sie unter **Host Root** folgende Tasks aus:
   - Für den Zugriff auf alle mit Active Directory verbundenen Konsolen wählen Sie das Kontrollkästchen **Active Directory verwenden** aus.
   - **Benutzername** – Der Standardbenutzername ist root und kann nicht geändert werden. Falls **Active Directory verwenden** ausgewählt ist, können Sie einen beliebigen Active Directory-Benutzernamen verwenden.

     ANMERKUNG: Der **Benutzername** lautet root; dieser Eintrag kann nicht geändert werden, wenn Sie nicht **Active Directory verwenden** wählen. Der iDRAC-Benutzer muss die root-Anmeldung nicht nutzen; ist Active Directory eingestellt, kann es sich um jeden Benutzer mit Administrator-Berechtigungen handeln.
   - **Kennwort** – Geben Sie das Kennwort ein.

     Die folgenden Zeichen sind für das Kennwort nicht zulässig: `/` (Schrägstrich), `&` (kaufmännisches Und), `\` (Umgekehrter Schrägstrich), `.` (Punkt), `"` (Anführungszeichen).
   - **Kennwort bestätigen** – Geben Sie das Kennwort erneut ein.
   - **Zertifikatprüfung aktivieren** – Standardmäßig ist dieses Kontrollkästchen nicht markiert. Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**. Wenn Sie keine Prüfung ausführen und das Zertifikat nicht speichern möchten, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren** nicht.

     ANMERKUNG: Wenn Sie Active Directory verwenden, wählen Sie **Zertifikatsprüfung aktivieren** aus.

     ANMERKUNG: Die OMSA-Anmeldeinformationen sind die gleichen, die auch für die ESXi-Hosts verwendet werden.

     ANMERKUNG: Bei Hosts, die nicht über eine iDRAC Express- oder Enterprise-Karte verfügen, lautet das Ergebnis für den iDRAC-Verbindungstest **Für dieses System nicht anwendbar**.

7. Klicken Sie auf **Weiter**.
8. Wählen Sie im Dialogfeld **Hosts auswählen** die Hosts für dieses Verbindungsprofil aus.
9. Auf **OK**.klicken.

   Im Dialogfeld **Zugeordneter Host** können Sie die iDRAC- und die Host-Anmeldeinformationen auf den ausgewählten Servern testen.
10. Führen Sie einen der folgenden Schritte aus:
    - Klicken Sie auf **Fertigstellen**, um ein Verbindungsprofil ohne Test der Anmeldeinformationen zu erstellen.
    - Wählen Sie zum Beginnen des Tests die zu überprüfenden Hosts aus und klicken Sie auf das Symbol

      

      . Die anderen Optionen sind inaktiv.

      ANMERKUNG: Die Testverbindung schlägt für alle Hosts fehl, auf denen ESXi 6.5 und/oder höher mit deaktiviertem WBEM-Dienst ausgeführt wird. Für solche Hosts wird der WBEM-Dienst automatisch aktiviert, wenn Sie eine Bestandsaufnahme auf diesen Hosts durchführen. Obwohl die Testverbindung fehlschlägt, wird empfohlen, dass Sie die Aktionen des Verbindungsprofilassistenten abschließen, die Bestandsaufnahme auf den Hosts durchführen und dann das Verbindungsprofil erneut prüfen.

      Sobald der Test abgeschlossen ist, klicken Sie auf **Fertigstellen**.
    - Klicken Sie zum Stoppen der Tests auf **Alle Tests abbrechen**. Klicken Sie im Dialogfeld **Tests abbrechen** auf **OK** und anschließend auf **Fertigstellen**.

ANMERKUNG: Die Felder **Änderungsdatum** und **Zuletzt geändert von** zeigen Änderungen an, die Sie über die Web-Client-Schnittstelle für ein Verbindungsprofil vorgenommen haben. Änderungen, die das OMIVV auf dem entsprechenden Verbindungsprofil vornimmt, haben keinen Einfluss auf diese beiden Felddetails.

Löschen von Verbindungsprofilen

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

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Verwalten**.
2. Klicken Sie auf **Profile**, und klicken Sie dann auf **Anmeldeprofile**.
3. Erweitern Sie **Anmeldedaten-Profile**, klicken Sie auf die Registerkarte **Verbindungsprofile**, und wählen Sie dann das Profil aus, das Sie löschen möchten.

4. Klicken Sie auf .
5. Um das Profil zu löschen, klicken Sie auf **Ja** für die Meldung „Löschen bestätigen“ oder, um die Löschen-Aktion abzubrechen, klicken Sie auf **Nein**.

ANMERKUNG: OMIVV verwaltet jedoch keine Hosts, die Bestandteil des Verbindungsprofils sind, das Sie gelöscht haben, bis diese Hosts zu einem anderen Verbindungsprofil hinzugefügt werden.

ANMERKUNG: Stellen Sie vor dem Löschen des Verbindungsprofils sicher, dass Sie den geplanten Firmware-Aktualisierungsjob löschen.

Testen von Verbindungsprofilen

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Verwalten**.
2. Klicken Sie auf **Profile**, und klicken Sie dann auf **Anmeldeprofile**.
3. Erweitern Sie **Anmeldeprofile**, und klicken Sie auf die Registerkarte **Verbindungsprofile**. Wählen Sie dann ein Verbindungsprofil aus.
4. Wählen Sie im Dialogfeld **Verbindungsprofil testen** die Hosts aus, die Sie testen wollen, und klicken Sie anschließend auf das Symbol .

   Wenn Sie kein Verbindungsprofil auswählen, dauert der Test einige Zeit.
5. Klicken Sie zum Stoppen aller ausgewählter Tests und zum Beenden des Testens auf **Alle Tests abbrechen**. Klicken Sie im Dialogfeld **Tests abbrechen** auf **OK**.
6. Klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Informationen zum Gehäuseprofil

OMIVV kann alle Dell EMC Servern zugeordneten Dell EMC Gehäuse überwachen. Für die Überwachung des Gehäuses wird ein Gehäuse-Profil benötigt. Sie können Gehäuse-Profile über folgende Aufgaben verwalten:

- Gehäuse-Profile anzeigen. Siehe Gehäuse-Profile anzeigen.
- Gehäuse-Profile erstellen. Siehe Erstellen eines Gehäuseprofils.
- Gehäuseprofile bearbeiten. Siehe Bearbeiten eines Gehäuseprofils.
- Gehäuse-Profile löschen. Siehe Löschen eines Gehäuseprofils.
- Gehäuseprofile testen. Siehe Testen eines Gehäuse-Profils.

Anzeigen von Gehäuseprofilen

Stellen Sie sicher, dass Sie ein Gehäuseprofil erstellen oder ein Gehäuseprofil vorhanden ist, bevor Sie die Anzeige starten.

Nachdem eines oder mehrere Gehäuseprofile erstellt wurden, können diese auf der Seite „Gehäuseprofile“ angezeigt werden.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Verwalten**.
2. Klicken Sie auf **Profile**, und klicken Sie dann auf **Anmeldeprofile**.
3. Erweitern Sie **Anmeldeprofile**, und klicken Sie auf die Registerkarte **Gehäuseprofile**.
   Die Gehäuseprofile werden angezeigt.
4. Um alle zugehörigen Gehäuse anzuzeigen, klicken Sie auf das Symbol für wenn mehrere Gehäuse mit dem Gehäuseprofil verbunden sind.
5. Zeigen Sie auf der Seite **Gehäuseprofile** die Gehäuseinformationen an.

Tabelle 8. Informationen zum Gehäuseprofil

Gehäusefelder	Beschreibung
Profilname	Zeigt den Namen des Gehäuseprofils an
Beschreibung	Zeigt eine Beschreibung an, falls vorhanden
Gehäuse-IP/Hostname	Zeigt die IP-Adresse oder den Hostnamen des Gehäuses an
Service-Tag-Nummer des Gehäuses	Zeigt die dem Gehäuse zugewiesene eindeutige Kennung an

Tabelle 8. Informationen zum Gehäuseprofil (fortgesetzt)

Gehäusefelder	Beschreibung
Date Modified (Geändertes Datum)	Zeigt das Datum an, an dem das Gehäuseprofil geändert wurde

Erstellen eines Gehäuse-Profils

Für die Überwachung des Gehäuses wird ein Gehäuse-Profil benötigt. Gehäuse-Anmeldeinformationenprofile können einem oder mehreren Gehäusen zugewiesen werden.

Sie können sich am iDRAC und dem Host mithilfe von Active Directory-Anmeldeinformationen anmelden.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Verwalten**.
2. Klicken Sie auf **Profile**, und klicken Sie dann auf **Anmeldeprofile**.
3. Erweitern Sie **Anmeldedaten-Profile**, und klicken Sie auf die Registerkarte **Gehäuseprofile**.
4. Klicken Sie auf der Seite **Gehäuse-Profile** auf das Symbol , um ein **Neues Gehäuse-Profil** zu erstellen.
5. Führen Sie auf der Seite des **Gehäuse-Profil-Assistenten** die folgenden Schritte aus:

   Führen Sie Folgendes im Abschnitt **Name und Anmeldeinformationen** unter **Gehäuseprofil** aus:

   a. Geben Sie den Profilnamen in das Textfeld **Profilname** ein.
   b. Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein, dies ist optional.

   Führen Sie Folgendes im Abschnitt **Anmeldeinformationen** aus:

   a. Geben Sie im Textfeld **Benutzername** den Benutzernamen mit Administratorrechten ein, der in der Regel für die Anmeldung am Chassis Management Controller verwendet wird.
   b. Geben Sie im Textfeld **Kennwort** das Kennwort für den entsprechenden Benutzernamen ein.
   c. Geben Sie im Textfeld **Kennwort überprüfen** dasselbe Kennwort ein, das Sie im Textfeld **Kennwort** eingegeben haben. Die Kennwörter müssen übereinstimmen.

   ANMERKUNG: Bei den Anmeldeinformationen kann es sich um lokale oder Active-Directory-Anmeldeinformationen handeln. Bevor Sie die Active Directory-Anmeldeinformationen mit einem Verbindungsprofil verwenden, müssen das Active Directory-Benutzerkonto in Active Directory vorhanden, und der Chassis Management Controller für die Active Directory-basierte Authentifizierung konfiguriert sein.

6. Klicken Sie auf **Weiter**.

   Es wird die Seite **Gehäuse auswählen** angezeigt, auf der alle verfügbaren Gehäuse aufgeführt werden.

   ANMERKUNG: Gehäuse werden erkannt und stehen erst nach erfolgreicher Durchführung der Bestandsaufnahme aller unter einem Gehäuse vorhandenen modularen Hosts für die Zuordnung zu diesem Gehäuseprofil zur Verfügung.

7. Um entweder ein einzelnes Gehäuse oder mehrere Gehäuse auszuwählen, wählen Sie die entsprechenden Kontrollkästchen neben der Spalte **IP/Host-Name** aus.

   Wenn das ausgewählte Gehäuse bereits Teil eines anderen Profils ist, wird eine Warnungsmeldung angezeigt, die darauf hinweist, dass das ausgewählte Gehäuse einem Profil zugeordnet ist.

   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.
8. Auf **OK**.klicken.

   Die Seite **Zugewiesene Gehäuse** wird angezeigt.
9. Wählen Sie das Symbol aus, um die Konnektivität des Gehäuses zu testen, wobei die Anmeldeinformationen geprüft werden und das Ergebnis in der Spalte **Testergebnis** als **Bestanden** oder **Durchgefallen** angezeigt wird.
10. Um das Profil abzuschließen, klicken Sie auf **Fertig stellen**.

Gehäuseprofil bearbeiten

Nachdem Sie ein Gehäuse-Profil erstellt haben, können Sie den Profilnamen, die Beschreibung, die zugeordneten Gehäuse und die Anmeldeinformationen bearbeiten.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Verwalten**.
2. Klicken Sie auf **Profile**, und klicken Sie dann auf **Anmeldeprofile**.

3. Erweitern Sie **Anmeldeprofile**, und klicken Sie auf die Registerkarte **Gehäuseprofile**. Wählen Sie dann ein Gehäuseprofil aus.
4. Klicken Sie auf das Symbol im Hauptmenü.
   Die Fenster **Gehäuse-Profil bearbeiten** wird angezeigt.
5. Unter **Gehäuse-Profil** können Sie den **Profilnamen** und eine **Beschreibung** bearbeiten, die optional ist.
6. Unter dem Bereich **Anmeldeinformationen** können Sie den **Benutzernamen**, das **Kennwort** und **Kennwort bestätigen** bearbeiten.
   Das Kennwort, das Sie in **Kennwort bestätigen** eingeben, muss dem im Feld **Kennwort** eingegebenen entsprechen. Die eingegebenen Anmeldeinformationen müssen über Administratorrechte auf dem Gehäuse verfügen.
7. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.
   Mit der Registerkarte **Zugeordnetes Gehäuse** können Sie Gehäuse und Anmeldeinformationen des ausgewählten Gehäuses testen. Führen Sie einen der folgenden Schritte aus:
   - Um den Test zu beginnen, wählen Sie entweder ein einzelnes Gehäuse oder mehrere Gehäuse zum Prüfen aus und klicken Sie anschließend auf das Symbol . klicken. Die Spalte **Testergebnis** zeigt an, ob die Testverbindung erfolgreich war oder nicht.
   - Sie können eines oder mehrere Gehäuse löschen oder zu einem Gehäuse-Profil hinzufügen.

   ANMERKUNG: Wenn die Gehäuse nicht inventarisiert sind, werden nur IP/Host-Name und Service-Tag-Nummer angezeigt. Die Felder **Gehäusename** und **Modell** werden angezeigt, sobald das Gehäuse inventarisiert ist.

Löschen von Gehäuseprofilen

ANMERKUNG: Stellen Sie vor dem Löschen des Gehäuseprofils sicher, dass die Gehäuseinstanzen nicht Teil anderer vCenter sind, bei denen OMIVV registriert ist.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Verwalten**.
2. Klicken Sie auf **Profile**, und klicken Sie dann auf **Anmeldeprofile**.
3. Erweitern Sie **Anmeldedaten-Profile**, und klicken Sie auf die Registerkarte **Gehäuseprofile**.
4. Wählen Sie ein Gehäuseprofil aus, das Sie löschen möchten, und klicken Sie auf .
   Es wird eine Bestätigungsmeldung angezeigt.
5. Um den Löschvorgang fortzusetzen, klicken Sie auf **Ja**, oder, um den Löschvorgang abzubrechen, klicken Sie auf **Nein**.
   Wenn alle einem Gehäuseprofil zugeordneten Gehäuseprofile gelöscht oder zu anderen Profilen verschoben wurden, wird eine Bestätigungsmeldung über das Löschen angezeigt, die besagt, dass das Gehäuseprofil keine zugeordneten Gehäuse aufweist und gelöscht wird. Klicken Sie auf **OK**, um das Gehäuseprofil zu löschen und die Bestätigungsmeldung zu erhalten.

ANMERKUNG: OMIVV überwacht solange nicht die Gehäuse, die mit den Gehäuse-Profilen verbunden sind, die Sie gelöscht haben, bis diese Gehäuse einem anderen Gehäuse-Profil hinzugefügt werden.

ANMERKUNG: Wenn das Gehäuseprofil gelöscht wird, werden die zugehörigen Daten zum Garantieverlauf nicht aus dem Garantieverlauf gelöscht.

Gehäuseprofil testen

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Verwalten**.
2. Klicken Sie auf **Profile**, und klicken Sie dann auf **Anmeldeprofile**.
3. Erweitern Sie **Anmeldeinformationsprofile** und klicken Sie auf die Registerkarte **Gehäuseprofile**. Wählen Sie ein einzelnes oder mehrere Gehäuseprofile zu Testen aus.
   Dieser Vorgang kann mehrere Minuten dauern.
4. Wählen Sie im Dialog **Gehäuse-Profil testen** das Gehäuse aus, das Sie testen möchten, und klicken Sie anschließend auf das Symbol .
5. Klicken Sie zum Abbrechen aller ausgewählter Tests und zum Beenden des Testens auf **Alle Tests abbrechen**. Klicken Sie im Dialogfeld **Tests abbrechen** auf **OK**.
6. Klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

9

Bestandsaufnahme. und Service-Management

Nachdem Sie OMIVV konfiguriert haben, können Sie die Bestandsaufnahme und Service-Jobs überwachen, Bereitstellungs-Jobs verwalten und Firmware-Aktualisierungsjobs in der Registerkarte **Überwachen** verwalten. Die Bestandsaufnahme und der Service werden im **Erstkonfigurationsassistenten** oder auf der Registerkarte **Einstellungen** eingerichtet.

Die Seite der Job-Warteschlange verwaltet die folgenden Jobs:

- Anzeigen der übermittelten Jobs zur Serverbereitstellung oder Firmwareaktualisierung.
- Aktualisieren von Firmwareaktualisierung und der Bereitstellungs-Jobs oder der Bestandsliste/Serviceverlauf-Warteschlangen.
- Planen einer Bestandsaufnahme oder eines Service-Jobs.
- Löschen der Einträge in der Bereitstellungs-Job- oder Firmwareaktualisierungs-Warteschlange.

ANMERKUNG: Um sicherzustellen, dass die Bestandsaufnahme-/Serviceliste aktuelle Informationen enthält, planen Sie einen Job für die Bestandsaufnahme-/Serviceliste, der mindestens einmal pro Woche ausgeführt wird.

Aufgaben, die Sie für diesen Zeitplan ausführen können, umfassen:

- Verwalten von Bereitstellungs-Jobs
- Verwalten von Firmwareaktualisierungs-Jobs
- Verwalten von Bestandsaufnahme-Jobs
- Verwalten von Service-Jobs

ANMERKUNG: Stellen Sie für alle erwähnten Jobs sicher, dass diese erneut geplant werden, wenn die Gerätezeit zu einem zukünftigen Datum geändert bzw. wiederhergestellt wird.

ANMERKUNG: Für die grundlegende Zustandsüberwachung stellen Sie sicher, dass Sie einen Neustart des OMIVV-Geräts vornehmen. Für die erweiterte Zustandsüberwachung stellen Sie sicher, dass Sie **Erweiterte Überwachung** deaktivieren und dann in der OMIVV-Verwaltungskonsole aktivieren.

Themen:

Bestandaufnahme-Jobs

Bestandaufnahme-Jobs werden unter Verwendung der Registerkarte **Einstellungen** oder des **Erstkonfigurationsassistenten** eingerichtet. Verwenden Sie die Registerkarte **Bestandsaufnahmenverlauf**, um die Bestandsaufnahme-Jobs anzuzeigen. Sie können diese Tasks von dieser Registerkarte aus durchführen:

- Anzeigen von Hosts oder Gehäuse-Bestandsaufnahme
- Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme
- Sofortiges Ausführen eines Gehäuse-Bestandsaufnahme-Jobs

Host-Bestand anzeigen

Eine erfolgreich beendete Bestandsaufnahme ist erforderlich, um die Daten zu sammeln. Wenn die Bestandsaufnahme vollständig ist, können Sie die Ergebnisse der Bestandsaufnahme für das ganze Rechenzentrum oder für ein einzelnes Hostsystem anzeigen. Sie können die Spalten der Bestandsliste in aufsteigender und/oder absteigender Reihenfolge sortieren.

ANMERKUNG: Im Folgenden sind einige mögliche Ursachen dafür aufgeführt, wenn vom Host keine Daten abgerufen und angezeigt werden können:

- Dem Host wurde kein Verbindungsprofil zugeordnet, weswegen kein Bestandsaufnahme-Job durchgeführt werden kann.
- Es wurde kein Bestandsaufnahme-Job auf dem Host ausgeführt, um die Daten zu erfassen. Somit können keine Daten angezeigt werden.
- Die Anzahl der Hostlizenzen wurde überschritten. Sie müssen zusätzliche Lizenzen erwerben, um den Bestandsaufnahme-Job vollständig abschließen zu können.
- Der Host verfügt nicht über die erforderliche iDRAC-Lizenz für PowerEdge-Server der 12. Generation oder höher. Sie müssen entsprechend die korrekte iDRAC-Lizenz erwerben.
- Die Anmeldeinformationen können möglicherweise falsch sein.
- Der Host ist möglicherweise nicht erreichbar.

So zeigen Sie die Details zum Host-Bestand an:

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.
2. Klicken Sie auf **Bestandsaufnahme-Warteschlange**, **Bestandsaufnahme-Verlauf** und klicken Sie dann auf **Host-Bestand**. Die Informationen über vCenter werden im oberen Raster angezeigt.
3. Wählen Sie zur Anzeige der Hostinformationen auf einem ausgewählten vCenter ein vCenter aus, um alle zugeordneten Host-Details anzuzeigen.
4. Überprüfen Sie die Host-Inventarinformationen.

Tabelle 9. vCenter, Host-Informationen

vCenter	
vCenter	Zeigt die vCenter-Adresse an
Bestandene Hosts	Zeigt alle ausgefallenen Hosts an
Letzte Bestandsaufnahme	Zeigt das Datum und die Uhrzeit an, zu dem der letzte Bestandsaufnahmenzeitplan ausgeführt wurde
Nächste Bestandsaufnahme	Zeigt das Datum und die Uhrzeit an, zu dem der nächste Bestandsaufnahmenzeitplan ausgeführt wird
Hosts	
Host	Zeigt die Host-Adresse an.
Status	Zeigt den Status an. Zu den Filteroptionen zählen: • Erfolgreich • Fehlgeschlagen • Wird durchgeführt • Geplant
Dauer (MM:SS)	Zeigt die Dauer des Jobs in Minuten und Sekunden an
Startdatum und -uhrzeit	Zeigt das Datum und die Uhrzeit an, zu dem der Bestandsaufnahmenzeitplan gestartet wurde
Enddatum und -zeit	Zeigt die Uhrzeit des Endes des Bestandsaufnahmenzeitplans an

Gehäuse-Bestandsaufnahme anzeigen

Eine erfolgreich beendete Bestandsaufnahme ist erforderlich, um die Daten zu sammeln. Sie können die Spalten der Bestandsliste in aufsteigender und/oder absteigender Reihenfolge sortieren.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.
2. Klicken Sie auf **Jobwarteschlange**, **Bestandsaufnahme-Verlauf** und erweitern Sie dann **Gehäuse-Bestandsaufnahme**.
3. Überprüfen Sie die Gehäuse-Bestandslisteninformationen.

Tabelle 10. Gehäuseinformationen

Gehäuse-Bestandsaufnahme	
Gehäuse-IP-Adresse	Zeigt die IP-Adresse des Gehäuses an

Tabelle 10. Gehäuseinformationen (fortgesetzt)

Gehäuse-Bestandsaufnahme	
Service Tag	Zeigt die Service-Tag-Nummer des Gehäuses an. Die Service-Tag-Nummer ist eine eindeutig identifizierbare Nummer, die vom Hersteller für Support und Wartung vergeben wird
Status	Zeigt den Status des Gehäuses an
Dauer (MM:SS)	Zeigt die Dauer des Jobs in Minuten und Sekunden an
Startdatum und -uhrzeit	Zeigt das Datum und die Uhrzeit an, zu dem der Bestandsaufnahmenzeitplan gestartet wurde
Enddatum und -zeit	Zeigt die Uhrzeit des Endes des Bestandsaufnahmenzeitplans an

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

Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme

Um sicherzustellen, dass die Bestandsaufnahme aktuelle Hostinformationen enthält, sollten Sie das Erstellen einer Bestandsaufnahme mindestens einmal wöchentlich planen. Der Bestandsaufnahme-Job erfordert nur minimale Ressourcen und wirkt sich nicht negativ auf die Hostleistung aus. Sie können den Zeitplan zum Erstellen einer Bestandsaufnahme im **Erstkonfigurationsassistenten** oder über die Registerkarte **Überwachen** ändern.

Der Plan für den Bestandsaufnahmejob legt einen Tag/eine Uhrzeit für das Ausführen von Jobs zum Erstellen von Bestandsaufnahmen fest. Beispiele:

- Wöchentlich zu einer bestimmten Uhrzeit und an bestimmten Tagen
- In einem bestimmten Zeitintervall

Zum Erstellen einer Bestandsaufnahme der Hostsysteme müssen Sie ein Verbindungsprofil erstellen, das Verbindungs- und Authentifizierungsinformationen bereitstellt.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.
2. Klicken Sie auf **Jobwarteschlange**, **Bestandsaufnahmenverlauf**, und klicken Sie dann auf **Host-Bestandsaufnahme**.
3. Wählen Sie ein vCenter aus und klicken Sie anschließend auf  .
4. Führen Sie im Dialogfeld **Abruf von Bestandsaufnahmedaten** Folgendes durch:
   a. Wählen Sie unter **Bestandsaufnahmedaten** das Kontrollkästchen **Bestandsaufnahme-Datenabruf aktivieren** aus.
   b. Wählen Sie unter **Datenabrufzeitpläne für Bestandsaufnahme** die Wochentage für den Job aus.
   c. Geben Sie im Textfeld **Uhrzeit für Bestandsaufnahme-Datenabruf** die Ortszeit für diesen Job ein. Möglicherweise müssen Sie den Zeitunterschied zwischen Job-Konfiguration und Job-Umsetzung berücksichtigen.
5. Klicken Sie zum Speichern der Einstellungen auf **Anwenden**, klicken Sie zum Zurücksetzen der Einstellungen auf **Löschen**, und klicken Sie zum Abbrechen des Vorgangs auf **Abbrechen**.
6. Um den Job sofort auszuführen, klicken Sie in OpenManage Integration für VMware vCenter auf der Registerkarte **Überwachen** > **Job-Warteschlange** auf **Bestandsaufnahmeverlauf** > **Host-Bestandsaufnahme**.
7. Klicken Sie auf  und klicken Sie im Dialogfeld **Erfolg** auf **Schließen**.

ANMERKUNG: Beim Ausführen einer modularen Host-Bestandsaufnahme werden entsprechende Gehäuse automatisch erkannt. Die Gehäusebestandsaufnahme wird automatisch nach der Hostbestandsaufnahme durchgeführt, wenn das Gehäuse bereits Teil eines Gehäuseprofils ist.

Nachdem Sie einen Bestandsaufnahmejob für jetzt geplant haben, befindet sich der Bestandsaufnahmejob in einer Warteschlange. Sie können keine Bestandsaufnahme für einen einzelnen Host ausführen. Ein Bestandsaufnahmejob startet für alle Hosts.

Ausführen von Bestandsaufnahme-Jobs

1. Sobald der **Konfigurationsassistent** fertig ist, wird die Bestandsaufnahme automatisch für alle Hosts, die einem Verbindungsprofil hinzugefügt sind, ausgelöst. Um eine nachfolgenden Bestandsaufnahme auf Anforderung durchzuführen, klicken Sie auf **Job-Warteschlange** > **Bestandsaufnahme** > **Jetzt ausführen**.

2. Klicken Sie auf **Aktualisieren**, um den Status des Bestandsaufnahme-Jobs zu aktualisieren.
3. Navigieren Sie zur Ansicht **Hosts und Cluster**, klicken Sie auf einen **Dell EMC Host** und dann auf die Registerkarte **OpenManage Integration**. Die folgenden Informationen sollten angezeigt werden:
   - Übersicht
   - System-Ereignisprotokoll
   - Hardware-Bestandsaufnahme
   - Bei Lagerung
   - Firmware
   - Stromüberwachung

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

   Die folgenden Host-Befehle funktionieren innerhalb der Registerkarte „OpenManage Integration“:
   - Blinkanzeigelicht
   - Firmware-Aktualisierungsassistent ausführen
   - Remote-Zugriff starten
   - OMSA starten
   - CMC starten
   - Systemsperrmodus konfigurieren

Sofortiges Ausführen eines Gehäuse-Bestandsaufnahme-Jobs

Sie können auf der Registerkarte **Gehäuse-Bestandsaufnahme** einen Gehäuse-Bestandsaufnahme-Job anzeigen und durchführen.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.
2. Klicken Sie auf **Jobwarteschlange**, **Bestandsaufnahmenverlauf**, und klicken Sie dann auf **Gehäuse-Bestandsaufnahme**. Die Liste der Gehäuse und deren Status für den letzten Bestandsaufnahme-Job werden angezeigt.

   ANMERKUNG: Die geplante Gehäuse-Bestandsaufnahme wird zur selben Zeit durchgeführt wie die geplante Host-Bestandsaufnahme.
3. Klicken Sie auf .
   Die Listen aktualisierter inventarisierter Gehäuse für jedes Gehäuse mit dem Status **Erfolgreich** oder **Fehlgeschlagen** werden angezeigt.

Service-Jobs

Hardware-Serviceinformationen werden von Dell Online abgerufen und von OMIVV angezeigt. Die Service-Tag-Nummer des Servers wird zur Sammlung von Serviceinformationen über den Server verwendet. Abfrage-Jobs für Servicedaten werden unter Verwendung des **Erstkonfigurationsassistenten** eingerichtet.

Zu den Aufgaben, die sie in dieser Registerkarte ausführen können, gehören:

- Anzeigen des Serviceverlaufs
- Ändern eines Service-Jobzeitplans
- Sofortiges Ausführen eines Host-Service-Jobs
- Sofortiges Ausführen eines Gehäusegarantie-Jobs

Anzeigen des Serviceverlaufs

Ein Garantie-Job ist ein geplanter Task zum Abrufen von Garantieinformationen auf allen Systemen von `support.dell.com`. Sie können die Spalten der Bestandsliste in aufsteigender und/oder absteigender Reihenfolge sortieren.

ANMERKUNG: Das OMIVV-Gerät benötigt eine Internetverbindung, um Garantieinformationen 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 Garantieinformationen abzurufen. Die Proxy-Daten können in der Administratorkonsole aktualisiert werden. Informationen dazu finden Sie unter Einrichten des HTTP-Proxy auf Seite 18.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.

2. Klicken Sie auf **Job-Warteschlange**, und klicken Sie dann auf **Serviceverlauf**.
3. Erweitern Sie den **Serviceverlauf**, um die **Host-Service** und die **Gehäusegarantie** anzuzeigen.
4. Um die entsprechenden Servicejob-Verlaufsinformationen anzuzeigen, wählen Sie **Host-Service** und wählen Sie dann eine vCenter, um alle diesbezüglichen Hosts-Details anzuzeigen.

Tabelle 11. vCenter Hosts-Verlaufsinformationen

vCenter-Verlauf	
vCenter	Zeigt die vCenter-Liste an
Bestandene Hosts	Zeigt die Anzahl der vCenter-Hosts an, die bestanden haben
Letzte Garantie	Zeigt das Datum und die Uhrzeit an, an dem der letzte Servicejob ausgeführt wurde
Nächste Garantie	Zeigt das Datum und die Uhrzeit an, zu dem der nächste Servicejob ausgeführt wird
Hosts-Verlauf	
Host	Zeigt die Host-Adresse an
Status	Zeigt den Status an. Zu den Optionen zählen: • Erfolgreich • Fehlgeschlagen • Wird durchgeführt • Geplant
Dauer (MM:SS)	Zeigt die Dauer des Service-Jobs in MM:SS an
Startdatum und -uhrzeit	Zeigt das Datum und die Uhrzeit an, zu der der Service-Job gestartet wurde
Enddatum und -zeit	Zeigt die Uhrzeit an, zu der der Service-Job beendet wurde

Gehäusegarantie anzeigen

Ein Service-Job ist ein geplanter Task zum Abrufen von Serviceinformationen auf allen Systemen von `Support.dell.com`. Die Spalten der Bestandsaufnahmeansicht sind in aufsteigender und absteigender Reihenfolge sortierbar.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.
2. Klicken Sie auf **Job-Warteschlange**, und klicken Sie dann auf **Serviceverlauf**.
3. Erweitern Sie den **Serviceverlauf**, um die **Host-Service** und die **Gehäusegarantie** anzuzeigen.
4. Klicken Sie auf **Gehäuseservice**.
5. Zeigen Sie die Details des Gehäuseservice an.

Tabelle 12. Gehäuseinformationen

Gehäusehistorie	
Gehäuse-IP-Adresse	Zeigt die IP-Adresse des Gehäuses an
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	Zeigt den Status des Gehäuses an
Dauer (MM:SS)	Zeigt die Dauer des Service-Jobs in MM:SS an
Startdatum und -uhrzeit	Zeigt das Datum und die Uhrzeit an, zu der der Service-Job gestartet wurde
Enddatum und -zeit	Zeigt die Uhrzeit an, zu der der Service-Job beendet wurde

Ändern von Service-Jobzeitplänen

Die Service-Jobs werden ursprünglich im **Erstkonfigurationsassistenten** konfiguriert. Sie können die Service-Jobzeitpläne auf der Registerkarte **Einstellungen** ändern.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.
2. Klicken Sie auf **Job-Warteschlange**, und klicken Sie dann auf **Serviceverlauf**.
3. Erweitern Sie den **Serviceverlauf**, um die **Host-Service** und die **Gehäusegarantie** anzuzeigen.
4. Zur Anzeige der entsprechenden Informationen zum Servicejob-Verlauf wählen Sie entweder **Host-Service** oder **Gehäuse-Service** aus.
5. Klicken Sie auf  .
6. Führen Sie im Dialogfeld **Abruf von Servicedaten** Folgendes durch:
   a. Wählen Sie unter **Servicedaten** das Kontrollkästchen **Servicedatenabruf aktivieren** aus.
   b. Wählen Sie unter **Serviceabrufzeitplan** die Wochentage für den Service-Job aus.
   c. Geben Sie im Textfeld **Uhrzeit für Bestandsaufnahme-Datenabruf** die Ortszeit für diesen Job ein.
   Möglicherweise ist es erforderlich, dass Sie für die Ausführung dieses Jobs zur richtigen Uhrzeit einen Zeitunterschied berechnen.
7. Klicken Sie auf **Anwenden**.

Sofortiges Ausführen eines Service-Jobs

Führen Sie mindestens einmal in der Woche einen Service-Job aus.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Überwachen**.
2. Klicken Sie auf **Job-Warteschlange**, und klicken Sie dann auf **Serviceverlauf**.
3. Erweitern Sie den **Serviceverlauf**, um die **Host-Service** und die **Gehäusegarantie** anzuzeigen.
4. Zur Anzeige der entsprechenden Informationen zum Servicejob-Verlauf wählen Sie entweder **Host-Service** oder **Gehäuse-Service** aus.
5. Wählen Sie den Servicejob aus, den Sie ausführen möchten, und klicken Sie dann auf die Schaltfläche .
6. Klicken Sie im Dialogfeld **Erfolgreich** auf **Schließen**.
   Es befindet sich nun ein Garantie-Job in der Warteschlange.

ANMERKUNG: Der Gehäuseservice wird für alle Gehäuse automatisch ausgeführt, sobald der Hostservice ausgeführt wird. In einer SSO-Umgebung mit mehreren vCentern wird der Gehäuseservice automatisch bei jedem vCenter ausgeführt, wenn der Service für ein beliebiges vCenter ausgeführt wird.

Sofortiges Ausführen eines Gehäusegarantie-Jobs

Führen Sie mindestens einmal in der Woche einen Service-Job aus.

1. Navigieren Sie in OpenManage Integration for VMware vCenter zur Registerkarte **Überwachen** > **Job-Warteschlange**.
2. Um den Service-Job auszuwählen, den Sie ausführen möchten, klicken Sie auf **Serviceverlauf** und dann auf **Gehäusegarantie**.
3. Klicken Sie auf .
4. Klicken Sie im Dialogfeld **Erfolgreich** auf **Schließen**.
   Es befindet sich nun ein Garantie-Job in der Warteschlange.

Überwachung eines einzelnen Hosts

OpenManage Integration for VMware vCenter ermöglicht die Anzeige detaillierter Informationen für einzelne Hosts. Sie können in VMware vCenter aus dem Navigatorbereich, der alle Hosts für alle Anbieter anzeigt, auf Hosts zugreifen. Um detailliertere Informationen zu erhalten, klicken Sie auf einen bestimmten Dell EMC Host. Um eine Liste der Dell EMC Hosts über das OpenManage Integration for VMware vCenter anzuzeigen, klicken Sie im Navigatorbereich auf **Dell EMC Hosts**.

Anzeigen der Hostzusammenfassungsdetails

Sie können die Details der Host-Zusammenfassung für einzelne Hosts auf der Seite **Host-Zusammenfassung**, auf der verschiedene Portlets angezeigt werden, einsehen. Zwei der Portlets sind für OpenManage Integration for VMware vCenter relevant. Die zwei Portlets sind:

- Dell EMC Host-Funktionszustand
- Dell EMC Host-Informationen

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. Klicken Sie in OpenManage Integration for VMware vCenter im Navigationsbereich auf **Hosts**.
2. Wählen Sie auf der Registerkarte **Objekte** einen spezifischen Host aus, den Sie überprüfen wollen.
3. Klicken Sie auf die Registerkarte **Zusammenfassung**.
4. Zeigen Sie die Hostzusammenfassungsdetails an:

Tabelle 13. Informationen zur Hostzusammenfassung

Informationen	Beschreibung
Anderes System	Zeigt Alarme für OpenManage Integration for VMware vCenter an. Diese werden unterhalb des Statusbereichs und oberhalb der Portlets in einem gelben Kästchen angezeigt.
Benachrichtigungsbereich	Zeigt Integrationsinformationen zu Dell Produkten auf der rechten Seite an. Hier finden Sie folgende Informationen: ● Letzte Tasks ● In Bearbeitung ● Alarme Dell-Alarminformationen werden in diesem Benachrichtigungsbereich-Portlet angezeigt.

5. Führen Sie zur Anzeige des Dell EMC Server Management-Portlets einen Bildlauf nach unten durch.

Tabelle 14. Dell EMC Server Management-Portlet

Informationen	Beschreibung
Service Tag	Zeigt die Service-Tag-Nummer des PowerEdge-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 neu. Dies gilt für PowerEdge-Server ab der 12. Generation 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

Tabelle 14. Dell EMC Server Management-Portlet (fortgesetzt)

Informationen	Beschreibung
	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 PowerEdge-Server der 14. Generation 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 Dell EMC 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 ● Verbindungsprofil – Zeigt den Verbindungsprofilnamen 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	Die Management-Konsolen dienen zum Starten der externen System Management-Konsolen. Dazu gehören: ● Starten der Remote-Zugriffskonsole (iDRAC) – Startet die Web-Benutzeroberfläche von Integrated Dell Remote Access Controller (iDRAC). ● Starten der OMSA-Konsole – Startet die OMSA-Konsole, um die OpenManage Server Administrator-Benutzeroberfläche aufzurufen.
Hostmaßnahmen	Für ein Blinken in verschiedenen Zeitintervallen muss der physische Server entsprechend eingerichtet werden. Siehe Blinkanzeigelicht.

