OpenManage Integration for VMware vCenter Version 4.0

Benutzerhandbuch Web Client

Anmerkungen, Vorsichtshinweise und Warnungen

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

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

Copyright © 2017 Dell Inc. oder deren Tochtergesellschaften. Alle Rechte vorbehalten. Dell, EMC und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Andere Marken können Marken ihrer jeweiligen Inhaber sein.

2017 - 02

Rev. A00

Inhaltsverzeichnis

1 Einführung....9

Was ist neu in dieser Version?....9

OpenManage Integration for VMware vCenter-Funktionen....9

2 Informationen zur Verwaltungskonsole....11

Verwendung des Administration-Portal....11

Registrieren eines vCenter Servers durch einen Nicht-Administratorbenutzer....11

Registrieren eines vCenter-Servers....14

Hochladen einer Lizenz auf das Administration-Portal....16

Verwalten des virtuellen Geräts....16

Einrichten globaler Alarme....21

Verwalten von Backups und Wiederherstellungen....21

Informationen zur vSphere Client-Konsole....23

3 Verwaltung mehrerer Geräte....26

4 Aufrufen der OpenManage-Integration aus dem Webclient....27

Navigieren im VMware vCenter-Webclient....27

Symbole im Webclient....27

Softwareversion finden....28

Aktualisieren des Bildschirminhalts....28

Anzeigen von Dell Hosts....28

Anzeigen der Lizenzregisterkarte OpenManage Integration for VMware vCenter....29

Aufrufen von Hilfe und Support....29

Fehlerbehebungspaket herunterladen....30

Durchführen des iDRAC-Resets....30

Öffnen der Online-Hilfe....31

Starten der Administrationskonsole....31

Anzeigen des Protokollverlaufs....32

Protokolle anzeigen....33

Protokolldateien exportieren....33

5 OpenManage Integration for VMware vCenter-Lizenzierung....34

Software-Lizenz erwerben und hochladen....34

6 Gerätekonfiguration für VMware vCenter....36

Konfigurationstasks im Konfigurationsassistenten....36

Anzeigen des Begrüßungsdialogs des Konfigurationsassistenten....36

Auswählen der vCenter....36

Verbindungsprofil erstellen....37

Planen von Bestandsaufnahme-Jobs....39

Ausführen von Serviceabfrage-Jobs....40

Konfigurieren von Ereignissen und Alarmen 40
Konfigurationsaufgaben über die Registerkarte Einstellungen 41
Geräteeinstellungen 41
vCenter-Einstellungen 43

7 Profile 46
Informationen zum Verbindungsprofil 46
Verbindungsprofile anzeigen 46
Verbindungsprofil erstellen 47
Ändern von Verbindungsprofilen 49
Löschen von Verbindungsprofilen 51
Testen von Verbindungsprofilen 51
Informationen zum Gehäuseprofil 51
Anzeigen von Gehäuseprofilen 52
Erstellen eines Gehäuse-Profils 52
Gehäuseprofil bearbeiten 53
Löschen von Gehäuseprofilen 53
Gehäuseprofil testen 54

8 Bestandsaufnahme. und Service-Management 55
Bestandaufnahme-Jobs 55
Host-Bestand anzeigen 55
Gehäuse-Bestandsaufnahme anzeigen 57
Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme 57
Ausführen von Bestandsaufnahme-Jobs 58
Sofortiges Ausführen eines Gehäuse-Bestandsaufnahme-Jobs 58
Service-Jobs 58
Anzeigen des Serviceverlaufs 59
Gehäusegarantie anzeigen 60
Ändern von Service-Jobzeitplänen 60
Sofortiges Ausführen eines Service-Jobs 60
Sofortiges Ausführen eines Gehäusegarantie-Jobs 61
Überwachung eines einzelnen Hosts 61
Anzeigen der Hostzusammenfassungsdetails 61
Anzeigen der Hardware-Details für einen einzigen Host 64
Anzeigen der Speicherdetails für einen einzigen Host 65
Über Systemereignisprotokolle im Webclient 68
Anzeigen zusätzlicher Hardware-Details für einen einzigen Host 69
Überwachen der Hosts auf Clustern und von Rechenzentren 70
Anzeigen einer Übersicht der Rechenzentren und Cluster 70
Anzeigen von Hardware-Details für Rechenzentren und Cluster 71
Anzeigen von Speicherdetails für Datacenter und Cluster 73
Anzeigen zusätzlicher Hardware-Details für Rechenzentren und Cluster 75
Einrichten eines Blinkanzeigelichts an der Frontblende eines physischen Servers 77

9 Allgemeines zu Firmware-Aktualisierungen 78

Ausführen des Firmwareaktualisierungsassistenten für einen einzelnen Host....78
Ausführen des Firmwareaktualisierungsassistenten für Cluster....80
Verwalten von Firmware-Aktualisierungs-Jobs....82

10 Ereignisse, Alarme und Systemüberwachung....84
Informationen zu Ereignissen und Warnmeldungen für Hosts....84
Informationen zu Ereignissen und Warnmeldungen für Gehäuse....85
Anzeigen von Gehäuseereignissen....85
Anzeigen von Gehäusealarmen....85
Ereignisse im Zusammenhang mit der Virtualisierung....86
Proaktive HA-Ereignisse....94
Anzeigen der Alarm- und Ereigniseinstellungen....95
Anzeigen von Ereignissen....95
Funktionszustand der Hardwarekomponenten - Proaktive HA....95
Proaktive HA für Rack-Server konfigurieren....96
Aktivieren von proaktiver HA auf Clustern....96
Überschreiben des Schweregrads der Funktionszustands-Aktualisierungsbenachrichtigung....98
Starten von Verwaltungskonsolen....98
Starten der Remote-Zugriffskonsole (iDRAC)....98
OMSA-Konsole starten....99
Starten der Chassis Management Controller-Konsole (CMC)....99

11 Gehäuseverwaltung....100
Anzeigen von Details der Gehäusezusammenfassung....100
Anzeigen von Informationen zur Hardware-Bestandsliste für Gehäuse....101
Anzeigen zusätzlicher Hardwarekonfiguration für Gehäuse....103
Zugeordneten Host für Gehäuse anzeigen....105

12 Bereitstellen von Hypervisors....106
Geräteerkennung....107
Manuelle Ermittlung....107
Auto Discovery (Automatische Ermittlung) in OpenManage Integration for VMware vCenter....107
Entfernen eines Bare-Metal-Servers....111
Bereitstellen....111
Hardwareprofil konfigurieren....112
Aktivieren von CSIOR auf einem Referenzserver....112
Anpassen von Referenzserver in Bezug auf Erstellen von Hardwareprofilen....113
Neues Hardwareprofil klonen....115
Verwalten von Hardwareprofilen....115
Erstellen eines Hypervisor-Profils....116
Verwalten von Hypervisor-Profilen....116
Erstellen von Bereitstellungsvorlagen....117
Verwalten von Bereitstellungsvorlagen....117
Infos zum Bereitstellungsassistenten....118
VLAN-Support....118
Bereitstellungsassistenten ausführen....119

Verwalten von Bereitstellungs-Jobs mithilfe der Job-Warteschlange.... 121
Festlegen der Zeit für den Bereitstellungs-Job....122
Server-Status innerhalb der Bereitstellungssequenz.... 122
Herunterladen von benutzerdefinierten Dell ISO-Images....122

13 Informationen zu Host-, Bare-Metal- und iDRAC-Konformität.... 124
Berichterstattung und Festsetzen der Kompatibilität für vSphere Hosts....124
Reparieren der iDRAC-Lizenzkonformität für vSphere-Hosts.... 125
Verwenden von OMSA mit Servern der 11. Generation.... 126
Bereitstellen von OMSA-Agent auf ESXi-System....126
OMSA-Trap-Ziel einrichten....126
Berichterstattung und Korrektur der Konformität von Bare-Metal-Servern....127
Reparatur der iDRAC-Lizenzkonformität für Bare-Metal-Server.... 128
Erneute Prüfung der Bare-Metal-Server-Konformität....128

14 Sicherheitsrollen und Berechtigungen.... 129
Datenintegrität....129
Zugangskontrollauthentifizierung, -autorisierung und -rollen....129
Dell Vorgangsrolle....130
Dell-Infrastrukturbereitstellungsrolle....130
Informationen zu Berechtigungen....130

15 Fehlerbehebung....133
Häufig gestellte Fragen (FAQs)....133
Warum ist es nicht möglich, über die Schaltfläche „Alle exportieren“ CSV-Dateien in Google Chrome zu exportieren?....133
Lizenztyp und Beschreibung von iDRAC werden für nicht kompatible vSphere-Hosts falsch angezeigt.... 133
Nach Aufhebung der Registrierung von vCenter in der früheren OMIVV-Version und Registrierung desselben vCenter mit späteren OMIVV-Versionen wird das Dell Symbol nicht mehr angezeigt.... 133
Die Einstellungen des Konfigurationsassistenten werden bei jedem Aufruf mit Standardeinstellungen überschrieben.... 134
Dell Anbieter wird nicht als Anbieter für Funktionszustandaktualisierung angezeigt.... 134
Warum schlägt die Bestandsaufnahme bei der Durchführung einer Firmware-Aktualisierungsaufgabe auf dem ESXi 5.x-Host fehl?....134
Aufgrund einer ungültigen oder unbekannten iDRAC-IP-Adresse ist die Host-Bestandsaufnahme oder Testverbindung fehlgeschlagen. Wie kann ich eine gültige iDRAC-IP-Adresse beziehen?....135
Bei Ausführung des Assistenten zum Beheben nicht kompatibler vSphere-Hosts wird der Status eines bestimmten Hosts als „Unbekannt“ angezeigt. Warum? 135
Dell Berechtigungen, die beim Registrieren des OMIVV-Geräts zugewiesen wurden, werden nach dem Aufheben der Registrierung von OMIVV nicht entfernt.... 135
Das Dell Management Center zeigt nicht alle entsprechenden Protokolle an beim Versuch, nach einer Schweregrad-Kategorie zu filtern. Wie kann ich alle Protokolle anzeigem?.... 135
Wie behebe ich den Fehlercode 2000000, der von der VMware Zertifizierungsstelle (VMCA) verursacht wird?.....136
Der Assistent der Firmware-Aktualisierung zeigt eine Meldung an, die besagt, dass die Bündel nicht aus dem Firmware Repository abgerufen wurden. Wie kann ich mit der Firmware-Aktualisierung fortfahren?....140

Warum wird in der Verwaltungskonsole das Feld Aktualisierungs-Repository-Pfad nicht auf den Standardpfad gesetzt, nachdem ich das Gerät auf die werkseitigen Einstellungen zurückgesetzt habe? ... 140
Warum die Firmwareaktualisierung für 30 Hosts auf Cluster-Ebene fehlschlägt ... 140
Warum wird der Service- und Bestandsaufnahme-Zeitplan für alle vCenter nicht angewendet, wenn er auf der Job-Warteschlangen-Seite ausgewählt ist? ... 140
Was soll ich tun, wenn ein Web-Kommunikationsfehler nach dem Ändern der DNS-Einstellungen in OMIVV Web-Kommunikationsfehler angezeigt wird? ... 141
Warum schlägt das Laden der Seite „Einstellungen“ fehl, wenn ich sie verlasse und dann noch einmal zurück auf die Seite „Einstellungen“ navigiere? ... 141
Warum wird der Fehler „Task kann nicht in der Vergangenheit geplant werden“ auf der Bestandsaufnahme-Zeitplan/Service-Zeitplan-Seite beim Assistenten zur Erstkonfiguration angezeigt? ... 141
Warum wird das Installationsdatum als 31.12.1969 für einige Firmwareversionen auf der Firmware-Seite angezeigt? ... 141
Wiederholte globale Aktualisierungsvorgänge verursachen, dass eine Ausnahme im aktuellen Aufgabenfenster angezeigt wird. Wie kann ich den Fehler beheben? ... 141
Warum ist die Web-Client-Benutzeroberfläche für einige der Dell-Bildschirme in IE 10 verzerrt? ... 142
Obwohl die Registrierung des Plug-ins im vCenter erfolgreich war, wird das OpenManage Integration-Symbol im Web-Client nicht angezeigt. Warum? ... 142
In meinem Repository sind Bundle für das ausgewählte 11G-System hinterlegt. Warum wird bei der Firmware-Aktualisierung dennoch ausgegeben, dass keine Bundle für eine Firmware-Aktualisierung verfügbar sind? ... 142
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? ... 142
OMIVV wird für die Aktualisierung der Intel-Netzwerkkarte mit Firmwareversion 13.5.2 nicht unterstützt ... 143
Die Aktualisierung der Intel-Netzwerkkarte von 14.5 oder 15.0 auf 16.x mit OMIVV kann aufgrund der Staging-Anforderung des DUP nicht erfolgreich durchgeführt werden ... 143
Nach einer Firmware-Aktualisierung mit einem ungültigen DUP wird als Status der Hardwareaktualisierung in der vCenter Konsole kein Fehler und auch nach mehreren Stunden keine Zeitüberschreitung gemeldet. In den LC-Aufforderungen wird der Status der Aufgabe jedoch als „Fehlgeschlagen“ gemeldet. Warum? ... 143
Warum zeigt das Administration-Portal nicht erreichbare Speicherorte für Aktualisierungs-Repositorys an? ... 143
Warum wurde mein System bei der Durchführung einer 1:n-Firmware-Aktualisierung nicht in den Wartungsmodus gesetzt? ... 143
Warum wird der globale Funktionszustand des Gehäuses noch als funktionsfähig angezeigt, obwohl der Status einiger Netzteile als kritisch gemeldet wird? ... 144
Warum wird auf der Seite „Systemüberblick“ in der Ansicht „Prozessor“ als Prozessorversion „nicht verfügbar“ angezeigt? ... 144
Warum wird eine Ausnahme zurückgegeben, wenn ich nach der Bearbeitung des Verbindungsprofils auf dem Web-Client auf „Fertigstellen“ klicke? ... 144
Warum werden die Verbindungsprofile, denen der Host zugeordnet ist, bei Erstellung/Bearbeitung eines Verbindungsprofils auf der Web-Benutzeroberfläche nicht angezeigt? ... 144
Warum ist das Feld „Hostfenster auswählen“ auf der Web-Benutzeroberfläche bei der Bearbeitung von Verbindungsprofilen leer? ... 144
Warum wird eine Fehlermeldung angezeigt, wenn ich auf den Firmware-Link klicke? ... 144
Welche Generation von Dell Servern konfiguriert und unterstützt OMIVV für SNMP-Traps? ... 145
Welche vCenter Server werden von OMIVV verwaltet? ... 145
Unterstützt OMIVV vCenter im verknüpften Modus? ... 145
Welche Porteinstellungen sind für OMIVV erforderlich? ... 145

Welche Mindestanforderungen gelten für die erfolgreiche Installation und den erfolgreichen Betrieb des virtuellen Geräts? 147
Das Kennwort des für die Bare-Metal-Erkennung verwendeten Benutzers wurde nicht geändert, obwohl das Hardwareprofil für den selben Benutzer erfolgreich angewendet wurde, dessen Anmeldeinformationen in der iDRAC-Benutzerliste geändert wurden. Warum 147
Warum kann ich die auf den vCenter Hosts und Clusterseiten aufgeführten Details zur neuen iDRAC-Version nicht anzeigen? 147
Wie teste ich Ereigniseinstellungen, indem ich mit OMSA Temperaturfehler an der Hardware simuliere? 148
OMSA-Agent ist auf dem OMIVV Hostsystem installiert. Trotzdem erhalte ich Fehlermeldungen, die darauf hinweisen, dass OMSA nicht installiert ist. Wie kann ich das Problem beheben? 148
Unterstützt OMIVV ESXi auch bei aktiviertem Sperrmodus? 148
Bei Verwendung des Sperrmodus ist ein Fehler aufgetreten 149
Welche Einstellung sollte ich für UserVars.CIMoeMProviderEnable mit ESXi 4.1 U1 verwenden? 149
Wie gehe ich vor, wenn die Erstellung des Hardwareprofils bei Verwendung von Referenzservern fehlschlägt? 149
Warum schlägt die Bereitstellung von ESXi auf Blade Server fehl? 149
Warum schlagen Hypervisor-Bereitstellungen auf PowerEdge R210-II-Maschinen fehl? 149
Warum werden automatisch ermittelte Systeme im Bereitstellungsassistent ohne Modellinformationen angezeigt? 149
Die NFS-Freigabe wurde mit ESXi-ISO eingerichtet, die Bereitstellung schlägt jedoch beim Laden des Freigabepfads fehl 149
Wie kann ich die Entfernung des virtuellen Geräts erzwingen? 150
Beim Eingeben eines Kennworts im Bildschirm „Jetzt sichern“ wird eine Fehlermeldung angezeigt 150
Wenn ich im vSphere-Web-Client auf das Dell Server Management-Portlet oder das Dell Symbol klicke, wird ein 404-Fehler ausgegeben 150
Wie gehe ich vor, wenn eine Firmware-Aktualisierung fehlschlägt? 150
Wie gehe ich vor, wenn die vCenter-Registrierung fehlgeschlagen ist? 150
Die Leistung ist während des Tests der Anmeldeinformationen im Verbindungsprofils langsam oder und die Anwendung reagiert nicht 151
Unterstützt OMIVV das VMware vCenter Server-Gerät? 151
Ich habe eine Firmware-Aktualisierung mit der Option „Beim nächsten Neustart anwenden“ ausgeführt und das System neu gestartet. Warum wurde die Firmware-Version nicht aktualisiert? 151
Warum wird der Host auch nach seiner Entfernung aus der vCenter-Struktur weiterhin unterhalb des Gehäuses angezeigt? 151
Warum wird in der Verwaltungskonsole das Feld Aktualisierungs-Repository-Pfad nicht auf den Standardpfad gesetzt, nachdem ich das Gerät auf die werkseitigen Einstellungen zurückgesetzt habe? 151
Warum werden die Alarm-Einstellungen nach Sicherung und Wiederherstellung von OMIVV nicht wiederhergestellt? 152
Probleme bei der Bare-Metal-Bereitstellung 152
Aktivieren der Auto-Ermittlung auf neu erworbenen Systemen 152

16 Zugehörige Dokumentation 153
Zugriff auf Dokumente der Dell Support-Website 153

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.