6. Anzeigen des Dell EMC Host-Funktionszustands-Portlets:

Tabelle 15. Dell EMC Host-Funktionszustand

Informationen	Beschreibung
Dell EMC Host-Funktionszustand	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

Tabelle 15. Dell EMC Host-Funktionszustand

Informationen	Beschreibung
	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: Für verkabelte Netzteile, ist die Stromüberwachung in OMIVV nicht verfügbar.

Anzeigen der Hardware-Details für einen einzigen Host

Sie können Hardware-Details für einzelne Hosts auf der Registerkarte **Dell EMC Host-Informationen** einsehen. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Die Hardwareansichten übernehmen direkt Daten aus OMSA und iDRAC. Siehe Bestandsaufnahme-Jobs durchführen.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigationsbereich auf **Hosts**.
2. Wählen Sie im Register **Host** einen spezifischen Host aus, für den Sie die Hardware anzeigen möchten: `<Component Name>`-Details.
3. Wählen Sie in der Registerkarte **Überwachen** die Registerkarte **Dell Emc Host-Information** aus.

   ANMERKUNG: Wenn der Systemsperrmodus für einen Host der 14. Generation aktiviert ist, wird oben ein gelber Streifen mit einem geschlossenen Sperrsymbol angezeigt.

   Auf der Hardware: In der Unterregisterkarte `<Component Name>` sehen Sie folgende Informationen zu den einzelnen Komponenten.

Tabelle 16. Hardware-Informationen für einen einzigen Host

Hardware: *Komponente*	Informationen
Hardware: FRU	● **Teilename** – Zeigt den Teilenamen an ● **Teilenummer** – Zeigt die FRU-Teilenummer an ● **Hersteller** – Zeigt den Herstellernamen an ● **Seriennummer** – Zeigt die Hersteller-Seriennummer an ● **Herstellungsdatum** – Zeigt das Herstellungsdatum an
Hardware: Prozessor	● **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	● **Typ** – Zeigt den Netzteiltyp an. Zu den Netzteiltypen zählen: ○ UNBEKANNT ○ LINEAR ○ SCHALTNETZTEIL ○ BATTERY ○ USV ○ UMWANDLER

Tabelle 16. Hardware-Informationen für einen einzigen Host (fortgesetzt)

Hardware: *Komponente*	Informationen
	○ 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
Hardware: 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
Hardware: Netzwerkschnittstellenkarten	• **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
Hardware: 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
Hardware: Remote-Zugriffskarte	• **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

Anzeigen der Speicherdetails für einen einzigen Host

Sie können Speicherdetails für einzelne Host auf der Registerkarte **Dell EMC Host-Informationen** anzeigen. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Die Hardware meldet Daten direkt von OMSA und iDRAC. Siehe Bestandsaufnahme-Jobs durchführen. Die Seite zeigt verschiedene Optionen an, abhängig von der Auswahl aus der Drop-Down-Liste **Ansicht**. Wenn Sie **Physikalische Laufwerke** wählen, wird eine andere Drop-Down-Liste angezeigt. Die nächsten Drop-Down-Liste wird „Filter“ genannt und ermöglicht Ihnen das Filtern der Optionen für die physikalische Festplatte. So zeigen Sie die Speicherdetails an:

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigationsbereich auf **Hosts**.
2. Wählen Sie im Register **Objekte** einen spezifischen Host aus, für den Sie „Speicher: Details zur physischen Festplatte“ anzeigen lassen wollen.
3. Wählen Sie in der Registerkarte **Überwachen** die Registerkarte **Dell Emc Host-Information** aus.

   Auf dem Unterregister **Speicher** wird Folgendes angezeigt:

Tabelle 17. Speicherdetails für einen einzigen Host

Komponente	Informationen
Speicher	Zeigt die Anzahl der virtuellen Festplatten, Controller, Gehäuse und der zugehörigen physischen Festplatten mit der Anzahl der globalen und dedizierten Hotspares. Wenn Sie aus der Drop-Down-Liste wählen, wird die ausgewählte Option markiert.
Ansicht	Zeigt die Optionen an, die Sie für diesen Host anzeigen möchten: ● Virtuelle Festplatten ● Physische Festplatten ● Controller ● Gehäuse

Anzeigen der Speicherdetails für die Anzeigeoption

Die Speicheroptionen auf der Seite **Host-Speicher** hängen davon ab, was Sie aus der Dropdown-Liste **Ansicht** auswählen.

Wählen Sie eine der erwähnten Optionen aus der Dropdown-Liste „Ansicht“ aus, und zeigen Sie folgende Optionen an:

Tabelle 18. 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 die virtuelle Festplatte befindet ● **Kapazität** – zeigt die Kapazität des virtuellen Laufwerks an ● **Layout** – Zeigt den Layout-Typ des virtuellen Speichers an. Damit ist der für diese virtuelle Festplatte konfigurierte RAID-Typ gemeint ● **Medientyp** – Zeigt entweder SSD oder HDD an ● **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 die in der virtuellen Festplatte enthaltenen physischen Festplatten 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

Tabelle 18. Speicherdetails für einen einzigen Host (fortgesetzt)

Informationen	Beschreibung
Physische Laufwerke - Wenn Sie diese Option auswählen, wird die Dropdown-Liste **Filter** angezeigt. Sie können physische Filter basierend auf den folgenden Optionen filtern: • Alle physischen Festplatten • Globale Hotspares • Dedizierte Ersatzgeräte • Diese Option wird angezeigt, wenn Sie virtuelle Laufwerke mit eigenen Namen erstellt haben	• **Name** – Zeigt den Namen des physischen Laufwerks an • **FQDD** – Zeigt Geräte-FQDD 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** – Zeigt den Typ des Hotspare 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 einer einzelnen virtuellen Festplatte zugewiesen ist. Wenn eine physische Festplatte in der virtuellen Festplatte versagt, wird der Hotspare aktiviert, um die fehlerhafte physische Festplatte ohne Unterbrechung des Systems oder erforderlichen Benutzereingriff zu ersetzen. • **Virtuelle Festplatte** – Zeigt den Namen der virtuellen Festplatte an • **Bus-Protokoll** – Zeigt das Bus-Protokoll 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 • **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
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

Tabelle 18. Speicherdetails für einen einzigen Host (fortgesetzt)

Informationen	Beschreibung
	• **Service-Tag-Nummer** – Zeigt die Service-Tag-Nummer an

Über Systemereignisprotokolle im Webclient

Das Systemereignisprotokoll (SEL) zeigt Statusinformationen für von OMIVV entdeckte Hardware an, die auf den folgenden Kriterien basieren:

Status	Es gibt verschiedene Status-Symbole: Informativ (blaues Ausrufezeichen), Warnung (gelbes Dreieck mit Ausrufezeichen), Fehler (rotes X) und Unbekannt (Kästchen mit „?").
Uhrzeit (Server-Uhrzeit)	Gibt die Uhrzeit und das Datum an, an dem das Ereignis aufgetreten ist.
Diese Seite durchsuchen	Zeigt die bestimmte Meldung, Servernamen, Konfigurationseinstellungen usw. an.

Die Schweregrade sind definiert als:

Info	Der OMIVV-Vorgang wurde erfolgreich abgeschlossen.
Warnung	Der OMIVV-Vorgang ist teilweise fehlgeschlagen und wurde teilweise erfolgreich abgeschlossen.
Fehler	OMIVV-Vorgang ist fehlgeschlagen.

Sie können das Protokoll in einer externen csv-Datei speichern. Siehe Systemereignisprotokoll für einen bestimmten Host anzeigen.

Anzeigen von Ereignisprotokollen für einen einzelnen Host

Um die Ereignisse anzuzeigen, führen Sie folgende Schritte durch:

1. Für den Zugriff auf die Registerkarte **Überwachen** und das Öffnen der Unter-Registerkarte **Systemereignisprotokoll** führen Sie einen der folgenden Schritte durch:

Option	Beschreibung
Aus OMIVV	Führen Sie in dieser Option die folgenden Schritte aus: a. Klicken Sie in OpenManage Integration for VMware vCenter im Navigationsbereich auf **Hosts**. b. Doppelklicken Sie auf der Registerkarte **Objekte** auf einen spezifischen Host, für den Sie das SEL-Protokoll anzeigen möchten.
Von der **Startseite** aus	Klicken Sie auf der **Startseite** auf **Hosts und Cluster**.

2. Wählen Sie in der Registerkarte **Überwachen Dell EMC Host-Informationen** > **Systemereignisprotokoll**.
   Die letzten Einträge des Systemprotokolls umfassen die 10 aktuellsten Systemereignisprotokolleinträge.
3. Führen Sie zum Aktualisieren des **Systemereignisprotokolls** eine globale Aktualisierung aus.
4. Wählen Sie eine der folgenden Optionen, um die Anzahl der Ereignisprotokolleinträge zu beschränken (filtern):
   - Geben Sie in das Textfeld für den Suchfilter eine Textzeichenfolge ein, um die Protokolleinträge dynamisch zu filtern.
   - Klicken Sie zum Leeren des Textfeldes für den Filter auf das **X**. Es werden wieder alle Ereignisprotokolleinträge angezeigt.
5. Klicken Sie zum Löschen aller Ereignisprotokolleinträge auf **Protokoll löschen**.
   Es wird eine Meldung angezeigt, die besagt, dass alle Protokolleinträge gelöscht werden und Sie anschließend eine der folgenden Optionen auswählen können:
   - Klicken Sie zum Löschen der Protokolleinträge auf **Protokoll löschen**.
   - Klicken Sie zum Abbrechen des Vorgangs auf **Abbrechen**.
6. Klicken Sie zum Exportieren des Ereignisprotokolls in eine .csv-Datei auf  .
7. Klicken Sie auf **Speichern**, um zum Speicherort zu navigieren und das Systemereignisprotokolls zu speichern.

Anzeigen zusätzlicher Hardware-Details für einen einzigen Host

Sie können Firmware, Stromüberwachung und Servicestatusdetails für einzelne Hosts in der Registerkarte **Dell EMC Host-Informationen** anzeigen. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Hardwareansichten melden direkt Daten aus OMSA und iDRAC. Siehe Sofortiges Ausführen eines Gehäuse-Bestandsaufnahme-Jobs.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigationsbereich auf **Hosts**.
2. Wählen Sie im Register **Objekte** einen spezifischen Host aus, für den Sie die `<Component Name>`-Details anzeigen lassen wollen.
3. Wählen Sie in der Registerkarte **Überwachen** die Registerkarte **Dell Emc Host-Information** aus.

   Auf der Hardware: Im Unterregister `<Component Name>` sehen Sie folgende Informationen zu den einzelnen Komponenten:

Tabelle 19. Informationen zu einzelnem Host

Komponente	Informationen
Firmware Die Host-Seite ermöglicht Ihnen die Verwendung der Suche, des Filters und der Exportfunktion für eine CSV-Datei der Firmware-Information	• **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
Stromüberwachung **ANMERKUNG:** Die Hostzeit, wie sie hier verwendet wird, bedeutet die Zeit des Orts, an dem sich der Host befindet.	• **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. • **Messwert** – Zeigt den Durchschnittswert der Messwerte über einen Zeitraum von einer Minute an • **Spitzenzeit (Host Time)** – 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
Garantie **ANMERKUNG:** Um einen Servicestatus anzuzeigen, müssen Sie einen Service-Job ausführen. Siehe Ausführen eines Serviceabfrage-Jobs. 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 • **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

Überwachen der Hosts auf Clustern und von Rechenzentren

OpenManage Integration for VMware vCenter ermöglicht die Anzeige detaillierter Informationen für alle Hosts, die in einem Rechenzentrum oder Cluster enthalten sind. Durch Klicken auf den Zeilenkopf der Datentabelle können Sie die Daten sortieren. Die Rechenzentrums- und Cluster-Seiten ermöglichen Ihnen den Export von Informationen in eine .csv-Datei und stellen Filter-/Suchfunktionen in der Datentabelle bereit.

Anzeigen einer Übersicht der Rechenzentren und Cluster

Zeigen Sie die Host-Details für Rechenzentren oder Cluster auf der Registerkarte „EMC Dell Rechenzentrums -/Cluster-Informationen“ an. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Die angezeigten Daten können abhängig von der für den Datenzugriff gewählten Ansicht unterschiedlich ausfallen. Hardwareansichten melden direkt Daten aus OMSA und iDRAC. Siehe Bestandsaufnahme-Jobs durchführen.

ANMERKUNG: Rechenzentrums- und Cluster-Seiten ermöglichen Ihnen den Export von Informationen in eine .csv-Datei und stellen Filter-/Suchfunktionen im Datenraster bereit.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigationsbereich auf **vCenter**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie im Register **Objekte** ein spezifisches Rechenzentrum oder einen Cluster aus, für den Sie die Host-Details anzeigen lassen wollen.
4. Wählen Sie auf der Registerkarte **Überwachen Dell EMC Rechenzentrums/- Cluster-Informationen** > **Übersicht** aus, und zeigen Sie die Details an.

   ANMERKUNG: Wählen Sie zur Anzeige der vollständigen Detailsliste einen spezifischen Host vom Datengitter aus.

Tabelle 20. Übersicht der Rechenzentren und Cluster

Informationen	Beschreibung
Datacenter-/Cluster-Informationen	Zeigt die folgenden Optionen an: ● Datacenter-/Clustername ● Anzahl der Dell-verwalteten Hosts ● Gesamtenergieverbrauch
Systemsperrmodus	Zeigt den Status des iDRAC-Sperrmodus an. Der Status des iDRAC-Sperrmodus wird folgendermaßen für alle Hosts angezeigt: ● Eingeschaltet ● Ausgeschaltet ● Nicht zutreffend (Nur für Server der 14. Generation)
Hardware-Ressourcen	Zeigt die folgenden Optionen an: ● Gesamtanzahl der Prozessoren ● Total Memory (gesamter Speicher) ● Kapazität von virtuellen Laufwerken
Garantiezusammenfassung	Zeigt den Servicestatus für den ausgewählten Host an. Die Statusoptionen beinhalten: ● Abgelaufene Garantie ● Aktive Garantie ● Unbekannte Garantie
Host	Zeigt den Host-Namen 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

Tabelle 20. Übersicht der Rechenzentren und Cluster (fortgesetzt)

Informationen	Beschreibung
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 Power Edge-Server der 14. Generation: Zeigt den iDRAC-Sperrmodus des Host an: Eingeschaltet, Ausgeschaltet oder Unbekannt. Für Power Edge-Server vor der 14. Generation ist der angezeigte Systemsperrmodus nicht relevant.
iDRAC IP (iDRAC-IP)	Zeigt die IP-Adresse des iDRACs an
Service-Konsolen-IP	Zeigt die Service-Konsolen-IP an
CMC URL	Zeigt die CMC-URL an, die bei Blade-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
Verbindungsprofil	Zeigt den Namen des Verbindungsprofils an
Version der Remote-Zugriffskarte	Zeigt die Version der Remote-Zugriffskarte an
BIOS-Firmware-Version	Zeigt die Firmware-Version des BIOS an

Anzeigen von Hardware-Details für Rechenzentren und Cluster

Sie können Hardware-Details für einzelne Hosts auf der Registerkarte **Dell EMC Rechenzentrums-/ Cluster-Informationen** anzeigen. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Rechenzentrums- und Cluster-Seiten ermöglichen Ihnen den Export von Informationen in eine .csv-Datei und stellen Filter-/Suchfunktionen in der Datentabelle bereit. Die angezeigten Daten können abhängig von der für den Datenzugriff gewählten Ansicht unterschiedlich ausfallen. Die Hardwareansichten übernehmen direkt Daten aus OMSA und iDRAC. Siehe Bestandsaufnahme-Jobs durchführen.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigationsbereich auf **vCenter-Bestandslisten**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie im Register **Objekte** ein spezifisches Rechenzentrum oder einen Cluster aus, für den Sie die komponentenspezifischen Details anzeigen lassen wollen.
4. Wählen Sie in der Registerkarte **Überwachen Dell EMC Rechenzentrums-/Cluster-Information** aus.

   Auf der Hardware: In der Unterregisterkarte `<Component Name>` sehen Sie folgende Informationen zu den einzelnen Komponenten.

Tabelle 21. 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 Teilenamen an • **Teilenummer** – Zeigt die FRU-Teilenummer an • **Hersteller** – Zeigt den Herstellernamen an • **Seriennummer** – Zeigt die Hersteller-Seriennummer an • **Herstellungsdatum** – Zeigt das Herstellungsdatum an

Tabelle 21. Hardware-Informationen für Rechenzentren und Cluster (fortgesetzt)

Hardware: *Komponente*	Informationen
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
	• **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

Tabelle 21. Hardware-Informationen für Rechenzentren und Cluster (fortgesetzt)

Hardware: *Komponente*	Informationen
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

Anzeigen von Speicherdetails für Datacenter und Cluster

Sie können die Details der physischen Festplatte eines Rechenzentrums oder Clusters auf der Registerkarte **Rechenzentrums-/ Cluster-Informationen** anzeigen. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Die Rechenzentrums- und Cluster-Seiten ermöglichen Ihnen den Export von Informationen in eine .csv-Datei und stellen Filter-/Suchfunktionen in der Datentabelle bereit. Die Hardwareansichten übernehmen direkt Daten aus OMSA und iDRAC. Siehe Bestandsaufnahme-Jobs durchführen.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigationsbereich auf **vCenter-Bestandslisten**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie im Register **Objekte** ein spezifisches Rechenzentrum oder einen Cluster aus.
4. Wählen Sie auf der Registerkarte **Überwachen** die Option **Dell EMC Rechenzentrums-/ Cluster-Informationen** aus, und navigieren Sie zu **Speicher** > **Physisches Laufwerk/Virtuelles Laufwerk**.

   Wählen Sie zur Anzeige der vollständigen Detailsliste einen spezifischen Host von der Datentabelle aus.

Tabelle 22. 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:
	  ○ 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 Speicherverwaltungs-Benutzerhandbuch. Dieses befindet sich auf `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

Tabelle 22. Speicherdetails für ein Rechenzentrum und Cluster (fortgesetzt)

Speicher: Festplatten	Beschreibung

	• **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
	• **Hotspare-Typ** – Zeigt den Typ des Hotspare 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 einer einzelnen virtuellen Festplatte zugewiesen ist. Wenn eine physische Festplatte in der virtuellen Festplatte versagt, 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 die virtuelle Festplatte 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 diese virtuelle Festplatte 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
	• **Bus-Protokoll** – Zeigt die Technologie an, die die in der virtuellen Festplatte enthaltenen physischen Festplatten verwenden. Die möglichen Wert sind:
	  ○ SCSI
	  ○ SAS
	  ○ SATA
	• **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

Tabelle 22. Speicherdetails für ein Rechenzentrum und Cluster (fortgesetzt)

Speicher: Festplatten	Beschreibung
	• **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

Anzeigen zusätzlicher Hardware-Details für Rechenzentren und Cluster

Sie können Firmware, Stromüberwachung und Servicestatusdetails für ein Rechenzentrum und Cluster im Register **Dell EMC Rechenzentrums-/ Cluster-Informationen** einsehen. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Die Rechenzentrums- und Cluster-Seiten ermöglichen Ihnen den Export von Informationen in eine .csv-Datei und stellen Filter-/Suchfunktionen in der Datentabelle bereit. Hardwareansichten melden direkt Daten aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigationsbereich auf **vCenter**.
2. Klicken Sie auf **Datacenters** oder **Cluster**.
3. Wählen Sie in der Registerkarte **Objekte** ein spezifisches Datacenter oder einen Cluster aus, für den Sie die Host-Komponenten-Details anzeigen lassen wollen.
4. Wählen Sie in der Registerkarte **Überwachen Dell EMC Rechenzentrums-/Cluster-Information** aus.

   Das Unterregister `<Component Name>` zeigt folgende Informationen für die einzelnen Komponenten an:

Tabelle 23. Informationen zu einzelnem Host

Komponente	Informationen
Firmware	• **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
Stromüberwachung **ANMERKUNG:** Wählen Sie zur Anzeige der vollständigen Detailsliste einen spezifischen Host von der Datentabelle aus.	• **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

Tabelle 23. Informationen zu einzelnem Host (fortgesetzt)

Komponente	Informationen
	• **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
Garantiezusammenfassung **ANMERKUNG:** Um einen Servicestatus anzuzeigen, müssen Sie einen Service-Job ausführen. Siehe Ausführen eines Serviceabfrage-Jobs. 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

Einrichten eines Blinkanzeigelichts an der Frontblende eines physischen Servers

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. Klicken Sie in OpenManage Integration for VMware vCenter im Navigatorbereich unter „Bestandslisten“ auf **Hosts**.
2. Doppelklicken Sie im Register **Objekt** auf den gewünschten Host.
3. Scrollen Sie im Register **Zusammenfassung** nach unten bis zum Dell EMC Server Management Portlet.
4. Wählen Sie unter **Hostaktionen**, die Option **Blinkanzeigelicht**.
5. Wählen Sie eine der folgenden Optionen:
   - Klicken Sie zum Einschalten des Blinkens und zum Einrichten einer Dauer im Dialogfeld **Anzeigelicht** auf **Blinken** eingeschaltet, und wählen Sie in der Dropdown-Liste Zeitüberschreitung eine Dauer aus, dann klicken Sie auf **OK**.

- Klicken Sie zum Ausschalten des Blinkens im Dialogfeld **Anzeigelicht** auf **Blinken ausgeschaltet** und dann auf **OK**.

Konfigurieren des Systemsperrmodus.

Die Einstellung Systemsperrmodus ist mit iDRAC für die 14. Generation der Power Edge-Server verfügbar. Aktiviert sperrt die Einstellung die Systemkonfiguration, einschließlich Firmware-Aktualisierungen. 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. 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. Firmware-Aktualisierung, BS-Bereitstellung, Löschen der Systemereignisprotokolle, Reset des iDRAC und Konfiguration des iDRAC-Trap-Ziels.

Zur Konfiguration der Systemsperrmodus eines Hosts oder Cluster auf Host- oder Cluster-Ebene führen Sie folgende Schritte aus:

1. Zum Start des Assistenten zur Konfiguration des Systemsperrmodus führen Sie einen der folgenden Unterschritte aus:
   a. Klicken Sie im Bereich **Navigator** auf **Hosts und Cluster**, wählen Sie einen Host oder Cluster und klicken Sie mit der rechten Maustaste auf diesen, klicken Sie auf die Dropdown-Liste **Aktionen** und wählen Sie anschließend **Alle OpenManage Integrationsmaßnahmen** > **Konfigurieren des Systemsperrmodus**.
   b. In OpenManage Integration klicken Sie auf die Seite **Hosts** oder **Cluster**, mit der rechten Maustaste auf einen Host oder Cluster oder wählen einen Host oder Cluster aus, klicken auf die Drop-Down-Liste **Aktionen** und wählen anschließend **Alle OpenManage Integrationsmaßnahmen** > **Konfigurieren des Systemsperrmodus**.
   c. Wählen Sie im Bereich **Navigator** einen Host, und klicken Sie dann auf **Zusammenfassung** > **Dell EMC Host-Informationen** > **Konfigurieren des Systemsperrmodus**.
   d. Wählen Sie im Bereich **Navigator** einen Host oder Cluster aus und klicken Sie dann auf **Überwachen** > **Dell EMC Host-Information** > **Firmware** > **Konfigurieren des Systemsperrmodus**.
2. Um den Systemsperrmodus zu aktivieren, wählen Sie die Option **Einschalten**, oder, um den Sperrmodus zu deaktivieren, **Ausschalten**.
3. Klicken Sie auf **Anwenden**.

Wenn Sie versuchen, den Sperrmodus für Power Edge-Server der 11. Bis 13. Generation zu konfigurieren, werden Sie durch eine Meldung informiert, dass diese Funktion nicht auf dieser Plattform unterstützt wird.

Nachdem die Konfiguration des Systemsperrmodus abgeschlossen ist, können Sie den aktualisierten Status des Sperrmodus auf der Seite **Job-Warteschlange** einsehen. Die Informationen der Job-Warteschlange für den Sperrmodus sind nur auf Cluster-Ebene gültig. Um die Seite „Jobwarteschlange“ in OpenManage Integration zu öffnen, wählen Sie **Überwachen** > **Jobwarteschlange** > **Systemsperrmodus-Jobs**. In der iDRAC-Dokumentation finden Sie weitere Informationen zum Sperrmodus.

10

Ereignisse, Alarme und Systemüberwachung

Das Ziel der Hardware-Verwaltung besteht darin, Informationen zum Systemzustand und zur aktuellen Infrastruktur bereitzustellen, die der Administrator benötigt, um auf kritische Hardware-Ereignisse zu reagieren, ohne das OMIVV-Plug-in oder das vCenter zu verlassen.

Mit der Datencenter- und Hostsystem-Überwachung kann ein Administrator den Zustand der Infrastruktur durch Anzeigen von Hardware- (Server und Speicher) sowie Virtualisierung-bezogenen Ereignissen auf der Registerkarte **Tasks** und **Ereignisse** in vCenter überwachen. Außerdem können wichtige Hardware-Warnungen die OpenManage Integration for VMware v Center-Alarme auslösen und nur wenige für Dell virtualisierungsbezogene definierte Ereignisse können das verwaltete Host-System in den Wartungsmodus bringen.

Zum Empfangen von Ereignissen von Servern ist OMIVV als Trap-Ziel auf allen überwachten Geräten konfiguriert, und dies sind die verschiedenen Ziele:

- Das SNMP-Trap-Ziel ist in iDRAC oder Hosts der 12. Generation und höher festgelegt.
- Das Trap-Ziel ist in OMSA für Hosts vor der 12. Generation festgelegt.
- Das Trap-Ziel ist im CMC für Gehäuse festgelegt.

ANMERKUNG: OMIVV unterstützt SNMP v1- und v2-Warnungen für Hosts der 12. Generation und höher. Bei Hosts vor der 12. Generation unterstützt OMIVV nur SNMP v1-Warnungen.

Führen Sie folgende Schritte aus, um zu überwachen:

- Konfigurieren Sie die Einstellungen für **Ereignisse und Alarme**.
- Konfigurieren Sie SNMP-OMSA-Trap-Ziele, falls erforderlich.
- Überprüfen Sie die Ereignisinformationen auf der Registerkarte **Tasks** und **Ereignisse**.

Themen:

Informationen zu Ereignissen und Warnmeldungen für Hosts

Sie können Ereignisse und Alarme über das Dell OpenManage Integration for VMware vCenter auf der Registerkarte **Einstellungen verwalten** > bearbeiten. Von hier aus können Sie die Ereignisanzeigeebene auswählen, Alarme für die Dell EMC Hosts aktivieren, oder Standardalarme wiederherstellen. Sie können Ereignisse oder Alarme für einzelne vCenter oder alle registrierten vCenter nacheinander konfigurieren.

Dies sind die vier Ereignisanzeigeebenen:

Tabelle 24. Ereignisanzeigeebene

Ereignis	Beschreibung
Keine Ereignisse anzeigen	Dell OpenManage Integration for VMware vCenter soll keine Ereignisse oder Alarme an betroffene vCenter weiterleiten.
Alle Ereignisse anzeigen	Anzeigen aller Ereignisse, einschließlich informeller Ereignisse, die das OpenManage Integration for VMware vCenter von den verwalteten Dell EMC Hosts der betroffenen vCenter erhält.

Tabelle 24. Ereignisanzeigeebene (fortgesetzt)

Ereignis	Beschreibung
Nur kritische Ereignisse und Warnungsereignisse anzeigen	Veröffentlicht nur kritische Ereignisse und Warnungen an die entsprechenden vCenter.
Nur kritische Ereignisse und Warnungsereignisse hinsichtlich der Visualisierung anzeigen	Veröffentlichen von Hosts empfangener virtualisierungsrelevanter Ereignisse an die entsprechenden vCenter. Virtualisierungsrelevante Ereignisse sind Ereignisse, die Dell für Hosts, die virtuelle Maschinen ausführen, für höchst bedeutend erachtet.

Wenn Sie Ereignisse und Alarme konfigurieren, können Sie sie aktivieren. In diesem Fall führen kritische Hardware-Alarme dazu, dass das OMIVV das Hostsystem in den Wartungsmodus versetzt und die virtuellen Maschinen in bestimmten Fällen auf ein anderes Hostsystem migriert. OpenManage Integration for VMware vCenter leitet die von den verwalteten Dell EMC Hosts empfangenen Ereignisse 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 duale 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. 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 EMC Alarmen. In den Details der Bildschirmmeldungen werden alle eventuell betroffenen Cluster in dieser vCenter-Instanz aufgeführt. Prüfen Sie, ob die Cluster betroffen sind, bevor Sie Ereignisse und Alarme aktivieren.

Wenn Sie die Standard-Alarmeinstellungen wiederherstellen müssen, können Sie dies über einen Klick auf die Schaltfläche **Standard-Alarmeinstellungen wiederherstellen** tun. Über diese Schaltfläche 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 durch den Klick auf diese Schaltfläche zurückgesetzt.

ANMERKUNG: Um die Dell Ereignisse zu erhalten, müssen Sie die Ereignisse aktivieren.

ANMERKUNG: Das OpenManage Integration for VMware vCenter trifft eine Vorauswahl der erforderlichen virtualisierungsrelevanten Ereignisse, damit Hosts virtuelle Rechner erfolgreich ausführen können. Standardmäßig sind Dell Hostalarme deaktiviert. Sind die Dell Alarme aktiviert, sollten die Cluster DRS verwenden, um sicherzustellen, dass virtuelle Rechner, die kritische Ereignisse senden, automatisch migriert werden.

Informationen zu Ereignissen und Warnmeldungen für Gehäuse

Die Ereignisse und Alarme für ein Gehäuse werden nur auf vCenter-Ebene angezeigt. Die Einstellungen für Ereignisse und Alarme für Hosts an den einzelnen vCentern gelten auch auf Gehäuseebene. Sie können die Einstellungen für Ereignisse und Alarme über das OpenManage Integration for VMware vCenter innerhalb der Registerkarte **Verwalten** > **Einstellungen** bearbeiten. Von hier aus können Sie die Ereignisanzeigeebene auswählen, Alarme für Dell EMC Hosts und Gehäuse aktivieren oder Standardalarme wiederherstellen. Sie können Ereignisse und Alarme für einzelne vCenter oder für alle registrierten vCenters auf einmal konfigurieren.

Anzeigen von Gehäuseereignissen

1. Wählen Sie im linken Fensterbereich „vCenter“ aus und klicken Sie auf vCenter Server.
2. Klicken Sie auf ein bestimmtes vCenter.
3. Klicken Sie auf die Registerkarte **Ereignisse** > **überwachen** .
4. Wählen Sie ein spezifisches Ereignis aus, um weitere Ereignisdetails anzeigen zu lassen.

Anzeigen von Gehäusealarmen

1. Wählen Sie im linken Fensterbereich „vCenter“ aus und klicken Sie auf vCenter Server.

2. Klicken Sie auf ein bestimmtes vCenter.
   Die Alarme werden angezeigt. Nur die ersten vier Alarme werden angezeigt.
3. Zur Ansicht der kompletten Liste muss **Alle anzeigen** angeklickt werden, um die detaillierte Liste in der Registerkarte **Überwachen** als **Alle Probleme** anzuzeigen.
4. Klicken Sie unter **Ausgelöste Alarme** auf **Alarm**, um die Alarmdefinition anzuzeigen.

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 25. Virtualisierungsereignisse

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
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 getrennt wurde, fehlerhaft oder nicht vorhanden ist	Fehler	Setzen Sie das System in den Wartungsmodus.
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 benutzerdefinierbaren Warnungsschwellenwert überschritten	Warnung	Keine Maßnahme

Tabelle 25. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene 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 Benutzer 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
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

Tabelle 25. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene 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
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	Fehler	Setzen Sie das System in den Wartungsmodus.

Tabelle 25. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
	ein Überschreiten des Fehlerschwellenwerts erkannt		
Dell – Temperatursensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine oder dem Festplattenträger im angegebenen System erkannte einen Fehler, der nicht behoben werden kann	Fehler	Keine Maßnahme
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
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

Tabelle 25. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene 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 hat eine Warnung erkannt	Warnung	Keine Maßnahme
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.

Tabelle 25. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
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 oder kritisches Ereignis	Fehler	Setzen Sie das System in den Wartungsmodus.
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.

Tabelle 25. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
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.
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

Tabelle 25. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene 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.
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 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	Warnung	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie

Tabelle 25. Virtualisierungsereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
	entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.		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.

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.

ANMERKUNG: Der Funktionszustand der proaktiven HA der unterstützten Komponenten kann normal (grün), Warnung (gelb), kritisch (rot) oder unbekannt (grau) sein.

Tabelle 26. Proaktive HA-Ereignisse

Dell Inc. Provider Ereignis	Komponententyp	Beschreibung
DellFanRedundancy	Lüfter	Lüfterredundanz-Ereignis
DellPowerRedundancy	Netzteil (PSU)	Stromredundanz-Ereignis
DellIDSDMRedundancy	Storage	IDSDM-Redundanz-Ereignis

Für einen Host mit proaktiver HA werden die folgenden Traps von OMIVV als Auslöser zur Bestimmung des redundanten Zustands der Komponenten verwendet. Basierend auf den redundanten Zustandsinformationen kann eine Funktionszustandsaktualisierung der proaktiven HA für diesen Host an vCenter gesendet werden. Diese Traps werden nicht direkt an ein vCenter für einen proaktiven HA-Host weitergeleitet.

Tabelle 27. 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

Tabelle 27. Proaktive HA-Ereignisse (fortgesetzt)

Name des Ereignisses	Beschreibung	Schweregrad
Redundanzverlust	Redundanzverlust	Kritisch
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

Anzeigen der Alarm- und Ereigniseinstellungen

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. Erweitern Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Einstellungen verwalten** > unter **vCenter-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. Siehe Konfigurieren von Ereignissen und Alarmen.

Die Anzeige von Ereignis-Veröffentlichungsstufen finden Sie unter Über Ereignisse und Alarme.

Anzeigen von Ereignissen

Konfigurieren Sie Ereignisse, bevor Sie diese in der Registerkarte **Ereignisse** anzeigen lassen können. Siehe Konfigurieren von Ereignissen und Alarmen.

Lassen Sie die Ereignisse für einen Host, ein Cluster oder ein Datacenter auf der Registerkarte „Ereignisse“ anzeigen.

1. Klicken Sie in OpenManage Integration for VMware vCenter Navigator auf **Hosts**, **Datacenter** oder **Cluster**.

2. Wählen Sie auf der Registerkarte **Objekte** einen spezifischen Host, ein Datacenter oder einen Cluster aus, für den Sie Ereignisse anzeigen lassen wollen.
3. Klicken Sie auf der Registerkarte **Überwachen** auf **Ereignisse**.
4. Wählen Sie ein spezifisches Ereignis aus, um die Ereignisdetails anzeigen zu lassen.

Funktionszustand der Hardware-Komponentenredundanz – Proaktive HA

ANMERKUNG: Für die proaktive HA sind nur Server berechtigt, die den Redundanz-Funktionszustand für unterstützte Komponenten (Netzteil, Lüfter und IDSDM) unterstützen.

ANMERKUNG: Die konfigurierten Richtlinien für die proaktive HA auf dem proaktiven HA-Cluster können betroffen sein, wenn globale Warnungen über OMIVV konfiguriert werden.

ANMERKUNG: Die proaktive HA steht nur auf den Plattformen zur Verfügung, die Redundanz auf Netzteil, Lüfter und IDSDM unterstützen.

ANMERKUNG: Die proaktive Hochverfügbarkeit wird für diejenigen Netzteile nicht unterstützt, für die keine Redundanz konfiguriert werden kann (zum Beispiel Netzteile mit Kabel).

Die proaktive HA ist eine Funktion von vCenter (vCenter 6.5 und höher), 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.

ANMERKUNG: Alle Hosts ab der 12. Generation von PowerEdge und die ESXi-Versionen v6.0 und höher, die Teil eines Verbindungsprofils sind und erfolgreich inventarisiert wurden, sind für die proaktive HA berechtigt.

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:

- Funktionsfähig (Informationen) – Komponente arbeitet normal.
- Warnung (Mäßig herabgesetzt) – Komponente weist einen nichtkritischen Fehler auf.
- Kritisch (Stark herabgesetzt) – Komponente weist einen kritischen Fehler auf.

ANMERKUNG: Die mäßig herabgesetzten und stark herabgesetzten Zustände werden als *Warnung* in der Spalte **Typ** auf der Seite **Ereignisse** angezeigt.

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.

Proaktive HA für Rack- und Tower-Server konfigurieren

Führen Sie zur Konfiguration für Rack- und Tower-Server folgende Schritte durch:

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

1. Erstellen Sie ein Verbindungsprofil und weisen Sie den Hosts ein Verbindungsprofil zu. Siehe Erstellen eines neuen Verbindungsprofils.
2. Stellen Sie sicher, dass die Host-Bestandsaufnahme erfolgreich abgeschlossen wurde. Siehe Anzeigen von Host-Bestandsaufnahmen.
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 im Aktionsprotokoll des Benutzers die Verfügbarkeit eines Hosts für einen proaktiven HA-Cluster über die Registerkarte **OpenManage Integration** > **Überwachen** > **Protokoll** bestätigt wird.

4. Aktivieren Sie die proaktive HA auf einem Cluster. Siehe Aktivieren von proaktiver HA auf einem Cluster.

Proaktive HA für modulare Server konfigurieren

Führen Sie zur Konfiguration für modulare Server folgende Schritte durch:

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 Gehäusefehler hat Auswirkungen auf alle seine Blades.

1. Erstellen Sie ein Verbindungsprofil und weisen Sie den Hosts ein Verbindungsprofil zu. Siehe Erstellen eines neuen Verbindungsprofils.
2. Stellen Sie sicher, dass die Host-Bestandsaufnahme erfolgreich abgeschlossen wurde. Siehe Anzeigen von Host-Bestandsaufnahmen.
   ANMERKUNG: Stellen Sie sicher, dass im Aktionsprotokoll des Benutzers die Verfügbarkeit eines Hosts für einen proaktiven HA-Cluster über die Registerkarte **OpenManage Integration** > **Überwachen** > **Protokoll** bestätigt wird.
3. Erstellen Sie ein Gehäuseprofil für die zugeordneten Gehäuse. Siehe Erstellen eines Gehäuseprofils.
4. Stellen Sie sicher, dass die Gehäuse-Bestandsaufnahme erfolgreich abgeschlossen wurde. Siehe Gehäuse-Bestandsaufnahme anzeigen.
5. Starten Sie CMC und überprüfen Sie, ob das Trap-Ziel für das Gehäuse als IP-Adresse des OMIVV-Geräts eingestellt wurde.
6. Gehen Sie im **Gehäuse-Verwaltungscontroller** zu **Setup** > **Allgemein**.
7. Wählen Sie auf der Seite **Allgemeine Gehäuseeinstellungen Verbesserte Protokollierung von Gehäuse und Ereignissen aktivieren**.
8. Aktivieren Sie die proaktive HA auf einem Cluster. Siehe Aktivieren von proaktiver HA auf einem Cluster.

Aktivieren von proaktiver HA auf Clustern

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 Verbindungsprofils und erfolgreich inventarisiert sein und das Gehäuse sollte, falls erforderlich, über ein Gehäuseprofil verfügen.

1. Klicken Sie in OpenManage Integration auf **Cluster**.
2. Unter **Cluster** klicken Sie auf einen Cluster, wählen Sie **Konfigurieren von** > **vSphere-Verfügbarkeit** und klicken Sie dann auf **Bearbeiten**.
   Das Fenster **Exchange-Einstellungen bearbeiten** wird angezeigt.
3. Klicken Sie auf **vSphere DRS**, und wählen Sie **vSphere-DRS einschalten**, wenn Sie diese Option nicht ausgewählt haben.
4. Klicken Sie auf **vSphere-Verfügbarkeit** und wählen Sie **Proaktive HA einschalten**, wenn Sie diese Option nicht ausgewählt haben.
5. Klicken Sie im linken Fensterbereich unter **vSphere-Verfügbarkeit** auf **Proaktive HA-Ausfälle und Antworten**.
   Der Bildschirm **Proaktive HA-Ausfälle und Antworten** wird angezeigt.
6. Im Bildschirm **Proaktive HA-Ausfälle und Antworten** erweitern Sie die **Automationsebene**.
7. Für die **Automationsebene** wählen Sie **Manuell** oder **Automatisch**.
8. 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.
9. Verwenden Sie für den **Proaktiven HA-Anbieter** das Kontrollkästchen, um den Anbieter Dell für den Cluster auszuwählen.
10. Klicken Sie auf **Bearbeiten** neben dem ausgewählten Dell Anbieter.
    Das Dialogfeld **Bearbeiten blockiert Fehlerbedingungen** für den Proaktiven HA-Anbieter wird angezeigt.
11. Um Fehlerbedingungen zu blockieren, verwenden Sie die Kontrollkästchen zur Auswahl von Ereignissen (erzeugt über Traps oder Abfragen) von der Tabelle **Fehlerbedingungen**.

    Sie können den Inhalt des Fehlerbedingungen-Datenrasters durch Verwendung des Felds **Filtern** filtern oder per Drag-and-Drop von Spalten innerhalb des Fehlerbedingungen-Datenrasters. Die Fehlerbedingungen können auf einer Cluster-Ebene oder Host-Ebene angewendet werden.
12. Zur Anwendung auf alle aktuellen und zukünftigen Hosts im Cluster, wählen Sie das Kontrollkästchen **Cluster-Level**.
13. Um die Änderungen in **Bearbeiten blockiert Fehlerbedingungen** anzuwenden, klicken Sie auf **OK** oder zum Abbrechen des Vorgangs auf **Abbrechen**.

14. Um die Änderungen zu speichern, klicken Sie im Assistenten **Clustereinstellungen bearbeiten** auf **OK** oder zum Abbrechen des Vorgangs auf **Abbrechen**.

Nachdem die proaktive HA auf einem Cluster aktiviert ist, durchsucht OMIVV alle Hosts innerhalb des Clusters und initialisiert den Funktionszustand der proaktiven HA auf allen unterstützten Hostserver-Komponenten. OMIVV kann jetzt die Benachrichtigung zur Funktionszustandaktualisierung der unterstützten Komponenten an den vCenter-Server senden. Basierend auf der Benachrichtigung zur Funktionszustandaktualisierung von OMIVV unternimmt der vCenter-Server die manuelle oder automatische Aktion, die Sie für **Fehlerbehebung** ausgewählt haben.

Informationen zum Überschreiben des vorhandenen Schweregrads finden Sie unter Überschreiben des Schweregrads der Funktionszustands-Aktualisierungsbenachrichtigung auf Seite 93.

Überschreiben des Schweregrads der Funktionszustands-Aktualisierungsbenachrichtigung

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 der Registerkarte **Verwalten** auf **Proaktive HA-Konfiguration** > **Proaktive HA-Ereignisse**.
2. Klicken Sie, um Informationen über die Liste der unterstützten Ereignisse zu erhalten.
   Die Datentabelle zeigt alle unterstützten proaktiven HA-Ereignisse an und enthält Spalten, Ereignis-IDs, Ereignisbeschreibung, Komponententyp, Standardschweregrad und die Spalte „Schweregrad überschreiben“ für die Anpassung des Schweregrads des Hosts und den dazugehörigen Komponenten.
3. Um den Schweregrad eines Hosts oder seiner Komponente zu ändern, wählen Sie in der Spalte **Schweregrad überschreiben** den gewünschten Status aus der Dropdownliste aus.
   Diese Richtlinie gilt für alle proaktiven HA-Hosts auf alle vCenter-Servern, die bei OMIVV registriert sind.
4. Wiederholen Sie Schritt 3 für alle Ereignisse, die angepasst werden sollen.
5. Führen Sie eine der folgenden Aktionen aus:
   a. Zum Speichern der Anpassung klicken Sie auf **Änderungen anwenden**.
   b. Um den überschriebenen Schweregrad nach der Auswahl einer Schweregradebene wiederherzustellen, klicken Sie auf **Abbrechen**.
   c. Um den standardmäßigen Schweregrad auf den überschriebenen Schweregrad anzuwenden, klicken Sie auf **Auf Standardeinstellung zurücksetzen**.

Starten von Verwaltungskonsolen

Sie können drei Verwaltungskonsolen vom Dell EMC Server Management Portlet aus starten. Dazu gehen Sie wie folgt vor:

- Um auf die iDRAC-Benutzerschnittstelle zuzugreifen, starten Sie die Remote-Zugriffskonsole. Siehe Starten der Remote-Zugriffskonsole (iDRAC).
- Um auf die OpenManage Server Administrator Benutzeroberfläche zuzugreifen, starten Sie die OMSA-Konsole. Vor dem Start der OMSA-Konsole muss die OMSA-URL in Open Management Integration for VMware vCenter konfiguriert sein. Siehe Starten der OMSA-Konsole.
- Um auf die Gehäuse-Benutzeroberfläche zuzugreifen, klicken Sie auf die Blade-Gehäuse-Konsole. Siehe Starten der Chassis Management Controller-Konsole (CMC).

  ANMERKUNG: Wenn Sie ein Blade-System verwenden, starten Sie die CMC-Konsole, um die Benutzeroberfläche des Chassis Management Controller zu starten. Wenn Sie kein Blade-System verwenden, wird die Benutzeroberfläche des Chassis Management Controller nicht angezeigt.

Starten der Remote-Zugriffskonsole

Sie können die iDRAC-Benutzeroberfläche vom Dell EMC Server Management Portlet aus starten.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigatorbereich unter „Bestandslisten“ auf **Hosts**.
2. Doppelklicken Sie im Register **Objekt** auf den gewünschten Host.
3. Scrollen Sie im Register **Zusammenfassung** nach unten bis zum Dell EMC Server Management Portlet.
4. Klicken Sie auf **Management-Konsolen** > **Remote-Zugriffskonsole (iDRAC)**.

OMSA-Konsole starten

Bevor Sie die OMSA-Konsole starten, müssen Sie die OMSA-URL einrichten und den OMSA-Webserver installieren und konfigurieren. Sie können die OMSA-URL über die Registerkarte **Einstellungen** erstellen.

ANMERKUNG: Installieren Sie OMSA, um PowerEdge-Server der 11. Generation mit OpenManage Integration for VMware vCenter zu überwachen und zu verwalten.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigatorbereich unter „Bestandslisten“ auf **Hosts**.
2. Doppelklicken Sie im Register **Objekt** auf den gewünschten Host.
3. Scrollen Sie auf der Registerkarte **Zusammenfassung** nach unten bis zu den **Dell EMC Host-Informationen**.
4. Klicken Sie im Abschnitt **Dell EMC Host-Informationen** auf **OMSA-Konsole**.

Starten der Chassis Management Controller-Konsole

Sie können die Gehäuse-Benutzeroberfläche vom Dell EMC Server Management Portlet aus starten.

1. Klicken Sie in OpenManage Integration for VMware vCenter im Navigatorbereich unter „Bestandslisten“ auf **Hosts**.
2. Doppelklicken Sie im Register **Objekt** auf den gewünschten Blade-Server.
3. Scrollen Sie im Register **Zusammenfassung** nach unten bis zum Dell EMC Server Management Portlet.
4. Klicken Sie auf **Verwaltungskonsolen** > **Geräte-Management Controller-Konsole (CMC)**.

11

Allgemeines zu Firmware-Aktualisierungen

Das OMIVV-Gerät ermöglicht Ihnen die Ausführung des BIOS und der Firmware-Aktualisierungsjobs auf den verwalteten Hosts. Sie können Firmware-Aktualisierungsjobs auf mehreren Clustern oder nicht gruppierten Hosts gleichzeitig ausführen. Die gleichzeitige Ausführung der Firmware-Aktualisierung auf zwei Hosts desselben Clusters ist nicht zulässig.

Die folgende Tabelle listet die Anzahl der Firmware-Aktualisierungsjobs auf, die Sie gleichzeitig in verschiedenen Bereitstellungsmodi ausführen können, dennoch können Sie eine beliebige Anzahl an Firmware-Aktualisierungsjobs planen:

Tabelle 28. Firmware-Aktualisierungsjobs in verschiedenen Bereitstellungsmodi

Bereitstellungsmodus "Klein"	Bereitstellungsmodus "Mittel"	Bereitstellungsmodus "Groß"
5	10	15

Im Folgenden werden die zwei Methoden beschrieben, mit denen Sie die Firmware aktualisieren können:

- Einzelnes DUP – führt eine Firmware-Aktualisierung für iDRAC, BIOS, oder LC durch, indem direkt auf den DUP-Speicherort gezeigt wird (entweder CIFS- oder NFS-Freigabe). Die Methode des einzelnen DUP kann nur auf Hostebene ausgeführt werden.·

  Repository: führt BIOS-Aktualisierungen und alle unterstützten Firmware-Aktualisierungen aus. Diese Methode kann sowohl au Host-Ebene als auch auf Cluster-Ebene genutzt werden. Es gibt folgende zwei Speicherorte für Repositorys:

  - Dell Online: Der Speicherort nutzt das Repository für die Firmware-Aktualisierung von Dell (ftp.dell.com). OpenManage Integration for VMware vCenter lädt ausgewählte Firmware-Aktualisierungen vom Dell Repository herunter und aktualisiert die verwalteten Hosts.

    ANMERKUNG: Basierend auf den Netzwerkeinstellungen müssen Proxy-Einstellungen aktiviert werden, wenn das Netzwerk Proxy benötigt.
  - Freigegebener Netzwerkordner: Sie können über ein lokales Repository der Firmware in einer CIFS-basierten oder NFS-basierten Netzwerkfreigabe verfügen. Dieses Repository kann ein Abbild der Server Update Utility (SUU), das Dell regelmäßig veröffentlicht, oder ein benutzerdefiniertes Repository sein, das unter Verwendung von DRM erstellt wurde. OMIVV muss auf diese Netzwerkfreigabe zugreifen können.

    ANMERKUNG: Wenn Sie CIFS-Freigabe verwenden, dürfen die Kennwörter für Repositorien nicht mehr als 31 Zeichen umfassen. Folgende Zeichen dürfen dabei nicht für das Kennwort verwendet werden: @, &,%, ', ", ,(Komma), <, >.

    ANMERKUNG: Stellen Sie sicher, dass Sie die neueste DRM-Version (3.x) verwenden.

Weitere Informationen zum Einrichten von Repositorys zur Firmwareaktualisierung finden Sie unter Repository für die Firmwareaktualisierung einrichten auf Seite 40.

Der **Assistent zur Aktualisierung der Firmware** prüft stets die mindestens erforderlichen Firmware-Versionen für iDRAC, BIOS und den Lifecycle Controller und versucht, diese auf die mindestens erforderlichen Versionen zu aktualisieren. In der *OpenManage Integration for VMware v Center-Kompatibilitätsmatrix* finden Sie weitere Informationen zu den minimal erforderlichen Firmware-Versionen für iDRAC, BIOS und Lifecycle Controller. Wenn die iDRAC-, Lifecycle Controller- und BIOS-Firmware-Versionen die Mindestanforderungen erfüllen, ermöglicht der Vorgang zur Aktualisierung der Firmware alle Firmware-Versionsaktualisierungen, einschließlich iDRAC, Lifecycle Controller, RAID, NIC/LOM, Netzteile, BIOS usw.

Themen:

Ausführen der Firmwareaktualisierung für nicht-vSAN-Hosts

ANMERKUNG: Stellen Sie während des Prozesses der Firmware-Aktualisierung sicher, Folgendes nicht zu löschen:

- Den Host aus vCenter, für den der Job zur Aktualisierung der Firmware gerade ausgeführt wird.
- Das Verbindungsprofil des Hosts, für das die Aktualisierung der Firmware gerade ausgeführt wird.

Führen Sie die folgenden Schritte aus, um die Firmwareaktualisierung für einen nicht-vSAN-Host durchzuführen:

1. Klicken Sie für den Zugriff auf den Assistenten zur Firmwareaktualisierung in der OpenManage Integration auf **Hosts** und führen Sie die folgenden Schritte aus:
   - Klicken Sie mit der rechten Maustaste, wählen Sie anschließend **Alle OpenManage Integration-Aktionen** > **Firmwareaktualisierung** aus.
   - Klicken Sie auf der Seite **Hosts** auf einen Host, und wählen Sie **Alle OpenManage Integration-Aktionen** > **Firmwareaktualisierung** aus.
   - Wählen Sie im Bereich **Navigator** einen Host aus und klicken Sie dann auf **Zusammenfassung** > **Dell EMC Host-Information** > **Firmware-Assistent ausführen**.
   - Wählen Sie im Bereich **Navigator** einen Host aus und klicken Sie dann auf **Überwachen** > **Dell EMC Host-Information** > **Firmware** > **Firmware-Assistent ausführen**.

   OMIVV überprüft die Konformität des Hosts und ob andere Firmware-Aktualisierungs-Job auf einem Host im gleichen Cluster durchgeführt werden. Nach der Überprüfung wird der **Firmwareaktualisierungsassistent** angezeigt.

   ANMERKUNG: Wenn Sie von einer älteren Version von OMIVV auf eine verfügbare Version aktualisieren und bereits ein Job zur Firmwareaktualisierung geplant ist, können Sie den Assistenten zur Firmwareaktualisierung im selben Host starten, nachdem Sie die OMIVV Datenbank gesichert und in der verfügbaren Version wiederhergestellt haben.
2. Zeigen Sie die Informationen auf der Seite **Willkommen** an, lesen Sie die Anweisungen und klicken Sie auf **Weiter**.
   Die Seite **Aktualisierungsquelle auswählen** wird angezeigt.
3. Wählen Sie auf der Seite **Aktualisierungsquelle auswählen** eine der folgenden Optionen aus:
   a. Der **Aktuelle Repository-Speicherort** wird angezeigt; wählen Sie das Aktualisierungspaket für die Firmware aus der Dropdownliste **Ein Aktualisierungspaket auswählen** aus.

      ANMERKUNG: 64-Bit-Pakete werden nicht unterstützt für Hosts der 12. Generation mit iDRAC-Version 1.51 und niedriger.

      ANMERKUNG: 64-Bit-Pakete werden nicht unterstützt für Hosts der 11. Generation mit allen iDRAC-Versionen.

      ANMERKUNG: OMIVV unterstützt 32-Bit- und 64-Bit-Pakete für eine Firmwareaktualisierung. Abgesehen von den erwähnten Paketen erstellt OMIVV auch ein hybrides Paket, wenn 32-Bit- und 64-Bit-Paket im Katalog für ein bestimmtes Modell mit derselben Versions-ID verfügbar sind.

   b. Wählen Sie zum Laden einer einzelnen Firmwareaktualisierung aus einer Datei die Option **Einzelnes DUP**. Wenn Sie die Option **Einzelnes DUP** auswählen, fahren Sie mit Schritt 6 fort.
      Ein einzelnes DUP kann in einer CIFS- oder NFS-Freigabe verfügbar sein, auf die das virtuelle Gerät zugreifen kann. Geben Sie den **Dateispeicherort** in einem der nachfolgenden Formate ein:
      - NFS-Freigabe – `<host>:/<share_path/FileName.exe`
      - CIFS-Freigabe – `\\<host accessible share path>\<FileName>.exe`

        Bei der CIFS-Freigabe werden Sie vom OMIVV dazu aufgefordert, einen Benutzernamen und ein Kennwort in einem Domänenformat einzugeben, das auf das Freigabelaufwerk zugreifen kann.

        ANMERKUNG: Die Zeichen @, % und , werden für die Verwendung in Benutzernamen/Kennwörtern für freigegebene Netzwerkordner nicht unterstützt.

        ANMERKUNG: OMIVV unterstützt nur Server Message Block(SMB)-Version 1.0- und SMB-Version 2.0-basierte CIFS-Freigaben.
4. Klicken Sie auf **Weiter**.
   Die Seite **Komponenten auswählen** wird angezeigt.
5. Verwenden Sie die Kontrollkästchen zur Auswahl von mindestens einer Firmwarekomponente aus der Liste und klicken Sie dann auf **Weiter**.

   Die Komponenten, die zurückgestuft werden oder für die derzeit eine Aktualisierung geplant ist, können nicht ausgewählt werden. Sie können durch Auswahl der Option **Zurückstufen zulassen** die Komponenten auswählen, die für das Zurückstufen aufgelistet sind.

   Die Seite **Firmwareaktualisierung planen** wird angezeigt.

   ANMERKUNG: Wenn Sie eine ältere Version von OMIVV auf eine verfügbare Version aktualisieren, zeigt das Feld für den erforderlichen Neustart „Nein“ für alle Komponenten an, außer, wenn Sie das Repository für die Firmwareaktualisierung aktualisieren.

Sie können kommagetrennte Werte aus dem Inhalt der verschiedenen Komponenten der Datentabelle herausfiltern, indem Sie **Filter** verwenden.

Sie können auch Spalten innerhalb der Komponentendatentabelle per Drag-and-Drop verschieben. Klicken Sie zum Export aus dem Assistenten auf  .

ANMERKUNG: Wenn Sie Komponenten auswählen, die einen Neustart erfordern, stellen Sie sicher, dass die vCenter-Umgebung so konfiguriert ist, dass die Arbeitsauslastungen migriert werden können.

6. Führen Sie auf der Seite **Firmwareaktualisierung planen** Folgendes aus:
   a. Geben Sie den Jobnamen im Feld **Jobname der Firmwareaktualisierung** und die Beschreibung im Feld **Beschreibung der Firmwareaktualisierung** ein. Diese Feldeingabe ist optional.

      Den Namen des Firmwareaktualisierungs-Jobs ist obligatorisch. So wird sichergestellt, dass Sie keinen bereits vorhandenen Namen verwenden. Wenn Sie den Firmwareaktualisierungsjob entfernen, können Sie den Jobnamen wiederverwenden.
   b. Geben Sie den Zeitüberschreitungswert für den Wartungsmodus an (in Minuten). Wenn die Wartezeit den angegebenen Wert überschreitet, schlägt der Update-Job fehl und die Wartungsaufgabe wird abgebrochen oder weist eine Zeitüberschreitung auf. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.

      ANMERKUNG: Der Mindest-Zeitüberschreitungswert beträgt 60 Minuten.

      ANMERKUNG: Der Höchst-Zeitüberschreitungswert beträgt einen Tag.

   c. Wählen Sie eine der folgenden Optionen aus:
      - Wählen Sie **Jetzt aktualisieren** zum sofortigen Start der Firmwareaktualisierung aus.

        Standardmäßig ist die Option *Wartungsmodus nach Abschluss der Firmware-Aktualisierung beenden* ausgewählt.

        Standardmäßig ist die Option *Ausgeschaltete und angehaltene virtuelle Maschinen zu anderen Hosts im Cluster verschieben* ausgewählt. Wird diese Option deaktiviert, wird die virtuelle Maschine getrennt, bis das Host-Gerät online ist.
      - Um den Firmwareaktualisierungs-Job später auszuführen, wählen Sie **Aktualisierung planen**. Sie können den Firmwareaktualisierungs-Job 30 Minuten im Voraus planen.
        - Wählen Sie im Kontrollkästchen Kalender den Monat und Tag aus.
        - Geben Sie die Uhrzeit in dem Format SS:MM in das Textfeld „Zeit“ ein. Die Uhrzeit entspricht der OMIVV Appliance-Zeit.
      - Zur Vermeidung von Serviceunterbrechungen wählen Sie **Aktualisierungen beim nächsten Neustart anwenden**.
      - Zur Anwendung der Aktualisierung und zum Neustart, auch wenn der Host sich nicht im Wartungsmodus befindet, wählen Sie **Aktualisierungen anwenden und den Neustart erzwingen, ohne in den Wartungsmodus überzugehen** aus. Die Verwendung dieser Methode wird nicht empfohlen.
7. Klicken Sie auf **Weiter**.
   Die Seite **Zusammenfassung** wird angezeigt. Diese Seite stellt Details über alle Komponenten nach der Firmwareaktualisierung bereit.
8. Klicken Sie auf **Fertigstellen**.

Der Firmwareaktualisierungs-Job kann bis zu mehreren Minuten dauern und die Dauer hängt von der Anzahl der enthaltenen Komponenten ab, die beim Firmwareaktualisierung-Job aktualisiert werden. Sie können den Status der Firmwareaktualisierungs-Jobs auf der Seite **Jobwarteschlange** anzeigen. Um die Seite „Jobwarteschlange“ in OpenManage Integration zu öffnen, wählen Sie **Überwachen** > **Jobwarteschlange** > **Firmwareaktualisierungen** aus. 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 **Firmwareaktualisierung planen** ausgewählt wurde.

Ausführen des Firmwareaktualisierungsassistenten für vSAN-Hosts

Stellen Sie vor dem Planen der Aktualisierung sicher, dass die folgenden Voraussetzungen erfüllt sind:

- DRS ist aktiviert.
- Der Host ist nicht im Wartungsmodus.
- Die vSAN-Datenobjekte sind fehlerfrei.

  Um die obigen Überprüfungen zu überspringen, deaktivieren Sie das Kontrollkästchen **Voraussetzungen überprüfen** auf der Seite **Firmwareaktualisierung planen**.
- Die ausgewählten Treiber und Firmware-Versionen entsprechen den VMware vSAN-Richtlinien. Ausgewählte Treiber werden vor der Firmwareaktualisierung installiert.

- Der Cluster erfüllt die vSAN-Anforderungen für die ausgewählte Datenmigrationsoption.
- Führen Sie die Bestandsaufnahme nach dem Aktivieren von vSAN erneut aus.

ANMERKUNG: Dell EMC empfiehlt, während des Vorgangs zur Firmwareaktualisierung Folgendes nicht zu löschen:

- Den Host aus vCenter, für den der Job zur Aktualisierung der Firmware gerade ausgeführt wird.
- Das Verbindungsprofil des Hosts, für das die Aktualisierung der Firmware gerade ausgeführt wird.

Führen Sie die folgenden Schritte aus, um die Firmwareaktualisierung für einen einzelnen Host durchzuführen:

1. Klicken Sie für den Zugriff auf den Assistenten zur Firmwareaktualisierung in der OpenManage Integration auf **Hosts** und führen Sie die folgenden Schritte aus:
   - Klicken Sie mit der rechten Maustaste, wählen Sie anschließend **Alle OpenManage Integration-Aktionen** > **Firmwareaktualisierung** aus.
   - Klicken Sie auf der Seite **Hosts** auf einen Host, und wählen Sie **Alle OpenManage Integration-Aktionen** > **Firmwareaktualisierung** aus.
   - Wählen Sie im Bereich **Navigator** einen Host aus und klicken Sie dann auf **Zusammenfassung** > **Dell EMC Host-Information** > **Firmware-Assistent ausführen**.
   - Wählen Sie im Bereich **Navigator** einen Host aus und klicken Sie dann auf **Überwachen** > **Dell EMC Host-Information** > **Firmware** > **Firmware-Assistent ausführen**.

   OMIVV überprüft die Konformität des Hosts und ob andere Firmware-Aktualisierungs-Job auf einem Host im gleichen Cluster durchgeführt werden. Nach der Überprüfung wird der **Firmwareaktualisierungsassistent** angezeigt.

   ANMERKUNG: Wenn Sie von einer älteren Version von OMIVV auf eine verfügbare Version aktualisieren und bereits ein Job zur Firmwareaktualisierung geplant ist, können Sie den Assistenten zur Firmwareaktualisierung im selben Host starten, nachdem Sie die OMIVV Datenbank gesichert und in der verfügbaren Version wiederhergestellt haben.
2. Zeigen Sie die Informationen auf der Seite **Willkommen** an, lesen Sie die Anweisungen und klicken Sie auf **Weiter**.

   Die Seite **Aktualisierungsquelle auswählen** wird angezeigt.
3. Führen Sie auf der Seite **Aktualisierungsquelle auswählen** Folgendes aus:
   a. Wählen Sie das Treiber-Repository-Profil, das Firmware-Repository-Profil oder die jeweiligen Kombinationen aus der Dropdown-Liste aus.

      Falls das Baseline-Repository im Cluster-Profil zugeordnet ist, werden die zugehörigen Firmware- und Treiber-Repositorys automatisch ausgewählt.

   b. Wählen Sie ein geeignetes Paket aus dem Dropdownmenü **Aktualisierungspaket auswählen** aus.
      Bei Auswahl des Treiber-Repositorys wird die Seite **Treiberauswahl** angezeigt. Die Seite zeigt die Details der Treiberkomponente an, wie z. B. **Hostname**, **Service-Tag-Nummer**, **Komponentenname**, **Anbieter**, **Paketname**, **Aktuell**, **Verfügbar**, **Update verfügbar**, **Neustart erforderlich**.

   c. Wählen Sie auf der Seite **Treiberauswahl** die gewünschte Treiberkomponente aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter**.

      Wenn Sie eine Treiberkomponente für die Aktualisierung auswählen, werden alle Komponenten im Paket ausgewählt.

      Bei Auswahl des Firmware-Repositorys wird die Seite **Komponentenauswahl** angezeigt. Die Seite zeigt die Komponentendetails an, wie **Hostname**, **Service-Tag-Nummer**, **Modellname**, **Komponente**, **Aktuell**, **Verfügbar**, **Dringlichkeit**, **Neustart erforderlich**.

   d. Verwenden Sie die Kontrollkästchen zur Auswahl von mindestens einer Firmwarekomponente aus der Liste und klicken Sie dann auf **Weiter**.

      Die Komponenten, die zurückgestuft werden oder für die derzeit eine Aktualisierung geplant ist, können nicht ausgewählt werden. Sie können durch Auswahl der Option **Zurückstufen zulassen** die Komponenten auswählen, die für das Zurückstufen aufgelistet sind.

      Die Seite **Firmwareaktualisierung planen** wird angezeigt.

      Sie können kommagetrennte Werte aus dem Inhalt der verschiedenen Komponenten der Datentabelle herausfiltern, indem Sie **Filter** verwenden.

      Sie können auch Spalten innerhalb der Komponentendatentabelle per Drag-and-Drop verschieben. Klicken Sie zum Export aus dem Assistenten auf  .

      ANMERKUNG: Wenn Sie Komponenten auswählen, die einen Neustart erfordern, stellen Sie sicher, dass die vCenter-Umgebung so konfiguriert ist, dass die Arbeitsauslastungen migriert werden können.
4. Führen Sie auf der Seite **Firmwareaktualisierung planen** Folgendes aus:
   a. Geben Sie den Jobnamen im Feld **Jobname der Firmwareaktualisierung** und die Beschreibung im Feld **Beschreibung der Firmwareaktualisierung** ein. Diese Feldeingabe ist optional.

Den Namen 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.

ANMERKUNG: Standardmäßig ist das Kontrollkästchen **Voraussetzungen überprüfen** aktiviert. Der Firmwareaktualisierung-Job wird unter folgenden Voraussetzungen gestoppt:

- DRS ist nicht aktiviert.
- Der Wartungsmodus ist für einige Hosts im Cluster aktiviert.
- Der vSAN-Objektzustand ist nicht fehlerfrei.

b. Geben Sie den Zeitüberschreitungswert für den Wartungsmodus an (in Minuten). Wenn die Wartezeit den angegebenen Wert überschreitet, schlägt der Update-Job fehl und die Wartungsaufgabe wird abgebrochen oder weist eine Zeitüberschreitung auf. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.

ANMERKUNG: Der Mindest-Zeitüberschreitungswert beträgt 60 Minuten.

ANMERKUNG: Der Höchst-Zeitüberschreitungswert beträgt einen Tag.

c. Wählen Sie eine der folgenden Optionen aus:

- Wählen Sie **Jetzt aktualisieren** zum sofortigen Start der Firmwareaktualisierung aus.

  Standardmäßig ist die Option *Wartungsmodus nach Abschluss der Firmware-Aktualisierung beenden* ausgewählt.

  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.

- Um den Firmwareaktualisierungs-Job später auszuführen, wählen Sie **Aktualisierung planen**. Sie können den Firmwareaktualisierungs-Job 30 Minuten im Voraus planen.
  - Wählen Sie im Kontrollkästchen Kalender den Monat und Tag aus.
  - Geben Sie die Uhrzeit in dem Format SS:MM in das Textfeld „Zeit“ ein. Die Uhrzeit entspricht der OMIVV Appliance-Zeit.
- Zur Vermeidung von Serviceunterbrechungen wählen Sie **Aktualisierungen beim nächsten Neustart anwenden**.
- Zur Anwendung der Aktualisierung und zum Neustart, auch wenn der Host sich nicht im Wartungsmodus befindet, wählen Sie **Aktualisierungen anwenden und den Neustart erzwingen, ohne in den Wartungsmodus überzugehen** aus. Die Verwendung dieser Methode wird nicht empfohlen.

5. Klicken Sie auf **Weiter**.
   Die Seite **Zusammenfassung** wird angezeigt. Diese Seite stellt Details über alle Komponenten nach der Firmwareaktualisierung bereit.
6. Klicken Sie auf **Fertigstellen**.

Der Firmwareaktualisierungs-Job kann bis zu mehreren Minuten dauern und die Dauer hängt von der Anzahl der enthaltenen Komponenten ab, die beim Firmwareaktualisierung-Job aktualisiert werden. Sie können den Status der Firmwareaktualisierungs-Jobs auf der Seite **Jobwarteschlange** anzeigen. Um die Seite „Jobwarteschlange“ in OpenManage Integration zu öffnen, wählen Sie **Überwachen** > **Jobwarteschlange** > **Firmwareaktualisierungen** aus. 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 **Firmwareaktualisierung planen** ausgewählt wurde.

Ausführen des Firmwareaktualisierungsassistenten für nicht-vSAN-Cluster

OMIVV ermöglicht Ihnen das Durchführen von BIOS- und Firmware-Aktualisierungen auf allen Hosts eines Clusters. Der Assistent aktualisiert nur Hosts, die Teil eines Verbindungsprofils sind und in Bezug auf die Firmware, den CSIOR-Status, den Hypervisor und den OMSA-Status (nur bei Servern der 11. Generation) kompatibel sind. OMIVV führt eine clusterfähige Firmwareaktualisierung durch, wenn Distributed Resource Scheduling (DRS) auf dem Cluster aktiviert ist. Dazu wird die Arbeitsauslastung migriert, wenn ein Host in den Wartungsmodus wechselt oder diesen beendet.

Stellen Sie sicher, dass die folgenden Bedingungen zutreffen, bevor der Firmwareaktualisierungs-Assistent ausgeführt wird:

- Der Firmwareaktualisierung-Repository ist bereits eingestellt. Informationen zur Einrichtung eines Repository zur Firmwareaktualisierung finden Sie unter Einrichten des Firmware-Aktualisierungs-Repositorys.
- Es sind keine aktiven Firmware-Aktualisierungs-Jobs für Hosts unter dem Cluster vorhanden, den Sie aktualisieren.
- Die Hosts im Cluster werden zu einem Verbindungsprofil hinzugefügt und die Bestandsaufnahme wird erfolgreich ausgeführt.
- DRS ist aktiviert.

ANMERKUNG: VMware empfiehlt, Cluster mit identischer Server-Hardware aufzubauen.

ANMERKUNG: Dell EMC empfiehlt, während des Vorgangs zur Firmwareaktualisierung Folgendes nicht zu löschen:

- Den Host/die Hosts eines Clusters von vCenter, für die der Firmware-Aktualisierungsjob ausgeführt wird.
- Das Verbindungsprofil des/der Hosts, für den/die die Aktualisierung der Firmware gerade ausgeführt wird.

1. Klicken Sie für den Start des Assistenten zur Firmwareaktualisierung in der OpenManage Integration auf **Cluster** und führen Sie einen der nächsten Schritte aus:
   - Klicken Sie auf ein Cluster, wählen Sie anschließend **Aktionen** > **Alle OpenManage Integration-Aktionen** > **Firmwareaktualisierung** aus.
   - Wählen Sie in der Registerkarte **Objekte** die Optionen **Aktionen** > **Alle OpenManage Integration-Aktionen** > **Firmwareaktualisierung** aus.
   - Klicken Sie auf ein Cluster und wählen Sie **Überwachen** > **Dell EMC Clusterinformationen** > **Firmware** aus. Klicken Sie im Bildschirm **Firmware** auf den Link **Firmware-Assistent ausführen**.
   - Klicken Sie mit der rechten Maustaste auf ein Cluster und wählen Sie anschließend **Aktionen** > **Alle OpenManage Integration-Aktionen** > **Firmwareaktualisierung** aus.

   OMIVV überprüft die Konformität des Hosts und ob andere Firmware-Aktualisierungs-Job auf einem Host im gleichen Cluster durchgeführt werden. Nach der Überprüfung wird die Seite **Firmwareaktualisierung** angezeigt.
2. Zeigen Sie die Informationen auf der Seite **Willkommen** an, lesen Sie die Anweisungen, und klicken Sie auf **Weiter**.
   Die Seite **Server auswählen** wird angezeigt.
3. Verwenden Sie die Kontrollkästchen auf der Seite **Server auswählen** in der Strukturansicht **Name**, um die Hosts auszuwählen.
4. Klicken Sie auf **Weiter**.

   Die Seite **Aktualisierungsquelle auswählen** wird angezeigt. Hier können Sie die Pakete auswählen. Der Repository-Standort wird auch angezeigt.
5. Auf der Seite **Aktualisierungsquelle auswählen** verfügt jedes Modell des ausgewählten Hosts über eine Dropdownliste neben dem Modellnamen, aus der Sie das gewünschte Paket auswählen können. Wählen Sie das gewünschte Paket für die Firmware-Aktualisierung aus.

   ANMERKUNG: OMIVV unterstützt 32-Bit- und 64-Bit-Pakete für eine Firmwareaktualisierung. Abgesehen von diesen Paketen erstellt OMIVV auch ein hybrides Paket, wenn 32-Bit- und 64-Bit-Pakete im Katalog für ein bestimmtes Modell mit derselben Versions-ID verfügbar sind.

   ANMERKUNG: 64-Bit-Pakete werden nicht unterstützt für Hosts der 12. Generation mit iDRAC-Version 1.51 und niedriger.

   ANMERKUNG: 64-Bit-Pakete werden nicht unterstützt für Hosts der 11. Generation mit allen iDRAC-Versionen.
6. Klicken Sie auf **Weiter**.
   Die Seite **Komponenten auswählen** wird angezeigt. Die Seite zeigt die Komponentendetails an, wie **Hostname**, **Service-Tag-Nummer**, **Modellname**, **Komponente**, **Aktuell**, **Verfügbar**, **Dringlichkeit**, **Neustart erforderlich**.
7. Verwenden Sie auf der Seite **Komponenten auswählen** die Kontrollkästchen zur Auswahl von mindestens einer Komponente aus der Liste, und klicken Sie dann auf **Weiter**, um fortzufahren.

   Die Komponenten, die zurückgestuft werden oder für die derzeit eine Aktualisierung geplant ist, können nicht ausgewählt werden. Sie können durch Auswahl der Option **Zurückstufen zulassen** die Komponenten auswählen, die für das Zurückstufen aufgelistet sind.

   Sie können kommagetrennte Werte aus dem Inhalt der verschiedenen Komponenten der Datentabelle herausfiltern, indem Sie **Filter** verwenden.

   Sie können auch Spalten innerhalb der Komponentendatentabelle per Drag-and-Drop verschieben. Klicken Sie zum Export aus dem Assistenten auf  .
8. Auf der Seite **Informationen zur Firmwareaktualisierung** sehen Sie alle Details zur Firmwareaktualisierung.
9. Klicken Sie auf **Next** (Weiter).

   Die Seite **Firmwareaktualisierung planen** wird angezeigt.
   a. Geben Sie den Namen des Firmwareaktualisierungs-Jobs im Feld **Firmwareaktualisierungs-Jobname** ein.
      Den Namen des Firmwareaktualisierungs-Jobs ist obligatorisch und entspricht keinem bereits vorhandenen Namen. Wenn Sie den Namen des Firmwareaktualisierungs-Jobs entfernen, können Sie ihn wiederverwenden.
   b. Geben Sie die Beschreibung der Firmwareaktualisierung im Feld **Firmwareaktualisierungsbeschreibung** ein. Dieser Wert ist optional.
   c. Geben Sie den Zeitüberschreitungswert für den Wartungsmodus an (in Minuten). Wenn die Wartezeit den angegebenen Wert überschreitet, schlägt der Update-Job fehl und die Wartungsaufgabe wird abgebrochen oder weist eine Zeitüberschreitung auf. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.

      ANMERKUNG: Der Mindest-Zeitüberschreitungswert beträgt 60 Minuten.

ANMERKUNG: Der Höchst-Zeitüberschreitungswert beträgt einen Tag.

d. Wählen Sie unter **Firmwareaktualisierungen planen** eine der folgenden Optionen aus:
   - Um den Aktualisierungs-Job jetzt auszuführen, klicken Sie auf **Jetzt aktualisieren**.
   - Möchten Sie den Aktualisierungsjob später ausführen, klicken Sie auf **Aktualisierung planen** und führen die folgenden Teilvorgänge aus:
     i. Wählen Sie im Kontrollkästchen **Kalender** den Monat und Tag aus.
     ii. Geben Sie die Uhrzeit in dem Format SS:MM in das Textfeld **Zeit** ein.

10. Klicken Sie auf **Next**.
    Die Seite **Zusammenfassung** wird angezeigt.
11. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertigstellen**, und es wird die Meldung **Der Firmwareaktualisierungsjob wurde erfolgreich erstellt** angezeigt.