Was ist neu in dieser Version?

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

- Unterstützung für vSphere 6.5 und 6.0 U2
- Unterstützung für vSphere 6.5 Proactive HA und Anpassung des Schweregrads von Dell Host und Gehäusekomponenten
- Unterstützung für parallele Firmwareaktualisierungs-Jobs auf mehreren Clustern
- Unterstützung für die Integration mit vRealize-Vorgängen
- Unterstützung für OMSA 8.3 und OMSA 8.4
- Benachrichtigung zur Verfügbarkeit der aktuellen Version von OMIVV
- Unterstützung für bis zu 1000 Hosts mit einer einzelnen vCenter-Instanz oder mehreren vCenter
- Support für alle Plattformen der 13. Generation

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: • Serverdetails zu Dell PowerEdge, wie Speichermenge und -typ, NIC, PSU, Prozessoren, RAC, Serviceinformationen, Ansicht auf Server-, Cluster- und Rechenzentrumsebene • Gehäusedetails, wie z. B. Informationen zum Gehäuse-Verwaltungscontroller, Gehäusenetzteil, KVM-Status, Lüfter-/Wärmeinformationen, Serviceinformationen, Informationen zu Empty Switch/Server
Überwachen und Senden von Warnungen	Die Überwachung und die Warnmeldungen umfassen folgende Funktionalitäten: • Erkennen wichtiger Hardwarefehler und Durchführen virtualisierungsbezogener Maßnahmen (zum Beispiel Migrieren von Arbeitslasten oder Versetzen von Hosts in den Wartungsmodus). • Bereitstellung von zusätzlichen Informationen wie z. B. zum Bestand, zu Ereignissen, Alarmen zur Diagnose von Serverproblemen.
Firmware-Aktualisierungen	Aktualisieren von Dell-Hardware auf die aktuellste Version des BIOS und der Firmware.

Funktionen	Beschreibung
Bereitstellung	Erstellen von Hardwareprofilen, Hypervisor-Profilen und Remote-Bereitstellung des BS auf Bare-Metal-Servern von Dell PowerEdge unter Verwendung von VMware vCenter, ohne Einsatz von PXE.
Service-Informationen	Abrufen von Serviceinformationen für Dell Server und die zugehörigen Gehäuse aus der Dell Servicedatenbank und Ermöglichen einer einfachen Online-Serviceaktualisierung.
Sicherheitsrollen und Berechtigungen	Integration mit Standardauthentifizierung, -rollen und -berechtigungen von vCenter.

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

ANMERKUNG: Für vCenter ab Version 6.5 ist das OMIVV-Gerät nur für die Flash-Version verfügbar. Das OMIVV-Gerät ist nicht für die HTML5-Version verfügbar.

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)

Verwendung des Administration-Portal

Sie können mit dem Administrator-Portal folgende Aufgaben ausführen:

- Registrieren eines v Center-Servers. Siehe Registrieren eines v Center-Servers.
- Ändern von vCenter-Anmeldedaten. Siehe Ändern der vCenter Anmeldeinformationen.
- Aktualisierung von SSL-Zertifikaten. Siehe 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. Siehe Hochladen einer Lizenz zum Administration-Portal.
- OMIVV aktualisieren. Siehe Aktualisieren des Repository-Speicherorts des virtuellen Geräts und des virtuellen Geräts.
- Fehlerbehebungsbündel erstellen. Siehe Herunterladen des Fehlerbehebungsbündels.
- OMIVV neu starten. Siehe Virtuelles Gerät neu starten.
- Sichern und wiederherstellen. Siehe Aktualisieren des Geräts durch Sichern und Wiederherstellen.
- Warnungen konfigurieren. Siehe Einrichten globaler Alarme.

Registrieren eines vCenter Servers durch einen Nicht-Administratorbenutzer

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

Info über diese Aufgabe

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

Schritte

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 oder Ändern einer Rolle und dem Auswählen der Berechtigungen im vSphere-Webclient. Informationen zum Auswählen 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 Nicht-Administrator-Benutzer von vCenter Server mit den erforderlichen Berechtigungen kann jetzt vCenter registrieren und/oder die Registrierung aufheben, Anmeldeinformationen ändern oder das Zertifikat aktualisieren.

3. Registrieren Sie einen vCenter Server unter Verwendung eines Nicht-Administrator-Benutzers mit den erforderlichen Berechtigungen. Siehe Registrieren eines vCenter Servers unter Verwendung eines Nicht-Administrator-Benutzers mit den erforderlichen Berechtigungen.
4. Weisen Sie die Dell Berechtigungen der Rolle zu, die in Schritt 1 erstellt oder geändert wurde. Siehe Zuweisen von Dell Berechtigungen zur Rolle im vSphere-Webclient.

Jetzt kann ein Nicht-Administrator-Benutzer mit den erforderlichen Berechtigungen die OMIVV Funktionen mit den Dell 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:

- Funktionszustand-Update-Anbieter
  - Registrieren
  - Registrierung aufheben
  - Aktualisierung
- Host
  - CIM
    - CIM-Interaktion
  - Konfiguration
    - Erweiterte Einstellungen
    - Verbindung
    - Wartung
    - Abfragen von Patches
    - Sicherheitsprofil und Firewall

ANMERKUNG: Weisen Sie die folgenden Berechtigungen zu, wenn Sie VMware vCenter 6.5 verwenden:

* Host-Konfig.
  - Erweiterte Einstellungen
  - Verbindung
  - Wartung
  - Abfragen von Patches
  - Sicherheitsprofil und Firewall

– Bestandsaufnahme

* Hinzufügen von Hosts zu einem Cluster
* Hinzufügen von eigenständigen Hosts

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

Registrieren von vCenter Server durch Nicht-Administrator - Benutzer mit den erforderlichen Berechtigungen

Sie können einen vCenter Server für eine OMIVV Anwenndung durch einen Nicht-Administrator mit den entsprchenden Bereichtigungen registrieren lassen. Siehe Registrieren eines vCenter-Servers der Informationen zum Registrieren eines vCenter Server über einen Nicht-Administrator -Benutzer bzw. Administrator.

Dell Berechtigungen vorhandener Rolle zuweisen

Info über diese Aufgabe

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.

Schritte

1. Melden Sie sich mit Administratorrechten beim vSphere Web Client an.
2. Navigieren Sie im vSphere-Webclient zu **Verwaltung → Rollen**.
3. Wählen Sie ein vCenter Serversystem aus der Dropdownliste **Rollenanbieter** aus.
4. Wählen Sie die Rolle aus der Liste **Rollen** und klicken Sie auf das Symbol für klicken.
5. Wählen Sie die folgenden Dell Berechtigungen für die ausgewählte Rolle aus und klicken Sie 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 sind sofort wirksam. Der Benutzer mit erforderlichen Berechtigungen kann nun die OpenManage Integration for VMware vCenter Vorgänge ausführen.

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

Info über diese Aufgabe

Sie können die OMIVV-Geräte auch nach der Installation von OpenManage Integration for VMware vCenter registrieren. OpenManage Integration for VMware vCenter verwendet ein Administrator- oder anderes Benutzerkonto mit den erforderlichen Berechtigungen für vCenter Operations. OpenManage Integration for VMware vCenter unterstützt bis zu 1000 Hosts mit einer einzigen vCenter Instanz oder mehreren vCenter Servern im verknüpften Modus.

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

Schritte

1. Öffnen Sie das **Administration-Portal** von einem unterstützten Browser aus.

   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:\\<AppliancelP|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 die Registrierung von OMIVV am VMware vCenter mit dem FQDN (Fully Qualified Domain Name). 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 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.

Beispiel

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:\\<AppliancelP|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.

Info über diese Aufgabe

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:

Schritte

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:\\<AppliancelP|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

Info über diese Aufgabe

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.

Schritte

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:\\<AppliancelP|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. Um Proaktive HA zu deaktivieren, navigieren Sie zum Bildschirm Proaktive HA-Ausfälle und Antworten eines Clusters. Wählen Sie hierfür Konfigurieren → Dienste → vSphere Verfügbarkeit und klicken Sie dann auf Bearbeiten. 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

Info über diese Aufgabe

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:

Schritte

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:\\<AppliancelP|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

Info über diese Aufgabe

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:

Schritte

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:\\<AppliancelP|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

Info über diese Aufgabe

Führen Sie folgende Schritte durch:

Schritte

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

Voraussetzungen

Um sicherzustellen, dass alle Daten geschützt sind, führen Sie ein Backup der Datenbank OMIVV vor dem Aktualisieren des virtuellen Geräts aus. Siehe Verwalten von Backups und Wiederherstellungen.

Schritte

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

   ANMERKUNG: Das OMIVV-Gerät erfordert eine Internetverbindung zur Anzeige der verfügbaren Aktualisierungsmechanismen und der Durchführung der RPM-Aktualisierung. Stellen Sie sicher, dass das OMIVV-Gerät über eine Internetverbindung verfügt. Aktivieren Sie je nach Netzwerkeinstellungen den Proxy und geben Sie Proxy-Einstellungen an, wenn das Netzwerk einen Proxy benötigt. Siehe Einrichten des HTTP-Proxy.

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

   Für die verfügbare virtuelle Geräteversion werden die jeweiligen Aktualisierungsmechanismen für die RPM und OVF virtuelle Geräte mit einem Häkchen angezeigt. Im Folgenden werden die möglichen Optionen für Aktualisierungsmechanismen dargestellt, Sie können jeden der Tasks für den Aktualisierungsmechanismus durchführen:

   - Wenn ein Häkchen neben RPM angezeigt wird, können Sie kein RPM-Upgrade von der vorhandenen Version auf die neueste verfügbare Version durchführen. Lesen Sie Ein Upgrade von einer vorhandenen Version auf die neueste Version durchführen.
   - 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 Geräte-Version ausführen. Siehe Aktualisieren des Geräts über Backup und Wiederherstellung.
   - 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 RPM-Upgrade.
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 (PSK) aktualisieren.
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:

- Stellen Sie sicher, dass als **Aktualisierungs-Repository -Pfad** der Pfad http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ angegeben ist. 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**.
- Falls keine Internetverbindung besteht, laden Sie alle Dateien und Ordner vom Pfad http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ herunter und kopieren Sie sie auf eine HTTP-Freigabe. Klicken Sie im Fenster **Gerätemanagement** im Bereich **Geräteaktualisierung** auf **Bearbeiten**, und fügen Sie dann im Textfeld **Aktualisierungs-Repository -Pfad** den Pfad zur Offline-HTTP-Freigabe ein. 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: 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 in den Bereich Geräteaktualisierung. Prüfen Sie, ob die Versionen der verfügbaren und aktuellen virtuellen Geräte gleich sind.

Aktualisieren des Geräts durch Sichern und Wiederherstellen

Info über diese Aufgabe

Führen Sie die folgenden Schritte aus, um das OMIVV-Gerät von OMIVV-Version x auf die Version y zu aktualisieren:

Schritte

1. Sichern Sie die Datenbank für die ältere Version.
2. Fahren Sie das ältere OMIVV-Gerät von vCenter herunter.

   ANMERKUNG: Heben Sie die Registrierung des OMIVV-Plug-ins in 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 die neue OpenManage Integration Version y OVF bereit.
4. Starten Sie das OpenManage Integration Version y-Gerät.
5. Richten Sie für die Version und das Gerät das Netzwerk, die Zeitzone usw ein.

   ANMERKUNG: Stellen Sie sicher, dass die neue OpenManage Integration Version y-Gerät 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 Gerät der y-Version 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. Stellen Sie die Datenbank auf dem neuen OMIVV-Gerät wieder her. Siehe Wiederherstellen der Datenbank aus einem Backup.
7. Überprüfen Sie das Gerät. Siehe Installationsprüfung im *Installationshandbuch zu OpenManage Integration for VMware vCenter*, das unter Dell.com/support/manuals bereitgestellt wird.
8. Führen Sie die **Bestandsaufnahme** auf allen registrierten vCenter-Servern aus.

   ANMERKUNG: Dell empfiehlt, dass Sie nach der Aktualisierung die Bestandsaufnahme auf allen durch das Plug-in verwalteten Hosts durchführen. Informationen zur Ausführung des Bestandsaufnahme-Befehls finden Sie unter Planen von Bestandsaufnahme-Jobs.

   ANMERKUNG: Wenn die IP-Adresse der neuen OMIVV-Version y von der OMIVV-Version x abweicht, muss das Trap-Ziel der SNMP-Traps neu konfiguriert werden, um auf das neue Gerät zu verweisen. Für Server der 12. Generation und höher wird das Problem durch das Ausführen der Bestandsaufnahme auf diesen Hosts behoben. Bei Hosts vor der 12. Generation, die mit früheren Versionen kompatibel waren, wird diese IP-Änderung als nicht konform angezeigt, und Sie werden aufgefordert, Dell OpenManage Server Administrator (OMSA) zu konfigurieren. Zum Beheben von Konformitätsproblemen bei vSphere-Hosts lesen Sie Ausführen des Assistenten zum Beheben nicht konformer vSphere-Hosts.

Herunterladen des Fehlerbehebungsbündels

1. Klicken Sie unter **GERÄTEMANAGEMENT** auf **Fehlerbehebungsbündel erstellen**.
2. Klicken Sie auf den Link **Fehlerbehebungsbündel 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 **Apply (Anwenden)**.

NTP-Server (Network Time Protocol) einrichten

Info über diese Aufgabe

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

Schritte

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

Info über diese Aufgabe

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
Small (Klein)	bis zu 250	2	8
Mittel	bis zu 500	4	16
Large (Groß)	bis zu 1000	8	32

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.

Schritte

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

Voraussetzungen

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

Info über diese Aufgabe

Das Erzeugen einer Zertifikatsignierungsanforderung (CSR) verhindert, dass Zertifikate mit zuvor erstellten CSR auf das Gerät hochgeladen werden. Zum Erstellen einer CSR führen Sie Folgendes aus:

Schritte

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 können. Klicken Sie zum Fortfahren 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

Voraussetzungen

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

Info über diese Aufgabe

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 Verwaltungskonsole 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.

Schritte

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 müssen.

Wiederherstellen des standardmäßigen HTTPS-Zertifikats

Info über diese Aufgabe

ANMERKUNG: Wenn Sie ein benutzerdefiniertes Zertifikat für Ihr Gerät hochladen möchten, müssen Sie das neue Zertifikat vor der vCenter-Registrierung hochladen. Wenn Sie das neue benutzerdefinierte Zertifikat nach der vCenter-Registrierung hochladen, werden Kommunikationsfehler im Web-Client angezeigt. Um dieses Problem zu beheben, müssen Sie die Registrierung aufheben und das Gerät erneut im vCenter registrieren.

Schritte

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

Info über diese Aufgabe

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

Schritte

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:\\<AppliancelP|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

Info über diese Aufgabe

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.

Schritte

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.

Info über diese Aufgabe

ANMERKUNG: NTP-Einstellungen werden nicht gespeichert und wiederhergestellt.

Schritte

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

Nächste Schritte

Konfigurieren Sie nach diesem Verfahren einen Backup-Zeitplan.

Planen von automatischen Backups

Info über diese Aufgabe

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

Schritte

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 **Apply (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

Info über diese Aufgabe

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

Schritte

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

Schritte

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 im Register **Objekt Aktion → Konsole öffnen** aus.
   - Rechtsklicken Sie die ausgewählte virtuelle Maschine und wählen Sie dann **Konsole öffnen**.

Nächste Schritte

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

Info über diese Aufgabe

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

Schritte

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

Info über diese Aufgabe

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

Schritte

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`.

Virtuelles Gerät auf werkseitige Einstellungen zurücksetzen

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 werkseitigen Einstellungen 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 Geräte verwalten und überwachen, die Sie an vCenter-Servern registrieren, die zum gleichen Plattform Service Controller (PSK) gehören und die gleiche vCenter Version haben.

Voraussetzungen

Dell empfiehlt, dass Sie eine globale Aktualisierung durchführen, wenn die Seite im Cache gespeichert wird.

Schritte

1. Klicken Sie auf der Startseite des VMware vCenters auf das Symbol **OpenManage Integration.**
2. Klicken Sie im **Navigator** unter der Gruppe **Dell** 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 eine Verknüpfung unter Verwendung der IP-Adresse oder FQDN für jedes OMIVV-Gerät an. Klicken Sie zum Anzeigen und Überwachen gerätespezifischer Informationen auf einen bestimmten Gerätenamen-Link. Durch Klicken auf einen Gerätenamen-Link gelangen Sie zum Hauptinhaltsbereich des OMIVV-Geräts. Sie können die OMIVV-Vorgänge verwalten und die 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:

     1. Klicken Sie in OpenManage Integration for VMware vCenter auf das Register **Hilfe und Support**.
     2. 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 Plugin kompatibel 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 vCenter an, auf die Sie aus der angemeldeten Sitzung heraus zugreifen können und die an Geräten registriert sind. Wenn Sie ein Gerät an mehreren vCentern registrieren, werden die vCenter in einer erweiter- und reduzierbaren Liste angezeigt. Klicken Sie auf einen vCenter-Link, um zur Seite **vCenter Server** zu gelangen, wo alle vCenter im Navigatorbereich aufgeführt werden.

4

Aufrufen der OpenManage-Integration aus dem Webclient

Wenn Sie sich nach der Installation von OMIVV am VMware vCenter anmelden und auf die Startseite und die Registerkarte **Start** gelangen, befindet sich das Symbol der **OpenManage Integration** im Hauptinhaltsbereich unter der Gruppe **Administration**. Verwenden Sie das Symbol der **OpenManage Integration**, um zur Seite **OpenManage Integration for VMware vCenter** zu gelangen. Die Gruppe **Dell** wird im **Navigator**-Bereich angezeigt.