Der Firmwareaktualisierungsjob kann mehrere Minuten dauern und die Dauer hängt von der Anzahl der Hosts ab, die ausgewählt wurden, und der Anzahl der Komponenten in jedem Host. Sie können den Status der Firmwareaktualisierungs-Jobs auf der Seite **Jobwarteschlange** anzeigen. Um die Seite „Jobwarteschlange“ in OpenManage Integration zu öffnen, wählen Sie **Überwachen** > **Jobwarteschlange** > **Firmwareaktualisierungen** aus. Wenn eine Firmwareaktualisierungsaufgabe abgeschlossen ist, läuft die Bestandsaufnahmeprüfung automatisch auf den ausgewählten Hosts. Die Hosts beenden automatisch den Wartungsmodus.

Ausführen des Firmwareaktualisierungsassistenten für vSAN-Cluster

Stellen Sie sicher, dass die folgende Bedingung zutrifft, bevor der Firmwareaktualisierungsassistent ausgeführt wird:

- DRS ist aktiviert.
- Hosts sind nicht im Wartungsmodus.
- Die vSAN-Datenobjekte sind fehlerfrei. Wenn der vSAN-Objektzustand für den ersten Host nicht fehlerfrei ist, schlägt der Firmwareaktualisierungsjob fehl. Bei anderen Hosts wird 60 Minuten gewartet, ob der vSAN-Objektzustand wieder fehlerfrei wird.
- Ausgewählte Treiber und Firmware entsprechen den VMware vSAN-Richtlinien. Ausgewählte Treiber werden vor der Firmwareaktualisierung installiert.
- Cluster erfüllt die vSAN-Anforderungen für die ausgewählte Datenmigrationsoption. Es wird dringend empfohlen, das Baseline-(Clusterprofil)-Firmware- oder Treiber-Repository auszuwählen.
- Sie müssen ein Treiber-Repository-Profil und Firmware-Repository-Profil erstellen, bevor Sie mit der Firmwareaktualisierung beginnen. Weitere Informationen über die Erstellung von Treiber- und Firmware-Repositorys finden Sie unter Erstellen eines Repository-Profils auf Seite 45.
- Es sind keine aktiven Firmware-Aktualisierungs-Jobs für Hosts unter dem Cluster vorhanden, den Sie aktualisieren.
- Die Hosts im Cluster werden zu einem Verbindungsprofil hinzugefügt und die Bestandsaufnahme wird erfolgreich ausgeführt.
- Führen Sie die Bestandsaufnahme nach dem Aktivieren von vSAN erneut aus.

ANMERKUNG: VMware empfiehlt, Cluster mit identischer Server-Hardware aufzubauen.

ANMERKUNG: Dell EMC empfiehlt, während des Vorgangs zur Firmwareaktualisierung Folgendes nicht zu löschen:

- Den Host/die Hosts eines Clusters von vCenter, für die der Firmware-Aktualisierungsjob ausgeführt wird.
- Das Verbindungsprofil des/der Hosts, für den/die die Aktualisierung der Firmware gerade ausgeführt wird.
- Die Repositorys in CIFS oder NFS.

1. Klicken Sie für den Start des Assistenten zur Firmwareaktualisierung in der **OpenManage Integration** auf **Cluster** und führen Sie einen der nächsten Schritte aus:
   - Klicken Sie auf ein Cluster, wählen Sie anschließend **Aktionen** > **Alle OpenManage Integration-Aktionen** > **Firmwareaktualisierung** aus.
   - Wählen Sie in der Registerkarte **Objekte** die Optionen **Aktionen** > **Alle OpenManage Integration-Aktionen** > **Firmwareaktualisierung** aus.
   - Klicken Sie auf ein Cluster und wählen Sie **Überwachen** > **Dell EMC Clusterinformationen** > **Firmware** aus. Klicken Sie im Bildschirm **Firmware** auf den Link **Firmware-Assistent ausführen**.
   - Klicken Sie mit der rechten Maustaste auf ein Cluster und wählen Sie anschließend **Aktionen** > **Alle OpenManage Integration-Aktionen** > **Firmwareaktualisierung** aus.

   OMIVV überprüft die Konformität des Hosts und ob andere Firmware-Aktualisierungs-Job auf einem Host im gleichen Cluster durchgeführt werden. Nach der Überprüfung wird die Seite **Firmwareaktualisierung** angezeigt.
2. Zeigen Sie die Informationen auf der Seite **Willkommen** an, lesen Sie die Anweisungen, und klicken Sie auf **Weiter**.

Die Seite **Server auswählen** wird angezeigt.

3. Verwenden Sie die Kontrollkästchen auf der Seite **Server auswählen** in der Strukturansicht **Name**, um die Hosts auszuwählen.
4. Klicken Sie auf **Weiter**.

   Die Seite **Aktualisierungsquelle auswählen** wird angezeigt.
5. Führen Sie auf der Seite **Aktualisierungsquelle auswählen** Folgendes aus:
   a. Wählen Sie das Treiber-Repository-Profil, das Firmware-Repository-Profil oder die jeweiligen Kombinationen aus der Dropdown-Liste aus.

      Falls das Baseline-Repository im Cluster-Profil zugeordnet ist, werden die zugehörigen Firmware- und Treiber-Repositorys automatisch ausgewählt.

      Standardmäßig wird der Modellname des Hosts im Bereich **Paket auswählen** ausgewählt.
   b. Wenn das Firmware-Repository ausgewählt wurde, verfügen alle Modelle des ausgewählten Hosts über eine Dropdownliste neben dem Modellnamen, aus der Sie das erforderliche Paket für die Firmwareaktualisierung auswählen können. Wählen Sie über die Dropdown-Liste das gewünschte Paket aus und klicken Sie auf **Weiter**.

      Bei Auswahl des Treiber-Repositorys wird die Seite **Treiberauswahl** angezeigt. Die Seite zeigt die Details der Treiberkomponente an, wie z. B. **Hostname**, **Service-Tag-Nummer**, **Komponentenname**, **Anbieter**, **Paketname**, **Aktuell**, **Verfügbar**, **Update verfügbar**, **Neustart erforderlich**.

   ANMERKUNG: OMIVV unterstützt 32-Bit- und 64-Bit-Pakete für eine Firmwareaktualisierung. Abgesehen von diesen Paketen erstellt OMIVV auch ein hybrides Paket, wenn mehrere Pakete im Katalog mit derselben Versions-ID verfügbar sind.

   ANMERKUNG: 64-Bit-Pakete werden nicht unterstützt für Hosts der 12. Generation mit iDRAC-Version 1.51 und niedriger.
6. Wählen Sie auf der Seite **Treiberauswahl** die gewünschte Treiberkomponente aus, die Sie aktualisieren möchten, und klicken Sie auf **Weiter**.
   Bei Auswahl des Firmware-Repositorys wird die Seite **Komponentenauswahl** angezeigt. Die Seite zeigt die Komponentendetails an, wie **Hostname**, **Service-Tag-Nummer**, **Modellname**, **Komponente**, **Aktuell**, **Verfügbar**, **Dringlichkeit**, **Neustart erforderlich**.
7. Wählen Sie auf der Seite **Komponentenauswahl** die gewünschte Komponente aus, für die Sie die Firmware aktualisieren möchten, und klicken Sie auf **Weiter**.

   Die Komponenten, die zurückgestuft werden oder für die derzeit eine Aktualisierung geplant ist, können nicht ausgewählt werden. Sie können durch Auswahl der Option **Zurückstufen zulassen** die Komponenten auswählen, die für das Zurückstufen aufgelistet sind.

   Sie können kommagetrennte Werte aus dem Inhalt der verschiedenen Komponenten der Datentabelle herausfiltern, indem Sie **Filter** verwenden.

   Sie können auch Spalten innerhalb der Komponentendatentabelle per Drag-and-Drop verschieben. Klicken Sie zum Export aus dem Assistenten auf  .
8. Auf der Seite **Informationen zur Firmwareaktualisierung** sehen Sie alle Details zur Firmwareaktualisierung. Klicken Sie auf **Weiter**. Die Seite **Firmwareaktualisierung planen** wird angezeigt.
9. Führen Sie auf der Seite **Firmwareaktualisierung planen** Folgendes aus:
   a. Geben Sie den Namen des Firmwareaktualisierungs-Jobs im Feld **Firmwareaktualisierungs-Jobname** ein.

      ANMERKUNG: Den Namen des Firmwareaktualisierungs-Jobs ist obligatorisch und entspricht keinem bereits vorhandenen Namen. Wenn Sie den Namen des Firmwareaktualisierungs-Jobs entfernen, können Sie ihn wiederverwenden.
   b. Geben Sie die Beschreibung der Firmwareaktualisierung im Feld **Firmwareaktualisierungsbeschreibung** ein. Dieser Wert ist optional.
   c. Geben Sie den Zeitüberschreitungswert für den Wartungsmodus an (in Minuten). Wenn die Wartezeit den angegebenen Wert überschreitet, schlägt der Update-Job fehl und die Wartungsaufgabe wird abgebrochen oder weist eine Zeitüberschreitung auf. Die Komponenten werden jedoch möglicherweise automatisch aktualisiert, wenn der Host neu gestartet wird.

      ANMERKUNG: Der Mindest-Zeitüberschreitungswert beträgt 60 Minuten.

      ANMERKUNG: Der Höchst-Zeitüberschreitungswert beträgt einen Tag.
   d. Um den Aktualisierungs-Job jetzt auszuführen, klicken Sie auf **Jetzt aktualisieren**.
   e. Wählen Sie die entsprechenden Optionen aus der Dropdown-Liste **Virtuelle vSAN-Datenmigration** aus. Standardmäßig ist **Zugriff sicherstellen** ausgewählt.

      ANMERKUNG: 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.

f. Möchten Sie den Aktualisierungsjob später ausführen, klicken Sie auf **Aktualisierung planen** und führen die folgenden Vorgänge aus:
   i. Wählen Sie im Kontrollkästchen **Kalender** den Monat und Tag aus.
   ii. Geben Sie die Uhrzeit in dem Format SS:MM in das Textfeld **Zeit** ein.
   iii. Wählen Sie die entsprechenden Optionen aus der Dropdown-Liste **Virtuelle vSAN-Datenmigration** aus. Standardmäßig ist **Zugriff sicherstellen** ausgewählt.

   ANMERKUNG: 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.

10. Klicken Sie auf **Weiter**.
    Die Seite **Zusammenfassung** wird angezeigt.
11. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertigstellen**, und es wird die Meldung **Der Firmwareaktualisierungsjob wurde erfolgreich erstellt** angezeigt.

Der Firmwareaktualisierungsjob kann mehrere Minuten dauern und die Dauer hängt von der Anzahl der Hosts ab, die ausgewählt wurden, und der Anzahl der Komponenten in jedem Host. Sie können den Status der Firmwareaktualisierungs-Jobs auf der Seite **Jobwarteschlange** anzeigen. Um die Seite „Jobwarteschlange“ in OpenManage Integration zu öffnen, wählen Sie **Überwachen** > **Jobwarteschlange** > **Firmwareaktualisierungen** aus. Wenn eine Firmwareaktualisierungsaufgabe abgeschlossen ist, läuft die Bestandsaufnahmeprüfung automatisch auf den ausgewählten Hosts. Die Hosts beenden automatisch den Wartungsmodus.

12

Gehäuseverwaltung

OMIVV ermöglicht das Anzeigen zusätzliche Informationen für Gehäuse, die einem modularen Server zugeordnet sind. Auf der Registerkarte „Gehäuseinformationen" können Sie Details der Gehäuse-Übersicht für ein einzelnes Gehäuse sowie Informationen über die Hardware-Bestandsaufnahme, die Firmware und den Verwaltungscontroller, den Funktionszustand der individuellen Gehäusekomponenten sowie Gehäuse und Serviceinformationen anzeigen. Die folgenden drei Registerkarten werden für jedes Gehäuse angezeigt und unterscheiden sich bei manchen Gehäusen abhängig von den Gehäusemodellen:

- Registerkarte Zusammenfassung
- Registerkarte „Überwachen"
- Registerkarte Manage (Verwalten)

ANMERKUNG: Stellen Sie zum Anzeigen aller Informationen sicher, dass das Gehäuse einem Gehäuse-Profil zugeordnet ist und die Gehäusebestandsaufnahme erfolgreich abgeschlossen wurde. Weitere Informationen finden Sie unter Informationen über Gehäuse-Profile.

Themen:

Anzeigen von Details der Gehäusezusammenfassung

Sie können die Details der Gehäusezusammenfassung für ein einzelnes Gehäuse auf der Seite **Gehäuse-Zusammenfassung** anzeigen.

1. Klicken Sie auf der **Startseite** auf **vCenter**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell EMC Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Zusammenfassung**.

   Die folgenden Informationen über das ausgewählte Gehäuse werden angezeigt:
   - Name
   - Modell
   - Firmware-Version
   - Service-Tag-Nummer
   - CMC

   ANMERKUNG: Wenn Sie auf den Link CMC klicken, wird die Seite **Chassis Management Controller** angezeigt.

   ANMERKUNG: Wenn Sie keine Gehäuse inventarisieren, sehen Sie nur die Service-Tag-Nummer und die CMC-IP-Adresse.

5. Zeigen Sie den Funktionszustand der dem ausgewählten Gehäuse zugeordneten Geräte an.
   Das Hauptfenster zeigt den allgemeinen Funktionszustand eines Gehäuses an. Die gültigen Funktionsindikatoren lauten **Funktionsfähig**, **Warnung**, **Kritisch**, **Nicht vorhanden**. 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 Versionen vor 4.3 werden nur zwei Funktionsindikatoren angezeigt, z. B. Funktionsfähig und Warnung oder Kritisch (invertiertes Dreieck mit einem orangefarbenem Ausrufungszeichen).

   ANMERKUNG: Der Gesamtfunktionszustand zeigt den Funktionszustand basierend auf dem Gehäuse mit den schlechtesten Funktionszustandswerten. Werden zum Beispiel 5 Zeichen für Funktionsfähig und 1 Warnzeichen angezeigt, wird der Gesamtfunktionszustand als „Warnung" angezeigt
6. Zeigen Sie **CMC Enterprise** oder **Express** mit dem Lizenztyp und dem Ablaufdatum für ein Gehäuse an.

   Die genannten Details gelten nicht für M1000e-Gehäuse.
7. Klicken Sie auf das Symbol **Service**, und zeigen Sie die Anzahl der verbleibenden Tage und die verstrichenen Tage für einen Host an.

Wenn Sie mehr als einen Service besitzen, wird der letzte Tag des letzten Service für die Berechnung der verbleibenden Servicetage verwendet.

8. Zeigen Sie die Fehler in den Tabellenlisten **Aktive Fehler** für ein Gehäuse an, die auf der Seite **Gehäuse-Funktionszustand** angezeigt werden.

   ANMERKUNG: Für M1000e Version 4.3 und früher werden die aktiven Fehler nicht angezeigt.

Anzeigen von Informationen zur Hardware-Bestandsliste für Gehäuse

Sie können Informationen über den Hardwarebestand für das ausgewählte Gehäuse anzeigen. Um die Informationen auf dieser Seite anzuzeigen, führen Sie unbedingt einen Bestandsaufnahme-Job aus und exportieren Sie eine CSV-Datei mit den Komponenteninformationen.

1. Klicken Sie auf der **Startseite** auf **vCenter**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell EMC Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Monitor** (Überwachen).

   Um die relevanten Informationen zu Komponenten anzuzeigen, navigieren Sie durch OMIVV:

Tabelle 29. Hardwarebestandsaufnahmedaten

Hardware-Bestandsliste: Komponente	Navigation durch OMIVV	Informationen
Lüfter	Verwenden Sie eine der folgenden Methoden: ● Klicken Sie auf der Registerkarte **Übersicht** auf **Lüfter**. ● Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und klicken Sie dann auf **Lüfter**.	Informationen über Lüfter: ● Name ● Vorhanden ● Stromzustand ● Lesen ● Warnungsschwelle ● Kritischer Schwellenwert ○ Minimum ○ Maximal
Netzteile	Verwenden Sie eine der folgenden Methoden: ● Klicken Sie auf der Registerkarte **Übersicht**auf **Netzteile**. ● Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und klicken Sie dann auf **Netzteile**.	Informationen zu den Netzteilen: ● Name ● Kapazität ● Vorhanden ● Stromzustand
Temperatursensoren	Verwenden Sie eine der folgenden Methoden: ● Klicken Sie auf der Registerkarte **Übersicht** auf **Temperatursensoren**. ● Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und	Informationen zu Temperatursensoren: ● Standort ● Lesen ● Warnungsschwelle ○ Maximal ○ Minimum ● Kritischer Schwellenwert ○ Maximal ○ Minimum

Tabelle 29. Hardwarebestandsaufnahmedaten (fortgesetzt)

Hardware-Bestandsliste: Komponente	Navigation durch OMIVV	Informationen
	klicken Sie dann auf **Temperatursensoren**.	**ANMERKUNG:** Für PowerEdge M1000e-Gehäuse werden Informationen über Temperatursensoren nur für Gehäuse angezeigt. Für andere Gehäuse werden Informationen über Temperatursensoren für Gehäuse und zugehörige modulare Server angezeigt.
E/A-Module	Verwenden Sie eine der folgenden Methoden: ● Klicken Sie auf der Registerkarte **Übersicht** auf **E/A-Module**. ● Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme**, und klicken Sie dann auf **E/A-Module**.	Informationen über E/A-Module: ● Einschub/Standort ● Vorhanden ● Name ● Struktur ● Service Tag ● Stromstatus Um zusätzliche Informationen anzuzeigen, wählen Sie das entsprechende E/A-Modul aus und die folgenden Informationen werden angezeigt: ● Rolle ● Firmware-Version ● Hardwareversion ● IP-Adresse ● Subnetzmaske ● Gateway ● MAC-Adresse ● DHCP aktiviert
PCIe	Verwenden Sie eine der folgenden Methoden: ● Klicken Sie auf der Registerkarte **Übersicht** auf **PCIe**. ● Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und klicken Sie dann auf **PCIe**.	Informationen über PCIe: ● PCIe-Steckplatz ○ Steckplatz ○ Name ○ Stromstatus ○ Struktur ● Serversteckplatz ○ Name ○ Nummer Um zusätzliche Informationen anzuzeigen, wählen Sie das entsprechende PCIe-Element aus und die folgenden Informationen werden angezeigt: ● Steckplatztyp ● Server-Zuordnung ● Zuweisungsstatus ● Zugewiesener Steckplatzstrom ● PCI-ID ● Hersteller-ID **ANMERKUNG:** PCIe-Informationen sind nicht auf das M1000e-Gehäuse anwendbar.
iKVM	Verwenden Sie eine der folgenden Methoden: ● Klicken Sie auf der Registerkarte **Übersicht** auf **iKVM**.	Informationen zum iKVM: ● iKVM-Name ● Vorhanden ● Firmware-Version ● Frontblenden USB/Video aktiviert

Tabelle 29. Hardwarebestandsaufnahmedaten (fortgesetzt)

Hardware-Bestandsliste: Komponente	Navigation durch OMIVV	Informationen
	• Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme**, und klicken Sie dann auf **iKVM**.	• Zugriff auf die CMC-CLI erlauben **ANMERKUNG:** Sie können Informationen über das iKVM-Modul nur für PowerEdge M1000e-Gehäuse anzeigen. **ANMERKUNG:** Die iKVM-Registerkarte wird nur dann angezeigt, wenn das Gehäuse ein iKVM-Modul enthält.

Anzeigen zusätzlicher Hardwarekonfiguration für Gehäuse

Sie können Informationen über Service, Speicher, Firmware und zum Management Controller für das ausgewählte Gehäuse anzeigen. Um die Informationen auf dieser Seite anzuzeigen, müssen Sie einen Bestandsaufnahme-Job ausführen und eine .csv-Datei mit den Komponentendetails exportieren.

Zur Anzeige der Service-, Speicher-, Firmware-, Management-Controller-Details für Gehäuse, führen Sie folgende Schritte durch:

1. Klicken Sie auf der **Startseite** auf **vCenter**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell EMC Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Monitor** (Überwachen).

   Um die Informationen von Service, Speicher, Firmware und Verwaltungscontroller anzuzeigen, navigieren Sie durch OMIVV.

Tabelle 30. Firmwaredetails

Hardwarekonfiguration	Navigation durch OMIVV	Informationen
Firmware	a. Klicken Sie in der Registerkarte **Überwachen** auf die Doppelpfeil-Markierung, erweitern Sie den linken Fensterbereich, und klicken Sie anschließend auf **Firmware**. b. Wenn Sie in der Registerkarte **Überwachen** auf **CMC starten** klicken, wird die Seite **Chassis Management Controller** angezeigt.	Informationen über Firmware: • Komponente • Aktuelle Version

Tabelle 31. Management-Controller-Details

Hardwarekonfiguration	Navigation durch OMIVV	Informationen
Management Controller	a. Klicken Sie in der Registerkarte **Überwachen** auf die Doppelpfeil-Markierung, erweitern Sie den linken Fensterbereich, und klicken Sie anschließend auf **Management Controller**. b. Um zusätzliche Informationen anzuzeigen, klicken Sie auf der Seite **Management Controller** auf die Pfeilmarkierung und erweitern die linke Spalte.	Informationen über Verwaltungscontroller: • Allgemein ○ Name ○ Firmware-Version ○ Zeitpunkt der letzten Aktualisierung ○ CMC-Standort ○ Hardwareversion • Gemeinsames Netzwerk ○ DNS-Domänenname ○ DHCP für DNS verwenden ○ MAC-Adresse

Tabelle 31. Management-Controller-Details

Hardwarekonfiguration	Navigation durch OMIVV	Informationen
		○ Redundanzmodus ● CMC-IPv4-Informationen ○ IPv4 aktiviert ○ DHCP aktiviert ○ IP-Adresse ○ Subnetzmaske ○ Gateway ○ Bevorzugter DNS-Server ○ Alternativer DNS-Server

Tabelle 32. Speicherinformationen

Hardwarekonfiguration	Navigation durch OMIVV	Informationen
Speicher	Klicken Sie auf der Registerkarte **Überwachen** auf **Speicher**.	Informationen über Speicher: ● Virtuelle Festplatten ● Controller ● Gehäuse ● Physische Festplatten ● Ersatzlaufwerke **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. 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) ● Struktur ● Gruppenname ● Gruppen-IP-Adresse (Link zur Speichergruppe)

Tabelle 33. Garantieinformationen

Hardwarekonfiguration	Navigation durch OMIVV	Informationen
Garantie	Klicken Sie auf der Registerkarte **Überwachen** auf **Service**.	Informationen über den Service: ● Anbieter ● Beschreibung ● Status ● Startdatum ● Enddatum ● Verbleibende Tage ● Letzte Aktualisierung **ANMERKUNG:** Zur Anzeige des Servicestatus müssen Sie einen Service-Job ausführen. Siehe Ausführen eines Serviceabfrage-Jobs.

Zugeordneten Host für Gehäuse anzeigen

Sie können Informationen über die zugeordneten Hosts für das ausgewählte Gehäuse auf der Registerkarte **Verwalten** anzeigen.

1. Klicken Sie auf der **Startseite** auf **vCenter**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell EMC Gehäuse**.
3. Wählen Sie im linken Fensterbereich die entsprechende Gehäuse-IP-Adresse aus.
4. Klicken Sie auf die Registerkarte **Verwalten**.

   Die folgenden Informationen über den zugeordneten Host werden angezeigt:
   - Host-Name (Falls Sie auf die ausgewählte Host-IP-Adresse klicken, werden die Details zum Host angezeigt.)
   - Service Tag
   - Modell
   - iDRAC IP (iDRAC-IP)
   - Einschubposition
   - Letzte Bestandsaufnahme

13

Bereitstellen von Hypervisors

OMIVV ermöglicht Ihnen die Konfiguration der folgenden Komponenten in unterstützten Bare-Metal-Servern zusammen mit der Bereitstellung des Hypervisors und dem Hinzufügen zu dem angegebenen Rechenzentrum und Cluster in einem vCenter.

- Einstellung der Startreihenfolge
- RAID-Konfiguration
- BIOS-Konfiguration
- iDRAC-Konfiguration

Sie können Hardware-, System- und Hypervisor-Profile auf Bare-Metal PowerEdge-Servern mithilfe von VMware vCenter erstellen, ohne PXE zu verwenden.

ANMERKUNG: Es wird empfohlen, bei der Hypervisor-Bereitstellung ein Systemprofil für Server ab der 14. Generation zu verwenden.

Um das Vorhandensein der Hardware bei der Bereitstellung zu garantieren, stellen Sie sicher, dass die physischen Server im Bereitstellungsassistenten angezeigt werden. Prüfen Sie, ob alle physischen Server den folgenden Anforderungen entsprechen:

- Erfüllen bestimmter Hardware-Support-Informationen, die in der *OpenManage Integration for VMware vCenter Kompatibilitäts-Matrix* verfügbar sind.
- Die mindestens erforderlichen Versionen der iDRAC-Firmware, des Lifecycle Controller und des BIOS. Informationen zu den spezifischen Firmware-Support-Informationen finden Sie unter *OpenManage Integration for VMware vCenter – Versionshinweise*.
- Sie können die NICs in den PCI-Steckplätzen manuell nach der Bereitstellung konfigurieren. Wenn Sie NIC-Add-ons verwenden, muss auf dem System Host-LAN on Motherboard (LOM) oder die NDC (Netzwerk-Tochterkarte) aktiviert und mit dem Netzwerk verbunden sein. OMIVV unterstützt die Bereitstellung mit ausschließlich eingebetteten oder integrierten LOMs.
- Erfüllen der Speicheranforderungen des IDSDM. Die Speicheranforderungen des IDSDM finden Sie in der VMware-Dokumentation. Sie müssen das IDSDM über das BIOS vor dem Bereitstellen des Hypervisors mit OMIVV aktivieren. OMIVV ermöglicht die Bereitstellung auf IDSDM oder auf lokalen Festplatten.
- Stellen Sie sicher, dass eine Route zwischen den vCenter- und den iDRAC-Netzwerken besteht, wenn vCenter und iDRAC sich in verschiedenen Netzwerken befinden.
- Stellen Sie sicher, dass die Funktion CISOR (Collect System Inventory on Reboot, bei Neustart Systeminformationen erfassen) aktiviert ist. Außerdem müssen Sie vor dem Initiieren des automatischen/manuellen Erkennens sicherstellen, dass die abgerufenen Daten aktuell sind, indem Sie das System vollständig herunterfahren und erneut einschalten (Kaltstart).
- Die Dell EMC Server sollten mit werkseitig vorkonfigurierter Auto-Erkennung und Handshake-Option bestellt werden. 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 Hypervisor-Bereitstellung erfüllt sind, wenn OMIVV nicht für die Hardwarekonfiguration verwendet wird:
  - Aktivieren Sie die Virtualization Technology (VT) Kennzeichnung im BIOS.
  - Stellen Sie die Bootreihenfolge des Systems entweder auf eine bootfähige virtuelle Festplatte oder IDSDM für die Installation des Betriebssystems ein.
- Stellen Sie sicher, dass die BIOS-Einstellung für VT automatisch aktiviert ist, auch wenn die BIOS-Konfiguration kein Teil des Hardwareprofils ist, wenn OMIVV zur Hardwarekonfiguration verwendet wird. Die Express/Clone RAID-Konfiguration ist erforderlich, wenn noch keine virtuelle Festplatte auf dem Zielsystem vorhanden ist.
- Stellen Sie sicher, dass benutzerdefinierte ESXi-Images, die alle Dell-Treiber enthalten, für die Bereitstellung vorhanden sind. Sie finden die korrekten Images auf `support.dell.com` auf der Seite **Dell Treiber & Downloads**. Speichern Sie die benutzerdefinierten Images an einem gemeinsam genutzten 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*. Details zur Verwendung der korrekten Images finden Sie unter Herunterladen von benutzerdefinierten Dell ISO-Images.
- Stellen Sie sicher, dass der BIOS-Modus im Referenzprofil der Hardware vor dem Anwenden des Hypervisor-Profils ausgewählt ist, da OMIVV den BIOS-Modus nur zur automatischen Bereitstellung des Hypervisor auf dem Zielserver unterstützt. Falls kein Hardwareprofil ausgewählt wurde, müssen Sie den Startmodus manuell auf BIOS konfigurieren und den Server neu starten, bevor Sie das Hypervisorprofil anwenden.

Bei Server-Versionen vor PowerEdge-Server der 12. Generation führt der Bereitstellungsvorgangs folgende Aufgaben aus:

- Das OMSA-Paket wird auf dem Zielsystem installiert.
- Es wird automatisch das SNMP-Trap-Ziel in OMSA so konfiguriert, dass es auf OMIVV zeigt.

Themen:

Geräteerkennung

Die „Erkennung“ ist der Prozess zum Hinzufügen unterstützter PowerEdge Bare-Metal-Server. Nachdem ein Server erkannt wurde, können Sie ihn zur Bereitstellung von Hypervisor und Hardware verwenden. In der *OpenManage Integration for VMware vCenter-Kompatibilitätsmatrix* finden Sie eine Liste der für die Bereitstellung erforderlichen Power Edge-Server. Es ist eine Netzwerkkonnektivität vom iDRAC des Dell EMC Bare-Metal-Servers zur virtuellen OMIVV-Maschine erforderlich.

ANMERKUNG: Hosts mit bereits vorhandenem Hypervisor sollten nicht in OMIVV erkannt, sondern zum vCenter hinzugefügt werden. Fügen Sie diese einem Verbindungsprofil hinzu, und stellen Sie die Verbindung zum OpenManage Integration for VMware vCenter mit dem Host-Konformitätsassistenten wieder her.

ANMERKUNG: Wenn Bare-Metal-Server vor OMIVV 4.0 ermittelt wurden, stellen Sie sicher, dass Sie die Maschinen aus der Bare-Metal-Serverliste entfernen und neu ermitteln.

ANMERKUNG: Stellen Sie bei der Durchführung einer Betriebssystem-Bereitstellung von SD-Karte für Bare-Metal Power Edge Server der 12. Generation, dass iDRAC 2.30.30.30 oder höher installiert ist.

Manuelle Ermittlung

Sie können einen Bare Metal Server, der vom Ermittlungsprozess nicht hinzugefügt wurde, manuell hinzufügen. Nachdem der Server hinzugefügt wurde, erscheint er in der Liste der Server im Bereitstellungsassistenten.

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Bereitstellung** > **verwalten** auf das Symbol für ➕.
   Das Dialogfeld **Gruppe hinzufügen** wird angezeigt.
2. Führen Sie im Dialogfeld **Server hinzufügen** die folgenden Schritte aus:
   a. Geben Sie die iDRAC-IP-Adresse in das Textfeld **iDRAC-IP-Adresse** ein.
   b. Geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.
   c. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
3. Klicken Sie auf **Server hinzufügen**.
   Die Aufgabe des Hinzufügens des Servers kann mehrere Minuten in Anspruch nehmen.

Auto Discovery (Automatische Ermittlung) in OpenManage Integration for VMware vCenter

Automatische Ermittlung ist der Prozess zum Hinzufügen von PowerEdge Bare-Metal-Servern. Wenn ein Server ermittelt wurde, verwenden Sie ihn zur Bereitstellung von Hypervisor 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 wurde. Power Edge-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 einem bereits vorhandenen Hypervisor sollten nicht bei OMIVV ermittelt werden. Fügen Sie stattdessen den Hypervisor zu einem Verbindungsprofil hinzu, und gleichen Sie dann OMIVV durch Verwendung des Host Konformitätsassistenten ab.

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

- Strom – Schließen Sie den Server an die Stromversorgung an. Der Server darf dabei nicht eingeschaltet sein.
- Netzwerkkonnektivität – Stellen Sie sicher, dass der iDRAC des Servers über eine Netzwerkverbindung verfügt und mit dem Bereitstellungsserver über Port 4433 kommuniziert. Sie erhalten Sie die IP-Adresse, indem Sie einen DHCP-Server verwenden oder diese manuell im iDRAC-Konfigurationshilfsprogramm angeben.
- Zusätzliche Netzwerkeinstellungen – Aktivieren Sie bei Verwendung von DHCP die Einstellung „DNS-Serveradresse über DHCP anfordern“, damit eine DNS-Namensauflösung erfolgen kann.
- Speicherort des Bereitstellungsdienstes – Dem iDRAC muss die IP-Adresse oder der Host-Name des Servers mit dem Bereitstellungsdienst bekannt sein. Siehe Speicherort des Bereitstellungsdienstes.
- Kontozugriff deaktiviert – Aktivieren Sie den Zugriff des Verwaltungskontos auf den iDRAC. Falls iDRAC-Konten mit Administratorrechten vorhanden sind, müssen Sie diese zuerst über die iDRAC-Webkonsole deaktivieren. Nachdem die automatische Ermittlung erfolgreich durchgeführt wurde, wird das iDRAC-Verwaltungskonto wieder aktiviert.
- Autom. Ermittlung aktiviert – Auf dem iDRAC des Servers muss die Funktion für die automatische Ermittlung aktiviert sein, damit die automatische Ermittlung starten kann.

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-Benutzerkonfiguration, 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 Provisioning-Leistungswert nicht manuell in der iDRAC-Konsole angegeben ist, versucht iDRAC, den DHCP-Bereichsoptionswert zu verwenden. Wenn die DHCP-Bereichsoption nicht vorhanden ist, versucht iDRAC die Nutzung des Leistungswerts von DNS.

Ausführliche Informationen zum Konfigurieren der DHCP-Bereichsoption und des DNS-Leistungssatzes finden Sie im Dokument „Dell Auto-Discovery Network Setup Specification“ unter http://en.community.dell.com/techcenter/extras/m/white_papers/20178466.

Aktivieren und Deaktivieren von Verwaltungskonten auf iDRAC

Deaktivieren Sie vor dem Einrichten der automatischen Ermittlung alle Verwaltungskonten, ausgenommen das Root-Konto. Das Root-Konto sollte während des automatischen Ermittlungsvorgangs deaktiviert werden. Sobald Sie die automatische Ermittlung erfolgreich eingerichtet haben, kehren Sie zur iDRAC-Benutzeroberfläche zurück und aktivieren Sie alle Verwaltungskonten, die zuvor deaktiviert wurden, ausgenommen das Root-Konto.

ANMERKUNG: Als Schutzmaßnahme für den Fall des Fehlschlagens der automatischen Ermittlung können Sie ein Konto auf dem iDRAC aktivieren, das kein Verwaltungskonto ist. Auf diese Weise verfügen Sie über die Möglichkeit eines Remote-Zugriffs, falls die automatische Ermittlung fehlschlägt.

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 iDRAC6: Wählen Sie im linken Fenster die Registerkarte **iDRAC-Einstellungen** > **Netzwerk/Sicherheit** > **Benutzer** aus.
   - Bei iDRAC7: Wählen Sie im linken Fenster die Registerkarte **iDRAC-Einstellungen** > **Benutzerauthentifizierung** > **Benutzer** aus.
   - Bei iDRAC8: Wählen Sie im linken Fenster die Registerkarte **iDRAC-Einstellungen** > **Benutzerauthentifizierung** > **Benutzer** aus.

4. Machen Sie im Register **Benutzer** alle Verwaltungskonten ausfindig, bei denen es sich nicht um das Stammkonto handelt.
5. Wählen Sie zum Deaktivieren eines Kontos unter „Benutzer-ID“ die entsprechende **ID** aus.
6. Klicken Sie auf **Weiter**.
7. Heben Sie auf der Seite **Benutzerkonfiguration** unter **Allgemein** die Markierung des Kontrollkästchens **Benutzer aktivieren** auf.
8. Klicken Sie auf **Anwenden**.
9. Nachdem Sie die automatische Ermittlung erfolgreich eingerichtet haben, müssen Sie die einzelnen Konten wieder aktivieren. Wiederholen Sie dazu die Schritte 1 bis 8, wobei Sie jedoch diesmal das Kontrollkästchen **Benutzer aktivieren** markieren und anschließend auf **Anwenden** klicken.

Manuelles Konfigurieren eines PowerEdge-Servers der 11. Generation für die automatische Ermittlung

Stellen Sie sicher, dass Sie die iDRAC- und die Host-IP-Adressen haben.

Falls Ihr Bare-Metal-Gerät nicht ab Werk für die Verwendung der AutoErmittlung eingerichtet ist, können Sie die Funktion auch manuell einrichten.

Bei erfolgreicher AutoErmittlung der Bare-Metal-Server wird das neue Verwaltungskonto erstellt bzw. ein vorhandenes Konto mit den vom Handshake-Dienst übergebenen Anmeldeinformationen aktiviert. Alle anderen Verwaltungskonten, die vor der automatischen Ermittlung deaktiviert wurden, werden nicht automatisch wieder aktiviert. Sie müssen diese nach erfolgreichem Abschluss der automatischen Ermittlung selbst wieder aktivieren. Lesen Sie dazu den Abschnitt Aktivieren und Deaktivieren von Verwaltungskonten auf iDRAC-Servern.

ANMERKUNG: Falls die AutoErmittlung aus irgendeinem Grund nicht vollständig durchgeführt wurde, gibt es keine Möglichkeit, eine Remote-Verbindung zum iDRAC herzustellen. Sie können eine solche Remote-Verbindung nur dann herstellen, wenn Sie auf dem iDRAC ein Konto aktiviert haben, das kein Verwaltungskonto ist. Falls auf dem iDRAC kein aktiviertes Konto vorhanden ist, können Sie nur auf den iDRAC zugreifen, indem Sie sich lokal am Gerät anmelden und das Konto auf dem iDRAC aktivieren.

1. Geben Sie die **iDRAC-IP**-Adresse in einen Browser ein.
2. Melden Sie sich an der **GUI von iDRAC Enterprise** an.
3. Klicken Sie in der Registerkarte **Integrated Dell Remote Access Controller 6 – Enterprise** > **Systemzusammenfassung**in der Vorschau der virtuellen Konsole auf **Starten**.
4. Klicken Sie im Dialogfeld **Warnung – Sicherheit** auf **Ja**.
5. Drücken Sie in der iDRAC-Dienstprogramm-Konsole **F12** einmal oder zweimal.
   Das Dialogfeld **Authentifizierung erforderlich** wird angezeigt.
6. Im Dialogfeld **Authentifizierung erforderlich** wird der Name angezeigt. Drücken Sie die **Eingabetaste**.
7. Geben Sie ein **`Kennwort`** ein.
8. Drücken Sie die **Eingabetaste.**
9. Wenn das Dialogfeld **Herunterfahren/Neustart** angezeigt wird, drücken Sie auf **F11**.
10. Der Host wird neu gestartet und der Bildschirm zeigt Informationen zum Laden des Speichers und dann zu RAID an. Wenn iDRAC angezeigt wird und Sie aufgefordert werden, die Tastenkombination STRG + E zu drücken, drücken Sie unverzüglich auf **STRG + E**. Wenn dieses Dialogfeld angezeigt wird, war Ihre Aktion erfolgreich. Wechseln Sie anderenfalls in das Menü „Strom“, schalten Sie das System aus und wieder ein, und wiederholen Sie den Vorgang.