Das VMware vCenter-Layout enthält die folgenden drei Abschnitte:

Tabelle 3. OpenManage Integration for VMware vCenter-Abschnitte

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

Navigieren im VMware vCenter-Webclient

Die **OpenManage Integration for VMware vCenter** befindet sich in einer speziellen **Dell** 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.
   - Hosts, Rechenzentren und Cluster im Navigator-Bereich unter **vCenter-Bestandsaufnahmeliste** überwachen. Wählen Sie den Host, das Rechenzentrum oder den Cluster aus, den Sie überprüfen möchten, und wählen Sie dann die Registerkarte **Objekte** aus, und klicken Sie 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
	Aktivieren des WBEM-Service

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 Hosts

Wenn Sie schnell nur Dell-Hosts ansehen möchten, können Sie dies von innerhalb der Dell OpenManage Integration for VMware vCenter tun, indem Sie im Navigator **Dell-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-Hosts**.
3. Auf der Registerkarte **Dell-Host** können Sie folgende Informationen einsehen:
   - **Hostname** – Zeigt einen Link an, der die IP-Adresse für jeden Dell-Host verwendet. Klicken Sie zum Anzeigen von Dell Host-Informationen auf einen bestimmten Hostlink.

- **vCenter** – Zeigt die IP-Adresse von vCenter für diesen Dell-Host an.
- **Cluster** – Zeigt den Clusternamen an, wenn der Dell-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: • **OpenManage Integration for VMware vCenter – Hilfe** – Stellt einen Link zur Produkthilfe bereit, die sich im Produkt befindet. Verwenden Sie das Inhaltsverzeichnis oder Suche, um die Hilfe, die Sie brauchen, zu finden. • **Info** – Dieser Link zeigt das Dialogfeld **Versionsinformationen** an. Sie können die Produktversion hier einsehen.
Dell Handbücher	Stellt Live-Links für Folgendes bereit:

Name	Beschreibung
	· **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 Fehlerbehebungsbündels bereit. Stellen Sie dieses Bündel bereit, oder betrachten Sie es, wenn Sie mit dem technischen Support Kontakt aufnehmen. Weitere Informationen finden Sie unter Herunterladen eines Fehlerbehebungsbündels.
Dell empfiehlt	Stellt einen Link zum 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

Info über diese Aufgabe

Sie können das Fehlerbehebungspaket für eine leichtere Fehlerbehebung verwenden oder um Informationen an den technischen Support zu senden. Zum Aufrufen der Fehlerbehebungsinformationen führen Sie folgende Schritte aus:

Schritte

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 für den Reset des iDRAC auf der Registerkarte **Hilfe und Support**. Der Reset des iDRAC führt einen normalen iDRAC-Neustart durch. Der iDRAC-Neustart startet den Host nicht neu. Nach der Ausführung eines Reset dauert es bis zu 2 Minuten, zu einem verwendbaren Zustand zurückzukehren. Verwenden Sie Reset in Fällen, in denen der iDRAC in der OpenManage Integration for VMware vCenter nicht reagiert.

Info über diese Aufgabe

ANMERKUNG: Dell empfiehlt, dass Sie den Host in den Wartungsmodus versetzen, bevor Sie ein Reset von iDRAC ausführen. Sie können diese Reset-Aktion auf einem Host ausführen, der Teil eines Verbindungsprofils ist, das mindestens einmal in einer Bestandsaufnahme aufgenommen wurde. Die Reset-Aktion bringt den iDRAC evtl. nicht in einen verwendbaren Zustand zurück. In diesem Fall ist ein harter Reset erforderlich. Weitere Informationen über einen harten Reset finden Sie in Ihrer 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.

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

Schritte

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-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.
- Globale Einstellungen über die Art der Speicherung von Warnungen für alle vCenter-Instanzen konfigurieren. 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

Protokollinformationen	Beschreibung
	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. Auf der Registerkarte **Protokoll** können Sie die Benutzermaßnahmenprotokolle für OpenManage Integration for VMware vCenter anzeigen. Weitere Informationen zu den angezeigten Protokollen finden Sie unter Protokollverlauf.
3. Klicken Sie auf die Spaltenüberschrift, um die Daten im Gitter zu sortieren.
4. Um nach Kategorien oder Zeitblöcken zu sortieren, verwenden Sie die dem Gitter 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. Klicken Sie zum Exportieren einer von Inhalt in eine CSV-Datei in der rechten unteren Ecke des Bildschirms auf das Symbol für .
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 **Save (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. Diese Standard-Test-Lizenz ist nur für Dell Server ab der 11. Generation verfügbar und ist 90 Tage lang gültig.
- 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 Store 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 eine Lizenz erwerben, können Sie die XML-Datei (Lizenzschlüssel) über den Dell Digital Store herunterladen. Wenn Sie einen Lizenzschlüssel nicht herunterladen können, wenden Sie sich an den Dell Support. Die Telefonnummer für das regionale Dell Supportteam für Ihr Produkt finden Sie auf www.dell.com/support/softwarecontacts.

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.

Info über diese Aufgabe

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

Schritte

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 Store heruntergeladen haben, an einem bekannten Speicherplatz.
3. Geben Sie die Verwaltungskonsolen-URL in einen Web-Browser ein.
   Verwenden Sie dieses 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 sein (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.

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.
- Auswählen der vCenter OMIVV_UG Auswählen von vCenter
- Erstellen eines neuen Verbindungsprofils OMIVV_UG Erstellen eines neuen Verbindungsprofils
- Konfigurieren von Ereignissen und Alarmen Siehe Konfigurieren von Ereignissen und Alarmen.
- Planen von Bestandsaufnahme-Jobs Finden Sie im Planen von Jobs zum Erstellen von Bestandsaufnahmen.
- So führen Sie einen Garantieabfrage-Job aus: OMIVV_UG 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

Info über diese Aufgabe
Im Dialogfeld **vCenter-Auswahl** können Sie die folgenden vCenter konfigurieren:

- Ein spezifisches vCenter

- Alle registrierten vCenter

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

Schritte

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 aus, das noch nicht konfiguriert wurde, oder falls Sie Ihrer Umgebung ein neues 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 Sie die Konfiguration eines einzelnen vCenters ausgewählt haben, müssen Sie die Schritte 1 bis 3 wiederholen, bis Sie jedes vCenter konfiguriert haben.

Verbindungsprofil erstellen

Voraussetzungen

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.

Info über diese Aufgabe

Ein Verbindungsprofil speichert die iDRAC- und Host-Anmeldeinformationen, die OMIVV für die Kommunikation mit Dell-Servern verwendet. Jeder Dell-Server muss einem Verbindungsprofil zugeordnet sein, das von OMIVV verwaltet werden kann. Sie können mehrere Server einem einzelnen Verbindungsprofil zuweisen. Sie können das Verbindungsprofil unter Verwendung des Konfigurationsassistenten oder von der Registerkarte **OpenManage Integration for VMware vCenter** → **Einstellungen** aus 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.

Auf allen Hosts, auf denen ESXi 6.5 oder höher ausgeführt wird, ist der Web-Based Enterprise Management (WBEM)-Service standardmäßig deaktiviert. OMIVV erfordert für die Kommunikation mit dem Host, dass dieser Service ausgeführt wird. Dieser Service kann über den Verbindungsprofil-Assistenten aktiviert werden. OMIVV verwendet den WBEM-Service zum ordnungsgemäßen Synchronisieren der ESXi Host- und iDRAC-Beziehungen.

Schritte

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, Anwendung von Hardware-Profilen und die Bereitstellung des Hypervisors.

   - Für iDRACs, auf denen Sie Active Directory benutzen möchten, und die für Active Directory bereits konfiguriert und aktiviert wurden, wählen Sie **Active Directory verwenden** aus. Anderenfalls gehen Sie nach unten, um die iDRAC-Anmeldeinformationen zu konfigurieren.

     1. Geben Sie unter „Active Directory“ im Feld **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.
     2. Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.

3. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
4. 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:
  1. Geben Sie im Textfeld **Benutzername** den Benutzernamen ein. Der Benutzername darf maximal 16 Zeichen enthalten. Weitere Informationen zu Benutzernamen-Einschränkungen für die von Ihnen verwendete Version von iDRAC finden Sie in der iDRAC-Dokumentation.
  2. Geben Sie im Textfeld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 20 Zeichen enthalten.
  3. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
  4. 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:
     1. Geben Sie in Active Directory unter **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 druckbaren Zeichen
        - Keine ungültigen Zeichen wie: " / \ [ ] : ; | = , + * ? < > @

        Host-Domänen-Anforderungen:
        - Zwischen 1 und 64 Zeichen lang
        - Das erste Zeichen muss ein alphabetisches Zeichen sein.
        - Es kann kein Leerzeichen enthalten.
        - Keine ungültigen Zeichen wie: " / \ [ ] : ; | = , + * ? < > @
     2. Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
     3. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
     4. 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:
     1. Im Textfeld **Benutzername** ist der Benutzername `root`. Dies ist der Standardbenutzername, und Sie können den Benutzernamen nicht ändern. Falls das Active Directory jedoch eingestellt ist, können Sie einen beliebigen Active Directory-Benutzer auswählen, und nicht root.
     2. Geben Sie im Textfeld **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.

3. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
4. 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**.

   ANMERKUNG: Wenn Sie Hosts auswählen, auf denen ESXi 6.5 oder höher ausgeführt wird, stellen Sie sicher, dass Sie auf das Symbol klicken, um den WBEM-Dienst auf allen diesen Hosts zu aktivieren.
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 oder nicht. Dieser Schritt ist zwar optional, Dell empfiehlt jedoch, dass Sie das Verbindungsprofil prüfen.

   ANMERKUNG: Die Testverbindung schlägt fehl, wenn der WBEM-Dienst für Hosts mit ESXi 6.5 oder höher nicht aktiviert ist.
8. Zur Erstellung des Profils klicken Sie auf **Weiter**.

   Sobald Sie auf „Weiter“ klicken, werden alle Details, die Sie in diesen Assistenten eingegeben haben, gespeichert und Sie können sie nicht mehr über den Assistenten ändern. Sie können mehr Verbindungsprofile für dieses vCenter-Detail auf der Seite **Verwalten** → **Profile Verbindungsprofile** ändern oder erstellen, nachdem die Konfiguration über den Konfigurationsassistenten abgeschlossen ist. Siehe Ändern von Verbindungsprofilen.

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.

Planen von Bestandsaufnahme-Jobs

Info über diese Aufgabe

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, empfiehlt Dell, dass Sie einen regelmäßigen Bestandsaufnahme-Job planen. Der Bestandsaufnahme-Job erfordert nur minimale Ressourcen und wirkt sich nicht negativ auf die Hostleistung aus.

ANMERKUNG: Das Gehäuse wird automatisch erkannt, nachdem 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.

Schritte

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 Next (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.

Ausführen von Serviceabfrage-Jobs

Info über diese Aufgabe

Die Konfiguration des Serviceabfrage-Jobs ist in der Einstellungsoption in OMIVV verfügbar. Darüber hinaus können Sie den Serviceabfrage-Job auch über **Job-Warteschlange** → **Service** ausführen. Geplante Jobs werden in der Job-Warteschlange aufgelistet. In einer SSO-Umgebung mit mehreren vCenter-Servern wird der Gehäuse-Service automatisch mit jedem vCenter ausgeführt, wenn der Service für ein beliebiges vCenter ausgeführt wird. Der Service wird jedoch nicht automatisch ausgeführt, wenn er nicht zu einem Gehäuse-Profil 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 Garantieabfrage-Job konfiguriert haben, stellen Sie sicher, dass Sie diesen Zeitplan-Garantieabfrage-Job auf dieser Seite vor Abschluss der Assistentenfunktionen replizieren, damit die vorherige Garantieabfrage nicht durch die Standardeinstellungen außer Kraft gesetzt wird.

Schritte

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.

      Die Zeit, die Sie eingeben, ist Ihre lokale Zeit. 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.

   Sobald Sie auf Weiter klicken, werden alle Details, die Sie in diesen Assistenten eingegeben haben, gespeichert und Sie können sie nicht mehr über den Assistenten ändern. Sie können die Zeitpläne für die Service-Jobs auf der Registerkarte **Einstellungen** ändern, nachdem die Konfiguration über den Konfigurationsassistenten abgeschlossen ist. Siehe Ändern von Service-Jobzeitplänen.

Konfigurieren von Ereignissen und Alarmen

Sie können Ereignisse und Alarme unter Verwendung des **Erstkonfigurationsassistenten** oder der Registerkarte **Einstellungen** für Ereignisse und Alarme einrichten. Zum Erhalt der Server-Ereignisse ist OMIVV als das Trap-Ziel konfiguriert. Bei Hosts ab der 12. Generation muss das SNMP-Trap-Ziel in iDRAC festgelegt werden. Bei Hosts vor der 12. Generation muss das Trap-Ziel in OMSA festgelegt werden.

Info über diese Aufgabe

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.

Schritte

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. Aktivieren Sie **Alarme für Dell Hosts aktivieren**, um alle Hardware-Alarme und -ereignisse zu aktivieren.

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

   Das Dialogfeld **Aktivieren der Dell 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 Hosts aktivieren ausgewählt wurde.
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 Änderung übernommen wird.

   ANMERKUNG: Nach dem Wiederherstellen des Geräts werden die Einstellungen für die Ereignisse und Alarme nicht aktiviert, selbst wenn sie von der grafischen Benutzeroberfläche als aktiviert angezeigt werden. Sie können die Einstellungen für die Ereignisse und Alarme auf der Registerkarte Einstellungen erneut aktivieren.
5. Klicken Sie auf **Apply (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 **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. Um Serviceablaufschwellenwerte für eine Warnung über das Ablaufen des Service zu konfigurieren, klicken Sie auf das Symbol für rechts neben **Serviceablaufbenachrichtigung**.
4. Verfahren Sie im Dialogfeld **Serviceablaufbenachrichtigung** wie folgt:

a. Falls Sie diese Einstellung aktivieren möchten, wählen Sie **Serviceablaufbenachrichtigung für Hosts aktivieren** aus.

   Das Wählen des Kontrollkästchens aktiviert die Garantieablaufbenachrichtigung.

b. Verfahren Sie unter **Mindesttageschwellenwertalarm** wie folgt:

   1. Wählen Sie in der Drop-Down-Liste **Warnung** den zeitlichen Abstand in Tagen aus, mit dem Sie vor Ablauf des Service gewarnt werden wollen.
   2. 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 **Apply (Anwenden)**.

Repository für die Firmwareaktualisierung einrichten

Info über diese Aufgabe

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

Schritte

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Einstellungen** → **Verwalten** unter **Geräteeinstellungen** auf der rechten Seite des **Repository für die Firmwareaktualisierung** auf das Symbol für klicken.

2. Wählen Sie im Dialogfeld **Repository für die Firmware-Aktualisierung** eine der folgenden Optionen aus:

- **Dell Online** – Sie erhalten Zugriff auf den Speicherort, der das Repository zur Firmware-Aktualisierung von Dell (ftp.dell.com) verwendet. OpenManage Integration for VMware vCenter lädt die ausgewählten Firmware-Aktualisierungen von 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 des 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.

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

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

ANMERKUNG: Es kann bis zu 20 Minuten ab Lesen des Katalog von der Quelle und aktualisieren der OMIVV-Datenbank dauern.

Konfigurieren der Benachrichtigung über aktuelle Geräteversion

Info über diese Aufgabe

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:

Schritte

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.

Info über diese Aufgabe

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.

Schritte

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

Voraussetzungen

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*.

Info über diese Aufgabe

ANMERKUNG: OMSA wird nur auf Dell PowerEdge-Servern bis zur 11. Generation benötigt.

Schritte

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 Sie, ob der OMSA-Konsolenlink im Abschnitt **Dell Host-Information** aktiv ist.

Konfigurieren von Ereignissen und Alarmen

Info über diese Aufgabe

Im Dialogfeld „Ereignisse und Alarme“ im Dell Management Center werden alle Hardware-Alarme aktiviert oder deaktiviert. 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 im vCenter unter **Einstellungen** die Überschrift **Ereignisse und Alarme**, um die vCenter-Alarme für Dell Hosts (aktiviert oder deaktiviert) und die Ereignisanzeigeebene anzuzeigen.

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.

Schritte

1. Erweitern Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Einstellungen** unter **vCenter Einstellungen Ereignisse und Alarme**.

   Die aktuellen **vCenter Alarme für Dell Hosts** (aktiviert oder deaktiviert) oder alle vCenter Alarme und die **Ereignisanzeigeebene** werden angezeigt.
2. Klicken Sie auf das Symbol rechts neben **Ereignisse und Alarme**.
3. Aktivieren Sie **Alarme für alle Dell-Hosts aktivieren**, um alle Hardware-Alarme und -Ereignisse zu aktivieren.

   ANMERKUNG: Die Dell-Hosts mit aktivierten Alarmen reagieren auf kritische Ereignisse, indem sie in den Wartungsmodus übergehen, und 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.

   Dieser Schritt kann bis zu einer Minute dauern, bis die Änderung in Kraft tritt und ist nur verfügbar, wenn **Alarme für Dell 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.

7

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.

Informationen zum Verbindungsprofil

Über die Registerkarte **Verbindungsprofile** können Sie die Verbindungsprofile verwalten und konfigurieren, die die Anmeldeinformationen enthalten, die durch das virtuelle Gerät für die Kommunikation mit Dell Servern verwendet werden. Ordnen Sie jedem Dell Server nur ein Verbindungsprofil für die Verwaltung durch OpenManage Integration for VMware vCenter zu. Sie können mehrere Server einem einzelnen Verbindungsprofil zuweisen. Nach der Ausführung des **Erstkonfigurationsassistenten** können Sie die Verbindungsprofile in OpenManage Integration for VMware vCenter mithilfe folgender Tasks 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 Sie ein oder mehrere Verbindungsprofile erstellt haben, können Sie diese auf der Seite **Verbindungsprofil** anzeigen. OpenManage Integration for VMware vCenter verwendet in den Profilen angegebene Anmeldeinformationen, um mit Dell-Hosts zu kommunizieren.

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, die diesem Verbindungsprofil zugeordnet sind. Wenn es mehr als einen gibt, können sie das Erweiterungssymbol verwenden, um alle anzuzeigen.
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

Felder der Verbindungsprofile	Beschreibung
Date Created (Erstellungsdatum)	Zeigt das Datum an, an dem das Verbindungsprofil erstellt wurde
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

Info über diese Aufgabe

Sie können einem einzelnen Verbindungsprofil mehrere Hosts zuweisen. Erstellen Sie ein Verbindungsprofil mit Hilfe der folgenden Schritte:

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

Auf allen Hosts, auf denen ESXi 6.5 oder höher ausgeführt wird, ist der Web-Based Enterprise Management (WBEM)-Service standardmäßig deaktiviert. OMIVV erfordert für die Kommunikation mit dem Host, dass dieser Service ausgeführt wird. Dieser Service kann über den Verbindungsprofil-Assistenten aktiviert werden. OMIVV verwendet den WBEM-Service zum ordnungsgemäßen Synchronisieren der ESXi Host- und iDRAC-Beziehungen.

Schritte

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Profile** → **Anmeldeprofile** → **Verbindungsprofile** auf das Symbol für ✚ klicken.
2. Klicken Sie auf der **Startseite** 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 aus der Dropdownliste aus, für die das Profil erstellt werden sollen.
      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 Textfeld **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. Weitere Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zu 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 im Textfeld **Benutzername** den Benutzernamen ein. Der Benutzername darf maximal 16 Zeichen enthalten. Weitere Informationen zur Benutzername-Einschränkungen 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 im Textfeld **Kennwort** das 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 Textfeld **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. Weitere Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zu 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 **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 das Symbol für wählen Sie die Hosts und klicken Sie dann auf **OK**.

ANMERKUNG: Wenn Sie Hosts auswählen, auf denen ESXi 6.5 oder höher ausgeführt wird, stellen Sie sicher, dass Sie auf das Symbol klicken, um den WBEM-Dienst auf allen diesen Hosts zu aktivieren.

7. Um das Verbindungsprofil zu prüfen, wählen Sie einen oder mehrere Hosts aus und klicken Sie auf das Symbol für **Verbindung testen**.

   ANMERKUNG: Dieser Schritt ist optional und überprüft, ob die Host- und iDRAC-Anmeldeinformationen korrekt sind oder nicht. Dieser Schritt ist zwar optional, Dell empfiehlt jedoch, dass Sie das Verbindungsprofil prüfen.

   ANMERKUNG: Die Testverbindung schlägt fehl, wenn der WBEM-Dienst für Hosts mit ESXi 6.5 oder höher nicht aktiviert ist.

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**.

Ändern von Verbindungsprofilen

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

Info über diese Aufgabe

ANMERKUNG: Die vCenter, die während dieses Vorgangs angezeigt werden, wurden mit derselben Single Sign On (SSO) authentifiziert. Falls Sie keinen vCenter-Host sehen, befindet er 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.

Schritte

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 das Symbol klicken.
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. Lesen Sie den obigen Hinweis dazu, warum die Hosts hier angezeigt werden.

   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 Textfeld **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: Domäne\Benutzername oder Domäne/Benutzername oder benutzername@domäne. Der Benutzername darf maximal 256 Zeichen enthalten. Weitere Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zu 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 Domäne darf nur alphanumerische Zeichen enthalten wie – (Bindestrich) und . (Punkt) (Begrenzung auf 254 Zeichen). Das erste und letzte Zeichen der Domäne 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 deaktiviert. 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 und dieser Eintrag kann nicht geändert werden, wenn Sie nicht die Option Active Directory verwenden auswählen. Es ist nicht erforderlich, dass der iDRAC-Benutzer die root-Anmeldeinformationen verwendet. Es kann sich um jeden Benutzer mit Administrator-Berechtigungen handeln, falls das Active Directory eingestellt ist.

- **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 deaktiviert. 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. Klicken Sie auf **OK**.

   Im Dialogfeld **Zugeordneter Host** können Sie die iDRAC- und die Host-Anmeldeinformationen auf den ausgewählten Servern testen.

   ANMERKUNG: Wenn Sie Hosts auswählen, auf denen ESXi 6.5 oder höher ausgeführt wird, stellen Sie sicher, dass Sie auf das Symbol klicken, um den WBEM-Dienst auf allen diesen Hosts zu aktivieren.
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 **Verbindung testen**. Die anderen Optionen sind inaktiv.

  ANMERKUNG: Die Testverbindung schlägt fehl, wenn der WBEM-Dienst für Hosts mit ESXi 6.5 oder höher nicht aktiviert ist.

  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 beinhalten Änderungen, die Sie über die Webclient-Oberfläche an einem Verbindungsprofil durchführen. Änderungen, die das OMIVV-Gerät an dem entsprechenden Verbindungsprofil durchführt, haben keinen Einfluss auf diese beiden Felder.

Löschen von Verbindungsprofilen

Info über diese Aufgabe

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.

Schritte

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 das Symbol ✖.
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.

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 **Verbindung testen**.

   Wenn Sie kein Verbindungsprofil auswählen, dauert der Test einige Zeit.
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.

Informationen zum Gehäuseprofil

OMIVV kann alle mit den durch OMIVV verwalteten Dell Servern verbundenen Dell Gehäuse überwachen. Für die Überwachung des Gehäuses wird ein Gehäuse-Profil benötigt. Sie können das Gehäuseprofil durch Ausführung folgender Aufgaben verwalten:

- Anzeigen des Gehäuseprofils. Siehe Anzeigen des Gehäuseprofils.
- Erstellen eines Gehäuseprofils. Siehe Erstellen eines Gehäuseprofils.
- Bearbeiten eines Gehäuseprofils. Siehe Bearbeiten eines Gehäuseprofils.
- Löschen eines Gehäuseprofils. Siehe Löschen eines Gehäuseprofils.

- Testen eines Gehäuseprofils. Siehe Testen eines Gehäuseprofils.

Anzeigen von Gehäuseprofilen

Voraussetzungen

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

Info über diese Aufgabe

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

Schritte

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
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. Ein Gehäuse-Anmeldeinformationenprofil kann erstellt und einem einzelnen oder mehreren Gehäusen zugeordnet werden.

Info über diese Aufgabe

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

Schritte

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 für 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 Anmeldedaten kann es sich um lokale oder um Active Directory-Anmeldeinformationen handeln. Bevor Sie die Active Directory-Anmeldeinformationen mit einem Gehäuse-Profil zusammen verwenden, muss das Active Directory-Benutzerkonto in Active Directory vorhanden sein, und der Gehäuse-Verwaltungscontroller muss für die Active Directory-basierte Authentifizierung konfiguriert sein.

6. Klicken Sie auf **Next (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, eine Verbindung zwischen Gehäuse A und **Test 1** herzustellen, wird eine Warnmeldung angezeigt.

8. Klicken Sie auf **OK**.

   Die Seite **Zugeordnete Gehäuse** wird angezeigt.

9. Wählen Sie das Symbol **Verbindung testen** 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, dass Sie im Feld **Kennwort überprüfen** eingeben, muss das gleiche wie das im Feld **Kennwort** eingegebene sein. Die eingegebenen Anmeldeinformationen müssen Administratorrechte am Gehäuse besitzen.

7. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

   Mit der Registerkarte **Zugeordnetes Gehäuse** können Sie das Gehäuse und die Anmeldeinformationen auf dem ausgewählten Gehäuse testen. Führen Sie einen der folgenden Schritte durch:

   - Um den Test zu beginnen, wählen Sie entweder ein einzelnes Gehäuse oder mehrere Gehäuse zum Prüfen aus, und klicken Sie anschließend auf das Symbol **Verbindung testen**. Die Spalte **Testergebnis** zeigt an, ob die Testverbindung erfolgreich war.
   - 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 die Service-Tag-Nummer angezeigt. Die Felder Gehäusename und Modell werden angezeigt, sobald das Gehäuse inventarisiert ist.

Löschen von Gehäuseprofilen

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 das Symbol für .

   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 Gehäuse-Profil zugeordneten Gehäuse-Profile gelöscht oder zu anderen Profilen verschoben wurden, wird eine Bestätigungsmeldung über das Löschen angezeigt, die besagt, dass das Gehäuse-Profil keine zugeordneten Gehäuse aufweist und gelöscht wird. Klicken Sie auf **OK**, um das Gehäuse-Profil 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.

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 **Verbindung testen**.
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.

8

Bestandsaufnahme. und Service-Management

Nach der Konfiguration von OMIVV können Sie die Bestandsaufnahme, Service-Jobs, Bereitstellungsverwaltungs-Jobs und die Jobs zur Verwaltung von Firmwareaktualisierungen in der Registerkarte **Überwachen** überwachen. Die Bestandsaufnahme und der Service werden im **Erstkonfigurationsassistenten** 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 über die OMIVV Administration Console erneut aktivieren.

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

Zum Sammeln der Daten ist eine erfolgreich beendete Bestandsaufnahme erforderlich. Nachdem die Bestandsaufnahme beendet ist, können Sie die Bestandsaufnahmeergebnisse für das ganze Datacenter oder für ein einzelnes Hostsystem anzeigen. Sie können die Reihenfolge der Spalten der Bestandsaufnahmeansicht absteigend und/oder aufsteigend sortieren.

Info über diese Aufgabe

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 Server der 12. Generation von Dell PowerEdge-Servern und später, und Sie müssen deshalb 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:

Schritte

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. Die Optionen beinhalten: · 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 abgeschlossene Bestandsaufnahme ist erforderlich, um die Daten zu sammeln. Sie können die Spalten mit der Ansicht „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
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 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

Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme

Um sicherzustellen, dass die aktuellen Host-Informationen vorliegen, sollten Sie das Erstellen einer Bestandsaufnahme mindestens einmal wöchentlich planen. Das Erstellen einer Bestandsaufnahme erfordert nur minimale Ressourcen und wirkt sich nicht negativ auf die Hostleistung aus. Sie können den Bestandsaufnahme-Jobzeitplan auf der Registerkarte **Erstkonfigurationsassistent** oder **Überwachen** ändern.

Info über diese Aufgabe

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.

Schritte

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 und klicken Sie dann auf das Symbol für .
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 for VMware vCenter auf der Registerkarte **Überwachen → Job-Warteschlange** auf **Bestandsaufnahmenverlauf → Host-Bestandsaufnahme**.

7. Klicken Sie auf Klicken Sie im Dialogfeld **Erfolg** auf **Schließen**.

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

Nach der Planung eines sofortigen Bestandsaufnahmejobs gelangt dieser sofort in eine Warteschlange. Sie können keine Bestandsaufnahme für einen einzelnen Host ausführen. Ein Bestandsaufnahmejob wird für alle Hosts gestartet.

Ausführen von Bestandsaufnahme-Jobs

1. Nachdem der **Konfigurationsassistent** beendet wurde, wird für alle Hosts, die einem Verbindungsprofil hinzugefügt werden, automatisch eine Bestandsaufnahme veranlasst. Für eine nachfolgende Bestandsaufnahme auf Anforderung klicken Sie auf **Job-Warteschlange** → **Inventar** → **Jetzt ausführen**, um einen Bestandsaufnahme-Job auszuführen.
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 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

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 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.

Info über diese Aufgabe

ANMERKUNG: Das OMIVV-Gerät erfordert eine Internetverbindung zum Extrahieren der Serviceinformationen. Stellen Sie sicher, dass das OMIVV-Gerät über eine Internetverbindung verfügt. Je nach den Netzwerkeinstellungen benötigt OMIVV möglicherweise Proxy-Informationen für die Interneterreichbarkeit und das Abholen der Serviceinformationen. Die Proxy-Details können in der Administrationskonsole aktualisiert werden. Siehe Einrichten des HTTP-Proxy.

Schritte

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. Die Optionen beinhalten: • 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 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 das Symbol klicken.
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 **Apply (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 Service-Job aus, den Sie ausführen möchten, und klicken Sie auf das Symbol für .
6. Klicken Sie im Dialogfeld **Erfolgreich** auf **Schließen**.
   Es befindet sich nun ein Garantie-Job in der Warteschlange.

ANMERKUNG: Die Gehäusegarantie wird automatisch für alle Gehäuse ausgeführt, sobald die Host-Service ausgeführt wird. In einer SSO-Umgebung mit mehreren vCentern wird die Gehäusegarantie automatisch bei jedem vCenter ausgeführt, wenn der Service für ein beliebiges vCenter manuell 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 das Symbol klicken.
4. Klicken Sie im Dialogfeld **Erfolgreich** auf **Schließen**.
   Es befindet sich nun ein Garantie-Job in der Warteschlange.

Überwachung eines einzelnen Hosts

Die Dell OpenManage Integration for VMware vCenter ermöglicht Ihnen die Anzeige detaillierter Informationen für einen einzelnen Host. Sie können vom Navigator-Fensterbereich aus auf Hosts in VMware vCenter zugreifen. Dadurch werden alle Hosts für alle Anbieter angezeigt. Klicken Sie auf einen spezifischen Dell Host, um detailliertere Informationen zu erhalten. Um innerhalb der Dell OpenManage Integration for VMware vCenter eine Liste von Dell Hosts anzuzeigen, klicken Sie im Navigator-Fensterbereich auf **Dell Hosts**.

Anzeigen der Hostzusammenfassungsdetails

Info über diese Aufgabe

Sie können die Hostzusammenfassungsdetails für einen individuellen Host auf der Seite **Hostzusammenfassung** anzeigen, die verschiedene Portlets anzeigt. Zwei dieser Portlets sind für die OpenManage Integration for VMware vCenter gültig. Diese beiden Portlets sind:

- Dell Host-Funktionszustand
- Dell 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. Zeigen Sie die Hostzusammenfassungsdetails folgendermaßen an:

Schritte

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:

Informationen	Beschreibung
	• Letzte Tasks • In Bearbeitung • Alarme Dell-Alarminformationen werden in diesem Benachrichtigungsbereich-Portlet angezeigt.

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

Tabelle 14. Dell Server Management-Portlet

Informationen	Beschreibung
Service Tag	Zeigt die Service-Tag-Nummer Ihres Dell PowerEdge Servers an. Verwenden Sie diese ID, wenn Sie den Support anrufen.
Modellname	Zeigt den Modellnamen des Servers an.
Fault Resilient Memory	Zeigt den Status eines BIOS-Attributs an. Das BIOS-Attribut wird während dem ersten Einrichten des Servers im BIOS aktiviert und zeigt den Speicherbetriebsmodus auf dem Server an. Sie müssen Ihr System neu starten, wenn Sie den Speicherbetriebsmodus-Wert ändern. Dies gilt für Server der 12. Generation von PowerEdge-Servern und später, die die Option „FRM“ (Fault Resilient Memory, Fehlerbeständiger Speicher) unterstützt und auf denen ESXi 5.5 oder höher ausgeführt wird. Die vier verschiedenen Werte für das BIOS-Attribut 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. • Aktiviert und nicht geschützt: Dieser Wert zeigt an, dass Systeme mit Betriebssystem-Versionen niedriger als ESXi 5.5 unterstützt werden. • Deaktiviert: Dieser Wert zeigt an, dass gültige Systeme mit jeglichen Betriebssystem-Versionen unterstützt werden und der Speicherbetriebsmodus in BIOS nicht auf FRM gesetzt ist. • Leer: Wenn der Speicherbetriebsmodus in BIOS nicht unterstützt wird, wird das FRM-Attribut nicht angezeigt.
Identifikation	Zeigt die folgenden Optionen an: • Hostname – Zeigt den Namen des Dell 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 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

Informationen	Beschreibung
	• 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 Host-Funktionszustands-Portlets:

Tabelle 15. Dell Host-Funktionszustand

Informationen	Beschreibung
Dell Host-Funktionszustand	Der Funktionszustand einer Komponente ist eine grafische Darstellung des Status aller wichtigen Host-Server-Komponenten: globaler Status des Servers, Server, Netzteile, Temperaturen, Spannungen, Prozessoren, Batterien, Eingriff, Hardware-Protokoll, Energieverwaltung, Leistung und Speicher. Die Gehäusefunktionszustandsparameter gelten für die Modelle VRTX Version 1.0 und höher, M1000e Version 4.4 und höher. Für Versionen unter 4.3 werden nur zwei Anzeigen für den Funktionszustand angezeigt: Funktionsfähig und Warnung oder Kritisch (Umgekehrtes Dreieck mit einem Ausrufezeichen in orangener Farbe). Der Gesamtfunktionszustand zeigt den Funktionszustand basierend auf dem Gehäuse mit dem niedrigsten Funktionszustandsparameter an. Zu den Optionen gehören: • 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.

Anzeigen der Hardware-Details für einen einzigen Host

Info über diese Aufgabe

Sie können Hardware-Details für einen einzelnen Host auf der Registerkarte **Dell Host-Informationen** anzeigen. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Ausführen von Bestandsaufnahme-Jobs.

Schritte

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: `<Komponentenname>`-Details.
3. Wählen Sie in der Registerkarte **Überwachen** die Registerkarte **Dell Host-Information** aus.

   Auf der Hardware: Unterregister `<Komponentenname>`, Anzeige der folgenden Informationen zu jeder einzelnen Komponente.

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. Die Netzteiltypen beinhalten Folgendes: – 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
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: *Komponente*	Informationen
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

Info über diese Aufgabe

Sie können die Speicherdetails für einen einzigen Host auf der Registerkarte **Dell Host-Informationen** anzeigen. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Die Hardware meldet die Daten direkt aus OMSA und iDRAC. Siehe Ausführen von Bestandsaufnahme-Jobs. Diese Seite zeigt verschiedene Optionen an, abhängig von der Auswahl aus der Dropdownliste **Ansicht**. Wenn Sie **Physische Festplatten** auswählen, erscheint eine weitere Dropdownliste. Diese nächste Dropdownliste wird „Filter“ genannt und ermöglicht es Ihnen, die Optionen für Ihre physische Festplatte zu filtern. So zeigen Sie die Speicherdetails an:

Schritte

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 Host-Information** aus.