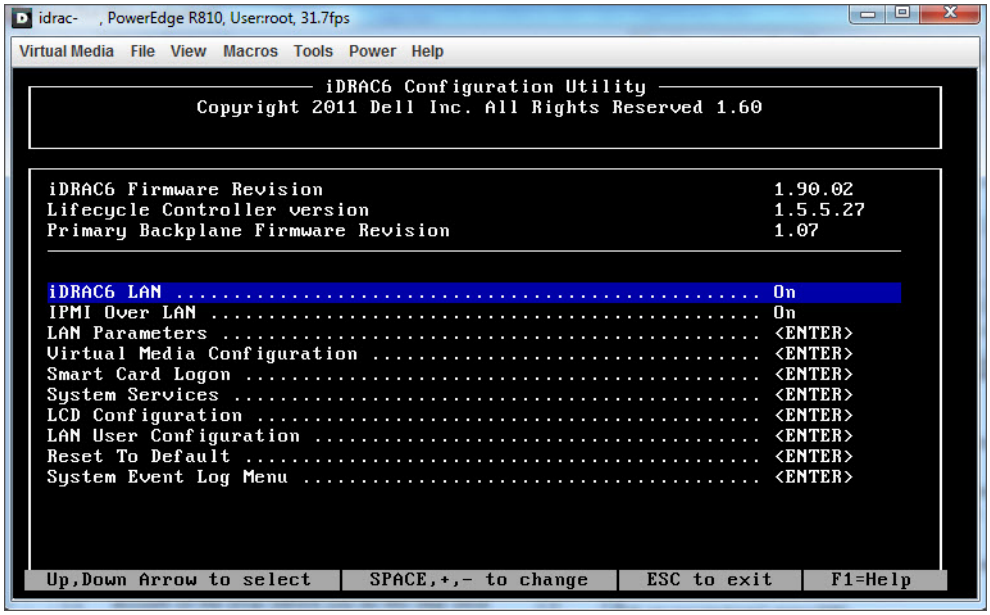

Abbildung 1. iDRAC-Konfigurationsdienstprogramm

11. Markieren Sie im iDRAC6-Konfigurationshilfsprogramm mithilfe der Pfeiltasten die Option **LAN-Parameter**.
12. Drücken Sie die **Eingabetaste**.
13. Falls es sich bei diesem Host um ein Blade-System handelt, verwenden Sie zum Konfigurieren der NIC die Leertaste, um die Optionen auf **Aktiviert** zu setzen.
14. Wählen Sie bei Verwendung von DHCP mithilfe der Pfeiltasten die Option **Domänenname über DHCP** aus.
15. Setzen Sie die Option mithilfe der Leertaste auf **Eingeschaltet**.
16. Wechseln Sie bei Verwendung von DHCP mithilfe der Pfeiltasten zu den IPv4-Einstellungen, und markieren Sie die Option **DNS-Server über DHCP**.
17. Setzen Sie die Option mithilfe der Leertaste auf **Eingeschaltet**.
18. Drücken Sie zum Beenden die Taste **Esc** auf Ihrer Tastatur.
19. Markieren Sie mithilfe der Pfeiltasten die Option **LAN-Benutzerkonfiguration**.
20. Markieren Sie mithilfe der Pfeiltasten die Option **Bereitstellungsserver**.
21. Drücken Sie die **Eingabetaste.**
22. Geben Sie die IP-Adresse des Hosts ein.
23. Drücken Sie erneut auf **Esc**.
24. Markieren Sie mithilfe der Pfeiltasten die Option **Kontozugriff**.
25. Setzen Sie die Option mithilfe der Leertaste auf **Deaktivieren**.
26. Markieren Sie mithilfe der Pfeiltasten die Option **Automatische Ermittlung**.
27. Setzen Sie die Option mithilfe der Leertaste auf **Aktiviert**.
28. Drücken Sie auf Ihrer Tastatur auf **Esc**.
29. Drücken Sie ein zweites Mal auf **Esc**.

Manuelles Konfigurieren eines PowerEdge-Servers der 12. Generation und später für die Auto-Ermittlung

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 dann nach der Lieferung von Dell EMC und Montage und Verbindung des iDRAC-Kabels automatisch erkannt und auf der ersten Seite des Bereitstellungsassistenten angezeigt.

ANMERKUNG: Für automatisch erkannte Server werden die Anmeldeinformationen unter **Verwalten** > **Einstellungen** > **Anmeldeinformationen für die Bereitstellung** als Administrator-Anmeldeinformationen gesetzt und zur weiteren Kommunikation

mit dem Server verwendet, bis die Bereitstellung des BS abgeschlossen ist. Nach einer erfolgreichen Bereitstellung des BS werden die im zugehörigen Verbindungsprofil 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. Um zum System-Setup zu wechseln, starten/neustarten Sie das Zielsystem, und drücken Sie F2 während des anfänglichen Starts.
2. Gehen Sie zu **iDRAC-Einstellungen** > **Benutzerkonfiguration**, und deaktivieren Sie den Root-Benutzer. Stellen Sie bei der Deaktivierung des Root-Benutzers sicher, dass keine anderen Benutzer 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-Benutzer aktiviert, und das Kontrollkästchen **Auto-Ermittlung aktivieren** wird automatisch deaktiviert.

Entfernen eines Bare-Metal-Servers

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

1. Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Bereitstellung** > **verwalten**.
2. Wählen Sie auf der Seite **Bare Metal Server** die Server aus, und klicken Sie auf .

Bereitstellen

Alle automatisch/manuell ermittelten, konformen Bare-Metal-Systeme sind für OMIVV zur Hardewareeinrichtung und Hypervisor-Bereitstellung verfügbar. Zur Einrichtung und Bereitstellung gehen Sie wie folgt vor:

Tabelle 34. Vorbereitung auf die Bereitstellung

Schritte	Beschreibung
Erstellen eines Systemprofils	Enthält die Systemkonfigurationseinstellungen, die von einem Referenzserver der 14. Generation gesammelt wurden, der zum Konfigurieren der neuen Server genutzt wird.
Erstellen eines Hardwareprofils	Enthält die Hardwareeinstellungen, die von einem Referenzserver gesammelt wurden, der zum Bereitstellen neuer Server genutzt wird. Informationen dazu finden Sie unter Erstellen oder Anpassen des Hardwareprofils auf Seite 119. **ANMERKUNG:** Es wird empfohlen, ein Hardwareprofil für Server bis zur 13. Generation zu verwenden.
Erstellen eines Hypervisor-Profils	Enthält die Hypervisor-Installationsinformationen, die für die ESXi-Bereitstellung erforderlich sind. Informationen dazu finden Sie unter Erstellen eines Hypervisor-Profils auf Seite 122.
Erstellen einer Bereitstellungsvorlage	Eine Bereitstellungsvorlage enthält ein Systemprofil, Hardwareprofil, Hypervisor-Profil, eine Kombination aus Systemprofil und Hypervisor-Profil oder eine Kombination aus Hardwareprofil und Hypervisor-Profil. Sie können diese Profile je nach Bedarf speichern und für alle verfügbaren Rechenzentrumsserver erneut verwenden.

Nachdem eine Bereitstellungsvorlage erstellt wurde, verwenden Sie den Bereitstellungsassistenten, um die zum Erstellen eines geplanten Auftrags notwendigen Informationen zu sammeln und Serverhardware und neue Hosts im vCenter bereitstellen zu können. Weitere Informationen zum Ausführen des Bereitstellungsassistenten finden Sie unter Bereitstellungsassistenten ausführen auf Seite 125. Zuletzt lassen Sie den Auftragsstatus über die Job-Warteschlange anzeigen und ändern die ausstehenden Bereitstellungsaufträge.

Systemprofile

Die Systemprofil-Funktion steht im iDRAC für PowerEdge Server zur Verfügung, die die Konfiguration von CNA, FCoE sowie die Konfiguration von Startreihenfolge, RAID, BIOS, iDRAC unterstützen. OMIVV unterstützt Systemprofile von iDRAC der 14. Generation als „Systemprofil“. Durch die Unterstützung von Server-Konfigurationsprofilen ermöglicht OMIVV das Exportieren der gesamten Konfiguration eines Dell EMC Servers der 14. Generation und den Import auf Ziel-Server.

Beim Anwenden eines Systemprofils auf einem in einem FX2 Gehäuse installierten modularen Server, auf einen anderen, ähnlichen Server, der in einem anderen FX2 Gehäuse installiert ist, müssen die Steckplatznummern beider Server gleich sein.

Ein Beispiel ist das folgende Szenario: 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.

ANMERKUNG: Das Systemprofil bietet keine Unterstützung für die folgenden Konfigurationen:

- Startoptionen aktivieren und deaktivieren
- BOSS-bezogene Konfiguration (CIFS-Konfiguration)

ANMERKUNG: Bei Verwendung des Systemprofils schlägt der Export eines Systemprofils mit einer Unternehmenslizenz und Import des gleichen Systemprofils auf Servern mit Express-Lizenz fehl und umgekehrt.

ANMERKUNG: Systemprofile können nicht mit einer Express-Lizenz der iDRAC9 Firmware 3.00.00.00 importiert werden. Sie benötigen hierzu eine Enterprise-Lizenz.

ANMERKUNG: 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 wird empfohlen, ein Referenz-Systemprofil von jedem Steckplatz des Gehäuses bereitzuhalten und diese Systemprofile für das gesamte Gehäuse nur für die entsprechenden Steckplätze anzuwenden.

Typische Aufgaben bei Verwendung eines Systemprofils sind:

- Erstellen/Erfassen von Systemprofilinformationen von einem Referenzserver. Informationen dazu finden Sie unter Systemprofil erstellen auf Seite 116.
- Anwenden des Profils auf ausgewählte Server unter Verwendung der Bereitstellungsvorlage. Informationen dazu finden Sie unter Erstellen von Bereitstellungsvorlagen auf Seite 123.

ANMERKUNG: Es wird empfohlen, ein Systemprofil für Server ab der 14. Generation zu verwenden.

Zum Starten der Seite des Systemprofils führen Sie folgende Schritte durch:

1. Wählen Sie in OpenManage Integration für VMware vCenter auf der Registerkarte **Verwalten** > **Bereitstellung** die Option **Bereitstellungsvorlagen** > **Systemprofile**.
   a. Die Seite **Systemprofile** zeigt die Liste der Systemprofile, die Sie erstellt haben.

      Es wird eine Tabelle mit einer Liste der Systemprofile mit Profilnamen, Beschreibung, Server, Modell und Details zum Referenzserver angezeigt.

   b. Um weitere Details zu einem Systemprofilhost anzuzeigen, wählen Sie ein Systemprofil.

      Überprüfen Sie die Systemprofildetails, z. B. Profilnamen, iDRAC-IP-Adresse, iDRAC-Typ, Service-Tag, Hostname, Servermodell, Erstellungsdatum, Modifizierungsdatum und Geändert von.

   c. Um die Spalten innerhalb der Datentabelle zu vertauschen, nutzen Sie das Drag-and-Drop.
   d. Um die Inhalte der Datentabelle zu filtern oder zu durchsuchen, klicken Sie auf das Feld **Filtern**.
   e. Um die Details des Systemprofils in eine .csv-Datei zu exportieren, wählen Sie ein Systemprofil aus und klicken dann in der rechten Ecke der Datentabelle auf das Symbol  .

Systemprofil erstellen

Stellen Sie sicher, dass folgende Bedingungen vor dem Erstellen eines Systemprofil erfüllt werden:

- Der Referenzserver wird je nach Anforderung außerhalb von OMIVV konfiguriert. Die Änderung von Attributwerten wird mit Ausnahme der iDRAC-Benutzerkennwörter in der aktuellen Version nicht unterstützt.
- CSIOR (Collect System Inventory On Restart) ist auf einem Referenzserver aktiviert, der neu gestartet wird, sodass die vom iDRAC zurückgegebenen Daten auf dem neuesten Stand sind.
- OpenManage Integration hat auf jedem vom vCenter verwalteten Host erfolgreich eine Bestandsaufnahme durchgeführt.
- Auf Bare-Metal-Servern sind die erforderlichen BIOS- und Firmware-Mindestversion installiert. In der *OpenManage Integration for VMware v Center-Kompatibilitätsmatrix* finden Sie weitere Informationen zu den minimal erforderlichen Firmware-Versionen für iDRAC, BIOS und Lifecycle Controller.

Sie können ein Systemprofil nur mit einem Referenzserver der 14. Generation erstellen.

1. Wählen Sie in OpenManage Integration für VMware vCenter auf der Registerkarte **Verwalten** > **Bereitstellung** den Punkt **Bereitstellungsvorlagen** > **Systemprofile**.

2. Klicken Sie auf .
3. Zeigen Sie die Informationen auf der Seite **Willkommen** an, lesen Sie die Anweisungen, und klicken Sie auf **Weiter**.
   - Geben Sie den Profilnamen in das Textfeld **Profilname** ein.
   - Geben Sie in das Textfeld **Profilbeschreibung** eine Beschreibung ein. Die Beschreibung ist optional.
4. Klicken Sie auf **Weiter**.
   Das Dialogfeld **Referenzserver** wird angezeigt. Wählen Sie dazu Referenzserver der 14. Generation direkt aus dem Dialogfeld oder über die Schaltfläche zum Durchsuchen auf der Profilquellenseite aus.
5. Wählen Sie einen Referenzserver der 14. Generation, indem Sie einen der folgenden Unterschritte durchführen:

   ANMERKUNG: Alle Hosts der 11. bis 14 Generationen werden im Dialogfeld angezeigt; Auswahllinks sind aber nur für konforme Bare Metal-Server und Hosts der 14. Generation aktiviert, wobei nur Bare-Metal-Server der 14. Generation angezeigt werden und der Auswahllink nur für konforme Bare-Metal-Server aktiv ist.

   a. Klicken Sie im Dialogfeld **Referenzserver** auf den gewünschten Referenzserver der 14. Generation und dann auf den Link **Wählen** neben dem Referenzserver.

      ANMERKUNG: Der Link **Wählen** ist nur für konforme Server aktiv.

   b. Klicken Sie auf der Seite **Referenzserver** auf **Durchsuchen**, um einen konformen Host-Referenzserver der 14. Generation auszuwählen, der durch OMIVV oder einen konformen Bare-Metal-Server verwaltet wird und erfolgreich inventarisiert wurde.

   Das Dialogfeld **Bestätigung extrahieren**, das das Extrahieren der Einstellungen zeigt, wird angezeigt. Klicken Sie zum Extrahieren der Hardwarekonfiguration vom Referenzserver im Dialogfeld **Bestätigung extrahieren** auf **Ja**. Das Extrahieren ist dann nach wenigen Minuten abgeschlossen.

   Ausgewählter Servername, Typ des Referenzservers, iDRAC-IP-Adresse, Modell und Service-Tag werden auf der Seite **Profilquelle** angezeigt.

   ANMERKUNG: Wenn der **Typ des Referenzservers** Bare-Metal-Server ist, wird nur die iDRAC-IP angezeigt; ist der **Typ des Referenzservers** Host, werden sowohl die iDRAC-IP als auch die Host-IP/FQDN angezeigt.
6. Klicken Sie auf **Weiter**.
7. Erweitern Sie auf der Seite **Profileinstellungen** iDRAC zum Anzeigen der Systemprofil-Attribute. Sie können die Spalten der Datentabelle in aufsteigender oder absteigender Reihenfolge sortieren. Klicken Sie auf das Datenfilter-Symbol, um die Daten zu filtern.

   a. Klicken Sie zur schnellen Anzeige des Links „Kennwort anlegen“ in der Spalte **Wert** auf das , geben Sie in **Wert enthält** „password“ ein und geben Sie dann das Kennwort für den aktivierten Benutzer ein.

      ANMERKUNG: Dell EMC empfiehlt, dass Sie die gleichen Anmeldeinformationen angeben, die beim Hinzufügen des Bare-Metal-Servers verwendet wurden. Wenn Sie das Kennwort in der Bereitstellungsvorlage ändern, werden die Änderungen dem Root-Benutzer nicht angezeigt. Wenn während der OS-Bereitstellung das Hypervisor-Profil der Bereitstellungsvorlage zugeordnet wird, übernimmt die Bereitstellung das Kennwort des Verbindungsprofils (iDRAC und ESXi).

      ANMERKUNG: Die Option **Kennwort anlegen** ist nur für den für iDRAC aktivierten Benutzer mit einem gültigen Benutzernamen verfügbar.

      Außerdem können Sie die Profileinstellungen für die Komponenten basierend auf der Konfiguration der Dell Referenzserver wie iDRAC, BIOS, RAID, NIC, CNA, FCoE und EvenFilters anzeigen.

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

      Wenn Sie den Mauszeiger über den Attributen platzieren, werden weitere Informationen zu diesem Attribut angezeigt.

      Standardmäßig werden einige Attribute wie **Schreibgeschützt**, **Systemspezifisch** und **Destruktiv** zur Auswahl angezeigt.

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

   ANMERKUNG: Bei der Durchführung einer RPM-Aktualisierung oder Sicherung und Wiederherstellung gilt Folgendes für alle migrierten Profile:
   - Wenn Sie den Mauszeiger über die Attribute bewegen, werden die Attributnamen angezeigt.
   - Nur nicht-systemspezifische Attribute werden ausgewählt.
   - Der Abhängigkeitstext wird nicht angezeigt.
   - Aktivierte Attribute stellen die gesamte Anzahl der ausgewählten Attribute dar.
8. Klicken Sie auf **Weiter**.
   Die Seite **Zusammenfassung** wird angezeigt. Diese Seite stellt Informationen zu den Profildetails und die Attributstatistiken der Systemkonfigurationen zur Verfügung.

Die Attributstatistik zeigt die jeweilige Gesamtanzahl der Attribute, der aktivierten Attribute, der plattformspezifischen Attribute und der destruktiven Attribute.

9. Klicken Sie im Fenster **Zusammenfassung** auf **Fertigstellen**.
   Das Profil wird automatisch gespeichert und wird im **Systemprofil**-Fenster angezeigt.

Nicht alle systemspezifischen Attribute werden in der aktuellen Version unterstützt. Weitere Informationen zu systemspezifischen Attributen finden Sie unter Systemspezifische Attribute auf Seite 161.

Einige Attribute des Systemprofils werden überschrieben, damit OMIVV funktioniert. Weitere Informationen zu benutzerdefinierten Attributen finden Sie unter Anpassungsattribute auf Seite 165. Weitere Informationen über die Systemprofil-Konfigurationsvorlage, über Attribute und Workflows finden Sie unter Weitere Informationen auf Seite 166.

Verwalten von Systemprofilen

Systemprofile definieren die Systemkonfiguration eines Servers mithilfe eines Referenzservers. Im OpenManage Integration for VMware vCenter gibt es verschiedene Verwaltungsaktionen, die Sie an vorhandenen Systemprofilen durchführen können. Dazu gehören:

- Systemprofil anzeigen
- Systemprofil löschen

ANMERKUNG: Das Ändern des Systemprofils von OMIVV aus wird in der aktuellen Version nicht unterstützt. Konfigurieren Sie Ihren Computer zuerst außerhalb von OMIVV und verwenden Sie dann es als Referenzserver für das Systemprofil.

Hardwareprofil konfigurieren

Zum Konfigurieren der Serverhardwareeinstellungen müssen Sie zunächst ein Hardwareprofil erstellen. Ein Hardwareprofil ist eine Konfigurationsvorlage, die Sie an neu ermittelten Infrastrukturkomponenten anwenden können. Für ein Hardwareprofil sind die folgenden Informationen erforderlich:

Tabelle 35. Anforderungen für die Erstellung eines Hardwareprofils

Anforderungen	Beschreibung
Startreihenfolge	Die Startreihenfolge ist die Reihenfolge der Boot-Geräte und Festplatten, die Sie nur dann bearbeiten können, wenn der Boot-Modus auf BIOS gesetzt ist.
BIOS-Einstellungen	Die BIOS-Einstellungen umfassen: Speicher, Prozessor, SATA, integrierte Geräte, serielle Kommunikation, integrierte Serververwaltung, Energieverwaltung, Systemsicherheit und verschiedene andere Einstellungen. **ANMERKUNG:** OpenManage Integration for VMware vCenter ermöglicht unter der Gruppe „Prozessor“ im BIOS bestimmte BIOS-Einstellungen auf allen bereitgestellten Servern, unabhängig von den Einstellungen auf dem Referenzserver. Bevor Sie einen Referenzserver zum Erstellen eines neuen Hardwareprofils verwenden, muss auf dem Referenzserver die CSIOR-Einstellung aktiviert sein und ein Neustart durchgeführt werden, damit korrekte Bestandslisten- und Konfigurationsinformationen bereitgestellt werden.
iDRAC-Einstellungen	Die iDRAC-Einstellungen umfassen: Netzwerk, Benutzerliste und Benutzerkonfiguration.
RAID-Konfiguration	Die RAID-Konfiguration zeigt die aktuelle RAID-Topologie auf dem Referenzserver zu dem Zeitpunkt an, an dem das Hardwareprofil extrahiert wurde. **ANMERKUNG:** Im Hardware-Profil sind 2 RAID-Konfigurationsoptionen konfiguriert: 1. RAID1 anwenden + Erstellen eines dedizierten Ersatzgeräts, je nach Ausstattung – Verwenden Sie diese Option, wenn Sie Standard-RAID-Konfigurationseinstellungen auf den Zielserver anwenden möchten. 2. RAID-Konfiguration vom Referenzserver klonen – Verwenden Sie diese Option, wenn Sie die Referenzservereinstellung klonen möchten. Siehe Anpassen von Referenzservern zum Erstellen von Hardwareprofilen.

Die Aufgaben zum Erstellen von Hardwareprofilen umfassen:

- Aktivieren von CSIOR auf einem Referenzserver
- Anpassen von Referenzserver zum Erstellen eines Hardwareprofils
- Klonen eines Hardwareprofils

Aktivieren von CSIOR auf einem Referenzserver

Bevor Sie ein Hardwareprofil mit einem Referenzserver erstellen, aktivieren Sie die Einstellung „Collect System Inventory On Reboot“ (CSIOR) und booten Sie den Server neu, um die korrekten Informationen zur Bestandsliste und Konfiguration bereitzustellen.

Es gibt zwei Methoden zum Aktivieren von CSIOR:

Tabelle 36. Methoden zum Aktivieren von CSIOR

Methode	Beschreibung
Lokal	Hier wird ein individueller Host mit der Benutzeroberfläche „Dell Lifecycle Controller United Server Configurator“ (USC) verwendet.
Remote	Hier wird ein WS-Man-Skript verwendet. Weitere Informationen zu dieser Funktion finden Sie im *Dell Tech Center* und unter *DCIM Lifecycle Controller Management-Profil*.

So aktivieren Sie CSIOR lokal auf einem Referenzserver:

1. Schalten Sie das System ein, und drücken Sie während POST die Taste **<F2>**, um USC zu starten.
2. Wählen Sie **Hardwarekonfiguration** > **Teileaustauschkonfiguration**.
3. Aktivieren Sie die Einstellung **Bestandsliste des Systems beim Neustart erstellen** und beenden Sie USC.

Erstellen oder Anpassen des Hardwareprofils

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Bereitstellung** die Option **Bereitstellungsvorlagen** > **Hardwareprofile**.
2. Klicken Sie auf das Symbol  .
3. Klicken Sie im **Hardwareprofil-Assistenten** auf **Weiter** auf der Seite **Willkommen**, und führen Sie die folgenden Schritte aus:
   - Geben Sie den Profilnamen in das Textfeld **Profilname** ein.
   - Geben Sie in das Textfeld **Beschreibung** eine Beschreibung ein. Die Beschreibung ist optional.
4. Klicken Sie auf **Weiter**.
   Das Dialogfeld **Referenzserver** wird angezeigt. Wählen Sie dazu entweder den Referenzserver direkt im Dialogfeld oder über die Schaltfläche zum Durchsuchen im Referenzserver-Fenster.
5. Wählen Sie einen Referenzserver, indem Sie einen der folgenden Teilschritte durchführen:
   - Wählen Sie im Dialogfeld **Referenzserver** den richtigen Referenzserver, und klicken Sie auf den Link **Wählen** neben dem Referenzserver.

     Das Dialogfeld **Bestätigung extrahieren**, das das Extrahieren der Einstellungen zeigt, wird angezeigt. Klicken Sie zum Extrahieren der Hardwarekonfiguration vom Referenzserver im Dialogfeld **Bestätigung extrahieren** auf **Ja**. Das Extrahieren ist dann nach wenigen Minuten abgeschlossen.
   - Klicken Sie auf der Seite **Referenzserver** auf **Durchsuchen**, um einen konformen Referenzserver auszuwählen, der verwaltet wird und erfolgreich durch OMIVV oder einen konformen Bare-Metal-Servern inventarisiert wird.

     Zum Extrahieren der Hardwarekonfiguration vom Referenzserver, klicken Sie im Dialogfeld **Bestätigung extrahieren** auf **Ja**.

   Der ausgewählte Servername oder die iDRAC-IP-Adresse, das Modell und der Service-Tag werden auf der Seite **Referenzserver** angezeigt.
6. Auf der Seite **Referenzserver** klicken Sie zum Anpassen der Referenzservereinstellungen auf **Referenzservereinstellungen anpassen**, und wählen Sie die folgenden Einstellungen, die optional enthalten sind und benutzerdefiniert angepasst werden können:
   - **RAID Settings**
   - **BIOS-Einstellungen**
   - **Boot-Reihenfolge**
   - **iDRAC-Einstellungen**
     - **Netzwerkeinstellungen**
     - **Benutzerliste**
7. Wählen Sie im Fenster **RAID-Konfiguration** eine der folgenden Optionen aus, und klicken Sie auf **Weiter**:
   - **RAID1 anwenden + Erstellen eines dedizierten Ersatzgeräts, je nach Ausstattung** – Verwenden Sie diese Option, wenn Sie Standard-RAID-Konfigurationseinstellungen auf den Zielserver anwenden möchten. Die RAID-Konfigurationsaufgabe ist auf den ersten zwei RAID1-fähigen Laufwerken des integrierten Controllers standardmäßig auf RAID1 eingestellt. Außerdem wird ein

dediziertes Ersatzlaufwerk für das RAID1-Array erstellt, wenn ein potenzielles Laufwerk, das die RAID Kriterien erfüllt, vorhanden ist.

- **RAID-Konfiguration vom Referenzserver klonen, wie unten dargestellt** – Verwenden Sie diese Option, wenn Sie die Referenzservereinstellung klonen möchten.

8. Erweitern Sie auf der Seite **BIOS-Einstellungen**, um die BIOS-Einstellungen in das Profil aufzunehmen, eine Kategorie, um die möglichen Einstellungsoptionen anzuzeigen, und klicken Sie auf **Bearbeiten** zum Aktualisieren von einem der folgenden Punkte:
   - **Systeminformationen**
   - **Speichereinstellungen**
   - **Prozessoreinstellungen**
   - **SATA-Einstellungen**
   - **Starteinstellungen**
   - **Einmalstart**
   - **Integrierte Geräte**
   - **Steckplatzdeaktivierung**
   - **Serielle Kommunikation**
   - **Systemprofileinstellungen**
   - **Systemsicherheit**
   - **Verschiedene Einstellungen**

   Nachdem alle Aktualisierungen an einer Kategorie vorgenommen wurden, klicken Sie, um die Änderungen zu speichern, auf **Weiter**, oder, um alle Änderungen abzubrechen, klicken Sie auf **Abbrechen**.

   ANMERKUNG: Ausführliche BIOS-Informationen, einschließlich möglicher Einstellungen und Erklärungen finden Sie im *Hardware-Bedienungshandbuch* für den ausgewählten Server.

9. Führen Sie auf der Seite **Startreihenfolge** die folgenden Schritte aus, und klicken Sie auf **Weiter**:
   a. Erweitern Sie **Startreihenfolge**, um die Optionen zur Startreihenfolge anzuzeigen, und klicken Sie auf **Bearbeiten**, um folgende Aktualisierungen vorzunehmen:
      i. Wählen Sie in der Liste **Startmodus** `BIOS` oder `UEFI`.
      ii. Nehmen Sie Änderungen an der angezeigten Startreihenfolge in der Liste **Ansicht** unter **Startgeräte-Reihenfolge** vor. Dazu wählen Sie das Gerät aus und klicken entweder auf **Nach oben** oder **Nach unten**.
      iii. Wählen Sie **Wiederholung der Startreihenfolge aktivieren**, sodass der Server die Startreihenfolge automatisch erneut versucht.
      iv. Um die Änderungen anzuwenden, klicken Sie auf **OK**, oder, um alle Änderungen abzubrechen, klicken Sie auf **Abbrechen**.
   b. Um die Auswahloptionen für Festplatten anzuzeigen, erweitern Sie **Reihenfolge der Festplatten** und klicken Sie auf **Bearbeiten**. Aktualisieren Sie Folgendes:
      i. Um Änderungen an der angezeigten Reihenfolge der Festplatten vorzunehmen, wählen Sie das Gerät aus und klicken dann entweder auf **Nach oben** oder **Nach unten**.
      ii. Um die Änderungen anzuwenden, klicken Sie auf **OK**, oder, um alle Änderungen abzubrechen, klicken Sie auf **Abbrechen**.

   ANMERKUNG: Bei Servern einer älteren als der 13. Generation werden sowohl UEFI- als auch BIOS-Modus angezeigt, wohingegen bei Servern ab der 13. Generation entweder der BIOS- oder der UEFI-Modus angezeigt wird.

10. Führen Sie auf Seite **iDRAC-Einstellungen** die folgenden Schritte aus:
    a. Erweitern Sie eine Kategorie, um die möglichen Einstellungsoptionen anzuzeigen, und klicken Sie auf **Bearbeiten**:

       Aktualisieren Sie eine der folgenden Optionen:
       - **Netzwerkeinstellungen**
       - **Netzwerk**
       - **Virtueller Datenträger**

    b. Führen Sie im Abschnitt lokale **Benutzerliste** zu iDRAC einen der folgenden Vorgänge aus:
       - **Benutzer hinzufügen**: Geben Sie manuell einen iDRAC-Benutzer und die erforderlichen Informationen ein. Wenn Sie mit der Anwendung der Änderungen fertig sind, klicken Sie auf **Anwenden**, oder zum Abbrechen des Vorgangs auf **Abbrechen**.
       - **Benutzer löschen**: Löscht den ausgewählten Benutzer. Um einen Benutzer auszuwählen, verwenden Sie die Maus und klicken Sie auf **Löschen**. Um den Löschvorgang zu bestätigen, klicken Sie auf **Yes** (Ja).
       - **Benutzer bearbeiten**: Bearbeiten Sie manuell die Informationen zu einem iDRAC-Benutzer. Klicken Sie nach dem Festlegen der Einstellungen auf **Anwenden** oder zum Abbrechen des Vorgangs auf **Abbrechen**.

    Nachdem alle Aktualisierungen an einer Kategorie vorgenommen wurden, klicken Sie, um die Änderungen zu speichern, auf **Weiter**, oder, um alle Änderungen abzubrechen, klicken Sie auf **Abbrechen**.

ANMERKUNG: Ausführliche iDRAC-Informationen, einschließlich möglicher Einstellungen und Erklärungen, finden Sie im *iDRAC-Benutzerhandbuch* für den ausgewählten Server.

11. Klicken Sie auf **Weiter**.
12. Klicken Sie im Fenster **Zusammenfassung** auf **Fertigstellen**.

Das Profil wird automatisch gespeichert und wird im **Hardwareprofil**-Fenster angezeigt.

Erstellen oder Klonen eines Hardwareprofils

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte**Bereitstellung** > **verwalten** den Punkt **Bereitstellungsvorlagen** > **Hardwareprofile**.
2. Klicken Sie auf .
3. Klicken Sie im **Hardwareprofil-Assistenten** auf **Weiter** auf der Seite **Willkommen** und führen Sie die folgenden Schritte aus:
   - Geben Sie den Profilnamen in das Textfeld **Profilname** ein.
   - Geben Sie eine **Beschreibung** in das Textfeld **Beschreibung** ein. Die Beschreibung ist optional.
4. Klicken Sie auf **Weiter**.
5. Zum Auswählen eines konformen Referenzservers, der von vCenter verwaltet wird und erfolgreich vom Dell EMC OpenManage-Plugin inventarisiert wurde, klicken Sie auf der **Referenzserver**-Seite auf **Durchsuchen**.
6. Klicken Sie auf die Option **Einstellungen für geklonten Referenzserver**, um alle Hardwareeinstellungen des Referenzservers zu extrahieren.
7. Klicken Sie auf **Weiter**.
   Das Extrahieren der Einstellungen kann einige Minuten in Anspruch nehmen.
8. Klicken Sie auf **Weiter**.
   Die Einstellungen werden bestückt und der Name des ausgewählten Servers, die iDRAC IP-Adresse sowie die Service-Tag-Nummer werden im Referenzserver-Fenster angezeigt.

Das Profil wird gespeichert und zeigt das Fenster **Hardwareprofile** unter **Verfügbare Profile** an.

Verwalten von Hardwareprofilen

Die Hardwareprofile definieren die Hardwarekonfiguration eines Servers mithilfe von einem Referenzserver. Von OpenManage Integration for VMware vCenter gibt es verschiedene Verwaltungsmaßnahmen, die Sie an vorhandenen Hardwareprofilen durchführen können. Dazu gehören:

- Anzeigen oder Bearbeiten eines Hardwareprofils
- Löschen eines Hardwareprofils

Anzeigen oder Bearbeiten eines Hardwareprofils

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Bereitstellung** den Punkt **Bereitstellungsvorlagen** > **Hardwareprofile**.
   Die Hardwareprofile werden angezeigt.
2. Um ein Profil zu bearbeiten, wählen Sie es aus und klicken auf .
3. Klicken Sie im **Hardwareprofil**-Assistenten zum Konfigurieren mit unterschiedlichen Werten auf **Bearbeiten**.
4. Um die Änderungen anzuwenden, klicken Sie auf **Speichern** oder, um alle Änderungen abzubrechen, klicken Sie auf **Abbrechen**.

Löschen eines Hardwareprofils

ANMERKUNG: Das Löschen eines Hardwareprofils, das Teil einer laufenden Bereitstellungsaufgabe ist, kann dazu führen, dass die Löschungs-Aufgabe fehlschlägt.

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Bereitstellung** > **verwalten** den Punkt **Bereitstellungsvorlagen Hardwareprofile**.
2. Wählen Sie ein Profil aus und klicken Sie auf .

3. Um das Profil zu löschen, klicken Sie im Bestätigungsdialogfeld auf **Ja** oder zum Abbrechen des Vorgangs auf **Nein**.

Erstellen eines Hypervisor-Profils

Zum Bereitstellen und Konfigurieren von ESXi auf einem Server muss ein Hypervisor-Profil erstellt werden. Ein Hypervisor-Profil benötigt die folgenden Informationen:

- Ein auf Dell angepasstes ISO-Softwaremedium auf einer NFS- oder CIFS-Freigabe
- Eine vCenter-Instanz, die die bereitgestellten Hosts verwaltet, sowie ein optionales Hostprofil
- Das Ziel-Cluster oder -Datacenter, in dem das Plugin Server in vCenter bereitstellt

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Bereitstellung** den Punkt **Bereitstellungsvorlagen** > **Hypervisorprofile**.
2. Klicken Sie auf der Seite **Hypervisor-Profile** auf  .
3. Führen Sie im Dialogfeld **Hypervisor-Profil** die folgenden Teilvorgänge aus:
   - Geben Sie den Profilnamen in das Textfeld **Profilname** ein.
   - Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein, dies ist optional.
4. Geben Sie unter **Referenz-ISO-Pfad und Version wählen** im Textfeld **Installationsquelle (ISO)** den Pfad zu dem für Hypervisor freigegebenen Speicherort an.

   Eine Kopie des Hypervisor-Images wird modifiziert, um eine skriptgeführte Installation zuzulassen. Der Speicherort für das Referenz-ISO kann die folgende Syntax aufweisen:

   - `NFS-Format: host:/share/hypervisor.iso`
   - `CIFS-Format: \\host\freigabe\hypervisor.iso`

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

   Wenn Sie eine CIFS-Freigabe verwenden, geben Sie Werte in die Felder **Benutzername**, **Kennwort** und **Kennwort bestätigen** ein. Stellen Sie sicher, dass die Kennwörter übereinstimmen.
5. Wählen Sie in der Liste **Version auswählen** eine ESXi-Version.
   Alle Server, die mit diesem Hypervisor-Profil bereitgestellt werden, verfügen über dieses Image. Wenn die Server-Version niedriger als 12 ist, wird die letzte empfohlene Version von OMSA installiert.
6. Um Pfad und Authentifizierung zu prüfen, klicken Sie auf **Test starten** unter **Einstellungen testen**.
7. Klicken Sie auf **Anwenden**.

Verwalten von Hypervisor-Profilen

Es gibt verschiedene Verwaltungsmaßnahmen, die Sie an bestehenden Hypervisor-Profilen vornehmen können. Dazu gehören:

- Anzeigen oder Bearbeiten von Hypervisor-Profilen
- Löschen von Hypervisor-Profilen

Anzeigen oder Bearbeiten von Hypervisor-Profilen

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte**Bereitstellung** > **verwalten** den Punkt **Bereitstellungsvorlagen** > **Hypervisorprofile**.
   Die Hypervisorprofile werden angezeigt.
2. Wählen Sie ein Profil aus und klicken Sie auf  .
3. Geben Sie im Dialogfeld **Hypervisor-Profil** aktualisierte Werte an.
4. Um die Änderungen anzuwenden, klicken Sie auf **Speichern** oder, um alle Änderungen abzubrechen, klicken Sie auf **Abbrechen**.

Löschen eines Hypervisor-Profils

ANMERKUNG: Das Löschen eines Hypervisor-Profils, das Teil einer laufenden Bereitstellungsaufgabe ist, kann dazu führen, dass die Aufgabe fehlschlägt.

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Bereitstellung** den Punkt **Bereitstellungsvorlagen** > **Hypervisorprofile**.
2. Wählen Sie ein Profil aus und klicken Sie auf .
3. Klicken Sie im Bestätigungsdialogfeld, um das Profil zu löschen, auf **Löschen** oder zum Abbrechen des Vorgangs auf **Abbrechen**.

Erstellen von Bereitstellungsvorlagen

Eine Bereitstellungsvorlage enthält ein Systemprofil, Hardwareprofil, Hypervisor-Profil, eine Kombination aus Systemprofil und Hypervisor-Profil oder eine Kombination aus Hardwareprofil und Hypervisor-Profil. Der **Bereitstellungsassistent** verwendet diese Vorlage, um Serverhardware einzurichten und Hosts innerhalb von vCenter bereitzustellen.