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

   Tabelle 17. Speicherdetails für einen einzigen Host

Komponente	Informationen
Bei Lagerung	Zeigt die Anzahl der virtuellen Festplatten, Controller, Gehäuse und zugehörige physische Festplatten mit der Anzahl der Globalen Hotspares und dedizierten Hotspares an. Wenn Sie eine Option aus der Dropdown-Liste „Ansicht“ ausgewählt haben, wird die Auswahl hervorgehoben.
Ansicht	Zeigt die Optionen an, die Sie für diesen Host anzeigen möchten: • Virtuelle Festplatten • Physische Festplatten • Controller

Komponente	Informationen
	• 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 von den in der virtuellen Festplatte enthaltenen physischen Festplatten verwendete Technologie an. Mögliche Werte sind: – SCSI – SAS – SATA • **Default Read Policy** – Zeigt die durch den Controller standardmäßig unterstützte Leserichtlinie an. Zu den Optionen gehören: – Vorauslesen – Kein Vorauslesen – Adaptives Vorauslesen – Lese-Cache aktiviert – Lese-Cache deaktiviert • **Standard-Schreibrichtlinie** – Zeigt die durch den Controller standardmäßig unterstützte Leserichtlinie an. Zu den Optionen gehören: – Rückschreiben – Rückschreiben erzwingen – Rückschreiben aktiviert – Durchschreiben – Schreib-Cache aktiviert und geschützt. – Schreib-Cache deaktiviert • **Cache-Regel** – Wird angezeigt, wenn die Cache-Regeln aktiviert sind
Physische 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	• **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. Die Optionen umfassen: – ONLINE – BEREIT

Informationen	Beschreibung
• Diese Option wird angezeigt, wenn Sie virtuelle Laufwerke mit eigenen Namen erstellt haben	– 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 Hotspare-Typ an. Zu den Optionen gehören: – Nein – Bedeutet, dass kein Hotspare vorhanden ist – Global – Ein globales Hotspare ist eine nicht verwendete Backup-Festplatte, die ein Teil der Festplattengruppe ist – Dediziert – Ein dedizierter Hotspare ist 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 • **Mindestens erforderliche Firmware** – Zeigt die mindestens 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 • **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 Systemereignisprotokolle für einen bestimmten Host anzeigen.

Anzeigen von Ereignisprotokollen für einen einzelnen Host

Info über diese Aufgabe

Um die Ereignisse anzuzeigen, führen Sie folgende Schritte durch:

Schritte

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 von der **Überwachen Dell Hostinformationen** → **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

Info über diese Aufgabe

Sie können die Firmware, die Stromüberwachung und die Servicestatusdetails für einen einzelnen Host auf der Registerkarte **Dell Host-Informationen** anzeigen. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Hardwareansichten melden die Daten aus OMSA und iDRAC direkt. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

Schritte

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 Details `<Komponentenname>` anzeigen lassen wollen.
3. Wählen Sie in der Registerkarte **Überwachen** die Registerkarte **Dell Host-Information** aus.

   Auf der Hardware: Unterregister `<Komponentenname>`, Anzeige der folgenden Informationen zu jeder einzelnen Komponente:

   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	· **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

Komponente	Informationen
ANMERKUNG: Sie müssen einen Service-Job ausführen, um einen Servicestatus anzuzeigen. Siehe Ausführen eines Serviceabfrage-Jobs. Die Seite Servicezusammenfassung ermöglicht Ihnen die Überwachung des Service-Ablaufdatums. Die Serviceeinstellungen steuern, wann Server-Serviceinformationen von Dell Online heruntergeladen werden, indem der Servicezeitplan aktiviert oder deaktiviert wird und anschließend der Mindesttageschwellenwertalarm festgelegt wird.	

Überwachen der Hosts auf Clustern und von Rechenzentren

OpenManage Integration for VMware vCenter ermöglicht es Ihnen, detaillierte Informationen für alle Hosts, die in einem Rechenzentrum oder Cluster eingeschlossen sind, anzuzeigen. Sie können die Daten sortieren, indem Sie den Zeilenkopf des Datenrasters anklicken. Die Seiten „Rechenzentrum“ und „Cluster“ ermöglichen Ihnen den Export von Informationen in eine CSV-Datei und bieten Ihnen Filter oder Suchfunktionen im Datenraster.

Anzeigen einer Übersicht der Rechenzentren und Cluster

Info über diese Aufgabe

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

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

Schritte

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** das Register **Dell 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
Hardware-Ressourcen	Zeigt die folgenden Optionen an: · Gesamtanzahl der Prozessoren · Total Memory (gesamter Speicher) · Kapazität von virtuellen Laufwerken

Informationen	Beschreibung
Garantiezusammenfassung	Zeigt den Servicestatus für den ausgewählten Host an. Die Statusoptionen beinhalten Folgendes: • 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 Dell PowerEdge-Modell an
Asset Tag	Zeigt die Systemkennnummer an, wenn konfiguriert
Service-Tag-Nummer des Gehäuses	Zeigt die Gehäuse-Service-Tag-Nummer an, falls verfügbar
Betriebssystemversion	Zeigt die Version des ESXi-Betriebssystems an
Speicherort	Nur Blades: Zeigt die Steckplatzposition an. Sonst wird „Nicht zutreffend“ angezeigt.
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

Info über diese Aufgabe

Sie können Hardware-Details für einen einzelnen Host auf der Registerkarte **Dell Rechenzentrums-/Cluster-Informationen** anzeigen. Damit Informationen auf dieser Seite angezeigt werden, führen Sie einen Bestandsaufnahme-Job aus. Auf den Seiten „Rechenzentrum“ und „Cluster“ können Sie Informationen in eine CSV-Datei exportieren, und Filter- und Suchfunktionen im Datenraster ausführen. Die angezeigten Daten variieren je nach Anzeigeart, mit der Sie auf die Daten zugreifen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Ausführen von Bestandsaufnahme-Jobs.

Schritte

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** die Registerkarte **Dell Rechenzentrums-/Cluster-Information** aus.

   Auf der Hardware: Unterregister `<Komponentenname>`, Anzeige der folgenden Informationen zu jeder einzelnen Komponente.

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
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. Die Netzteiltypen beinhalten Folgendes: – 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 Status des Netzteils an. Zu den Statusoptionen gehören: – 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

Hardware: *Komponente*	Informationen
	• **Größe** – Zeigt die Speichergröße an • **Typ** – Zeigt den Speichertyp an
Hardware: Netzwerkschnittstellenkarten	• **Host** – Zeigt den Hostnamen an • **Service-Tag** – Zeigt den Service-Tag des Hosts an • **Name** – Zeigt den NIC-Namen an • **Hersteller** – Zeigt nur den Herstellernamen an • **MAC-Adresse** – Zeigt die MAC-Adresse der NIC an
Hardware: PCI-Steckplätze	• **Host** – Zeigt den Hostnamen an • **Service-Tag** – Zeigt den Service-Tag des Hosts an • **Steckplatz** – Zeigt den Steckplatz an • **Hersteller** – Zeigt den Herstellernamen des PCI-Steckplatzes an • **Beschreibung** – Zeigt die Beschreibung des PCI-Geräts an • **Typ** – Zeigt den Typ des PCI-Steckplatzes an • **Breite** – Zeigt die Datenbusbreite an, wenn verfügbar
Hardware: Remote-Zugriffskarte	• **Host** – Zeigt den Hostnamen an • **Service-Tag** – Zeigt den Service-Tag des Hosts an • **IP-Adresse** – Zeigt die IP-Adresse der Remote-Zugriffskarte an • **MAC-Adresse** – Zeigt die MAC-Adresse der Remote-Zugriffskarte an • **RAC-Typ** – Zeigt den Typ der Remote-Zugriffskarte an • **URL** – Zeigt die verfügbare URL für den iDRAC an, der diesem Host zugeordnet wurde

Anzeigen von Speicherdetails für Datacenter und Cluster

Info über diese Aufgabe

Zeigen Sie die Details des physischen Speichers für Rechenzentren oder Cluster auf der Registerkarte **Dell Rechenzentrum-/ Cluster-Informationen** an. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Auf den Seiten Rechenzentrum und Cluster können Sie Informationen in eine CSV-Datei exportieren und Filter- und Suchfunktionen im Datenraster ausführen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Ausführen von Bestandsaufnahme-Jobs.

Schritte

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 im Register **Überwachen** das Register **Dell Rechenzentrums-/ Cluster-Informationen** aus, und navigieren Sie zu **Speicher → Physisches Laufwerk/Virtuelles Laufwerk**.

   Wählen Sie zur Anzeige der vollständigen Detailsliste einen spezifischen Host vom Datengitter 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. Die Optionen umfassen:

Speicher: Festplatten	Beschreibung
	– ONLINE – BEREIT – HERABGESETZT – FEHLGESCHLAGEN – OFFLINE – NEUERSTELLUNG – INKOMPATIBEL – ENTFERNT – GELÖSCHT – ERKENNUNG VON SMART-WARNUNGEN – UNBEKANNT – FREMD – NICHT UNTERSTÜTZT **ANMERKUNG: Lesen Sie für weitere Informationen über die Bedeutung dieser Warnungen das 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 · **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 Hotspare-Typ an. Zu den Optionen gehören: – Nein – Bedeutet, dass kein Hotspare vorhanden ist – Global – Ein globales Hotspare ist eine nicht verwendete Backup-Festplatte, die ein Teil der Festplattengruppe ist – Dediziert – Ein dedizierter Hotspare ist 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. Damit ist der für diese virtuelle Festplatte konfigurierte RAID-Typ gemeint · **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

Speicher: Festplatten	Beschreibung
	· **Bus-Protokoll** – Zeigt die von den in der virtuellen Festplatte enthaltenen physischen Festplatten verwendete Technologie an. Mögliche Werte sind: – SCSI – SAS – SATA · **Stripe-Größe** – Bezieht sich auf die Menge an Speicherplatz, die jeder Stripe auf einer einzelnen Festplatte belegt · Default Read Policy – Zeigt die durch den Controller standardmäßig unterstützte Leserichtlinie an. Zu den Optionen gehören: – Vorauslesen – Kein Vorauslesen – Adaptives Vorauslesen – Lese-Cache aktiviert – Lese-Cache deaktiviert · **Standard-Schreibrichtlinie** – Zeigt die durch den Controller standardmäßig unterstützte Leserichtlinie an. Zu den Optionen gehören: – Rückschreiben – Rückschreiben erzwingen – Rückschreiben aktiviert – Durchschreiben – Schreib-Cache aktiviert und geschützt. – Schreib-Cache deaktiviert · **Festplatten-Cache-Regel** – Zeigt die durch den Controller standardmäßig unterstützte Cache-Regel an. Zu den Optionen gehören: – Aktiviert – Cache-E/A – Deaktiviert – Direct E/A

Anzeigen zusätzlicher Hardware-Details für Rechenzentren und Cluster

Info über diese Aufgabe

Sie können die Firmware-, Stromüberwachungs- und Servicestatusdetails für Rechenzentrum oder Cluster auf der Registerkarte **Dell Rechenzentrum-/Cluster-Informationen** anzeigen. Damit Informationen auf dieser Seite angezeigt werden, müssen Sie einen Bestandsaufnahme-Job ausführen. Von den Seiten Rechenzentrum und Cluster können Sie Informationen in eine CSV-Datei exportieren und Filter- und Suchfunktionen im Datenraster ausführen. Hardwareansichten melden die Daten direkt aus OMSA und iDRAC. Siehe Sofortige Ausführung eines Bestandsaufnahme-Jobs.

Schritte

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** die Registerkarte **Dell Rechenzentrums-/Cluster-Information** aus.

   Zeigen Sie auf der Unterregisterkarte `<Komponentenname>` die folgenden Informationen für jede der 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

Komponente	Informationen
	• **Version** – Zeigt die Version von sämtlicher Firmware auf diesem Host an
Stromüberwachung **ANMERKUNG: Wählen Sie zur Anzeige der vollständigen Detailsliste einen spezifischen Host vom Datengitter 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 • **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, stellen Sie sicher, dass Sie einen Service-Job auszuführen. Siehe Ausführen eines Serviceabfrage-Jobs. Auf der Seite Servicezusammenfassung können Sie das Service-Ablaufdatum überwachen. Die Service-Einstellungen kontrollieren durch das Aktivieren oder Deaktivieren des Servicezeitplans und das Einstellen der Mindesttageschwellenwertwarnung, wann Servergarantieinformationen von Dell Online abgerufen werden.**	• **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 Folgendes: – Aktiv – Der Host ist unter Service und hat keinen Schwellenwert überschritten – Warnung – Der Host ist aktiv, hat jedoch den Warnungsschwellenwert überschritten

Komponente	Informationen
	– 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

Info über diese Aufgabe

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.

Schritte

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. Führen Sie im Register **Zusammenfassung** einen Bildlauf nach unten bis zum Dell Server Management Portlet durch.
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**.

9

Allgemeines zu Firmware-Aktualisierungen

Das OMIVV-Gerät ermöglicht Ihnen die Durchführung von BIOS- und Firmware-Aktualisierungen auf den verwalteten Hosts. Sie können gleichzeitig mehrere Firmware-Aktualisierungen in mehreren Clustern oder auf Hosts ohne Clusterverbund durchführen. Es ist nicht zulässig, Firmware-Aktualisierungen gleichzeitig auf zwei Hosts im gleichen Cluster durchzuführen.

Die folgende Tabelle führt die Anzahl der Firmware-Aktualisierungen auf, die in verschiedenen Bereitstellungsmodi gleichzeitig ausgeführt werden können. Sie können jedoch eine beliebige Anzahl von Firmware-Aktualisierungen planen:

Tabelle 24. Firmware-Aktualisierungsaufträge 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 Firmware-Aktualisierungen für iDRAC, BIOS oder LC durch, indem es direkt auf den DUP-Speicherort (CIFS- oder NFS-Freigabe) zeigt. Die Methode „Einzelnes DUP“ kann nur auf Hostebene verwendet werden.
- Repository: Führt BIOS- und alle unterstützten Firmware-Aktualisierungen durch. Die Methode kann auf Host- und Clusterebene verwendet werden. Die folgenden beiden Repository-Speicherorte sind verfügbar:
  - Dell Online: Der Speicherort verwendet das Repository zur Firmware-Aktualisierung von Dell (**ftp.dell.com**). OpenManage Integration for VMware vCenter lädt die ausgewählten 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 ein lokales Repository der Firmware in einer CIFS- oder NFS-basierten Netzwerkfreigabe speichern. Dieses Repository kann entweder ein Dump des Server Update Utility (SUU) sein, das Dell in regelmäßigen Abständen freigibt, oder ein benutzerdefiniertes Repository, das mit DRM erstellt wurde OMIVV sollte 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 in einem Kennwort nicht verwendet werden: `@, &,%, ', ", ,` (comma), <, >.

  Informationen zur Einrichtung eines Repository zur Firmwareaktualisierung finden Sie unter Einrichten des Firmware-Aktualisierungs-Repositorys.

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 erforderlichen Mindestversionen zu aktualisieren. Weitere Informationen zu den erforderlichen Mindestversionen der Firmware für iDRAC, BIOS und Lifecycle Controller finden Sie in der *Kompatibilitätsmatrix für OpenManage Integration for VMware v Center*-. Wenn die iDRAC-, Lifecycle Controller- und BIOS-Firmware-Versionen die Mindestanforderungen erfüllen, ermöglicht der Prozess zur Firmware-Aktualisierung Aktualisierungen für alle Firmware-Versionen, einschließlich iDRAC, Lifecycle Controller, RAID, NIC/LOM, Netzteile und BIOS.

Ausführen des Firmwareaktualisierungsassistenten für einen einzelnen Host

Info über diese Aufgabe

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

ANMERKUNG: Dell 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.

Schritte

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 Host-Information** → **Firmware-Assistent ausführen**.
   - Wählen Sie im Bereich **Navigator** einen Host aus und klicken Sie dann auf **Überwachen** → **Dell 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 Assistent **Firmwareaktualisierung** Wizard angezeigt und Sie sehen die Seite **Willkommen**.

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

   Der Bildschirm **Aktualisierungsquelle auswählen** wird angezeigt.
3. Wählen Sie auf dem Bildschirm **Aktualisierungsquelle auswählen** eine der folgenden Optionen aus:
   - Wählen Sie **Aktueller Repository-Speicherort** aus, und wählen Sie das Aktualisierungsbündel für die Firmware aus der Dropdownliste **Ein Aktualisierungsbündel auswählen** aus.

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

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

     ANMERKUNG: OMIVV unterstützt 32-Bit- und 64-Bit-Bündel für eine Firmwareaktualisierung. Abgesehen von den erwähnten Bündeln erstellt OMIVV auch ein hybrides Bündel, wenn mehrere Bündel im Katalog mit derselben Versions-ID verfügbar sind.
   - Wählen Sie zum Laden einer einzelnen Firmwareaktualisierung aus einer Datei die Option **Einzelnes DUP**. 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.
4. Wenn Sie die Option **Einzelnes DUP** auswählen, fahren Sie mit Schritt 7 fort.
5. Klicken Sie auf **Next** (Weiter).

   Der Bildschirm **Komponenten auswählen** wird angezeigt. Dieser listet die Firmwaredetails für die Komponenten auf. Auf dem Bildschirm werden die Details zu den Komponenten wie Hostname, Service-Tag-Nummer, Modellname, Komponente, Version, Aktualisierungsversion, Kritikalität, Neustart erforderlich (Ja/Nein) sowie andere Details zum ausgewählten Host 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.
6. Verwenden Sie die Kontrollkästchen zur Auswahl von mindestens einer Komponente 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 kommagetrennte Werte aus dem Inhalt der die verschiedenen Komponenten des Datengitters herausfiltern, indem Sie das Feld **Filter** verwenden. Sie können auch Spalten innerhalb des Komponentendatengitters verschieben. Verwenden Sie zum Exportieren aus dem Assistenten die Schaltfläche **In CSV exportieren**. Falls Sie das Kontrollkästchen **Zurückstufung der Firmware gestatten** markieren, wählen Sie die Komponenten aus, die für die Zurückstufung aufgeführt werden sollen.

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.

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

   Der Bildschirm **Firmwareaktualisierung planen** wird angezeigt.

   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.

   b. Wählen Sie eine der folgenden Optionen aus:

      - Wählen Sie **Jetzt aktualisieren** zum sofortigen Start der Firmwareaktualisierung aus.
      - 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. Dell rät von dieser Methode ab.

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

   Die Seite **Zusammenfassung** wird angezeigt. Diese Seite stellt Details über alle Komponenten nach der Firmwareaktualisierung bereit.

9. 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 im Bildschirm **Firmwareaktualisierung planen** ausgewählt wurde.

Ausführen des Firmwareaktualisierungsassistenten für 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.

Voraussetzungen

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.

Info über diese Aufgabe

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

ANMERKUNG: Dell 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.

Schritte

1. Klicken Sie für den Start des Assistenten zur Firmwareaktualisierung in der OpenManage Integration auf **Cluster** und führen Sie die folgenden Teilschritte 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 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.

   Die **Willkommen**-Seite des Firmwareaktualisierungsassistenten wird angezeigt.
2. Zeigen Sie die **Willkommen**-Seite an, und klicken Sie auf **Weiter**.

   Der Bildschirm **Server auswählen** wird angezeigt.
3. Verwenden Sie die Kontrollkästchen im Fenster **Server auswählen** in der Strukturansicht **Name**, um die Hosts auszuwählen.
4. Klicken Sie auf **Next** (Weiter).

   Der Bildschirm **Aktualisierungsquelle auswählen** wird angezeigt. Hier können Sie die Bündel auswählen. Der Repository-Standort wird auch angezeigt.
5. Wählen Sie im Bildschirm **Aktualisierungsquelle wählen** den Modellnamen der ausgewählten Hosts aus der angezeigten Liste im Bereich **Bündel auswählen** aus.

   Alle Modelle des ausgewählten Hosts verfügen über eine Dropdownliste neben dem Hostnamen, aus der Sie das erforderliche Bündel auswählen können. Wählen Sie mindestens ein Bündel für die Firmwareaktualisierung aus.

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

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

   ANMERKUNG: 64-Bit-Bündel werden nicht unterstützt für Hosts der 11. Generation mit allen iDRAC-Versionen.
6. Klicken Sie auf **Next** (Weiter).

   Der Bildschirm **Komponenten auswählen** wird angezeigt. Der Bildschirm Komponenten auswählen wird angezeigt. Auf dem Bildschirm werden die Details zu den Komponenten wie Cluster, Modell, Hostname, Service-Tag-Nummer, Komponente, Version, Aktualisierungsversion, Kritikalität, Neustart erforderlich (Ja/Nein) sowie andere Details zum ausgewählten Host angezeigt.
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.

   Sie können kommagetrennte Werte aus dem Inhalt der die verschiedenen Komponenten des Datengitters herausfiltern, indem Sie das Feld **Filter** verwenden. Sie können auch Spalten innerhalb des Komponentendatengitters verschieben. Verwenden Sie zum Exportieren aus dem Assistenten die Schaltfläche **In CSV exportieren**. Wenn Sie das Kontrollkästchen **Firmwareherabstufung zulassen** markiert haben, können Sie eine ältere Firmwareversion als die aktuelle Version auswählen.
8. Auf der Seite **Informationen zur Firmwareaktualisierung** sehen Sie alle Details zur Firmwareaktualisierung.
9. Klicken Sie auf **Next** (Weiter).

   Der Bildschirm **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.

Die Beschreibung ist optional.

c. 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:

  a. Wählen Sie im Kontrollkästchen **Kalender** den Monat und Tag aus.

  b. Geben Sie die Uhrzeit in dem Format SS:MM in das Textfeld **Zeit** ein.

10. Klicken Sie auf **Next** (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 Firmwareaktualisierungs-Job 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.

Verwalten von Firmware-Aktualisierungs-Jobs

Voraussetzungen

Um Informationen auf dieser Seite anzuzeigen, führen Sie einen Firmware-Aktualisierungsjob für einen Cluster durch. Siehe Ausführen des Firmware-Aktualisierungsassistenten für Cluster.

Info über diese Aufgabe

Die Seite zeigt alle Firmware-Aktualisierungs-Jobs an. Auf dieser Seite können Sie Ihre Firmware-Aktualisierungs-Jobs anzeigen, aktualisieren, bereinigen oder abbrechen.

Schritte

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.

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 Rechenzentrums- und Hostsystemüberwachung kann ein Administrator den Funktionszustand der Infrastruktur überwachen, indem die Hardware- (Server und Massenspeicher) und Virtualisierungs-bezogenen Ereignisse auf der Registerkarte **Tasks** und **Ereignisse** in vCenter angezeigt werden. Darüber hinaus lösen wichtige Hardware-Warnungen Alarme in OpenManage Integration for VMware vCenter aus. Nur wenige, für Dell virtualisierungsbezogen definierte Ereignisse können das verwaltete Host-System in den Wartungsmodus versetzen.

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-Alarme 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**.

Informationen zu Ereignissen und Warnmeldungen für Hosts

Sie können Ereignisse und Alarme von Dell OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Einstellungen** bearbeiten. Von hier können Sie die Ereignisanzeigeebene auswählen, die Alarme für Dell Hosts aktivieren oder Standardalarme wiederherstellen. Sie können Ereignisse oder Alarme für einzelne vCenter oder alle registrierten vCenter gleichzeitig konfigurieren.

Dies sind die vier Ereignisanzeigeebenen:

Tabelle 25. 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 Dell OpenManage Integration for VMware vCenter von den verwalteten Dell Hosts der betroffenen vCenter erhält.
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.	Veröffentlicht von Hosts empfangene Virtualisierung-bezogene Ereignisse an die entsprechenden vCenter. Virtualisierung-

Ereignis	Beschreibung
	bezogene Ereignisse sind solche Ereignisse, in denen Dell für Hosts, die virtuelle Maschinen ausführen, die höchste Priorität zuweist.

Wenn Sie Ereignisse und Alarme konfigurieren, können Sie sie aktivieren. In diesem Fall führen kritische Hardware-Alarme dazu, dass das OMIVV Appliance das Hostsystem in den Wartungsmodus versetzt und die virtuellen Maschinen in bestimmten Fällen auf ein anderes Hostsystem migriert. Das Dell OpenManage Integration for VMware vCenter leitet die von verwalteten Dell-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 Distributed Resource Scheduling (DRS) 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. Verwenden Sie Cluster zusammen mit DRS-konfigurierten Dell Alarmen, um sicherzustellen, dass virtuelle Maschinen bei kritischen Hardware-Ereignissen automatisch migriert werden. Die Details der Benachrichtigung auf dem Bildschirm listen die Cluster auf dieser vCenter-Instanz auf, die betroffen sein können. Bestätigen Sie, dass die Cluster betroffen sind, bevor Sie Ereignisse und Alarme aktivieren.

Wenn Sie die Standard-Alarmeinstellungen wiederherstellen müssen, können Sie auf die Schaltfläche **Standard-Alarmeinstellungen wiederherstellen** klicken. Mit dieser Schaltfläche kann die standardmäßige Alarm-Konfiguration wiederhergestellt werden, ohne dass das Produkt de- und neuinstalliert werden muss. Alle nach der Installation geänderten Dell-Alarm-Konfigurationen werden durch Klicken auf diese Schaltfläche auf die Standardeinstellung zurückgesetzt.

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

ANMERKUNG: Dell OpenManage Integration for VMware vCenter trifft eine Vorauswahl der erforderlichen virtualisierungsbezogenen Ereignisse, damit Hosts virtuelle Maschinen erfolgreich ausführen können. Die Dell-Host Alarme sind in der Standardeinstellung deaktiviert. Wenn die Dell-Alarme aktiviert werden, sollten die Cluster DRS verwenden, um sicherzustellen, dass virtuelle Maschinen, die kritische Ereignisse senden, automatisch migriert werden.

Informationen zu Ereignissen und Warnmeldungen für Gehäuse

Ereignisse und Alarme zu einem Gehäuse werden nur auf vCenter-Ebene angezeigt. Ereignis- und Alarmeinstellungen, die für Hosts an jedem vCenter vorgenommen werden, betreffen auch die Gehäuseebene. Sie können die Ereignis- und Alarmeinstellungen aus OpenManage Integration für VMware vCenter auf der Registerkarte **Verwalten** → **Einstellungen** bearbeiten. Von hier aus können Sie die Ereignisanzeigeebene auswählen, Alarme für Dell-Hosts und -Gehäuse aktivieren oder Standardalarme wiederherstellen. Sie können die Ereignisse und Alarme für einzelne vCenter oder für alle registrierten vCenter gleichzeitig 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 **Überwachen** → **Ereignisse**.
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. Es werden nur die ersten vier Alarme 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.

Tabelle 26. Virtualisierungsereignisse

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Dell-Current sensor detected a warning value	Ein Stromsensor im angegebenen System hat seinen Warnungsschwellenwert überschritten	Warnung	Keine Maßnahme
Dell-Current sensor detected a failure value	Ein Stromsensor im angegebenen System hat seinen Fehlerschwellenwert überschritten	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell-Current sensor detected a non-recoverable value	Ein Stromsensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell-Redundancy regained	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell-Redundancy degraded	Ein Redundanzsensor in dem angegebenen System hat erkannt, dass eine der Komponenten der Redundanzeinheit fehlgeschlagen, die Einheit aber dennoch redundant ist	Warnung	Keine Maßnahme
Dell-Redundancy lost (Keine Stromversorgung)	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
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

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene 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
Dell – Prozessorsensor hat einen nicht wiederherstellbaren Wert erkannt	Ein Prozessorsensor im angegebenen System ist fehlerhaft.	Fehler	Keine Maßnahme

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene 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 temperaturbedingten Fehlerereignis herunterfährt. Wenn der Messwert eines Temperatursensors den Fehlerschwellenwert überschreitet, für den das System konfiguriert wurde, fährt das Betriebssystem herunter und das System wird ausgeschaltet. Bei bestimmten Systemen kann dieses Ereignis auch initiiert werden, wenn ein Lüftergehäuse für einen längeren Zeitraum aus dem System entfernt wird	Fehler	Keine Maßnahme
Dell – Temperatursensor auf Normalwert zurückgekehrt	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell – Temperatursensor hat einen Warnungswert erkannt	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine, der CPU oder dem Festplattenträger im angegebenen System hat ein Überschreiten des Warnungsschwellenwerts erkannt	Warnung	Keine Maßnahme
Dell – Temperatursensor hat einen Fehlerwert erkannt	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine oder dem Festplattenträger im angegebenen System hat ein Überschreiten des Fehlerschwellenwerts erkannt	Fehler	Setzen Sie das System in den Wartungsmodus.

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
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

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Dell – Speicher: Gehäuse-Hardware-Warnung	Warnung bezüglich Gehäuse-Hardware	Warnung	Keine Maßnahme
Dell – Speicher: Gehäuse-Hardware-Fehler	Fehler der Gehäuse-Hardware	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Array-Festplattenfehler	Fehler der Array-Festplatte	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: EMM-Fehler	EMM-Fehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Netzteilfehler	Netzteilfehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Temperatursondenwarnung	Temperatursondenwarnung der physischen Festplatte: zu kalt oder zu heiß.	Warnung	Keine Maßnahme
Dell – Speicher: Temperatursondenfehler	Temperatursondenfehler der physischen Festplatte: zu kalt oder zu heiß.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Lüfterfehler	Lüfterfehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Batteriewarnung	Akkuwarnung	Warnung	Keine Maßnahme
Dell – Speicher: Warnung: Virtuelle Festplatte wurde herabgesetzt	Warnung: Herabsetzung einer virtuellen Festplatte	Warnung	Keine Maßnahme
Dell – Speicher: Fehler: Virtuelle Festplatte wurde herabgesetzt	Fehler zur Herabsetzung einer virtuellen Festplatte.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speicher: Temperatursondeninformation	Informationen zur Temperatursonde	Info	Keine Maßnahme
Dell – Speicher: Array-Festplattenwarnung	Warnung zum Array-Laufwerk	Warnung	Keine Maßnahme
Dell – Speicher: Array-Festplatteninformation	Informationen zum Array-Laufwerk	Info	Keine Maßnahme
Dell – Speicher: Netzteilwarnung	Netzteilwarnung	Warnung	Keine Maßnahme
Dell – Fluid Cache Laufwerksfehler	Fluid Cache Laufwerksfehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Kabelfehler oder kritisches Ereignis	Kabelfehler oder kritisches Ereignis.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Chassis Management Controller hat eine Warnung erkannt	Gehäuse-Verwaltungscontroller 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.

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Dell – Verbindungsstatuswarnung	Verbindungsstatuswarnung	Warnung	Keine Maßnahme
Dell – Linkstatusfehler oder kritisches Ereignis	Verbindungsstatusfehler oder kritisches Ereignis	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Sicherheitswarnung	Sicherheitswarnung	Warnung	Keine Maßnahme
Dell - System: Softwarekonfigurationswarnung	System: Softwarekonfigurationswarnung	Warnung	Keine Maßnahme
Dell - System: Softwarekonfigurationswarnung	System: Softwarekonfigurationsfehler	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Speichersicherheitswarnung	Speichersicherheitswarnung	Warnung	Keine Maßnahme
Dell – Speichersicherheitsfehler oder kritisches Ereignis	Speichersicherheitsfehler oder kritisches Ereignis	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Softwareänderungs-Aktualisierungswarnung	Softwareänderungs-Aktualisierungswarnung.	Warnung	Keine Maßnahme
Dell – Chassis Management Controller Auditwarnung	Überprüfungswarnung zum Gehäuse-Verwaltungscontroller	Warnung	Keine Maßnahme
Dell – Chassis Management Controller Auditfehler oder kritisches Ereignis	Gehäuse-Verwaltungscontroller: Überprüfungsfehler oder kritisches Ereignis	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – PCI-Geräte-Auditwarnung	PCI-Geräte-Überprüfungswarnung	Warnung	Keine Maßnahme
Dell – Netzteil-Auditwarnung	Netzteil-Überprüfungswarnung	Warnung	Keine Maßnahme
Dell – Netzteil-Auditfehler oder kritisches Ereignis	Netzteil-Überprüfungsfehler oder kritisches Ereignis	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell – Stromverbrauchs-Auditwarnung	Stromverbrauchs-Überprüfungswarnung	Warnung	Keine Maßnahme
Dell – Stromverbrauchs-Auditfehler oder kritisches Ereignis	Stromverbrauchs-Überprüfungsfehler 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.

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Dell – Warnung zur Partition der virtuellen Festplatte	Warnung zu einer Partition der virtuellen Festplatte	Warnung	Keine Maßnahme
iDRAC-Ereignisse **ANMERKUNG: Für alle proaktiven HA-aktivierten Hosts, die Teil eines Clusters sind, werden die folgenden Virtualisierungsereignisse den proaktiven HA-Ereignissen zugeordnet, ausgenommen die Ereignisse „Die Lüfter sind nicht redundant“ und „Die Netzteile sind nicht redundant“.**			
Die Lüfter sind redundant	Keine	Info	Keine Maßnahme
Lüfterredundanz verloren	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Kritisch	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
Lüfter-Redundanz ist herabgesetzt	Ein oder mehrere Lüfter sind ausgefallen oder wurde entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Warnung	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
Die Lüfter sind nicht redundant	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Info	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
Die Lüfter sind nicht redundant. Keine ausreichenden Ressourcen zur Beibehaltung des normalen Betriebs	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Kritisch	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
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.

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene 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.
Das interne Dual SD-Modul ist redundant.	Keine	Info	Keine Maßnahme
Verlust der internen Dual-SD-Modulredundanz	Eine der beiden SD-Karten oder beide SD-Karten funktionieren nicht ordnungsgemäß.	Kritisch	Ersetzen Sie die fehlerhafte SD-Karte.
Interne Dual-SD-Modulredundanz ist herabgesetzt	Eine der beiden SD-Karten oder beide SD-Karten funktionieren nicht ordnungsgemäß.	Warnung	Ersetzen Sie die fehlerhafte SD-Karte.
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

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene 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 entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Warnung	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
Die Lüfter sind redundant	Keine	Info	Keine Maßnahme
Die Lüfter sind nicht redundant	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Info	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.
Die Lüfter sind nicht redundant. Keine ausreichenden Ressourcen zur Beibehaltung des normalen Betriebs	Ein oder mehrere Lüfter sind ausgefallen oder wurden entfernt, oder es wurde eine Konfigurationsänderung vorgenommen, die zusätzliche Lüfter erforderlich macht.	Kritisch	Entfernen Sie die fehlerhaften Lüfter und installieren Sie sie erneut oder installieren Sie zusätzliche Lüfter.

Proaktive HA-Ereignisse

Die folgende Tabelle enthält die proaktiven kritischen, normalen und Warnungs-HA-Ereignisse, einschließlich Zustands-Update-ID, Komponententyp und Beschreibung:

Tabelle 27. Proaktive HA-Ereignisse

Dell Inc. Provider Ereignis-ID	Komponententyp	Beschreibung
DellServerFan	Lüfter	Lüfterredundanz-Ereignis
DellServerPower	Strom	Stromredundanz-Ereignis
DellServerIDSDM	Storage	IDSDM-Redundanz-Ereignis

DellChassisFan	Lüfter	Simuliertes Gehäuse-Lüfterredundanz-Ereignis
DellChassisPower	Strom	Simuliertes Gehäuse-Stromredundanz-Ereignis

Anzeigen der Alarm- und Ereigniseinstellungen

Info über diese Aufgabe

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.

Schritte

1. Erweitern Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Einstellungen** unter **vCenter-Einstellungen Ereignisse und Alarme**.

   Es werden die folgenden Details angezeigt:

   - vCenter-Alarme für Dell Hosts – zeigt entweder **Aktiviert** oder **Deaktiviert** an.
   - Ereignisanzeigeebene
2. Ereignisse und Alarme konfigurieren. Siehe Konfigurieren von Ereignissen und Alarmen.

Nächste Schritte

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

Anzeigen von Ereignissen

Voraussetzungen

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

Info über diese Aufgabe

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

Schritte

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 Hardwarekomponenten - Proaktive HA

Proaktive HA ist eine vCenter (vCenter 6.5 und höher) Funktion mit OMIVV. Wenn Sie proaktive HA aktivieren, schützt die Funktion Ihre Arbeitslasten durch proaktive Maßnahmen während redundanter Komponentenfehler in einem Host.