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Bereitstellung** den Punkt **Bereitstellungsvorlagen**.
2. Klicken Sie auf .
3. Geben Sie im Dialogfeld **Bereitstellungsvorlage** einen Namen für die Vorlage ein.
4. Geben Sie **eine Beschreibung** für die Bereitstellungsvorlage ein, dies ist optional.
5. Klicken Sie auf **Systemprofil** oder **Hardwareprofil** und wählen Sie das entsprechende Profil aus dem Drop-down-Menü aus.

   ANMERKUNG: Es wird empfohlen, ein Systemprofil für Server der 14. Generation und ein Hardwareprofil für Server bis zur 13. Generation zu verwenden.
6. Wählen Sie ein **Hypervisor-Profil** aus dem Dropdown-Menü aus.
7. Klicken Sie zum Übernehmen der Profilauswahl und zum Speichern der Änderungen auf **Speichern**. Klicken Sie zum Abbrechen des Vorgangs auf **Abbrechen**.

Verwalten von Bereitstellungsvorlagen

Es gibt verschiedene Verwaltungsmaßnahmen, die Sie in der OpenManage-Integration an bestehenden Bereitstellungsvorlagen vornehmen können. Dazu gehören:

- Anzeigen bzw. Bearbeiten von Bereitstellungsvorlagen
- Löschen von Bereitstellungsvorlagen

Anzeigen bzw. Bearbeiten von Bereitstellungsvorlagen

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Bereitstellung** den Punkt **Bereitstellungsvorlagen**.
   Die Bereitstellungsvorlage Profile wird angezeigt.
2. Geben Sie im Dialogfeld **Bereitstellungsvorlage** den neuen Namen und eine Beschreibung der Vorlage ein.

   Stellen Sie sicher, dass die Vorlage einen eindeutigen Namen hat.
3. Ändern Sie das **Hardwareprofil** oder **Systemprofil** im Drop-down-Menü.
4. Ändern Sie das **Hypervisor-Profil** im Drop-down-Menü und klicken Sie auf **Speichern**.

Löschen von Bereitstellungsvorlagen

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Bereitstellung** den Punkt **Bereitstellungsvorlagen**.
2. Wählen Sie auf der Seite **Bereitstellungsvorlage** eine Vorlage aus und klicken Sie auf .
3. Um zu bestätigen, dass die Vorlage gelöscht ist, klicken Sie auf **Löschen** im Dialogfeld oder zum Abbrechen des Vorgangs auf **Abbrechen**.

Infos zum Bereitstellungs-Assistenten

Der Bereitstellungs-Assistent beschreibt den Bereitstellungsprozess, der wie folgt lautet:

- Auswahl konformer Bare-Metal-Server.

  ANMERKUNG: Wenn Sie Server der 14. Generation zur Bereitstellung auswählen, enthält die Bereitstellungsvorlagenliste ein Hardware- bzw. System- oder Hypervisor-Profil oder eine Kombination von Hardware- und Hypervisor-Profilen bzw. eine Kombination aus System- und Hypervisor-Profilen.

  ANMERKUNG: Wenn Sie Server einer anderen Generation oder eine Kombination aus Servern der 14. Generation und einer anderen Generation auswählen, enthält die Bereitstellungsvorlagen-Liste ein Hardware- oder Hypervisor-Profil bzw. eine Kombination aus Hardware- und Hypervisor-Profilen.
- Auswahl einer Bereitstellungsvorlage, die aus Hardware- und Hypervisor-Profilen besteht.
- Auswahl des Installationsziels (Festplatte oder iDSDM).

  Beim Bereitstellen von Hypervisor können Sie ein internes Dual SD-Modul bereitstellen. Das interne Dual SD-Modul muss über das BIOS aktiviert werden, bevor Sie einen Hypervisor mit OMIVV bereitstellen.
- Auswählen des dem Host zuzuordnenden Verbindungsprofils.
- Zuweisen der Network Details für jeden Host.
- Auswahl von vCenter, Ziel-Datacenter oder Cluster und ein optionales Hostprofil.
- Planen der auszuführenden Serverbereitstellungsjobs.

ANMERKUNG: Wenn Sie nur ein Hardwareprofil bereitstellen, werden die Optionen Server-Identifikation, Verbindungsprofil und Netzwerkdetails des Bereitstellungs-Assistenten übersprungen und Sie gelangen direkt zur Seite **Bereitstellung planen**.

ANMERKUNG: Mit einer Testlizenz können Sie den Bereitstellungs-Assistenten für die Dauer Ihrer Lizenz verwenden.

VLAN-Support

Das OMIVV unterstützt die Hypervisor-Bereitstellung zu einem umleitbaren VLAN, und Sie können den VLAN-Support im Bereitstellungsassistenten konfigurieren. In diesem Teil des Bereitstellungsassistenten gibt es eine Option, in der Sie die Verwendung von VLANs und eine VLAN-ID angeben können. Wenn eine VLAN-ID bereitgestellt wird, wird sie während der Bereitstellung auf die Verwaltungsschnittstelle des Hypervisors angewandt und markiert den ganzen Verkehr mit der VLAN-ID.

Achten Sie darauf, dass das während der Bereitstellung bereitgestellte VLAN mit dem virtuellen Gerät sowie mit dem vCenter-Server kommuniziert. Die Bereitstellung eines Hypervisors 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 ausgewählten Server anwenden**. Diese Option ermöglicht Ihnen die Anwendung derselben VLAN-ID zusammen mit den anderen Netzwerkeinstellungen auf alle Server im betreffenden Bereitstellungsjob.

ANMERKUNG: Das OMIVV unterstützt keine Multihomed-Konfiguration. Das Hinzufügen einer zweiten Netzwerkschnittstelle zum Gerät für die Kommunikation mit einem zweiten Netzwerk verursacht Workflow-Probleme, und zwar mit der Hypervisor-Bereitstellung, der Server-Übereinstimmung und Firmware-Aktualisierungen.

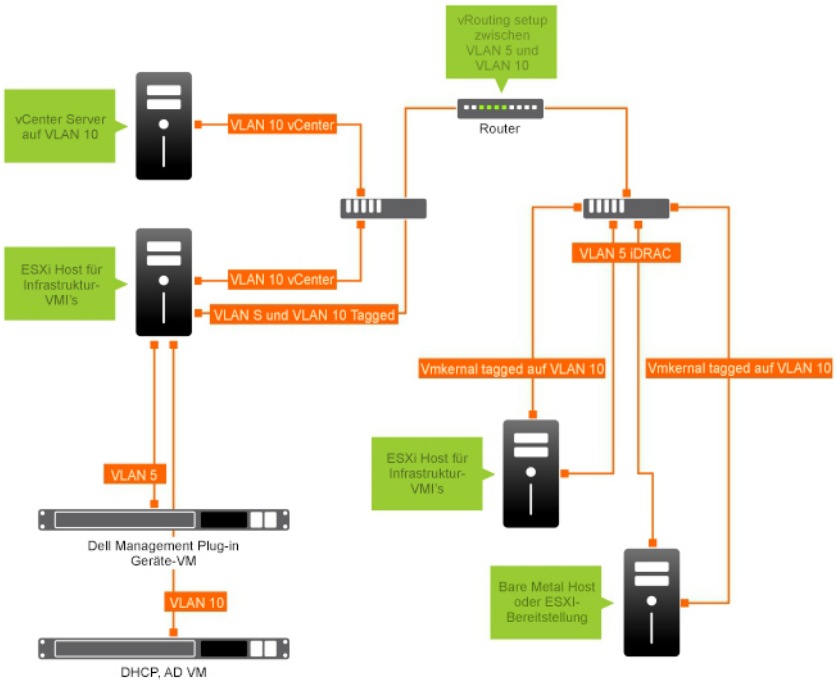

Abbildung 2. VLAN-Netzwerk.

In diesem Beispielnetzwerk befindet sich das OMIVV-Gerät auf einem VLAN 5, während das vCenter und der VMkernal der ESXi-Hosts auf VLAN 10 bereitgestellt werden. Da das OMIVV das Multi-VLAN-Homing nicht unterstützt, muss VLAN 5 für alle Systeme auf VLAN 10 umgeleitet werden, damit sie korrekt miteinander kommunizieren können. Falls das Routing zwischen diesen VLANs nicht aktiviert ist, schlägt die Bereitstellung fehl.

Bereitstellungsassistenten ausführen

Stellen Sie sicher, dass Sie eine Bereitstellungsvorlage mit Hardwareprofil, Systemprofil und Hypervisor-Profil und Verbindungsprofil für das vCenter vor dem Ausführen des Bereitstellungsassistenten erstellen.

Ausführen des Bereitstellungs-Assistenten:

1. Wählen Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Bereitstellung** > **verwalten**.
2. Klicken Sie im Fenster **Bare-Metal-Server** auf den Link **Bereitstellungsassistent ausführen**.
   Die Bereitstellungsassistentseite **Willkommen** wird angezeigt.
3. Zeigen Sie die Informationen auf der Seite **Willkommen** an, und klicken Sie auf **Weiter**.
4. Klicken Sie auf der Seite **Server für Bereitstellung wählen** die Kontrollkästchen neben der Serverliste an, um konforme Bare-Metal-Server einem Bereitstellungsjob zuzuweisen.
5. Klicken Sie auf **Next** (Weiter).
6. Führen Sie auf der Seite **Vorlage/Profil wählen** führen Sie einen der nächsten Schritte aus:
   a. Unter **Bereitstellungsvorlage**, zum Zuweisen einer Bereitstellungsvorlage auf den ausgewählten Servern wählen Sie eine vorhandene Bereitstellungsvorlage aus **Bereitstellungsvorlage wählen**.

      ANMERKUNG: Systemprofil-basierte Vorlage wird nur dann angezeigt, wenn Sie auf der Seite **Wählen Sie die Server für die Bereitstellung** die Server der 14. Generation auswählen.

      Sie können eine der folgenden Bereitstellungsvorlagen aus der Dropdownliste auswählen:
      - Wenn Sie eine Bereitstellungsvorlage nur für ein Hardware- oder Systemprofil auswählen, die nur die Serverhardware konfiguriert, fahren Sie mit Schritt 10 fort.
      - Wenn Sie eine Bereitstellungsvorlage für ein Hypervisor-Profil auswählen, die einen Hypervisor bereitstellt, fahren Sie mit Schritt 6 (b) fort.

        ANMERKUNG: Wenn Sie eine Bereitstellungsvorlage nur für ein Hardware- oder Systemprofil auswählen, werden Sie automatisch dazu aufgefordert, Informationen für die Seite **Bereitstellungszeitplan** anzugeben.

   b. Unter **Hypervisor-Installationsinformationen** wählen Sie eine der folgenden Optionen:

- **Erstes Startlaufwerk** – stellt einen Hypervisor auf der Festplatte (HDD), dem Solid-State-Laufwerk (SSD) oder einem von RAID-Controllern erstellten virtuellen Datenträger bereit.
- **Internes Dual-SD-Modul** – Stellt einen Hypervisor auf dem IDSDM bereit.

  ANMERKUNG: 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 **Festplatte** verfügbar.

  Wenn einer der ausgewählten Server kein IDSDM unterstützt oder während der Bereitstellung kein IDSDM vorhanden ist, führen Sie eine der folgenden Aktionen aus:

  ANMERKUNG: Stellen Sie sicher, dass **HardDiskFailOver** während der BS-Bereitstellung aktiviert ist.

  - Markieren Sie das Kontrollkästchen **Hypervisor auf dem ersten Startlaufwerk für die Server, die über kein internes Dual-SD-Modul verfügen**, wenn Sie möchten, dass ein Hypervisor auf dem ersten Startlaufwerk der Server bereitgestellt wird.

    VORSICHT: Wenn Sie diese Option auswählen und den Hypervisor auf dem ersten Startlaufwerk der Server bereitstellen, werden alle Daten auf den Festplattenlaufwerken gelöscht.
  - Zum Überspringen der Bereitstellung auf den ausgewählten Servern und zum Fortsetzen mit der Hypervisor-Bereitstellung auf dem nächsten Server, heben Sie die Markierung **Hypervisor auf dem ersten Startlaufwerk für die Server bereitstellen, die über kein internes Dual-SD-Modul verfügen** auf.

c. Führen Sie unter **Anmeldeprofil** eine der folgenden Aktionen aus:
   - Wählen Sie die Options-Schaltfläche **Verwenden Sie dieses Profil mit Anmeldeinformationen für alle Server**, und um alle Server zum gleichen bestehenden Profil zuzuweisen, wählen Sie ein Verbindungsprofil in der Dropdown-Liste aus.
   - Klicken Sie auf das Optionsfeld **Wählen Sie für jeden Server ein Verbindungsprofil aus**, und wählen Sie dann für jeden Server ein Verbindungsprofil in der Dropdown-Liste aus.

7. Klicken Sie auf **Next** (Weiter).
   Die Seite **Server-Identifikation** wird angezeigt.

   Die Server-Identifikation kann auf zwei Arten durchgeführt werden:
   - Durch Eingabe der Netzwerkinformationen (IP Adresse, Subnetzmaske und Gateway) – 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.
   - Verwenden Sie das dynamische Host-Konfigurationsprotokoll (DHCP) zum Konfigurieren von IP-Adressen, Subnetzmasken, Gateway-IPs, Hostnamen und bevorzugten/alternativen DNS-Servern. Die dem DHCP zugewiesene IP-Adresse wird beim Hinzufügen eines Hosts zu vCenter verwendet. Bei der Verwendung von DHCP wird empfohlen, eine Reservierung für ausgewählte NIC-MAC-Adressen zu verwenden.

   ANMERKUNG: Verwenden Sie einen vollständig qualifizierten Domänennamen (FQDN) als Hostnamen anstatt von localhost. Ab ESXi 5.1 beeinträchtigt ein localhost-Wert den Vorgang, bei dem das OMIVV-Plug-in die vom Host gesendeten Ereignisse verarbeitet. Erstellen Sie einen DNS-Datensatz, der die IP-Adresse mit dem vollständig qualifizierten Domänennamen (FQDN) auflöst Damit SNMP-Warnungen von ESXi 5.1 korrekt identifiziert werden, 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.

8. Führen Sie auf der Seite **Server-Identifikation** Folgendes aus:

   Die Seite enthält die Option zum Angeben einer VLAN-ID. Wenn eine VLAN-ID bereitgestellt wird, wird sie für die Verwaltungsschnittstelle des Hypervisor 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 (VLAN-Support).

   a. Um die jeweiligen Serverinformationen zu erweitern und anzuzeigen, klicken Sie unter **Ausgewählte Server** auf das .
   b. Geben Sie unter **Hostname und NIC** einen **vollständig qualifizierten Hostnamen** für den Server ein.
   c. Wählen Sie in der Dropdown-Liste **NIC Management Tasks** die Netzwerkschnittstellenkarte zur Verwaltung des Servers aus.
   d. Geben Sie IP-Adressen, Subnetzmaske, Standard-Gateway und DNS-Details ein, oder wählen Sie das Kontrollkästchen **Unter Verwendung von DHCP abrufen**.
   e. Wenn Sie auf einem Netzwerk implementieren, das eine VLAN-ID erfordert, markieren Sie das **VLAN**-Kontrollkästchen und geben dann die **VLAN**-ID ein.

      Verwenden Sie für die VLAN-ID die Zahlen 1 bis 4094. Die VLAN-ID-Nummer 0 ist für die Markierung der Priorität von Frames reserviert.
   f. Wiederholen Sie die Schritte a bis h für alle bereitzustellenden Server, oder aktivieren Sie das Kontrollkästchen **Einstellungen für alle ausgewählten Server anwenden**.

      Wenn Sie **Einstellungen für alle ausgewählten Server anwenden** auswählen, geben Sie FQDN-Name und IP-Adresse für die anderen Server ein.

ANMERKUNG: Stellen Sie mit festgelegtem FQDN-Namen für Server sicher, dass jeder Server einen eindeutigen Host-Namen hat.

9. Klicken Sie auf **Next** (Weiter).
10. Führen Sie auf der Seite **Bereitstellung planen** die folgenden Aktionen aus:
    a. Geben Sie einen **Jobnamen** und eine **Jobbeschreibung** ein.
    b. Für **vCenter-Einstellungen** geben Sie Folgendes ein:
        i. Wählen Sie in **vCenter-Instanz** die Server-Instanz, die einen Host nach der Bereitstellung verwaltet.
        ii. In **vCenter-Ziel-Container**, klicken Sie auf **Durchsuchen**, um nach den vCenter-Zielen zu suchen.
        iii. Wählen Sie in **vCenter-Hostprofil** ein Profil aus, das eine Hostkonfiguration enthält und das Verwalten der Hostkonfiguration unterstützt, die optional ist.
    c. Bestimmen Sie die Ausführung des Bereitstellungs-Jobs durch Auswahl eines Zeitplans:
        i. Wählen Sie **Zeitplan Bereitstellungs-Job**
            - Verwenden Sie das Kalender-Bedienfeld, um ein Datum auszuwählen.
            - Geben Sie die Uhrzeit ein.
        ii. Um den Job sofort auszuführen, wählen Sie **Bereitstellungs-Job jetzt ausführen**.

    Um zu der Job-Warteschlange zu gelangen, nachdem der Bereitstellungsauftrag beginnt, wählen Sie **Zu der Job-Warteschlange gehen, nachdem der Auftrag gestartet wurde**.
11. Klicken Sie auf **Fertigstellen**.

Nachdem die Aufgaben des Bereitstellungsassistenten abgeschlossen sind, können Sie die Bereitstellungs-Jobs mithilfe der **Job-Warteschlange** verwalten. .

Verwalten von Bereitstellungs-Jobs mithilfe der Job-Warteschlange

1. Klicken Sie in OpenManage Integration for VMware vCenter auf dem Register **Überwachen** > **Job-Warteschlange** auf **Bereitstellungsjobs**.

   Die folgenden Details zu Bereitstellungsjobs werden im oberen Raster angezeigt:
   - Name
   - Beschreibung
   - Geplante Zeit
   - Status
   - Erfassungsgröße
   - Fortschrittszusammenfassung
2. Klicken Sie zum Aktualisieren der **Details zu Bereitstellungsjobs** auf das Symbol für **Aktualisieren**.
3. Zur Anzeige der Details eines Bereitstellungsjobs, die ausführliche Informationen zu den Servern im Bereitstellungsjob enthalten, wählen Sie einen Bereitstellungsjob im oberen Raster.

   Es werden die folgenden Details im unteren Raster angezeigt:
   - Service-Tag-Nummer
   - iDRAC-IP-Adresse
   - Jobstatus
   - Warnungen
   - Details zum Bereitstellungsjob (führen Sie für weitere Informationen den Mauszeiger darauf).
   - Start- und Endzeit
   - Weitere Details

   Sie können die gesamten Informationen zu einem Bereitstellungsjob als Pop-up-Text anzeigen, indem Sie den Job auswählen und Ihren Cursor über die Spalte **Details** für diesen Bereitstellungsjob bewegen.

   Für weitere Einzelheiten zum Fehlschlagen von Systemprofil-basierten Jobs klicken Sie auf **Weitere Details**. Auf der Seite **Weitere Details** werden die folgenden Informationen 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 zu **Attributname** des Systemprofils beim Klicken auf **Weitere Details**.

Klicken Sie zum Exportieren der Details in eine CSV-Datei in der rechten Ecke des Datenraster auf  .

4. Um den Bereitstellungs-Job abzubrechen, klicken Sie auf das Symbol  .
5. Wenn die Meldung angezeigt wird, klicken Sie entweder auf **Job abbrechen**, um den Job abzubrechen, oder auf **Job nicht abbrechen**, um den Job weiter auszuführen.
6. Zur Anzeige des Fensters **Job-Warteschlange bereinigen** klicken Sie auf  . Wählen Sie **Älter als Datum und Job-Status** und klicken Sie auf **Anwenden**.
   Die ausgewählten Jobs werden aus der Warteschlange gelöscht.

Systemsperrmodus-Jobs

1. Klicken Sie auf der Seite **OpenManage Integration for VMware vCenter** auf die Registerkarte **Überwachen** > **Job-Warteschlange** und dann auf **Systemsperrmodus-Jobs**.
   Die folgenden Informationen zu Systemsperrmodus-Jobs werden im oberen Raster angezeigt:
   - Name
   - Beschreibung
   - Geplante Zeit
   - vCenter
   - Status
   - Erfassungsgröße
   - Fortschrittszusammenfassung
2. Klicken Sie zum Aktualisieren der **Details zu Systemsperrmodusjobs** auf das Symbol für **Aktualisieren**.
3. Zur Anzeige der Details eines Systemsperrmodus-Jobs mit ausführlichen Informationen zu den Servern im Systemsperrmodusjob wählen Sie einen Systemsperrmodusjob im oberen Raster.
   Es werden die folgenden Details im unteren Raster angezeigt:
   - Service Tag
   - iDRAC-IP
   - Host-Name
   - Status
   - Einzelheiten

     ANMERKUNG: Wird in der Spalte **Status Erfolgreich** angezeigt, ist die Spalte **Details** leer.

     Wird in der Spalte **Status Fehlerhaft** angezeigt, wird die Ursache des Fehlers in der Spalte **Details** angezeigt.
   - Startdatum und -uhrzeit
   - Enddatum und -zeit

   Sie können alle Informationen zu einem Systemsperrmodus-Job als Popup-Text anzeigen, indem Sie den Job auswählen und Ihren Cursor über die Spalte **Details** dieses Systemsperrmodus-Jobs bewegen.
4. Um die Systemsperrmodus-Jobs zu säubern, klicken Sie auf  . Wählen Sie **Älter als Datum und Job-Status** und klicken Sie auf **Anwenden**.
   Die ausgewählten Jobs werden aus der Job-Warteschlange gelöscht.

Abweichungserkennungsjobs

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

1. Klicken Sie auf der Seite **OpenManage Integration für VMware vCenter** auf die Registerkarte **Überwachen** > **Job-Warteschlange** und dann auf **Abweichungserkennungsjobs**.

   Die folgenden Informationen zu Abweichungserkennungsjobs werden in der oberen Tabelle angezeigt:
   - Name
   - Letzte Ausführung
   - Nächste Ausführung

- Status
- Erfassungsgröße
- Fortschrittszusammenfassung

2. Um die aktualisierten **Abweichungserkennungsjob-Details** aufzurufen, klicken Sie auf **Aktualisieren**.
3. Zur Anzeige der Details eines Abweichungserkennungsjobs, die ausführliche Informationen zu den Servern im Abweichungserkennungsjob enthalten, wählen Sie einen Abweichungserkennungsjob in der oberen Tabelle aus.

   Es werden die folgenden Details in der unteren Tabelle angezeigt:
   - Service Tag
   - iDRAC IP (iDRAC-IP)
   - Host-Name
   - Cluster
   - vCenter
   - Status
   - Startdatum und -uhrzeit
   - Enddatum und -zeit

4. Klicken Sie zum bedarfsgerechten Durchführen eines **Abweichungserkennungsjobs** auf die Schaltfläche .

ANMERKUNG: In einem Baseline-Cluster wird der Abweichungserkennungsjob nach dem Hinzufügen eines Host-Geräts zum Verbindungsprofil für ein neu hinzugefügtes Host-Gerät automatisch ausgeführt.

Verwalten von Firmware-Aktualisierungs-Jobs

Um Informationen auf dieser Seite anzuzeigen, führen Sie einen Firmware-Aktualisierungsjob für einen Cluster durch. Siehe Ausführen des Firmware-Aktualisierungsassistenten für Cluster.

Die Seite zeigt alle Firmware-Aktualisierungs-Jobs an. Auf dieser Seite können Sie Ihre Firmware-Aktualisierungs-Jobs anzeigen, aktualisieren, bereinigen oder abbrechen.

1. Wählen Sie von OpenManage Integration **Überwachen** > **Job-Warteschlange** > **Firmwareaktualisierungen**.
2. Zum Anzeigen der aktuellsten Informationen klicken Sie auf das Symbol für **Aktualisieren**.
3. Anzeige des Status in der Datentabelle.

   Das Raster enthält die folgenden Informationen über Firmware-Aktualisierungs-Jobs:
   - Status
   - Geplante Zeit
   - Name
   - Beschreibung
   - vCenter
   - Erfassungsgröße (Anzahl von Servern im Firmware-Bestandsaufnahme-Job)
   - Fortschrittszusammenfassung (Details zum Fortschritt der Firmware-Aktualisierung)

4. Um mehr Details zu einem bestimmten Job in der Datentabelle anzuzeigen, wählen Sie einen Job aus.

   Hier finden Sie die folgenden Details:
   - Host-Name
   - Status
   - Startzeit
   - Endzeit

5. Wenn Sie eine geplante Firmware-Aktualisierung, die nicht ausgeführt wird, abbrechen möchten, wählen Sie den entsprechenden Job und klicken Sie auf .

   ANMERKUNG: Wenn Sie einen Firmware-Aktualisierungsjob abbrechen wollen, der bereits an den iDRAC übermittelt wurde, wird die Firmware möglicherweise trotzdem auf dem Host aktualisiert, aber OMIVV meldet den Auftragsstatus als abgebrochen.

6. Wenn Sie frühere Firmware-Aktualisierungsjobs oder geplante Firmware-Aktualisierungen bereinigen möchten, klicken Sie auf  .
   Das Dialogfeld **Jobs zur Bereinigung der Firmware-Aktualisierung** wird angezeigt. Sie können Jobs nur säubern, die abgebrochen wurden, erfolgreich abgeschlossene oder ausgefallene Jobs können geplante oder aktive Jobs nicht bereinigen.
7. Wählen Sie im Dialogfeld **Firmware-Aktualisierungs-Jobs bereinigen Älter als**, und klicken Sie auf **Anwenden**.
   Die ausgewählten Jobs werden aus der Warteschlange gelöscht.

Festlegen der Zeit für den Bereitstellungs-Job

Die Bereitstellung von Bare-Metal-Servern kann zwischen 30 Minuten und mehreren Stunden dauern, abhängig von verschiedenen Faktoren. Beim Starten eines Bereitstellungs-Jobs sollten Sie die Bereitstellungszeit entsprechend der aufgeführten Richtlinien planen. Die erforderliche Zeit für eine vollständige Bereitstellung hängt von Bereitstellungstyp, der Komplexität und der Anzahl gleichzeitig ausgeführter Bereitstellungs-Jobs ab. Die folgende Tabelle enthält die ungefähre Dauer eines Bereitstellungs-Jobs: Bereitstellungs-Jobs werden in Batches von bis zu fünf gleichzeitigen Servern ausgeführt, um die Gesamtdauer der Bereitstellung zu verringern. Die genaue Anzahl gleichzeitiger Jobs hängt von den verfügbaren Ressourcen ab.

Tabelle 37. Mögliche Zeitszenarios für Bereitstellungs-Jobs

Bereitstellungstyp	Ungefähre Zeit pro Bereitstellung
Nur Hypervisor	30 bis 130 Minuten
Hypervisor- und Hardware-Profile	1–4 Stunden
Nur Systemprofil	5–6 Minuten
Systemprofil und Hypervisor-Profil	30–40 Minuten

Server-Status innerhalb der Bereitstellungssequenz

Wenn ein Auftrag zum Erstellen einer Bestandsliste ausgeführt wird, werden automatisch/manuell erfasste Bare-Metal-Systeme in unterschiedlichen Status klassifiziert, um feststellen zu können, ob der Server neu zum Rechenzentrum hinzugefügt wurde oder ob eine ausstehende Bereitstellung geplant ist. Die Administratoren können anhand dieser Zustände feststellen, ob ein Server mit in einen Bereitstellungsauftrag aufgenommen werden sollte. Folgende Zustände sind möglich:

Tabelle 38. Server-Status innerhalb der Bereitstellungssequenz

Serverstatus	Beschreibung
Nicht konfiguriert	Der Server hat OMIVV kontaktiert und wartet auf die Konfiguration.
Konfiguriert	Der Server wurde mit allen Hardwareinformationen konfiguriert, die für eine erforderliche Hypervisor-Bereitstellung erforderlich sind.

Herunterladen von benutzerdefinierten Dell EMC ISO-Images

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

1. Rufen Sie die Seite `support.dell.com` auf.
2. Klicken Sie auf **Aus allen Produkten auswählen** > **Server, Massenspeicher und Netzwerke**.
3. Klicken Sie unter **Wählen Sie ein Produkt** auf **PowerEdge**.
4. Klicken Sie auf ein PowerEdge-Servermodell.
5. Klicken Sie auf die Seite **Treiber und Downloads** des Server-Modells.
6. Klicken Sie auf den Link **Betriebssystem ändern**, und wählen Sie ein ESXi-System, das Sie möchten.
7. Klicken Sie auf **Enterprise-Lösungen**.
8. Wählen Sie in der Liste **Enterprise-Lösungen** die Version des erforderlichen ISO aus, und klicken Sie dann auf **Herunterladen**.

14

Informationen zu Host-, Bare-Metal- und iDRAC-Konformität

Um Hosts und Bare-Metal-Server mit OMIVV zu verwalten, müssen bestimmte Mindestkriterien erfüllt sein. Wenn sie nicht konform sind, werden sie nicht ordnungsgemäß vom OMIVV verwaltet. OMIVV zeigt Details über die fehlende Konformität auf einem Bare-Metal oder einem Host an und ermöglicht bei Bedarf die Korrektur der fehlenden Konformität.

In jedem Fall können Sie die Konformitätsprobleme beheben, indem Sie eine der folgenden Optionen ausführen:

- Zum Anzeigen und Beheben von Konformitätsproblemen bei vSphere-Hosts lesen Sie Ausführen des Assistenten zum Korrigieren nicht konformer vSphere-Hosts.
- Zum Anzeigen und Beheben von Konformitätsproblemen bei Bare-Metal-Servern lesen Sie Ausführen des Assistenten zum Korrigieren nicht konformer Bare-Metal-Server.

Themen:

Berichterstattung und Festsetzen der Kompatibilität für vSphere Hosts

Ein Host ist nicht kompatibel wenn:

- Der Host nicht einem Verbindungsprofil zugeordnet ist.
- Das „Collect System Inventory on Reboot“ (CSIOR) deaktiviert ist oder nicht ausgeführt wurde. Hierzu ist ein manueller Neustart erforderlich.
- Der OMSA-Agent wurde nicht installiert, ist veraltet oder wurde nicht richtig konfiguriert. Ein Neustart des ESXi-Hosts ist erforderlich, wenn OMSA für Server der 11. Generation installiert oder aktualisiert wurde.
- Das SNMP-Trap-Ziel des Host ist nicht auf die IP-Adresse des OMIVV-Geräts konfiguriert. Der Fehler in der Einstellung des SNMP-Trap-Ziels kann entstehen, wenn die im Verbindungsprofil angegebenen iDRAC- oder Host-Anmeldeinformationen ungültig sind, es keine freien Steckplätze in iDRAC gibt, oder der iDRAC-Sperrmodus bei Hosts der 14. Generation eingeschaltet ist.
- OMIVV aktiviert den WBEM-Dienst auf Hosts, auf denen ESXi 6.5 läuft, nicht.

VORSICHT: Hosts im Lockdown-Modus werden bei Konformitätsprüfungen nicht angezeigt, auch wenn sie nicht konform sind. Sie werden nicht angezeigt, weil ihr Konformitätsstatus nicht ermittelt werden kann. Stellen Sie sicher, dass Sie die Konformität dieser Systeme manuell überprüfen. In einem solchen Szenario wird eine Warnmeldung angezeigt.

Sie können den Assistenten zum korrigieren nicht konformer Hosts für nicht konforme vSphere-Hosts ausführen. Einige nicht konforme ESXi-Hosts müssen neu gestartet werden. Ein Neustart eines ESXi-Hosts ist erforderlich, wenn OMSA installiert oder aktualisiert werden musste. Darüber hinaus ist ein Neustart für jeden Host erforderlich, auf dem CSIOR noch nicht ausgeführt wurde. Wenn Sie wählen, einen ESXi-Host automatisch neu zu starten, finden die folgenden Aktionen statt:

- Bei einer CSIOR-Statuskorrektur:

  Wenn CSIOR noch nicht auf dem Host ausgeführt wurde, muss CSIOR auf dem Host auf **ON** gesetzt werden, dann wird der Host in den Wartungsmodus versetzt und neu gestartet.

- Für Hosts, auf denen OMSA nicht installiert ist oder eine nicht unterstützte Version von OMSA ausgeführt wird:
  - OMSA ist auf dem Host installiert.
  - Der Host wird in den Wartungsmodus versetzt und neu gestartet.
  - Nach dem abgeschlossenen Neustart ist OMSA so konfiguriert, dass alle Änderungen übernommen werden.
  - Der Host beendet den Wartungsmodus.

- Eine Bestandsaufnahme wird erstellt, um die Daten zu aktualisieren.
- Bei einer OMSA-Statuskorrektur, wobei eine unterstützte Version von OMSA installiert ist, diese aber konfiguriert werden muss:
  - OMSA ist auf dem Host konfiguriert.
  - Eine Bestandsaufnahme wird erstellt, um die Daten zu aktualisieren.

Anzeigen und Korrigieren nicht konformer Hosts:

1. Klicken Sie in OpenManage Integration for VMware vCenter aus der Registerkarte **Verwalten** auf **Konformität** > **vSphere-Hosts**.
   a. Zeigen Sie auf der Seite **vSphere Hosts** die Liste der Hosts an, die nicht konform sind.
      Eine Tabelle wird angezeigt, die nicht konforme Hosts zusammen mit Host-IP oder Hostname, Modell, Verbindungsprofil, CSIOR-, OMSA-, WBEM-, SNMP-Trap-Zielstatus, Hypervisor und iDRAC-Lizenzstatus auflistet.
   b. Um weitere Details zu einem Host, der nicht kompatibel ist, anzuzeigen, wählen Sie einen Host der nicht kompatibel ist.
   c. Um die Spalten innerhalb der Tabelle zu vertauschen, tun Sie dies per Drag-and-Drop innerhalb der Datentabelle.
2. Zum Korrigieren nicht konformer Hosts klicken Sie auf **Nicht-konforme vSphere-Hosts korrigieren**.
   Der Assistent **Nicht-konforme vSphere-Hosts korrigieren** wird gestartet. Hierbei handelt es sich um einen dynamischen Assistenten. Es werden nur solche Seiten angezeigt, die sich auf die ausgewählten nicht konformen Hosts beziehen.
   Wenn alle ausgewählten, nicht konformen Hosts CSIOR-konform sind, können Sie die Seite **CSIOR einschalten** des Assistenten anzeigen.
3. Klicken Sie im Assistenten **Nicht-konforme vSphere-Hosts korrigieren** auf **Weiter** auf der Seite **Willkommen**.
4. Aktivieren Sie auf der Seite **Assistent zum Korrigieren nicht konformer vSphere-Hosts auswählen** die Kontrollkästchen der Hosts, die Sie korrigieren möchten.
5. Klicken Sie auf **Next** (Weiter).
   Eine Warnmeldung wird angezeigt, wenn es ausgewählte Hosts gibt, die nicht einem Verbindungsprofil zugeordnet sind. Sie werden entweder zum Fortfahren mit dem Konformitätsassistenten oder zum Abbrechen des Assistenten für die Korrektur der Konformität aufgefordert. Um die Nichtkonformität des Verbindungsprofil zu korrigieren, führen Sie einen der folgenden Schritte aus:
   - Um den Host ohne zugewiesenes Verbindungsprofil vom Konformitätsassistenten auszuschließen, klicken Sie auf **Mit Konformitätsassistent fortfahren**.
   - Um den Assistenten zu beenden und die Systeme auf der Seite **Verbindungsprofil** zu korrigieren, klicken Sie auf **Abbrechen**. Informationen dazu finden Sie unter Verbindungsprofil erstellen auf Seite 36. Nach dem das Verbindungsprofil erstellt wurde, können Sie zum Assistenten zurückkehren.
6. Wenn Sie für die Warnmeldung auf **Mit Konformitätsassistent fortfahren** klicken, wählen Sie im Fenster **CSIOR einschalten** die Kontrollkästchen, zum Einschalten von **CSIOR** für die ausgewählten Hosts.
7. Klicken Sie auf **Next** (Weiter).
8. Aktivieren Sie im Fenster **OMSA beheben** die Kontrollkästchen, um **OMSA** für die ausgewählten Hosts zu korrigieren.
9. Klicken Sie auf **Next** (Weiter).
10. Zeigen Sie im Fenster **Hosts neustarten** die ESXi-Hosts an, die neu gestartet werden müssen.
    Ein Neustart des ESXi-Hosts ist erforderlich, wenn OMSA installiert oder aktualisiert wurde. Darüber hinaus ist ein Neustart für jeden Host erforderlich, auf dem CSIOR noch nicht ausgeführt wurde. Führen Sie einen der folgenden Schritte aus:
    - Wenn Sie Hosts bei Bedarf automatisch in den Wartungsmodus versetzen und neu starten möchten, aktivieren Sie das Kontrollkästchen **Hosts bei Bedarf automatisch in den Wartungsmodus versetzen und neu starten**.
    - Wenn Sie den Neustart manuell durchführen möchten, starten Sie den Host nach der Installation von OMSA, konfigurieren OMSA manuell oder über den Konformitätsassistenten, sobald der Host ausgeführt wird und OMSA nicht konfiguriert ist, und führen die Bestandsaufnahme erneut durch. Lesen Sie dazu Ausführen von Bestandsaufnahme-Jobs.
11. Klicken Sie auf **Next** (Weiter).
12. Prüfen Sie die Maßnahmen, die an nicht konformen Hosts durchgeführt werden, im Fenster **Zusammenfassung**.
    Manuelle Neustarts sind erforderlich, um Maßnahmen auf der Seite „Zusammenfassung“ in Kraft zu setzen.
13. Klicken Sie auf **Fertigstellen**.

Der Assistent konfiguriert den Status des SNMP-Trap-Ziels nach der Reparatur der iDRAC- oder Host-Anmeldeinformationen durch die Bereitstellung gültiger Informationen im Verbindungsprofil, 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 Server der 14. Generation relevant.

Sind nicht WBEM-konforme Hosts vorhanden, so müssen Sie die Elemente dieser Hosts, die zum Fehlschlag der Aktivierung des WBEM-Diensts führten, manuell berichtigen. Sie können die Fehlerbedingungen beheben, indem Sie diese in den Benutzerprotokollen einsehen und dann OMIVV erlauben, den WBEM-Dienst für diese Hosts während der Bestandsaufnahme zu aktivieren.

Reparieren der iDRAC-Lizenzkonformität für vSphere-Hosts

Der vSphere-Hosts, die auf den vSphere-Host-Konformitätsseiten aufgeführt sind, sind nicht konform, da sie keine kompatible iDRAC-Lizenz aufweisen. Die Tabelle zeigt den Status der iDRAC-Lizenz an. Sie können auf einen nicht konformen Host klicken, um weitere Details anzuzeigen, wie z. B. wie viele Tage der Laufzeit der iDRAC-Lizenz noch übrig sind. Dann können Sie sie nach Bedarf aktualisieren. Der Link **Bestandsaufnahme-Job ausführen** ist aktiv, wenn der iDRAC-Konformitätsstatus für einen beliebigen, einem Verbindungsprofil zugeordneten Host „nicht konform“ oder „unbekannt“ ist.

1. Klicken Sie in OpenManage Integration for VMware vCenter aus der Registerkarte **Verwalten** auf **Konformität** > **vSphere-Hosts**.
2. Wählen Sie einen Host, dessen **iDRAC-Lizenzstatus nicht konform** ist.
3. Wenn die Lizenz abgelaufen ist, klicken Sie auf **iDRAC-Lizenz erwerben/erneuern**.
4. Melden Sie sich bei der Seite **Dell License Management** an, und aktualisieren oder erwerben Sie eine neue iDRAC-Lizenz. Verwenden Sie die Informationen auf dieser Seite, um Ihren iDRAC zu identifizieren und zu aktualisieren.
5. Nachdem Sie eine iDRAC-Lizenz installiert haben, führen Sie einen Bestandsaufnahme-Job für den vSphere-Host durch und kehren Sie zu dieser Seite zurück, nachdem der Bestandsaufnahme-Job erfolgreich abgeschlossen wurde, damit der Host konform ist.

Anzeigen von Baseline Compliance

Die Seite **Baseline Compliance** zeigt den Status der Baseline Compliance basierend auf der Abweichungserkennung für alle OMIVV-verwalteten Hosts an, die zum Cluster-Profil gehören.

- Konfigurations-Konformität: zeigt die Abweichung zwischen Attributen des im Cluster-Profil verwendeten Systemprofils und den zugehörigen VSAN-Hosts an.
- Firmware- und Treiber-Konformität: zeigt die Abweichungen zwischen Firmware- und Treiberversion in den im Cluster und den zugehörigen VSAN-Hosts verwendeten Firmware- und/oder Treiber-Repository-Profilen an.

1. Klicken Sie auf der Seite **OpenManage Integration for VMware vCenter** auf **Verwalten** > **Compliance** > **Baseline Compliance**. Es wird eine Tabelle angezeigt, in der die nicht konformen Hosts aufgelistet werden, die zur Baseline gehören, sowie die Host-IP oder FQDN, vCenter-IP oder FQDN, der Cluster-Name, der Cluster-Profilname, der Konfigurations-Konformitätsstatus, der Firmware-Konformitätsstatus und der Treiber-Konformitätsstatus.

   ANMERKUNG: Nur nicht konforme Hosts werden auf der Seite **Baseline Compliance** angezeigt.

   Die Compliance-Kategorien teilen sich wie folgt auf:
   - **Konform**: zeigt an, dass die Komponenten im Host mit den zugehörigen Profilen in der Baseline konform sind.
   - **Nicht konform**: zeigt an, dass die Komponenten im Host mit den zugehörigen Profilen in der Baseline nicht konform sind.
   - **Nicht verfügbar**: zeigt die Firmware, den Treiber oder das Systemprofil an, die nicht zum Cluster-Profil gehören.

   a. Um weitere Details zu einem Host anzuzeigen, wählen Sie den gewünschten Host aus.

      Der **Hostname** und die **Letzte Abweichungserkennung** werden im unteren Fensterbereich angezeigt.

   b. Um die Spalten innerhalb der Tabelle zu vertauschen, ziehen Sie diese per Drag-and-Drop an die gewünschte Stelle.
   c. Um die Inhalte der Datentabelle zu filtern, verwenden Sie das Feld **Filtern**.

   ANMERKUNG: Sie können die folgenden Informationen auf der Seite **Baseline Compliance** anzeigen:
   - Gesamtzahl der nicht konformen Hosts
   - Gesamtzahl der nicht konformen Cluster
   - Gesamtzahl der Hosts und Cluster, die zur Baseline gehören
   - Gesamtzahl der Host-Verteilungen, die zum Abweichungstyp gehören
2. Nach erfolgreichem Ausführen eines Abweichungserkennungsjobs werden die Hosts in der Tabelle angezeigt, die zur Baseline gehören. Wählen Sie den gewünschten Host aus und klicken Sie auf **Abweichungsdetails anzeigen**, um die Abweichungsdetails anzuzeigen. Das Dialogfeld **Abweichungsdetails** wird angezeigt.
3. Im Dialogfeld **Abweichungsdetails** können Sie Folgendes anzeigen:
   - Wenn der Konformitäts-Abweichungserkennungsjob fehlschlägt, wird der Übereinstimmungsstatus als „nicht konform“ zusammen mit der Ursache für den Ausfall angezeigt. Verwenden Sie den angegebenen Grund, um das Problem zu lösen.
   - Wenn der Abweichungserkennungsjob erfolgreich war, wird der Übereinstimmungsstatus als „nicht konform“ angezeigt und es werden die folgenden Details auf der Seite **Abweichungsdetails** angezeigt:

     Für Hardware:
     - Instanz: zeigt den Hardware-Komponentennamen an.
     - Gruppe: zeigt den Gruppennamen der Attribute an.

- Attributname: zeigt den Attributnamen an.
- Aktueller Wert: zeigt den Host-Wert an.
- Baseline-Wert: zeigt den Wert der Baseline an.
- Abweichungstyp: zeigt den Grund für die Nichtkonformität an. Weitere Informationen zum Abweichungstyp finden Sie unter Vergleich von Komponenten- und Baseline-Version - Matrix auf Seite 167.

Für Firmware und Treiber:

- Komponentenname: zeigt den Namen der Komponente an.
- Aktueller Wert: zeigt den Host-Wert an.
- Baseline-Wert: zeigt den Wert der Baseline an.
- Abweichungstyp: zeigt den Grund für die Nichtkonformität an. Weitere Informationen zum Abweichungstyp finden Sie unter Vergleich von Komponenten- und Baseline-Version - Matrix auf Seite 167.
- Dringlichkeit (bei Firmware): zeigt die Prioritätsstufe für die Aktualisierung der Version einer identifizierten Komponente an.
- Empfehlung (bei Treiber): zeigt die Prioritätsstufe für die Aktualisierung der Version einer identifizierten Komponente an.
- Neustart erforderlich: zeigt an, ob ein Neustart des Geräts erforderlich ist oder nicht.

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

4. Klicken Sie auf **Fertigstellen**.

Verwenden von OMSA mit Servern der 11. Generation

Bei der Verwaltung von Power Edge-Servern der 11. Generation macht OMIVV es erforderlich, dass OMSA auf ihnen ausgeführt wird. Bei Hosts der 11. Generation, die über OMIVV bereitgestellt werden, wird OMSA automatisch installiert. Für Hosts der 11. Generation, die Sie manuell bereitstellen, können Sie eine der folgenden Optionen wählen:

- Installieren und konfigurieren von OMSA unter Verwendung von OMIVV. Informationen dazu finden Sie unter OMSA-Trap-Ziel einrichten auf Seite 135.
- Manuelle Installation und Konfiguration von OMSA. Informationen dazu finden Sie unter Bereitstellen von OMSA-Agent auf dem ESXi-System auf Seite 134.

ANMERKUNG: Bei Bereitstellung des OMSA-Agenten mit OMIVV startet OMIVV den HTTP-Client-Dienst, aktiviert den Port 8080 und gibt ihn ESXi 5.0 frei, um OMSA VIB herunterzuladen und zu installieren. Nach Abschluss der OMSA VIB-Installation wird der Dienst automatisch angehalten und der Port geschlossen.

ANMERKUNG: Abgesehen von den oben genannten Optionen können Sie die Web-Client-Host-Konformität verwenden. Auf diese Weise wird der OMSA-Agenten installiert und konfiguriert.

Bereitstellen von OMSA-Agent auf dem ESXi-System

Installieren Sie den OMSA VIB auf einem ESXi-System, um eine Bestandsliste und Alarminformationen von den Systemen zu erstellen.

ANMERKUNG: OpenManage-Agenten sind auf Dell Hosts vor den Dell PowerEdge-Servern der 12. Generation erforderlich. Installieren Sie OMSA unter Verwendung von OpenManage Integration for VMware vCenter oder installieren Sie es manuell auf den Hosts, bevor Sie OpenManage Integration for VMware vCenter installieren. Details über die manuelle Installation der OMSA-Agenten finden Sie unter http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx

1. Falls OMSA noch nicht installiert ist, installieren Sie das vSphere-Befehlszeilentool (vSphere CLI) von **www.vmware.com**.
2. Geben Sie folgenden Befehl ein:

```
Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
```

ANMERKUNG: Die Installation von OMSA kann einige Minuten dauern. Dieser Befehl erfordert nach Durchlauf einen Neustart des Hosts.

ANMERKUNG: Die SNMP-Communityzeichenfolge kann in **Verwalten** > **Einstellungen** > **Geräteeinstellungen** > **OMSA SNMP Trap-Communityzeichenfolge** konfiguriert werden. Weitere Informationen zur SNMP Trap-Communityzeichenfolge finden Sie unter Konfigurieren einer SNMP Trap-Communityzeichenfolge.

OMSA-Trap-Ziel einrichten

Auf allen Servern der 11. Generation von Hosts muss OMSA konfiguriert sein.

ANMERKUNG: OMSA ist nur auf Dell EMC Servern vor PowerEdge-Servern der 12. Generation erforderlich.

So richten Sie ein OMSA-Trap-Ziel ein:

1. Navigieren Sie zum OMSA-Agent von einem Webbrowser durch die Bereitstellung der URL `https://<HostIP>:1311/`.
2. Melden Sie sich an, und wählen Sie die Registerkarte **Alarmverwaltung**.
3. Wählen Sie **Alarm-Aktionen**, und stellen Sie sicher, dass die Option **Broadcast-Nachricht** für alle zu überwachenden Ereignisse gesetzt ist, sodass die Ereignisse gesendet werden.
4. Wählen Sie oben auf der Registerkarte die Option **Plattform-Ereignisse**.
5. Klicken Sie auf die graue Schaltfläche **Ziele konfigurieren** und dann auf den Link **Ziel**.
6. Aktivieren Sie das Kontrollkästchen **Ziel aktivieren**.
7. Geben Sie die OMIVV-Geräte-IP-Adresse in das Feld **Ziel-IP-Adresse** ein.
8. Klicken Sie auf **Apply Changes** (Änderungen anwenden).
9. Wiederholen Sie die Schritte 1 bis 8, um zusätzliche Ereignisse zu konfigurieren.

   ANMERKUNG: Die SNMP-Communityzeichenfolge kann in **Verwalten** > **Einstellungen** > **Geräteeinstellungen** > **OMSA SNMP Trap-Communityzeichenfolge** konfiguriert werden. Weitere Informationen zur SNMP Trap-Communityzeichenfolge finden Sie unter Konfigurieren einer SNMP Trap-Communityzeichenfolge.

Berichterstattung und Korrektur der Konformität von Bare-Metal-Servern

Ein Bare-Metal-Server ist nicht kompatibel wenn:

- Er kein unterstützter Server ist.
- Er nicht über eine unterstützte iDRAC-Lizenz verfügt (iDRAC Express ist die Mindestanforderung).
- Er über keine unterstützten Mindestversionen von iDRAC, BIOS oder LC verfügt.
- LOM oder rNDC nicht vorhanden ist.
- Der Systemsperrmodus ist eingeschaltet.

Anzeigen und Korrigieren der Liste von nicht konformen Bare-Metal-Servern:

1. Wählen Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Verwalten** > **Bereitstellung**.
   a. Zeigen Sie auf der Seite **Bare-Metal-Server** die Liste der Server an, die nicht konform sind.

      Eine Tabelle wird angezeigt, die die nicht konformen Server zusammen mit Service-Tag-Nummer, Modell, iDRAC-IP, Server-Status, Konformitätsstatus und iDRAC-Lizenz-Status auflistet.
   b. Um weitere Details zu einem Server, der nicht kompatibel ist, anzuzeigen, wählen Sie einen Server der nicht kompatibel ist.
   c. Klicken Sie zum Exportieren von nicht konformen Informationen eines Servers auf eine CSV-Datei in der rechten unteren Ecke der Tabelle auf  .
   d. Um die Inhalte der Datentabelle zu filtern, klicken Sie auf das Feld **Filtern**.
   e. Um die Spalten innerhalb der Tabelle zu vertauschen, tun Sie dies per Drag-and-Drop innerhalb der Datentabelle.
2. Zum Korrigieren nicht konformer Server klicken Sie auf **Nicht-konforme Server korrigieren** .

   ANMERKUNG: Der Link **Nicht-konforme Server reparieren** ist nur für nicht-konforme Server der 11. Generation aktiviert.
3. Klicken Sie im Assistenten **Bare-Metal-Konformität korrigieren** auf **Weiter** auf der Seite **Willkommen**.
4. Aktivieren Sie auf der Seite **Konformität korrigieren** die Kontrollkästchen der Server, die Sie korrigieren möchten.

   Die nicht konformen Server werden aufgelistet und die Firmware Komponente, mit der sie nicht kompatibel sind, wird angezeigt. Die aufgeführten nicht-konformen Server erfordern mindestens eine der folgenden Firmware-Komponenten:
   - **iDRAC-IP**

     ANMERKUNG: Sie können über OMIVV keine Bare-Metal-Server-Probleme beheben, wenn die iDRAC-Lizenzen dort sind nicht kompatibel sind. Stellen Sie sicher, dass Sie die unterstützte iDRAC-Lizenz auf diese Server außerhalb OMIVV hochladen und anschließend auf **Bare-Metal-Server aktualisieren** klicken. SieheAktualisieren von Bare-Metal-Servern auf Seite 136.

- **BIOS**
- **LC**
- **Systemsperrmodus**

  ANMERKUNG: Um aktuelle Informationen zu nicht-konformen Bare-Metal-Servern aus dem entsprechenden iDRAC abzurufen, klicken Sie auf **Bare-Metal-Details aktualisieren**. Wenn der Systemsperrmodus eingeschaltet ist, ist der Server nicht-konform, und umgekehrt.

5. Um Details zu Konformitätsproblemen einzusehen, klicken Sie auf **Konformitätsprobleme**.

   ANMERKUNG: Wenn ein Bare-Metal-Server aufgrund eines aktivierten Systemsperrmodus nicht konform ist, müssen Sie den Systemsperrmodus des Servers manuell über die iDRAC-Konsole konfigurieren.

6. Klicken Sie auf **Weiter**.
7. Prüfen Sie die Maßnahmen, die an den Firmwarekomponenten von nicht konformen Bare-Metal-Servern durchgeführt werden, im Fenster **Zusammenfassung**.
8. Klicken Sie auf **Fertigstellen**.

Reparatur der iDRAC-Lizenzkonformität für Bare-Metal-Server

Die Bare-Metal -Server, die auf Seite **Bare-Metal-Server** aufgeführt sind, sind nicht konform, da sie keine kompatible iDRAC-Lizenz aufweisen. Eine Tabelle zeigt den Status der iDRAC-Lizenz an. Sie können auf einen nicht konformen Bare-Metal-Server klicken, um weitere Details anzuzeigen, wie z. B. wie viele Tage der Laufzeit der iDRAC-Lizenz noch übrig sind. Dann können Sie sie nach Bedarf aktualisieren. Wenn der Link **Bare-Metal-Server aktualisieren** auf Seite **Bare-Metal-Server** aktiviert ist, gibt es Bare-Metal-Server, die aufgrund der iDRAC-Lizenz nicht konform sind.

1. Wählen Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Verwalten** > **Bereitstellung**. Auf der Seite **Bare-Metal-Server** können Sie die Liste der nicht konformen Server in einer Tabelle anzeigen.
2. Wählen Sie einen Bare-Metal-Server mit dem **iDRAC-Lizenz Status nicht konform** oder **unbekannt**.
3. Wenn die Lizenz abgelaufen ist, klicken Sie auf **iDRAC-Lizenz erwerben/erneuern**.
4. Melden Sie sich bei der Seite **Dell License Management** an, und aktualisieren oder erwerben Sie eine neue iDRAC-Lizenz. Verwenden Sie die Informationen auf dieser Seite, um Ihren iDRAC zu identifizieren und zu aktualisieren.
5. Nachdem Sie eine iDRAC-Lizenz installiert haben, klicken Sie auf **Bare-Metal-Server aktualisieren**.

Aktualisieren von Bare-Metal-Servern

1. Klicken Sie auf der Seite **OpenManage Integration for VMware vCenter** auf **Verwalten** > **Bereitstellung** > **Bare-Metal-Server**, und klicken Sie dann auf **Bare-Metal-Server aktualisieren**.
2. Wählen Sie im Fenster **Bare-Metal-Server aktualisieren** die Server aus, deren Daten Sie aktualisieren möchten, und klicken Sie dann auf **Ausgewählte Server aktualisieren**.

Die Aktualisierung von Bare-Metal-Server-Daten dauert u. U. einige Minuten.

Alle ausgewählten Bare-Metal-Server-Daten werden auf der Seite **Bare-Metal-Server** aktualisiert.

15

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. Enthält Rollen, operative Dell Rolle und Dell Infrastrukturbereitstellungsrolle.

Themen:

Datenintegrität

Die Kommunikation zwischen OpenManage-Integration for VMware vCenter, der Verwaltungskonsole und vCenter erfolgt über SSL/HTTPS. Das OpenManage-Integration for VMware vCenter generiert ein SSL-Zertifikat für die vertrauenswürdige Kommunikation zwischen vCenter und dem Gerät. Weiterhin wird das Serverzertifikat des vCenters vor der Kommunikation und der Registrierung des OpenManage Integration for VMware vCenter überprüft und ob es vertrauenswürdig ist. Die Konsolen-Registerkarte von OpenManage Integration for VMware vCenter verwendet Sicherheitsvorgänge zum Verhindern von inkorrekten Anfragen, während die Schlüssel zwischen der Verwaltungskonsole und dem Back-End-Service übertragen werden. Diese Art der Sicherheit führt dazu, dass Cross Site Request Forgeries (CSRF) fehlschlagen.

Eine sichere Verwaltungskonsolensitzung hat ein Leerlauf-Zeitlimit von fünf Minuten, und die Sitzung ist nur im aktuellen Browser-Fenster und/oder -Register gültig. Wenn Sie versuchen, die Sitzung in einem neuen Fenster oder Register zu öffnen, wird ein Sicherheitsfehler vorgegeben, der eine gültige Sitzung anfordert. Durch diese Aktion wird auch verhindert, dass der Benutzer auf eine schädliche URL klickt, die die Verwaltungskonsolensitzung angreifen könnte.

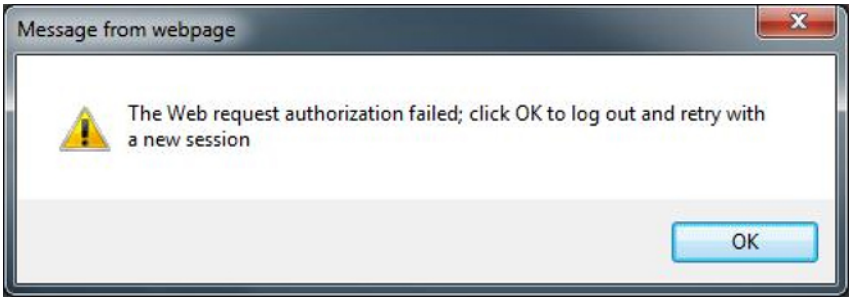

Abbildung 3. Sicherheitsfehlermeldung

Zugangskontrollauthentifizierung, -autorisierung und -rollen

Um vCenter-Abläufe durchzuführen, verwendet OpenManage Integration for VMware vCenter die aktuelle Benutzersitzung des Web-Client und die gespeicherten Administrations-Anmeldeinformationen für die OpenManage Integration. Das OpenManage Integration

for VMware vCenter nutzt die integrierten Rollen und das Berechtigungsmodell des vCenter-Servers, um Benutzeraktionen mit der OpenManage Integration und den verwalteten vCenter-Objekten (Hosts und Clusters) 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 39. Berechtigungsgruppen

Gruppenname	Beschreibung
Berechtigungsgruppe – Dell.Konfiguration	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.Bestandsaufnahme	Konfigurieren der Bestandsaufnahme, Konfigurieren des Serviceabrufs, Konfigurieren von ReadOnly
Berechtigungsgruppe – Dell.Überwachung	Konfigurieren der Überwachung, Überwachung
Berechtigungsgruppe – Dell.Berichterstellung (nicht verwendet)	Erstellen eines Berichts, Ausführen eines Berichts

Dell-Infrastrukturbereitstellungsrolle

Diese Rolle umfasst die Berechtigungen, die mit den Hypervisor-Bereitstellungsfunktionen verknüpft sind.

Die von dieser Rolle gewährten Berechtigungen sind Erstellen von Vorlagen, Konfigurieren des HW-Konfigurationsprofils, Konfigurieren des Hypervisor-Bereitstellungsprofils, Konfigurieren des Verbindungsprofils, Zuweisen einer Identität und Bereitstellen.

Berechtigungsgruppe – Dell.Bereitstellung - Provisionierung

Erstellen von Vorlagen, Konfigurieren des HW-Konfigurationsprofils, Konfigurieren des Hypervisor-Bereitstellungsprofils, Konfigurieren des Verbindungsprofils, Zuweisen einer Identität, Bereitstellen

Informationen zu Berechtigungen

Jede vom OpenManage Integration for VMware vCenter ausgeführte Aktion ist einer Berechtigung zugeordnet. In den folgenden Abschnitten werden die verfügbaren Aktionen und die zugeordneten Berechtigungen aufgeführt:

- Dell.Konfiguration.Ausführen von mit vCenter verknüpften Aufgaben
  - Beenden und Starten des Wartungsmodus
  - Aufrufen der vCenter-Benutzergruppe zur Abfrage von Berechtigungen
  - Registrieren und Konfigurieren von Warnungen, z. B. Aktivieren/Deaktivieren von Warnungen 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.Bestandsaufnahme.Konfigurieren von 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.Überwachung.Überwachen
  - 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.Konfiguration.Firmware-Aktualisierung
  - 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.Bereitstellung-Bereitstellen.Erstellen von Vorlagen
  - HW-Konfigurationsprofil konfigurieren
  - Hypervisor-Bereitstellungsprofil konfigurieren
  - Verbindungsprofil konfigurieren
  - Identität zuweisen
  - Bereitstellen
- Dell.Konfiguration.Ausführen von mit Hosts verknüpften Tasks
  - Blink-LED, Lösch-LED, Konfigurieren der OMSA-URL von der Registerkarte zur Dell-Serververwaltung
  - Starten der OMSA-Konsole
  - Starten der iDRAC-Konsole
  - Anzeigen und Löschen des SEL-Protokolls
- Dell.Bestandsaufnahme.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

16

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 158

Themen:

Häufig gestellte Fragen – FAQs

In diesem Abschnitt werden einige allgemeine Fragen und Lösungen beschrieben.

Die Schaltfläche „Alle exportieren“ exportiert nicht in eine .CSV-Datei in Google Chrome.

Nach dem Registrieren eines vCenter Servers gibt die Schaltfläche **Alle exportieren** einen Fehler aus, wenn Sie einen Host hinzufügen, ein Verbindungsprofil erstellen und dann die Bestandsaufnahmedetails anzeigen. Die Schaltfläche **Alle exportieren** exportiert die Informationen nicht in eine .CSV-Datei.

ANMERKUNG:

In allen Versionen des Google Chrome Browsers exportiert die Schaltfläche **Alle exportieren** im **Inkognito-Modus** die Informationen nicht in eine .CSV-Datei.

Lösung: Zum Exportieren der Informationen in eine .CSV-Datei mit der Schaltfläche **Alle exportieren** in Google Chrome deaktivieren Sie den **Inkognito-Modus** im Chrome Browser.

Betroffene Version: 4.0

Lizenztyp und Beschreibung von iDRAC werden für nicht kompatible vSphere-Hosts falsch angezeigt

Wenn ein Host bei Deaktivierung von CSIOR nicht kompatibel ist oder nicht ausgeführt wurde, werden die Informationen zur iDRAC-Lizenz falsch angezeigt, auch wenn eine gültigen iDRAC-Lizenz verfügbar ist. Der Host wird also in der Liste der vSphere Hosts angezeigt, wenn Sie jedoch auf den Host klicken, um Details anzuzeigen, werden in **iDRAC Lizenztyp** keine Informationen angezeigt und in **iDRAC-Lizenz Beschreibung** wird „Ihre Lizenz muss aktualisiert werden“ ausgegeben.

Lösung: Um dieses Problem zu beheben, aktivieren Sie CSIOR auf einem Referenzserver.

Betroffene Version: 4.0

Das Dell EMC Symbol wird nicht angezeigt, nachdem Sie die Registrierung einer früheren OMIVV-Version mit vCenter aufheben

und anschließend eine höhere OMIVV-Version im gleichen vCenter registrieren.

Wenn Sie die Registrierung einer früheren OMIVV-Version mit vCenter Server aufheben und anschließend eine höhere OMIVV-Version im gleichen vCenter Server registrieren, verbleibt ein Eintrag aus der früheren OMIVV-Version im Serenity-Ordner des Vsphere-Clients. Das Dell Symbol nach der Anmeldung bei der neueren OMIVV-Version wird nicht angezeigt, weil alte Daten, die für die frühere OMIVV Version spezifisch sind, im Serenity-Ordner des Vsphere Geräts vorhanden sind.

Antwort: Führen Sie folgende Schritte aus:

1. Um zu VMware vCenter zu gelangen, gehen Sie zu `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity` und um zu Windows vCenter zu gelangen, gehen Sie in den Ordner `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` im vCenter Gerät und prüfen Sie, ob alten Daten vorhanden sind, wie beispielsweise:
   - com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-3.0.0.197
2. Löschen Sie den Ordner für die frühere OMIVV-Version manuell.
3. Starten Sie den vSphere Web-Client-Service auf dem vCenter Server erneut.

Betroffene Versionen: Alle

Dell Anbieter wird nicht als Anbieter für Funktionszustandaktualisierung angezeigt

Wenn Sie einen vCenter Server mit OMIVV registrieren und die vCenter Server-Version anschließend aktualisieren, beispielsweise von vCenter 6.0 auf vCenter 6.5, wird der Dell Anbieter nicht in der Liste **Anieter Proactive HA** angezeigt.

Lösung: Sie können ein registriertes vCenter für Benutzer aktualisieren, die keine Administratoren oder Administratoren sind. Lesen Sie die Informationen zur Aktualisierung auf die neueste Version des vCenter Servers in der VMware-Dokumentation, und führen Sie dann eine der folgenden Optionen aus, sofern zutreffend:

- Für Nicht-Administratorbenutzer:
  1. Weisen Sie Benutzern, die keine Administratoren sind, bei Bedarf zusätzliche Berechtigungen zu. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für Nicht-Administrator-Benutzer auf Seite 12.
  2. Führen Sie einen Neustart des registrierten OMIVV-Geräts durch.
  3. Melden Sie sich vom Web-Client ab, und melden Sie sich dann erneut an.
- Für Administratorbenutzer:
  1. Führen Sie einen Neustart des registrierten OMIVV-Geräts durch.
  2. Melden Sie sich vom Web-Client ab, und melden Sie sich dann erneut an.

Der Dell Anbieter wird nun in der Liste der **Anieter Proactive HA** aufgeführt.

Betroffene Version: 4.0

Bestandsaufnahme schlägt bei der Durchführung von Firmware-Aktualisierungsaufgabe auf ESXi 5.x Host fehl.

Wenn Sie nach dem Registrieren eines vCenter Servers eine Firmware-Aktualisierungsaufgabe auf einem ESXi 5.x Host ausführen und iDRAC als Komponente im Bildschirm **Komponente auswählen** wählen, wird ESXi auf dem Host möglicherweise nicht mit der neuen iDRAC IP-Adresse synchronisiert, wodurch OMIVV eine ungültige iDRAC IP zur Verfügung gestellt wird. Deshalb können Sie auf diesem Host keine erfolgreiche Bestandsaufnahme durchführen.

Lösung: Starten Sie zur Behebung dieses Problems den „sfcdb daemon“ auf den ESXi Host: Weitere Informationen finden Sie unter https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2077693.

Betroffene Version: 4.0

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 Verbindungsprofil erstellen auf Seite 50.

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 „Unknown“ angezeigt. Der unbekannte 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 der vCenter Berechtigungenliste hinzugefügt. Sobald Sie die Registrierung von vCenter auf dem OMIVV-Gerät aufheben, werden die Berechtigungen von Dell nicht entfernt.

ANMERKUNG: Obwohl die Berechtigungen von Dell nicht entfernt werden, entstehen keine Auswirkungen auf OMIVVVorgänge.

Betroffene Version: 3.1

Das OMIVV zeigt beim Versuch, eine Schweregrad-Kategorie zu filtern, nicht alle entsprechenden Protokolle an

Wenn Sie eine Schweregrad-Kategorie zum Filtern der Protokolldaten durch Auswahl von **Alle Kategorien** in der Dropdown-Liste auswählen, werden alle Protokolle einer bestimmten Kategorie genau angezeigt. Wenn Sie jedoch durch Auswahl von **Info** in der Dropdown-Liste filtern, werden die Firmware-Aktualisierungsprotokolle nicht angezeigt und nur die Aufgabeninitiierungsprotokolle werden angezeigt.

Lösung: Zur Anzeige aller Protokolle wählen Sie im OMIVV **Alle Kategorien** aus der Dropdown-Liste für das Filtern.

Betroffene Version: 3.1

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 erhalten Sie unter http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 und http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689.

Aktualisieren der SSL-Anker in Windows vSphere 6.0

1. Laden Sie die Datei „lstoolutil.py.zip“ von http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 herunter.
2. Kopieren Sie die Datei lstoolutil.py in den Ordner `%VMWARE_CIS_HOME%"\VMware Identity Services\lstool\scripts\.`

   ANMERKUNG: Ersetzen Sie nicht die Datei lstoolutil.py, wenn Sie vSphere 6.0 Update 1 verwenden.

Sie können die folgenden einschlägigen Verfahren zum Aktualisieren der SSL-Anker verwenden:

- Aktualisieren der SSL-Anker für eine vCenter Installation unter dem Betriebssystem Windows: Ersetzen Sie die Zertifikate der vCenter Windows Installation mithilfe der Utility vSphere Certificate Manager. Informationen dazu finden Sie unter Ersetzen der Zertifikate einer vCenter Windows Installation auf Seite 143.
- Aktualisieren der SSL-Anker für eine vCenter Installation auf einem Server-Gerät: Ersetzen Sie die Zertifikate des vCenter Server-Geräts mithilfe des Dienstprogramms vSphere Certificate Manager. Informationen dazu finden Sie unter Ersetzen der Zertifikate auf dem vCenter Server-Gerät auf Seite 144.

Die durch die genannten Verfahren erhaltene Ausgabe sollte entsprechend `Updated 24 service (s)` bzw. `Updated 26 service (s)` anzeigen. Wenn die angezeigte Ausgabe `Updated 0 service (s)` ist, ist der alte Zertifikat-Fingerabdruck falsch. Sie können die folgenden Schritte ausführen, um den alten Zertifikat-Fingerabdruck abzurufen. Außerdem können Sie das folgende Verfahren zum Abrufen des alten Zertifikat-Fingerabdrucks verwenden, wenn **vCenter Certificate Manager** nicht zum Ersetzen der Zertifikat eingesetzt wird:

ANMERKUNG: Führen Sie die Datei `ls_update_certs.py` mit dem abgerufenen alten Fingerabdruck aus.

1. Rufen Sie das alte Zertifikat aus dem Managed Object Browser (MOB) ab. Informationen dazu finden Sie unter Abrufen des alten Zertifikats aus dem Managed Object Browser – MOB auf Seite 144.
2. Extrahieren Sie den Fingerabdruck vom alten Zertifikat. Informationen dazu finden Sie unter Extrahieren des Fingerabdrucks vom alten Zertifikat auf Seite 145.

Betroffene Version: 3.0 und höher, vCenter 6.0 und höher

Ersetzen der Zertifikate einer vCenter Windows Installation

Führen Sie die folgenden Schritte aus, wenn das Dienstprogramm vSphere Certificate Manager verwendet wird, um die Zertifikate einer vCenter Windows Installation zu ersetzen:

1. Stellen Sie eine Verbindung zum externen Plattform Services Controller über eine Remote-Desktop-Verbindung her.
2. Öffnen Sie die Eingabeaufforderung im Administratormodus.
3. Erstellen Sie den Ordner `c: \Certificates` mit dem folgenden Befehl: `mkdir c: \Certificates`
4. Rufen Sie das alte Zertifikat mithilfe des folgenden Befehls ab: `"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output c:\certificates\old_machine.crt`
5. Rufen Sie den Fingerabdruck des alten Zertifikats mithilfe des folgenden Befehls ab: `"%VMWARE_OPENSSL_BIN%" x509 -in C:\certificates\old_machine.crt -noout -sha1 -fingerprint`

   ANMERKUNG: Der abgerufene Zertifikat-Fingerabdruck ist in folgendem Format: `SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

Den Fingerabdruck ist eine Folge von Zahlen und Buchstaben, die wie folgt angezeigt wird:
`13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

6. Rufen Sie das neue Zertifikat mithilfe des folgenden Befehls ab: `"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output c:\certificates\new_machine.crt`
7. Führen Sie folgende Schritte durch:
   a. Führen Sie `ls_update_certs.py` mithilfe des folgenden Befehls aus: `"%VMWARE _PYTHON_BIN%" ls_update_certs.py --url`
   b. Ersetzen Sie "psc.vmware.com" durch "Lookup_Service_FQDN_of_Platform_Services_Controller" und den Fingerabdruck 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 mit dem Fingerabdruck aus Schritt 5 mithilfe des folgenden Befehls: `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile c:\certificates\new_machine.crt --user Administrator@vsphere.local --password Password`

   ANMERKUNG: Stellen Sie sicher, dass Sie gültige Anmeldeinformationen angeben.

8. Melden Sie sich ab und melden Sie sich am vCenter Web Client an, nachdem alle Dienste erfolgreich aktualisiert wurden.

OMIVV wird jetzt erfolgreich gestartet.

Ersetzen der Zertifikate auf dem vCenter Server-Gerät

Führen Sie die folgenden Schritte durch, wenn das Dienstprogramm vSphere Certificate Manager verwendet wird, um die Zertifikate eines vCenter Server-Geräts zu ersetzen:

1. Melden Sie sich am externen Plattform Services Controller-Gerät über die Konsole oder eine Secure-Shell-(SSH-)Sitzung an.
2. Führen Sie den folgenden Befehl zur Aktivierung des Zugriffs auf die Bash-Shell aus: `shell.set --enabled true`
3. Geben Sie **`shell`** ein, und drücken Sie die **Eingabetaste**.
4. Erstellen Sie Ordner oder Zertifikate mithilfe des folgenden Befehls: `mkdir /certificates`
5. Rufen Sie das alte Zertifikat mithilfe des folgenden Befehls ab: `/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output /certificates/old_machine.crt`
6. Rufen Sie den Fingerabdruck des alten Zertifikats mithilfe des folgenden Befehls ab: `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

   ANMERKUNG: Der abgerufene Zertifikat-Fingerabdruck ist in folgendem Format: `SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

   Der Fingerabdruck ist eine Folge von Zahlen und Buchstaben, die wie folgt angezeigt wird:
   `13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

7. Rufen Sie das neue Zertifikat mithilfe des folgenden Befehls ab: `/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output /certificates/new_machine.crt`
8. Führen Sie den folgenden Befehl aus, um das Verzeichnis zu ändern: `cd /usr/lib/vmidentity/tools/scripts/`
9. Führen Sie folgende Schritte durch:
   a. Führen Sie `ls_update_certs.py` mithilfe des folgenden Befehls aus: `python ls_update_certs.py --url`
   b. Ersetzen Sie "psc.vmware.com" durch "Lookup_Service_FQDN_of_Platform_Services_Controller" und den Fingerabdruck 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 mit dem Fingerabdruck aus Schritt 6 mithilfe des folgenden Befehls: `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile /certificates/new_machine.crt --user Administrator@vsphere.local --password "Password"`

   ANMERKUNG: Stellen Sie sicher, dass Sie gültige Anmeldeinformationen angeben.

10. Melden Sie sich ab und melden Sie sich am vCenter Web Client an, nachdem alle Dienste erfolgreich aktualisiert wurden.

OMIVV wird jetzt erfolgreich gestartet.

Abrufen des alten Zertifikats aus dem Managed Object Browser – MOB

Sie können das alte Zertifikat für das vCenter Server-System durch eine Verbindung mit dem Plattform Service Controller (PSC) unter Verwendung des Managed Object Browser (MOB) abrufen.

Um das alte Zertifikat abzurufen, müssen Sie das Feld „sslTrust“ im verwalteten Objekt ArrayOfLookupServiceRegistrationInfo finden, indem Sie die folgenden Schritte ausführen:

ANMERKUNG: In diesem Handbuch wird der Ordner `C: \Certificates\` zum Speichern aller Zertifikate verwendet.

1. Erstellen Sie den Ordner `C: \Certificates` auf dem PSC mit dem folgenden Befehl: `mkdir C:\certificates\`.
2. Öffnen Sie den folgenden Link in einem Browser: `https://<vCenter FQDN|IP address>/lookupservice/mob?moid=ServiceRegistration&method=List`
3. Melden Sie sich mit dem Benutzernamen `administrator@vsphere.local` an und geben Sie das Passwort ein, wenn Sie dazu aufgefordert werden.

   ANMERKUNG: Wenn Sie einen benutzerdefinierten Namen für die vCenter Single-Sign-On-(SSO-)Domain verwenden, geben Sie diesen Benutzernamen und das Kennwort ein.

4. Ändern Sie unter **filterCriteria** das Wertefeld so, dass nur die Tags **<filtercriteria></filtercriteria>** angezeigt werden und klicken Sie auf **Methode aufrufen**.
5. Suchen Sie nach dem folgenden Hostnamen je nachdem, welche Zertifikate Sie ersetzen wollen:

Tabelle 40. Suchkriterien-Informationen

Trust-Anker	Suchkriterien
vCenter Server	Drücken Sie Strg+F zum Suchen von "vc_hostname_or_IP.example.com" auf der Seite
Plattform Services Controller	Drücken Sie Strg+F zum Suchen von "psc_hostname_or_IP.example.com" auf der Seite

6. Suchen Sie nach dem Wert des entsprechenden sslTrust-Felds. Der Wert des sslTrust-Felds ist eine Base64-kodierte Zeichenfolge des alten Zertifikats.
7. Verwenden Sie die folgenden Beispiele beim Aktualisieren des Plattform Services Controller oder der Trust-Anker des vCenter Servers.