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

Um den Status redundanter Host-Server-Komponenten zu bewerten, aktualisiert das OMIVV-Gerät die Änderung des Host-Komponenten-Funktionszustands am vCenter-Server. Die Verfügbarkeitsstatus-Zustände der wichtigsten Hostserverkomponenten, z. B. Stromversorgung, Lüfter und internes Dual-SD-Modul (iDSDM) sind:

- 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.

Stellt OMIVV (über Traps oder Abfragen) eine Änderung des Funktionszustands einer Komponente fest, wird die Benachrichtigung über den aktualisierten Zustand der Komponente zusammen mit dem Status an den vCenter Server geleitet. Basierend auf der

Benachrichtigung ergreift der vCenter Server eine benutzerkonfigurierte manuelle oder automatische Maßnahme. Der vCenter Server führt eine der folgenden Aktionen aus:

- Versetzen von Hosts in den Quarantänemodus
- Versetzen von Hosts in den Wartungsmodus

Proaktive HA für Rack-Server konfigurieren

Info über diese Aufgabe

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

Schritte

1. Erstellen Sie ein Verbindungsprofil und ordnen Sie Hosts dem Verbindungsprofil zu. Siehe Erstellen eines 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.
4. Aktivieren Sie Proaktive HA auf einem Cluster. Siehe Aktivieren von Proaktiver HA auf einem Cluster.

Proaktive HA für modulare Server konfigurieren

Info über diese Aufgabe

Führen Sie zur Konfiguration für modulare Server folgende Schritte durch:

Schritte

1. Erstellen Sie ein Verbindungsprofil und ordnen Sie Hosts dem Verbindungsprofil zu. Siehe Erstellen eines Verbindungsprofils.
2. Stellen Sie sicher, dass die Host-Bestandsaufnahme erfolgreich abgeschlossen wurde. Siehe Anzeigen von Host-Bestandsaufnahmen.
3. Erstellen Sie ein Gehäuse-Profil für die zugeordneten Gehäuse. Siehe Erstellen eines Gehäuse-Profils.
4. Stellen Sie sicher, dass die Gehäuse-Bestandsaufnahme erfolgreich abgeschlossen wurde. Siehe Anzeigen von Gehäuse-Bestandsaufnahmen.
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 Proaktive HA auf einem Cluster. Siehe Aktivieren von Proaktiver HA auf einem Cluster.

Aktivieren von proaktiver HA auf Clustern

Voraussetzungen

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

- Ein Cluster, der DRS-aktiviert ist, 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.

Schritte

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. Weitere Informationen 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. Zur Anwendung auf einem Host verwenden Sie die Kontrollkästchen, um einen Host aus der Tabelle **anzuwenden unter** für den teilweisen Ausfall-Provider auszuwählen.

    Sie können den Inhalt des Datenrasters durch Verwendung des Felds **Filtern** filtern.
14. Um die Änderungen in **Bearbeiten blockiert Fehlerbedingungen** anzuwenden, klicken Sie auf **OK** oder zum Abbrechen des Vorgangs auf **Abbrechen**.
15. Um die Änderungen zu speichern, klicken Sie auf **OK** oder zum Abbrechen des Vorgangs auf **Abbrechen**.

Nächste Schritte

OMIVV kann nun die Funktionszustands-Aktualisierungsbenachrichtigung von Komponenten an das vCenter Server über Ereignisse auf dem Dell Server weiterleiten. Basierend auf der Benachrichtigung unternimmt der vCenter Server eine manuelle oder automatische Aktion, die Sie für **Fehlerbehebung** ausgewählt haben.

Integritätsabfrage von Dell Servern

Voraussetzungen

Bevor OMIVV stündlich abfragt, vergewissern Sie sich, dass die folgenden Bedingungen erfüllt sind:

- Ein Verbindungsprofil ist dem Host zugeordnet.
- Eine erfolgreich beendete Bestandsaufnahme steht für das Hostsystem bereit.

Info über diese Aufgabe

Es folgt eine Liste der Integritätsabfrage-Ereignisse:

Tabelle 28. Ereignisabfrage

Name des Ereignisses	Schweregrad	Empfohlene Maßnahme
Statusabfrage: Lüfterredundanz ist im Normalzustand	Info	Keine Maßnahme
Statusabfrage: Lüfterredundanz befindet sich im Warnzustand	Warnung	Lüfter austauschen
Statusabfrage: Lüfterredundanz ist in einem kritischen Zustand	Kritisch	Lüfter austauschen
Statusabfrage: Stromredundanz ist im Normalzustand	Info	Keine Maßnahme
Statusabfrage: Stromredundanz befindet sich im Warnzustand	Warnung	Netzteil austauschen
Statusabfrage: Stromredundanz ist in einem kritischen Zustand	Kritisch	Netzteil austauschen

Die Abfrage wird pro Stunde ausgeführt und Sie können den Zeitplan zur Statusabfrage konfigurieren. Die Abfrage steht als Ausfallsicherung für die Abdeckung eines Trap-Datenverlusts zur Verfügung.

ANMERKUNG: Die Abfrage stellt dem vCenter-Server keine Redundanz-Informationen von iDSDM-Komponenten bereit.

Überschreiben des Schweregrads der Funktionszustands-Aktualisierungsbenachrichtigung

Sie können konfigurieren, dass Sie den Systemschweregrad der Dell Host- und Gehäusekomponenten mit einem benutzerdefinierten Schweregrad überschreiben können, der auf Ihre Umgebung ausgerichtet ist. Der Standard-Schweregrad ist die gleiche wie der Systemschweregrad.

Info über diese Aufgabe

Es folgt eine Liste der verschiedenen Schweregrade:

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

ANMERKUNG: Sie können den Schweregrad von Komponenten mit dem Schweregrad Info anpassen.

Schritte

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** auf **Proaktive HA-Konfiguration → Proaktive HA-Ereignisse**.
2. Auf der Seite **Proaktive HA-Ereignisse** zeigen Sie die iDRAC- und CMC-Informationen für die Liste der Dell Host- und Gehäusekomponenten an.

   Die oberen und unteren Datenraster zeigen alle Abfrage- und proaktiven HA-Ereignisse an und umfassen die Ereignis-ID, Ereignisbeschreibung, aktuelle System-Schweregrad und den Überschreiben-Schweregrad der Host- und Gehäusekomponenten.

   ANMERKUNG: Der Schweregrad der IDSDM-Komponente kann nicht angepasst werden, und daher wird IDSDM in der Ereignisliste nicht angezeigt.
3. Um den Schweregrad einer Host- oder Gehäusekomponente zu ändern, wählen Sie in der Spalte **Schweregrad überschreiben** den gewünschten Status aus der Dropdownliste aus.
4. Wiederholen Sie Schritt 6 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 Server Management Portlet aus starten. Diese sind:

- Starten Sie zum Aufrufen der iDRAC-Benutzeroberfläche die Remote Access Console. Siehe Starten der Remote Access Console (iDRAC).
- Starten Sie für den Zugriff auf die Benutzeroberfläche von OpenManage Server Administrator die OMSA-Konsole. Vor dem Start der OMSA-Konsole muss die OMSA-URL in Open Management Integration for VMware konfiguriert werden. Siehe OMSA-Konsole starten.
- Für den Zugriff auf die Gehäuse-Benutzeroberfläche klicken Sie auf die Bladegehäuse-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 Gehäuse-Verwaltungscontrollers zu starten. Wenn Sie kein Blade-System verwenden, wird Benutzeroberfläche des Gehäuse-Verwaltungscontrollers nicht angezeigt.

Starten der Remote-Zugriffskonsole (iDRAC)

Info über diese Aufgabe

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

Schritte

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. Führen Sie im Register **Zusammenfassung** einen Bildlauf nach unten bis zum Dell Server Management Portlet durch.
4. Klicken Sie auf **Management-Konsolen** → **Remote-Zugriffskonsole (iDRAC)**.

OMSA-Konsole starten

Info über diese Aufgabe

Bevor Sie die OMSA-Konsole starten, müssen Sie die OMSA-URL einrichten und den OMSA-Webserver installieren und konfigurieren. Richten Sie die OMSA-URL von der Registerkarte **Einstellungen** aus ein.

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

Schritte

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 durch bis zu den **Dell Hostinformationen**.
4. Klicken Sie im Abschnitt **Dell Hostinformationen** auf **OMSA-Konsole**.

Starten der Chassis Management Controller-Konsole (CMC)

Info über diese Aufgabe

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

Schritte

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. Führen Sie im Register **Zusammenfassung** einen Bildlauf nach unten bis zum Dell Server Management Portlet durch.
4. Klicken Sie auf **Verwaltungskonsolen** → **Geräte-Management Controller-Konsole (CMC)**.

11

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.

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-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 Gesamtfunktionszustand eines Gehäuses an. Die gültigen Anzeigen des Funktionszustands lauten **Funktionsfähig**, **Warnung**, **Kritisch**, **Nicht vorhanden**. In der Rasteransicht **Gehäusefunktionszustand** wird der Funktionszustand jeder Komponente angezeigt. Die Funktionszustandsparameter von Gehäusen gelten für die Modelle VRTX Version 1.0 und höher, M1000e Version 4.4 und höher. Für Versionen unter 4.3 werden nur zwei Anzeigen angezeigt: Fehlerfrei und Warnung oder Kritisch (Umgekehrtes Dreieck mit einem Ausrufezeichen in orangener Farbe).

   ANMERKUNG: Der Gesamtfunktionszustand zeigt den Funktionszustand basierend auf dem Gehäuse mit dem niedrigsten Funktionszustandsparameter an. Wenn zum Beispiel 5 Zeichen für funktionsfähig und 1 Zeichen für Warnung vorhanden sind, 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-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	Informationen zu Temperatursensoren: · Standort · Lesen · Warnungsschwelle – Maximal – Minimum · Kritischer Schwellenwert

Hardware-Bestandsliste: Komponente	Navigation durch OMIVV	Informationen
	linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme** und klicken Sie dann auf **Temperatursensoren**.	– Maximal – Minimum **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

Hardware-Bestandsliste: Komponente	Navigation durch OMIVV	Informationen
		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**. • Erweitern Sie auf der Registerkarte **Überwachen** den linken Fensterbereich, klicken Sie auf **Hardware-Bestandsaufnahme**, und klicken Sie dann auf **iKVM**.	Informationen zum iKVM: • iKVM-Name • Vorhanden • Firmware-Version • Frontblenden USB/Video aktiviert • 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-, Verwaltungscontroller-Details innerhalb des ausgewählten Gehäuses anzeigen. Um die Informationen auf dieser Seite anzuzeigen, müssen Sie eine Bestandsaufnahme ausführen. Sie können eine CSV-Datei mit Komponenteninformationen exportieren.

Info über diese Aufgabe

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

Schritte

1. Klicken Sie auf der **Startseite** auf **vCenter**.
2. Klicken Sie im linken Fensterbereich unter **OpenManage Integration** auf **Dell-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 – 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
Bei Lagerung	Klicken Sie auf der Registerkarte **Überwachen** auf **Speicher**.	Informationen über Speicher: · Virtuelle Festplatten · Controller · Gehäuse · Physische Festplatten · Ersatzlaufwerke **ANMERKUNG: Wenn Sie auf einen einzelnen markierten Link unter „Speicher“ klicken, zeigt die Tabelle Ansicht die Details für jedes markierte Objekt an. Wenn Sie in der Ansichts-Tabelle auf jedes Zeilenobjekt 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)

Hardwarekonfiguration	Navigation durch OMIVV	Informationen
		• 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: Stellen Sie zur Anzeige des Servicestatus sicher, dass Sie einen Service-Job auszuführen. 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-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

12

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- und Hypervisor-Profile auf Bare-Metal Dell PowerEdge Servern mithilfe von VMware vCenter ohne PXE zu verwenden erstellen.

Für eine erfolgreiche Hardware-Einrichtung und -Bereitstellung müssen die physischen Server im Bereitstellungsassistenten angezeigt werden. Alle physischen Server müssen die folgenden Voraussetzungen erfüllen:

- Erfüllen bestimmter Hardware-Support-Informationen, die in der *OpenManage Integration for VMware vCenter Kompatibilitäts-Matrix* verfügbar sind.
- Erfüllen der unterstützten Mindestversionen von iDRAC-Firmware, Lifecycle-Controller und BIOS. Informationen zu den bestimmten Firmware-Support-Informationen finden Sie in der *OpenManage Integration for VMware vCenter Kompatibilitäts-Matrix*.
- Konfigurieren Sie NICs in den PCI-Steckplätzen manuell nach der Bereitstellung. Wenn Sie NIC-Zusatzadapter verwenden, müssen auf dem System das Host LAN on Motherboard (LOMs) aktiviert und mit dem Netzwerk verbunden sein. OMIVV unterstützt die Bereitstellung nur durch die Verwendung von eingebetteten oder integrierten LOMs.
- Erfüllen der technischen Daten des Speichers für das iDSDM. Die technischen Daten des Speichers für das iDSDM finden Sie in der VMware-Dokumentation. Stellen Sie sicher, dass Sie vor dem Bereitstellen des Hypervisors mit OMIVV das iDSDM im BIOS 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 von automatischer/manueller Ermittlung sicherstellen, dass die abgerufenen Daten aktuell sind, und zwar durch vollständiges Ausschalten des Systems und erneutes Einschalten (Kaltstart).
- Wählen Sie bei der Bestellung Dell-Server, die mit AutoErmittlung und Handshake-Optionen werksseitig vorkonfiguriert werden. Ist ein Server nicht mit diesen Optionen vorkonfiguriert, müssen Sie die IP-Adresse des OMIVV manuell eingeben oder Ihr lokales Netzwerk konfigurieren, um diese Informationen bereitzustellen.
- 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 für die Hardwarekonfiguration verwendet wird. Die Express/Clone RAID-Konfiguration ist erforderlich, wenn keine virtuelle Festplatte auf dem Zielsystem vorhanden ist.
- Für die Bereitstellung werden benutzerdefinierte ESXi-Images benötigt, die alle Dell-Treiber enthalten. Auf der Seite **support.dell.com** finden Sie unter **Dell Treiber und Downloads** die richtigen Images. Speichern Sie diese benutzerdefinierten Images auf einen für CIFS oder NFS freigegebenen Speicherort, auf den OMIVV während der Bereitstellung zugreifen kann. Eine aktuelle Liste mit allen unterstützten ESXi-Versionen für diese Version finden Sie in der *OpenManage Integration for VMware vCenter Kompatibilitäts-Matrix*. Informationen zur Verwendung der richtigen Images finden Sie unter Herunterladen benutzerdefinierter Dell ISO-Images.
- Stellen Sie vor dem Anwenden des Hypervisor-Profils sicher, dass Sie den BIOS-Modus im Referenz-Hardwareprofil ausgewählt haben, da OMIVV nur den BIOS-Modus unterstützt, um einen Hypervisor automatisch auf dem Zielserver bereitzustellen. Falls

kein Hardware-Profil ausgewählt wurde, stellen Sie sicher, dass Sie den Startmodus manuell als BIOS konfigurieren und starten Sie den Server vor dem Anwenden des Hypervisor-Profils neu.

ANMERKUNG: Wenn der Startmodus auf dem Zielsystem auf UEFI gesetzt ist, schlägt die Bereitstellung des Betriebssystems durch OMIVV fehl.

Bei Server-Versionen vor der Version der Dell PowerEdge-Server der 12. Generation, werden während des Bereitstellungsvorgangs folgende Aufgaben ausgeführt:

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

Geräteerkennung

Ermittlung ist der Prozess des Hinzufügens von unterstützten Dell PowerEdge Bare-Metal-Servern. Nachdem ein Server ermittelt wurde, können Sie ihn für Hypervisor- und Hardware-Bereitstellung verwenden. Informationen über die Liste der Power Edge-Server, die für die Bereitstellung erforderlich sind, finden Sie in der *OpenManage Integration for VMware vCenter-Kompatibilitäts-Matrix*. Die Netzwerkkonnektivität vom iDRAC des Dell Bare-Metal-Servers zu der virtuellen Maschine des OMIVV ist erforderlich.

ANMERKUNG: Die Hosts mit einem bereits vorhandenen Hypervisor sollten nicht in OMIVV ermittelt werden, sondern sollten dem vCenter hinzugefügt werden. Fügen Sie diese zu einem Verbindungsprofil hinzu, und stimmen sie sie dann mit dem Dell OpenManage Integration for VMware vCenter durch Verwendung des Host-Konformitätsassistenten ab.

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.

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

Die automatische Erkennung ist der Vorgang des Hinzufügens eines Dell PowerEdge Bare-Metal-Servers der 11., 12. und 13. Generation. Wenn ein Server erkannt wurde, verwenden Sie ihn für Hypervisor- und Hardware-Bereitstellung. Die automatische Erkennung ist eine iDRAC Funktion, die die Notwendigkeit einer manuellen Ermittlung eines Bare-Metal-Servers von OMIVV entfernt.

Voraussetzungen für Auto Discovery (Automatische Ermittlung)

Bevor Sie versuchen, die 11., 12. oder eine spätere Generation von Dell PowerEdge Bare-Metal-Servern zu ermitteln, stellen Sie sicher, dass OMIVV bereits installiert ist. Die 11., 12. und 13. Generation von Dell PowerEdge-Servern mit iDRAC Express oder iDRAC Enterprise können in einem Pool von Bare-Metal-Servern erkannt werden. Stellen Sie sicher, dass eine Netzwerkverbindung vom iDRAC des Dell 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 muss jedoch nicht eingeschaltet werden.
- Netzwerkkonnektivität – Der iDRAC des Servers muss über Netzwerkkonnektivität verfügen und über Port 4433 mit dem Bereitstellungsserver kommunizieren. Sie können die IP-Adresse über einen DHCP-Server anfordern 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. Informationen finden Sie unter 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

Damit Sie die automatische Ermittlung einrichten können, müssen Sie zuerst alle Verwaltungskonten, mit Ausnahme des Stammkontos, deaktivieren. Das Stammkonto sollte im Rahmen der AutoErmittlung deaktiviert worden sein. Nachdem Sie die AutoErmittlung erfolgreich eingerichtet haben, kehren Sie zurück zur iDRAC GUI und aktivieren Sie die Verwaltungskonten wieder, die Sie zuvor deaktiviert haben, aber nicht das Stammkonto.