   ANMERKUNG: Die tatsächliche Zeichenkette ist zur besseren Lesbarkeit deutlich verkürzt.

   - Für vCenter Server

Tabelle 41. Beispiel für vCenter Server

Name	Typ	Value
URL	anyURI	https://vcenter.vmware.local:443/sdk

   - Für Plattform Services Controller

Tabelle 42. Beispiel für Plattform Services Controller z. B.

Name	Typ	Value
URL	anyURI	https://psc.vmware.local/sts/STSService/vsphere.local

8. Kopieren Sie den Inhalt des Felds „sslTrust“ in ein Textdokument und speichern Sie das Dokument als `old_machine.txt`.
9. Öffnen Sie die Datei `old_machine.txt` in einem Texteditor.
10. Fügen Sie Folgendes jeweils am Anfang und Ende der Datei `old_machine.txt` ein:

    ```
    -----BEGIN CERTIFICATE-----
    -----END CERTIFICATE-----
    ```

11. Speichern Sie `old_machine.txt` jetzt als `old_machine.crt`.

Sie können nun den Fingerabdruck dieses Zertifikats extrahieren.

Extrahieren des Fingerabdrucks vom alten Zertifikat

Sie können den Fingerabdruck des alten Zertifikats extrahieren und in das Fenster „Plattform Services“ mithilfe der folgenden Optionen laden:

- Extrahieren Sie den Fingerabdruck mit dem Hilfsprogramm zur Zertifikatsanzeige. Lesen Sie dazu Extrahieren des Zertifikat-Fingerabdrucks mit dem Hilfsprogramm zur Anzeige von Zertifikaten auf Seite 146.
- Extrahieren Sie den Fingerabdruck unter Verwendung einer Befehlszeile auf dem Gerät. Lesen Sie dazu Extrahieren des Fingerabdrucks unter Verwendung der Befehlszeile auf Seite 146.

Extrahieren des Zertifikat-Fingerabdrucks mit dem Hilfsprogramm zur Anzeige von Zertifikaten

Führen Sie folgende Schritte durch, um den Zertifikat-Fingerabdruck zu entpacken:

1. Doppelklicken Sie in Windows auf die Datei `old_machine.txt`, um sie in der Zertifikatsanzeige von Windows zu öffnen.
2. Wählen Sie in der Zertifikatsanzeige von Windows das Feld **SHA1-Fingerabdruck**.
3. Kopieren Sie die Fingerabdruck-Zeichenkette in einen Texteditor und ersetzen Sie die Leerzeichen durch einen Doppelpunkt oder entfernen Sie die Leerzeichen aus der Zeichenkette.
   Zum Beispiel kann die Fingerabdruck-Zeichenkette als eine der folgenden Möglichkeiten angezeigt werden:
   - ea87e150bb96fbbe1fa95a3c1d75b48c30db7971
   - ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

Extrahieren des Fingerabdrucks unter Verwendung der Befehlszeile

Sie finden in den folgenden Abschnitten eine Beschreibung zum Extrahieren des Fingerabdrucks unter Verwendung der Befehlszeile auf dem Gerät und der Windows Installation.

Extrahieren des Fingerabdrucks unter Verwendung der Befehlszeile auf dem vCenter Server-Gerät

Führen Sie folgende Schritte durch:

1. Verschieben oder laden Sie das Zertifikat „old_machine.crt“ in den PSC am Speicherort `C:\certificates\old_machine.crt`, der in Schritt 1 des Verfahrens zum Abrufen des alten Zertifikats erstellt wurde. Sie können Windows Secure Copy (WinSCP) oder einen anderen SCP-Client zum Verschieben oder Hochladen des Zertifikats verwenden.
2. Melden Sie sich am externen Plattform Services Controller Gerät über Secure Shell (SSH) an.
3. Führen Sie den folgenden Befehl zur Aktivierung des Zugriffs auf die Bash-Shell aus: `shell.set --enabled true`.
4. Geben Sie `shell` ein, und drücken Sie die **Eingabetaste**.
5. Führen Sie den folgenden Befehl aus, um den Fingerabdruck zu extrahieren: `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

ANMERKUNG: Der Fingerabdruck wird als Sequenz von Zahlen und Buchstaben nach dem Gleichheitszeichen angezeigt und lautet wie folgt: `SHA1 Fingerprint= ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71`

Extrahieren des Fingerabdrucks unter Verwendung der Befehlszeile der Windows Installation

Führen Sie folgende Schritte durch:

1. Verschieben oder laden Sie das Zertifikat „old_machine.crt“ in den PSC am Speicherort `C:\certificates\old_machine.crt`, der in Schritt 1 des Verfahrens zum Abrufen des alten Zertifikats erstellt wurde. Sie können Windows Secure Copy (WinSCP) oder einen anderen SCP-Client zum Verschieben oder Hochladen des Zertifikats verwenden.
2. Stellen Sie eine Verbindung zum externen Plattform Services Controller über eine Remote-Desktop-Verbindung her.
3. Öffnen Sie die Eingabeaufforderung im Administratormodus.
4. Führen Sie den folgenden Befehl aus, um den Fingerabdruck zu extrahieren: `"%VMWARE_OPENSSL_BIN%" x509 -in c:\certificates\old_machine.crt -noout -sha1 -fingerprint`

ANMERKUNG: Der Fingerabdruck wird als Sequenz von Zahlen und Buchstaben nach dem Gleichheitszeichen angezeigt und lautet wie folgt: `SHA1 Fingerprint=09:0A:B7:53:7C:D9:D2:35:1B:4D:6D:B8:37:77:E8:2E:48:CD:12:1B`

Führen Sie „ls_update_certs.py“ mit dem alten Fingerabdruck aus. Melden Sie sich ab und melden Sie sich am vCenter Web Client an, nachdem die Dienste erfolgreich aktualisiert wurden. Das Dell Plug-in wird erfolgreich gestartet.

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**.

Der Service- und Bestandsaufnahmezeitplan für alle vCenter wird nicht angewendet, wenn er auf der Job-Warteschlangen-Seite ausgewählt ist.

Navigieren Sie zu **Dell Home** > **Überwachen** > **Job-Warteschlange** > **Service-/Bestandsaufnahmeverlauf** > **Zeitplan**. Wählen Sie ein vCenter aus und wählen Sie die Schaltfläche „Zeitplan ändern“ aus. Wenn ein Dialogfeld angezeigt wird, wird ein Kontrollkästchen mit der Meldung **Für alle registrierten vCenter anwenden** angezeigt. Wenn Sie das Kontrollkästchen auswählen und **Anwenden** drücken, wird die Einstellung auf ein bestimmtes, von Ihnen ausgewähltes vCenter angewendet, und nicht auf alle vCenter. Die Schaltfläche **Für alle registrierten vCenter anwenden** wird nicht angewendet, wenn der Service- oder Bestandsaufnahmezeitplan auf der Seite **Job-Warteschlange** geändert wird.

Lösung: Verwenden Sie den Service- oder Bestandsaufnahme-Zeitplan in der Job-Warteschlange nur zum Modifizieren des ausgewählten vCenters.

Betroffene Versionen: 2.2 und höher

Was soll ich tun, wenn ein Web-Kommunikationsfehler im vCenter Webclient nach dem Ändern der DNS-Einstellungen in OMIVV Web-Kommunikationsfehler angezeigt wird?

Wenn irgendeine Art von Web-Kommunikationsfehler in vCenter Web-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 Web Client an.

Warum schlägt das Laden der Seite „Einstellungen“ fehl, wenn ich sie verlasse und dann wieder zur Seite „Einstellungen“ zurückkehre?

Wenn Sie in vSphere v5.5 im Webclient auf eine andere Seite navigieren und danach zur Seite **Einstellungen** zurückkehren, schlägt das Laden der Seite manchmal fehl und das Drehfeld dreht sich weiter. Dies ist ein Aktualisierungsfehler und die Seite wird nicht korrekt aktualisiert.

Lösung: Klicken Sie auf die globale Aktualisierung, und der Bildschirm wird korrekt aktualisiert.

Betroffene Versionen: 2.2 und 3.0

Der Fehler „Aufgabe kann nicht in der Vergangenheit geplant werden“ auf der Seite „Bestandsaufnahmezeitplan/Servicezeitplan“ wird im Assistenten für die ursprüngliche Konfiguration angezeigt.

Im Web-Client wird der Fehler "Task kann nicht in der Vergangenheit geplant werden" angezeigt:

- Wenn Sie die Option "Alle registrierten vCenter" im Erstkonfigurationsassistenten auswählen und es gibt einige vCenter ohne Hosts.

- Wenn vCenter Bestandsaufnahme- oder Tasks Service-Tasks bereits geplant haben.
- Wenn noch einige vCenter ohne Bestandsaufnahme oder Servicezeitplan eingestellt sind.

Lösung: Führen Sie die Einstellungen des Bestandsaufnahme- und Servicezeitplans separat von der Seite **Einstellungen** für die vCenters durch.

Betroffene Versionen: 2.2 und höher

Das Installationsdatum wird für einige Firmware-Versionen auf der Firmware-Seite als 31.12.1969 angezeigt.

Im Webclient 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

Das wiederholte globale Aktualisieren führt im aktuellen Task-Fenster zu einer Ausnahme.

Wenn Sie versuchen, wiederholt auf die Schaltfläche „Aktualisieren“ zu drücken, tritt möglicherweise eine Ausnahme in der VMware-Benutzeroberfläche auf.

Lösung: Sie können diese Fehlermeldung schließen und fortfahren.

Betroffene Version: 2.2 und höher

Warum ist die Webclient-Benutzeroberfläche bei einigen Dell Bildschirmen in IE 10 verzerrt?

In einigen Fällen sind die Daten im Hintergrund bei der Anzeige eines Informationsdialogfelds vollständig weiß und sind verzerrt dargestellt.

Lösung: Schließen Sie das Dialogfeld, dann wird der Bildschirm wieder normal.

Betroffene Version: 2.2 und höher

Warum wird das OpenManage Integration Symbol im Webclient-Ereignis nicht angezeigt, selbst wenn die Registrierung des Plug-ins im vCenter erfolgreich war?

Das OpenManage Integration Symbol wird nicht im Webclient angezeigt, außer wenn die vCenter Webclient-Services neu gestartet werden. Bei der Registrierung der OpenManage Integration for VMware vCenter Appliance wird die Appliance beim Webclient 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 Webclient nicht angezeigt. Der Grund dafür liegt in einem Zwischenspeicherproblem von VMware. Zum Beheben des Problems stellen Sie sicher, dass Sie den Webclient-Service auf dem vCenter Server neu starten. Dann wird das Plug-in in der UI angezeigt.

Lösung: Starten Sie den Webclient-Service auf dem vCenter Server neu.

Betroffene Version: 2.2 und höher

Selbst wenn das Repository über Bundles für das ausgewählte 11G-System verfügt, zeigt die Firmware-Aktualisierung an, dass keine Bundles für eine Firmware-Aktualisierung verfügbar sind.

Wenn im Sperrmodus ein Host zum Verbindungsprofil hinzugefügt wird, startet die Bestandsaufnahme, die jedoch mit der Meldung „Es wurde kein Remote Access Controller gefunden, oder auf diesem Host wird keine Bestandsaufnahme unterstützt“ fehlschlug. Die Bestandsaufnahme sollte jedoch für einen Host im Sperrmodus funktionieren.

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 durchführen. Bei der Verwendung eines 11G-Host für die Firmware-Aktualisierung, zeigt der Assistent für die Firmware-Aktualisierung keine Bundles an, obwohl das Repository über Bundles für das System verfügt. Dies tritt auf, da der 11G-Host möglicherweise nicht konfiguriert wurde, damit OMSA Traps an die OpenManage Integration sendet.

Lösung: Stellen Sie sicher, dass der Host kompatibel ist, indem Sie den Host-Kompatibilitätsassistenten des OpenManage Integration Webclients verwenden. Wenn er nicht vorgabenkonform ist, verwenden Sie die Option „Host-Konformität beheben“, um die Konformität herzustellen.

Betroffene Version: 2.2 und höher

Warum werden die DNS-Konfigurationseinstellungen nach dem Neustart des Geräts auf die ursprünglichen Einstellungen zurückgesetzt, wenn Geräte-IP und DNS-Einstellungen mit DHCP-Werten überschrieben werden?

Der Fehler, dass statisch zugewiesene DNS-Einstellungen mit Werten aus DHCP ersetzt werden, ist bekannt. Der Fehler kann auftreten, wenn DHCP verwendet wird, um IP-Einstellungen abzurufen, und DNS-Werte statisch zugewiesen werden. Bei Verlängerung des DHCP-Lease oder Neustart des Geräts werden die statisch zugeordneten DNS-Einstellungen entfernt.

Lösung: Statische Zuordnung von IP-Einstellungen zuweisen, wenn sich die DNS-Servereinstellungen von DHCP unterscheiden.

Betroffene Version: Alle

OMIVV wird für die Aktualisierung der Intel-Netzwerkkarte mit Firmwareversion 13.5.2 nicht unterstützt.

Dies ist ein bekanntes Problem, das auf Dell PowerEdge Servern der 12. Generation und einigen Intel Netzwerkkarten mit der Firmwareversion 13.5.2 auftritt. Die Aktualisierung einiger Modelle von Intel Netzwerkkarten mit dieser Firmware-Version schlägt fehl, wenn die Firmware-Aktualisierung mit dem Lifecycle Controller angewendet wird. Kunden mit dieser Firmware-Version müssen die Netzwerktreibersoftware mit einem Betriebssystem aktualisieren. Wenn Version der Intel-Netzwerkkarte nicht 13.5.2 ist, können Sie mit OMIVV aktualisieren. 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: Hinweis: Vermeiden Sie bei 1:N-Firmware-Aktualisierungen die Auswahl von Intel-Netzwerkadaptern der Version 13.5.2. Anderenfalls wird die Aktualisierung fehlschlagen und die Aktualisierung der 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 fällt beim Versuch einer Firmware-Aktualisierung mit einer ungültigen DUP der Hardware-Aktualisierungsjobstatus auf der vCenter-Konsole stundenlang weder aus noch weist er eine Zeitüberschreitung auf, obwohl der Jobstatus in LC „FEHLGESCHLAGEN“ anzeigt?

Wenn die ungültige DUP für die Firmware-Aktualisierung abgerufen wird, bleibt der Status der Aufgabe im vCenter Konsolenfenster auf „In Bearbeitung“, die Meldung wird jedoch auf die Ursache des Fehlers geändert. Dies ist ein bekannter Fehler von VMware und wird in zukünftigen Versionen von VMware vCenter behoben.

Lösung: Die Aufgabe muss manuell abgebrochen werden.

Betroffene Version: Alle

Warum zeigt das Administrationsportal einen nicht erreichbaren Aktualisierungs-Repository-Speicherort an?

Wenn Sie einen nicht erreichbaren Aktualisierungs-Repository-Pfad bereitstellen, wird die Fehlermeldung „Failed: Fehler beim Herstellen einer Verbindung mit der URL...“ oben in der System-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 PowerEdge Dell Servern der 12. Generation und höher wird die Prozessor-Version in der Spalte Marke angezeigt. 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. Weitere Informationen über die Funktion von OMIVV im verknüpften Modus finden Sie im Whitepaper *OpenManage Integration for VMware vCenter: Working in Linked Mode* unter www.dell.com.

Erforderliche Porteinstellungen für OMIVV

ANMERKUNG: Wenn Sie den OMSA Agenten in OMIVV über den Link **Nicht vorgabenkonforme vSphere Hosts beheben** im Fenster **Kompatibilität** bereitstellen, startet OMIVV den HTTP-Client-Dienst und aktiviert auf Versionen ab ESXi 5.5 den Port 8080, um das OMSA VIB herunterzuladen und zu installieren. Nach Abschluss der OMSA VIB-Installation wird der Dienst automatisch angehalten und die Schnittstelle geschlossen.

Verwenden Sie die folgende Porteinstellungen für OMIVV:

Tabelle 43. 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.
69	TFTP	UDP	Keine	Ausgang	OMIVV-Gerät zu TFTP-Server	TFTP-Client	Wird für die Firmware-Aktualisierung auf 11G-Servern mit alter Firmware verwendet.
80	HTTP	TCP	Keine	Ausgang	OMIVV-Gerät zu Internet	Dell Online-Datenzugriff	Konnektivität zu Online-Service (Internet), Firmware und aktuellen RPM-Informationen.
80	HTTP	TCP	Keine	Eingang	ESXi-Server zu OMIVV-Gerät	HTTP-Server	Wird im Betriebssystem-Bereitstellungsprozess für Skripts nach der Installation zur Kommunikation mit dem OMIVV-Gerät verwendet.
162	SNMP-Agent	UDP	Keine	Eingang	iDRAC/ESXi zu OMIVV-Gerät	SNMP-Agent (Server)	Für den Empfang von SNMP-Traps von verwalteten Knoten.
443	HTTPS	TCP	128 Bit	Eingang	OMIVV UI zu OMIVV-Gerät	HTTPS-Server	Von OMIVV angebotene Webdienste. Diese Webdienste werden vom vCenter Web-Client und Dell Admin-Portal genutzt.
443	WSMAN	TCP	128 Bit	Ein/Aus	OMIVV-Gerät zu/von iDRAC/OMSA	iDRAC/OMSA-Kommunikation	iDRAC-, OMSA- und CMC-Kommunikation; wird zur Verwaltung und Überwachung der verwalteten Knoten verwendet.
445	SMB	TCP	128 Bit	Ausgang	OMIVV-Gerät zu CIFS	CIFS-Kommunikation	Für die Kommunikation mit Windows-Freigaben.
4433	HTTPS	TCP	128 Bit	Eingang	iDRAC zu OMIVV-Gerät	Automatische Ermittlung	Bereitstellungsserver, der für die automatische Ermittlung von verwalteten Knoten verwendet wird.
2049	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	Öffentliche NFS-Freigabe, die vom OMIVV-Gerät für die verwalteten Knoten verfügbar gemacht und für Firmwareaktualisierungs- und Betriebssystem-Bereitstellungsprozesse verwendet wird.

Tabelle 43. Virtual Appliance (fortgesetzt)

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
11620	SNMP-Agent	UDP	Keine	Eingang	iDRAC zu OMIVV-Gerät	SNMP-Agent (Server)	iDRAC-, OMSA- und CMC-Kommunikation; wird zur Verwaltung und Überwachung der verwalteten Knoten verwendet.
Benutzer definiert	beliebig	UDP/TCP	Keine	Ausgang	OMIVV-Gerät zu Proxy-Server	Proxy	Für die Kommunikation mit dem Proxy-Server

Tabelle 44. Verwaltete Knoten (ESXi)

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
162, 11620	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 (OMSA)	iDRAC/OMSA-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.
8080	HTTP	TCP	128 Bit	Ausgang	ESXi zu OMIVV-Gerät	HTTP-Server; lädt den OMSA VIB herunter und behebt nicht konforme vSphere-Hosts	Hilft ESXi beim Herunterladen des OMSA-/Treiber-VIB.

Tabelle 45. Verwaltete Knoten (iDRAC/CMC)

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
443	WSMAN /HTTPS	TCP	128 Bit	Eingang	OMIVV-Gerät zu iDRAC/CMC	iDRAC-Kommunikation	Wird verwendet, um Informationen für die Management Station bereitzustellen. Dieser Port muss über iDRAC und CMC geöffnet werden.
4433	HTTPS	TCP	128 Bit	Ausgang	iDRAC zu OMIVV-Gerät	Automatische Ermittlung	Für die automatische Ermittlung von iDRAC (verwalteten Knoten) in der Management Station.
2049	NFS	UDP	Keine	Ein/Aus	iDRAC zu/von OMIVV	Öffentliche Freigabe	Für iDRAC zum Zugriff auf die öffentliche NFS-Freigabe, die vom OMIVV-Gerät verfügbar gemacht wird. Wird für die Betriebssystembereitstellung und Firmwareaktualisierung verwendet. Zum Zugriff auf die DRAC-Konfigurationen über OMIVV. Wird im Bereitstellungsprozess verwendet.

Tabelle 45. Verwaltete Knoten (iDRAC/CMC) (fortgesetzt)

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
4001 zu 4004	NFS	UDP	Keine	Ein/Aus	iDRAC zu/von OMIVV	Öffentliche Freigabe	Für iDRAC zum Zugriff auf die öffentliche NFS-Freigabe, die vom OMIVV-Gerät verfügbar gemacht wird. Wird für die Betriebssystembereitstellung und Firmwareaktualisierung verwendet. Zum Zugriff auf die DRAC-Konfigurationen über OMIVV. Wird im Bereitstellungsprozess verwendet.
69	TFTP	UDP	128 Bit	Ein/Aus	iDRAC zu/von OMIVV	Trivial File Transfer (Einfache Dateiübertragung)	Wird für die erfolgreiche Verwaltung des iDRAC über die Management Station verwendet.

Das Passwort für den Benutzer, der für die Bare-Metal-Erkennung verwendet wird, wird nach der erfolgreichen Anwendung des Hardware- oder Systemprofils nicht geändert, das über den gleichen Benutzer mit neuen geänderten Anmeldeinformationen in der iDRAC-Benutzerliste verfügt.

Das Kennwort des Benutzers, der für die Erkennung verwendet wird, wird nicht zu neuen Anmeldeinformationen geändert, wenn nur Hardwareprofil- oder Systemprofilvorlage zur Bereitstellung ausgewählt wird. 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**.

Wie teste ich Event-Einstellungen mithilfe des OMSA, um einen Temperaturfehler an der Hardware zu simulieren?

Führen Sie folgende Schritte aus, um sicherzustellen, dass Ereignisse korrekt funktionieren:

1. Navigieren Sie in der OMSA-Benutzeroberfläche zu **Warnungsverwaltung** > **Plattformereignisse**.
2. Aktivieren Sie das Kontrollkästchen **Plattformereignisfilter-Warnungen aktivieren**.
3. Führen Sie einen Bildlauf bis ganz nach unten durch, und klicken Sie auf **Änderungen anwenden**.
4. Wählen Sie aus der Struktur auf der linken Seite die Option **Hauptsystemgehäuse aus**, um sicherzugehen, dass ein bestimmtes Ereignis aktiviert ist, wie z. B. die Temperaturwarnung.
5. Wählen Sie unter **Hauptsystemgehäuse Temperaturen** aus.
6. Wählen Sie die Registerkarte **Warnungsverwaltung** und anschließend **Temperatursondenwarnung** aus.

7. Aktivieren Sie das Kontrollkästchen **Broadcast-Übertragung einer Meldung**, und wählen Sie **Änderungen anwenden** aus.
8. Um das Temperaturwarnereignis auszulösen, wählen Sie in der Strukturansicht auf der linken Seite die Option **Hauptsystemgehäuse** aus.
9. Wählen Sie unter **Hauptsystemgehäuse** die Option **Temperaturen** aus.
10. Wählen Sie den Link **Umgebungstemp. der Systemplatine** und dann die Options-Schaltfläche **Auf Werte setzen** aus.
11. Stellen Sie den **maximalen Warnungsschwellenwert** auf einen Wert ein, der vor dem jeweiligen aktuellen angegebenen Messwert liegt.
    Wenn beispielsweise der aktuelle Messwert bei 27 liegt, stellen Sie den Schwellenwert auf **25** ein.
12. Wählen Sie **Änderungen übernehmen**, dann wird das Temperaturwarnungsereignis erzeugt.

    Wenn Sie ein weiteres Ereignis auslösen möchten, stellen Sie die ursprünglichen Einstellungen unter Verwendung der gleichen Option **Auf Werte setzen** wieder her. Ereignisse werden als Warnungen erzeugt und werden dann auf einen normalen Zustand gesetzt. Wenn alles ordnungsgemäß funktioniert, wechseln Sie zur Ansicht **vCenter Tasks & Events**. Dann sollte eine Temperatursondenwarnung angezeigt werden.

    ANMERKUNG: Es gibt einen Filter für doppelte Ereignisse. Wenn Sie versuchen, dasselbe Ereignis zu oft hintereinander auszulösen, erhalten Sie nur ein Ereignis. Zum Anzeigen aller Ereignisse müssen Sie mindestens 30 Sekunden zwischen dem Auslösen der Ereignisse warten.

Obwohl der OMSA-Agent auf dem OMIVV Hostsystem installiert ist, wird weiterhin die Fehlermeldung angezeigt, dass OMSA nicht installiert ist.

Um dieses Problem auf einem Server der 11. Generation zu beheben:

1. Installieren Sie den **OMSA** mit der Komponente **Remote-Aktivierung** auf dem Hostsystem.
2. Wenn Sie zum Installieren von OMSA die Befehlszeile verwenden, stellen Sie sicher, dass Sie die **-c option** angeben. Wenn OMSA bereits installiert ist, installieren Sie sie mit der Option -c neu und starten Sie den Dienst neu:

```
srvadmin-install.sh -c
srvadmin-services.sh restart
```

   Bei einem ESXi Host müssen Sie sicherstellen, dass **OMSA VIB** mithilfe des **VMware Remote CLI Tools** installiert wird, und das System neu starten.

Unterstützt OMIVV ESXi mit aktiviertem Sperrmodus?

Ja. Der Sperrmodus wird in dieser Version auf ESXi 5.0 Hosts und höher unterstützt.

Bei Verwendung des Sperrmodus ist ein Fehler aufgetreten

Als ich im Sperrmodus einen Host zum Verbindungsprofil 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 setzen oder den Sperrmodus beenden, müssen Sie 30 Minuten warten, bevor Sie den nächsten Vorgang in OMIVV durchführen können.

Die Erstellung von Hardwareprofil schlägt fehl, wenn ich einen Referenzserver verwende

Prüfen Sie, ob die empfohlenen Mindestversionen der iDRAC- und Lifecycle-Controller-Firmware sowie des BIOS installiert sind.

Zum Sicherstellen, dass die vom Referenzserver abgerufenen Daten aktuell sind, müssen Sie die Option **Systembestandsaufnahme beim Neustart sammeln (CSIOR)** aktivieren und den Referenzserver vor der Datenextrahierung neu starten.

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 sich die während der Zuweisung der Serveridentität ausgewählte **NIC** auf dem gleichen Netzwerk wie das virtuelle Gerät befindet.
3. 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.
4. Stellen Sie sicher, dass mindestens eine **virtuelle Festplatte** vom System erkannt wird.

   ESXi installiert ebenfalls auf einer internen SD-Karte.

Hypervisor-Bereitstellungen schlagen auf Dell PowerEdge R210 II Computern fehl.

Ein Zeitüberschreitungsproblem auf den Dell PowerEdge R210 II Systemen verursacht eine Hypervisor-Bereitstellungs-Fehlermeldung, da das BIOS nicht vom zugehörigen ISO starten kann.

Lösung: Installieren Sie den Hypervisor manuell auf dem Computer.

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 ESXi-ISO eingerichtet, die Bereitstellung schlägt jedoch beim Laden des Freigabepfads fehl.

Gehen Sie folgendermaßen vor, um die Lösung zu finden:

1. Stellen Sie sicher, dass der iDRAC einen Ping-Befehl an das Gerät senden kann.
2. Stellen Sie außerdem sicher, dass Ihr Netzwerk nicht zu langsam ist.
3. Stellen Sie sicher, dass die Ports 2049 und 4001 - 4004 offen sind und die Firewall entsprechend eingestellt ist.

So wird eine virtuelle Appliance zwangsweise aus dem vCenter entfernt

1. Navigieren Sie zu **Https://<vcenter_serverIPAddress>/mob**
2. Geben Sie die VMware vCenter Administrator-Anmeldeinformationen ein.
3. Klicken Sie auf **Inhalt**.
4. Klicken Sie auf **ExtensionManager**.
5. Klicken Sie auf **UnregisterExtension**.
6. Geben Sie den Erweiterungsschlüssel zur Deregistrierung von com.dell.plugin.openManage_integration_for_VMware_vCenter_WebClient ein und klicken Sie anschließend auf **Methode aufrufen**.
7. Schalten Sie im OMIVV im vSphere-Web-Client aus und löschen Sie es. Der Schlüssel zur Aufhebung der Registrierung muss für den Web-Client bestimmt sein.

Beim Eingeben eines Kennworts im Bildschirm „Jetzt sichern“ wird eine Fehlermeldung angezeigt.

Wenn Sie einen Monitor mit niedriger Auflösung verwenden, wird das Feld Verschlüsselungskennwort im Fenster JETZT SICHERN nicht angezeigt. Sie müssen auf der Seite nach unten scrollen, um das Verschlüsselungskennwort einzugeben.

Wenn ich im vSphere-Web-Client auf das Dell Server Management-Portlet oder das Dell Symbol klicke, wird ein 404-Fehler ausgegeben.

Überprüfen Sie, ob das OMIVV-Gerät ausgeführt wird. Starten Sie es andernfalls vom vSphere-Web-Client. Warten Sie einige Minuten, bis der Webservice des virtuellen Geräts startet und aktualisieren Sie dann die Seite. Wenn der Fehler weiterhin auftritt, versuchen Sie einen Ping-Befehl an das Gerät zu senden, Verwenden Sie dabei die IP-Adresse oder den vollständig qualifizierten Domänennamen über eine Befehlszeile. Wenn der Ping nicht aufgelöst werden kann, überprüfen Sie Ihre Netzwerkeinstellungen, um sicherzustellen, dass sie richtig sind.

Was mache ich, wenn eine Aktualisierung fehlschlägt?

Prüfen Sie in den Protokollen der virtuellen 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 Verbindungsprofils langsam oder und 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:
   - iDRAC6: Wählen Sie die Registerkarten **iDRAC-Einstellungen** > **Netzwerk/Sicherheit** > **Benutzer**.
   - iDRAC7: Wählen Sie die Registerkarten **iDRAC-Einstellungen** > **Benutzer**.
   - iDRAC8: Wählen Sie die Registerkarten **iDRAC-Einstellungen** > **Benutzer**.
4. Um die Einstellungen zu bearbeiten, klicken Sie in der Spalte „Benutzer-ID“ auf den Link für den Admin-(Stamm-)Benutzer.
5. Klicken Sie auf **Benutzer konfigurieren** und dann auf **Weiter**.
6. Aktivieren Sie auf der Seite **Benutzerkonfiguration** für den ausgewählten Benutzer das Kontrollkästchen neben „Benutzer aktivieren“, und klicken Sie dann auf **Anwenden**.

Unterstützt OMIVV die VMware vCenter Server Appliance?

Ja, OMIVV unterstützt die VMware vCenter Server Appliance ab v2.1.

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. Deshalb wird der Host bis zur nächsten Ausführung der Gehäuse-Bestandsaufnahme unter dem Gehäuse angezeigt, obwohl der Host aus der vCenter Struktur entfernt wurde.

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**.

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 in OpenManage Integration for VMware-GUI auf der Registerkarte **Verwalten** > **Einstellungen** manuell die Einstellungen für **Alarme und Events**.

Die Hypervisor-Bereitstellung schlägt fehl, wenn NPAR auf einem Zielknoten aktiviert und im Systemprofil deaktiviert ist

Die Hypervisor-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 durch das Systemprofil während der Bereitstellung ändern, stellen Sie sicher, dass Sie nur die erste Partition für das Verwaltungsnetzwerk im Bereitstellungsassistenten auswählen.

Betroffene Version: 4.1

Die verfügbare virtuelle 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.

Die 267027 Ausnahme wurde beim Hinzufügen des 12G Bare-Metal-Servers mit einer Expresslizenz 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 BS-Bereitstellung auf 14G schlägt das Anwenden des Hardwareprofils aufgrund eines iDRAC Fehlers fehl

Während der BS-Bereitstellung auf 14G-Server wird ein Konfigurationsaktualisierungsjob in iDRAC erstellt, wenn das Hardwareprofil angewandt wird. Dieser Job schlägt allerdings manchmal fehl und zeigt eine Meldung an, die angibt, dass der Konfigurationsjob bereits erstellt wurde.

Lösung: Zum Löschen den veralteten Einträge und dem erneuten Versuch der BS-Bereitstellung führen Sie den Befehl `racadm jobqueue delete -i JID_CLEARALL_FORCE` aus.

OMIVV RPM-Upgrade schlägt fehl, wenn Proxy mit Domain-Benutzerauthentifizierung konfiguriert ist

Wenn OMIVV Appliance 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.

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 Auto-Ermittlung auf neu erworbenen Systemen

Die Funktion der Auto-Ermittlung eines Hostsystems ist standardmäßig nicht aktiviert. Sie muss beim Kauf angefordert werden. Wenn die Auto-Ermittlung zum Zeitpunkt des Kaufs angefordert wird, wird das DHCP auf dem iDRAC aktiviert und Administratorkonten werden deaktiviert. Die Konfiguration einer statischen IP-Adresse ist für den iDRAC nicht erforderlich. Die Adresse wird vom DHCP-Server auf dem Netzwerk abgerufen. Um die automatische Ermittlung verwenden zu können, muss ein DHCP- und/oder DNS-Server zur Unterstützung des Ermittlungsprozesses konfiguriert werden. CSIOR sollte werkseitig bereits ausgeführt worden sein.

Falls die Auto-Ermittlung nicht zum Zeitpunkt des Kaufs angefordert wurde, kann sie wie folgt aktiviert werden:

1. Drücken Sie während der Startroutine **Strg+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
```

17

Zugehörige Dokumentation

Zusätzlich zu dieser Anleitung können Sie auf die anderen Anleitungen zugreifen, die unter `Dell.com/support` zur Verfügung stehen. Klicken Sie auf **Aus allen Produkten auswählen** und anschließend auf **Software und Sicherheit** > **Virtualisierungslösungen**. Klicken Sie auf **OpenManage Integration for VMware vCenter 4.2**, um auf die folgenden Dokumente zuzugreifen:

- *OpenManage Integration for VMware vCenter Version 4.2 Web-Client-Benutzerhandbuch*
- *OpenManage Integration for VMware vCenter Version 4.2-Versionshinweise*
- *OpenManage Integration for VMware vCenter Version 4.2-Kompatibilitäts-Matrix*

Sie finden die technischen Artefakte einschließlich Whitepapers unter **delltechcenter.com**. Klicken Sie auf der Dell TechCenter Wiki-Startseite auf **Systemverwaltung** > **OpenManage Integration for VMware vCenter**, um auf die Artikel zuzugreifen.

Themen:

Zugriff auf Dokumente von der Dell EMC Support-Website

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

- Verwendung der folgenden Links:
  - Für Dokumente zu Dell EMC Enterprise Systems Management, Dell EMC Remote Enterprise Systems Management sowie Dell EMC Virtualization Solutions – unter www.dell.com/esmmanuals
  - Für Dokumente zu Dell EMC OpenManage – Www.dell.com/openmanagemanuals
  - Für iDRAC Dokumente: Www.dell.com/idracmanuals
  - Für Dokumente zu Dell EMC OpenManage Connections Enterprise Systems Management – www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Für Dokumente zu Dell EMC Serviceability Tools – https://www.dell.com/serviceabilitytools
- Gehen Sie auf der Dell EMC Support-Website folgendermaßen vor:
  1. Navigieren Sie zu https://www.dell.com/support.
  2. Klicken Sie auf **Alle Produkte durchsuchen**.
  3. Klicken Sie auf der Seite **Alle Produkte** auf **Software** und klicken Sie dann auf einen der folgenden Links:
     - **Analysen**
     - **Client-Systemverwaltung**
     - **Unternehmensanwendungen**
     - **Verwaltung von Systemen der Enterprise-Klasse**
     - **Mainframe**
     - **Betriebssysteme**
     - **Lösungen für den öffentlichen Sektor**
     - **Wartungstools**
     - **Support**
     - **Dienstprogramme**
     - **Virtualisierungslösungen**
  4. Um ein Dokument anzuzeigen, klicken Sie auf das gewünschte Produkt und anschließend auf die gewünschte Version.
- Verwendung von Suchmaschinen:
  - Geben Sie den Namen und die Version des Dokuments in das Kästchen „Suchen“ ein.

A

Systemspezifische Attribute

iDRAC

Tabelle 46. 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
DNSDomainName	DNS-Domänenname	Statische NIC-Informationen
Adresse	IPv4-Adresse	Statische IPv4-Informationen
Netzwerkmaske	Netzwerkmaske	Statische IPv4-Informationen
Gateway	Gateway	Statische IPv4-Informationen
DNS1	DNS-Server 1	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 47. Systemspezifische Attribute für BIOS

Attributname	Anzeigeattributname	Gruppen-Anzeigename
AssetTag	Asset Tag	Verschiedene Einstellungen
IscsiDev1con1Gateway	Initiator-Gateway	Einstellungen für Verbindung 1
IscsiDev1con1IP-	Initiator-IP-Adresse	Einstellungen für Verbindung 1
IscsiDev1Con1Mask	Initiator-Subnetzmaske	Einstellungen für Verbindung 1

Tabelle 47. Systemspezifische Attribute für BIOS (fortgesetzt)

Attributname	Anzeigeattributname	Gruppen-Anzeigename
IscsiDev1Con1TargetIp	Ziel-IP-Adresse	Einstellungen für Verbindung 1
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 48. Systemspezifische Attribute für RAID

Attributname	Anzeigeattributname	Gruppen-Anzeigename
Angeforderter Gehäusekonfigurationsmodus	-	-
Aktueller Gehäusekonfigurationsmodus	-	-

CNA

Tabelle 49. 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

Tabelle 49. Systemspezifische Attribute für CNA (fortgesetzt)

Attributname	Anzeigeattributname	Gruppen-Anzeigename
IscsiInitiatorChapPwd	CHAP-Geheimschlüssel	iSCSI Initiator-Parameter
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 50. Systemspezifische Attribute für FC

Attributname	Anzeigeattributname	Gruppen-Anzeigename
VirtualWWN	Virtueller World Wide Knotenname	Port-Konfigurationsseite
VirtualWWPN	Virtueller World Wide Schnittstellenname	Port-Konfigurationsseite

B

Anpassungsattribute

Tabelle 51. 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.

C

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*

D

Vergleich von Komponenten- und Baseline-Version - Matrix

Tabelle 52. 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 Hardware-Komponente 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 oder das Attribut sind jedoch 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 Firmware-Komponente stimmt mit der zugehörigen Baseline überein.	Konform
	Verfügbar	Verfügbar	Die Firmware-Komponente stimmt nicht mit der zugehörigen Baseline überein.	Nicht 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 Treiberkomponente stimmt mit der zugehörigen Baseline überein.	Konform
	Verfügbar	Verfügbar	Die 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 Treiberkomponente ist in der zugehörigen Baseline verfügbar, die Komponente oder das Attribut oder die neue Komponente sind jedoch nicht verfügbar.	Nicht konform

Tabelle 52. Vergleich von Komponenten- und Baseline-Version - Matrix (fortgesetzt)

	Nicht verfügbar	Nicht verfügbar	Der Vergleichsstatus wird nicht berechnet oder ignoriert.	Konform