Info über diese Aufgabe

ANMERKUNG: Als Schutzmaßnahme für den Fall einer fehlgeschlagenen AutoErmittlung 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 AutoErmittlung fehlschlägt.

Schritte

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 Vorgänge 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 **Next (Weiter)**.
7. Heben Sie auf der Seite **Benutzerkonfiguration** unter **Allgemein** die Markierung des Kontrollkästchens **Benutzer aktivieren** auf.
8. Klicken Sie auf **Apply (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

Voraussetzungen

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

Info über diese Aufgabe

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.

Schritte

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.

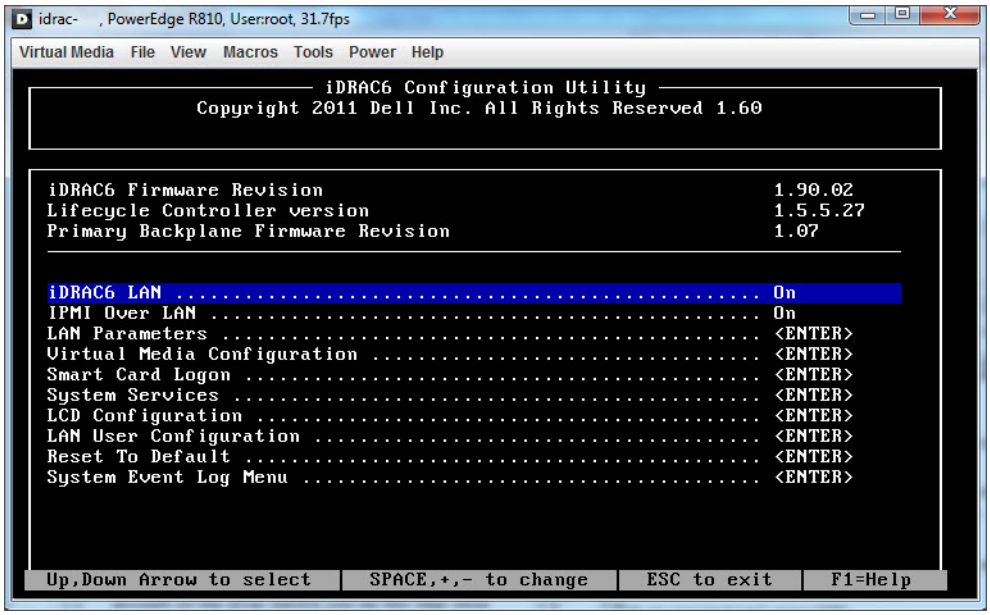

Abbildung 1. iDRAC-Konfigurationsdienstprogramm

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

Voraussetzungen

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

Info über diese Aufgabe

Während der Bestellung von Dell-Servern können Sie darum bitten, die automatische Ermittlungsfunktion auf den Servern zu aktivieren, nachdem Sie die Bereitstellungsserver-IP-Adresse zur Verfügung gestellt haben. Die Bereitstellungsserver-IP-Adresse sollte die IP-Adresse von OMIVV sein. Daher werden die Server nach Erhalt von Dell nach der Montage und Verbindung des iDRAC-Kabels automatisch ermittelt und auf der ersten Seite des Bereitstellungsassistenten aufgeführt.

ANMERKUNG: Für die Server, die automatisch ermittelt wurden, werden die Anmeldeinformationen, die unter Einstellungen → verwalten → Bereitstellungs-Anmeldeinformationen bereitgestellt wurden, zur weiteren Kommunikation mit dem Server verwendet, bis die Bereitstellung des Betriebssystems abgeschlossen ist. Nach einer erfolgreichen Bereitstellung des Betriebssystems, werden die im zugehörigen Verbindungsprofil festgelegten iDRAC-Anmeldeinformationen eingestellt.

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

Schritte

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 sicher, dass keine anderen Benutzer mit Administratorrechten auf dem iDRAC aktiviert sind, wenn Sie den Root-Benutzer deaktivieren.
3. Klicken Sie auf **Zurück** und klicken Sie 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 erfolgreicher automatischer 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 verfügbar für Hardewareeinrichtung und Hypervisor-Bereitstellung. Zur Einrichtung und Bereitstellung gehen Sie wie folgt vor:

Tabelle 34. Vorbereitung auf die Bereitstellung

Schritte	Beschreibung
Erstellen eines Hardwareprofils	Enthält die Hardwareeinstellungen, die von einem Referenzserver gesammelt wurden, der zum Bereitstellen neuer Server genutzt wird. Lesen Sie dazu Anpassen des Referenzservers zum Erstellen eines Hardwareprofils.
Erstellen eines Hypervisor-Profils	Enthält die Hypervisor-Installationsinformationen, die für die ESXi-Bereitstellung erforderlich sind. Lesen Sie auch Erstellen eines neuen Hypervisor-Profils.
Erstellen einer Bereitstellungsvorlage	Enthält optional ein Hypervisor-Profil oder Hardware- und Hypervisor-Profile. Sie können diese Profile bei Bedarf für alle verfügbaren Rechenzentrumsserver speichern und wiederverwenden. **ANMERKUNG: Nur die Hardware-Profil-Bereitstellung wird nicht unterstützt.**

Nachdem eine Bereitstellungsvorlage erstellt wurde, verwenden Sie den Bereitstellungsassistenten, um die notwendigen Informationen zu sammeln, die zum Erstellen eines geplanten Auftrags erforderlich sind, um Serverhardware einzurichten und neue Hosts im vCenter bereitzustellen. Weitere Informationen zum Ausführen des Bereitstellungsassistenten finden Sie unter Ausführen des Bereitstellungsassistenten. Abschließend verwenden Sie die Job-Warteschlange, um den Auftragsstatus anzuzeigen und Änderungen an ausstehenden Bereitstellungsaufträgen vorzunehmen.

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

Voraussetzungen

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.

Info über diese Aufgabe

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:

Schritte

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.

Anpassen von Referenzserver in Bezug auf Erstellen von Hardwareprofilen

Schritte

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 **Next** (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 Settings (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**
- **UEFI-Starteinstellungen**
- **One-Time Boot (Einmalstart)**
- **Integrierte Geräte**
- **Slot Disablement (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:
      1. Wählen Sie in der Liste **Startmodus** `BIOS` oder `UEFI`.
      2. 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**.
      3. Wählen Sie **Wiederholung der Startreihenfolge aktivieren**, sodass der Server die Startreihenfolge automatisch erneut versucht.
      4. 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:
      1. Um Änderungen an der angezeigten Reihenfolge der Festplatten vorzunehmen, wählen Sie das Gerät aus und klicken dann entweder auf **Nach oben** oder **Nach unten**.
      2. Um die Änderungen anzuwenden, klicken Sie auf **OK**, oder, um alle Änderungen abzubrechen, klicken Sie auf **Abbrechen**.

ANMERKUNG: Für Dell PowerEdge-Server der 13. Generation werden nur die Details des aktuellen Startmodus für die Hardwareprofile angezeigt.

ANMERKUNG: Betriebssystembereitstellung von OMIVV schlägt fehl, wenn der Boot-Modus auf dem Ziel-Computer auf UEFI gesetzt ist.

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. Wenn Sie mit dem Festlegen der Einstellungen fertig sind, klicken Sie 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 **Next** (Weiter).
12. Klicken Sie im Fenster **Zusammenfassung** auf **Fertigstellen**.

Nächste Schritte
Das Profil wird automatisch gespeichert und wird im **Hardwareprofil**-Fenster angezeigt.

Neues Hardwareprofil klonen

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte**Bereitstellung** → **verwalten** den Punkt **Bereitstellungsvorlagen** → **Hardwareprofile**.
2. Klicken Sie auf das Symbol klicken.
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 im Textfeld **Beschreibung** eine `Beschreibung` ein. Die Beschreibung ist optional.
4. Klicken Sie auf **Next (Weiter)**.
5. Zum Auswählen eines konformen Referenzservers, der von vCenter verwaltet wird und erfolgreich vom Dell OpenManage-Plugin auf der **Referenzserver**-Seite inventarisiert wird, klicken Sie auf **Durchsuchen**.
6. Klicken Sie auf die Option **Einstellungen für geklonten Referenzserver**, um alle Hardwareeinstellungen des Referenzservers zu extrahieren.
7. Klicken Sie auf **Next (Weiter)**.
   Das Extrahieren der Einstellungen kann einige Minuten in Anspruch nehmen.
8. Klicken Sie auf **Next (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**Bereitstellung** → **verwalten** den Punkt **Bereitstellungsvorlagen** → **Hardwareprofile**.
   Die Hardwareprofile werden angezeigt.
2. Um ein Profil zu bearbeiten, wählen Sie ein Profil aus, und klicken Sie 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

Info über diese Aufgabe

ANMERKUNG: Das Löschen eines Hardwareprofils, das Teil einer laufenden Bereitstellungsaufgabe ist, kann dazu führen, dass die Löschungs-Aufgabe fehlschlägt.

Schritte

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

Voraussetzungen

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

Schritte

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte**Bereitstellung** → **verwalten** den Punkt **Bereitstellungsvorlagen** → **Hypervisorprofile**.
2. Klicken Sie auf der Seite **Hypervisor-Profile** auf das Symbol für .
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. Speicherort für das Referenz-ISO kann eines der folgenden Formate sein:

   - NFS-Format: host:/freigabe/hypervisor_image.iso
   - CIFS-Format: \\host\freigabe\hypervisor.iso

   Wenn Sie eine CIFS-Freigabe verwenden, geben Sie Werte in die Felder **Benutzername**, **Kennwort** und **Kennwort bestätigen** ein. Die Kennwörter müssen 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 **Apply (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 das Symbol .
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

Info über diese Aufgabe

ANMERKUNG: Das Löschen eines Hypervisor-Profils, das Teil einer laufenden Bereitstellungsaufgabe ist, kann dazu führen, dass die Aufgabe fehlschlägt.

Schritte

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte**Bereitstellung** → **verwalten** den Punkt **Bereitstellungsvorlagen** → **Hypervisorprofile**.
2. Wählen Sie ein Profil aus und klicken Sie auf das Symbol klicken.
3. Klicken Sie im Bestätigungsdialogfeld, um das Profil zu löschen, auf **Löschen** oder zum Abbrechen des Vorgangs auf **Abbrechen**.

Erstellen von Bereitstellungsvorlagen

Info über diese Aufgabe

Eine Bereitstellungsvorlage enthält entweder ein Hardwareprofil, ein Hypervisor-Profil oder beides. Der Bereitstellungsassistent verwendet diese Vorlage, um Serverhardware einzurichten und Hosts innerhalb von vCenter bereitzustellen.

Schritte

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte**Bereitstellung** → **verwalten** **Bereitstellungsvorlagen**.
2. Klicken Sie auf das Symbol klicken.
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. Wählen Sie ein **Hardwareprofil** oder **Hypervisor-Profil**.
6. Klicken Sie zum Übernehmen der Profilauswahl und zum Speichern der Änderungen auf **Speichern**, oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.

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**Bereitstellung** → **verwalten** **Bereitstellungsvorlagen**.
   Die Bereitstellungsvorlage Profile wird angezeigt.
2. Wählen Sie auf der Seite **Bereitstellungsvorlage** eine Vorlage aus und klicken Sie auf das Symbol für .
3. Zum Ändern geben Sie den neuen Namen der Vorlage ein, und klicken Sie auf **Anwenden**.

Stellen Sie sicher, dass die Vorlage einen eindeutigen Namen hat.

Löschen von Bereitstellungsvorlagen

1. Wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte**Bereitstellung** → **verwalten Bereitstellungsvorlagen**.
2. Wählen Sie auf der Seite **Bereitstellungsvorlage** eine Vorlage aus und klicken Sie auf das Symbol für ✖.
3. Um zu bestätigen, dass die Vorlage gelöscht ist, klicken Sie auf **Löschen** im Dialogfeld oder zum Abbrechen des Vorgangs auf **Abbrechen**.

Infos zum Bereitstellungsassistenten

Der Bereitstellungsassistent beschreibt den Bereitstellungsprozess, der wie folgt lautet:

- Auswahl konformer Bare-Metal-Server.
- Auswahl einer Bereitstellungsvorlage, die aus Hardware- und Hypervisor-Profilen besteht.
- Auswahl des Installationsziels (Festplatte oder iDSDM).
  Wenn Sie einen Hypervisor bereitstellen, können Sie die Bereitstellung auf einem internen Dual-SD-Modul durchführen. Das interne Dual-SD-Modul sollte im 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 Bereitstellungsassistenten übersprungen und Sie gelangen direkt zur Seite Bereitstellung planen.

ANMERKUNG: Mit einer Testlizenz können Sie den Bereitstellungsassistenten 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.

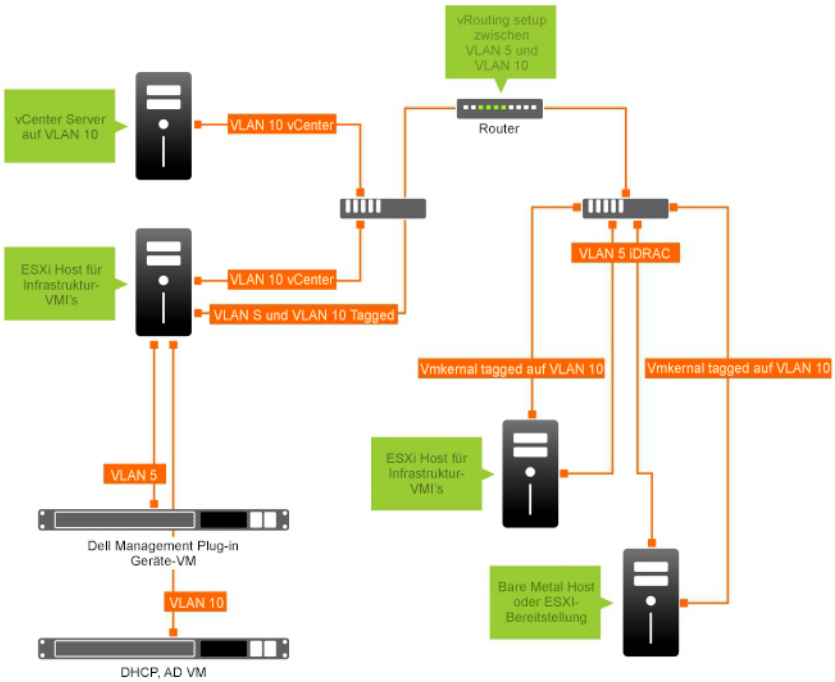

Abbildung 2. VLAN-Netzwerk.

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

Voraussetzungen

Stellen Sie sicher, dass Sie eine Bereitstellungsvorlage mit Hardwareprofil und Hypervisor-Profil und Verbindungsprofil für das vCenter vor dem Ausführen des Bereitstellungsassistenten erstellen.

Info über diese Aufgabe

Ausführen des Bereitstellungs-Assistenten:

Schritte

1. Wählen Sie in OpenManage Integration for VMware vCenter die Registerkarte **Verwalten** → **Bereitstellung**.
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** die folgenden Teilschritte aus:
   a. Unter **Bereitstellungsvorlage**, zum Zuweisen einer Bereitstellungsvorlage auf den ausgewählten Servern wählen Sie eine vorhandene Bereitstellungsvorlage aus **Bereitstellungsvorlage wählen**.

      Sie können eine der folgenden Bereitstellungsvorlagen aus der Dropdownliste auswählen:

      - Wenn Sie eine Bereitstellungsvorlage nur für ein Hardwareprofil 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 Hardwareprofil auswählen, werden Sie automatisch dazu aufgefordert, Informationen für die Seite Bereitstellungszeitplan anzugeben.

b. Unter **Hypervisor-Installationsinformationen** wählen Sie eine der folgenden Optionen:

- **Festplatte** – stellt einen Hypervisor auf der Festplatte 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:

– Markieren Sie das Kontrollkästchen **Hypervisor auf der ersten Festplatte für die Server, die über kein internes Dual-SD-Modul verfügen**, wenn Sie möchten, dass ein Hypervisor auf der ersten Festplatte der Server bereitgestellt wird.

VORSICHT: Wenn Sie diese Option auswählen und den Hypervisor auf der ersten Festplatte 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 der ersten Festplatte 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. Beim Verwenden von DHCP empfiehlt Dell, dass eine IP-Reservierung für ausgewählte NIC-MAC-Adressen verwendet wird.

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 .
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:
        1. Wählen Sie in **vCenter-Instanz** die Server-Instanz, die einen Host nach der Bereitstellung verwaltet.
        2. In **vCenter-Ziel-Container**, klicken Sie auf **Durchsuchen**, um nach den vCenter-Zielen zu suchen.
        3. 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:
        1. Wählen Sie **Zeitplan Bereitstellungs-Job**
            - Verwenden Sie das Kalender-Bedienfeld, um ein Datum auszuwählen.
            - Geben Sie die Uhrzeit ein.
        2. 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**.

Nächste Schritte

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
   - Details zum Bereitstellungsjob (führen Sie für weitere Informationen den Mauszeiger darauf)
   - Start- und Endzeit

Sie können die gesamten Informationen zu einem Bereitstellungsjob als Text-Popup anzeigen, indem Sie den Job auswählen und Ihren Cursor über die Spalte **Details** für diesen Bereitstellungsjob bewegen.

4. Klicken Sie zum Abbrechen des Bereitstellungsjobs auf das Symbol für klicken.
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.

Festlegen der Zeit für den Bereitstellungs-Job

Die Einrichtung und Bereitstellung von Bare-Metal-Servern kann abhängig von bestimmten Faktoren zwischen 30 Minuten und mehreren Stunden dauern. Beim Starten eines Bereitstellungs-Jobs sollten Sie Ihre Bereitstellungszeit anhand der aufgeführten Richtwerte planen. Die erforderliche Zeit für eine vollständige Einrichtung und Bereitstellung hängt von Bereitstellungstyp, der Komplexität und der Anzahl an gleichzeitig ausgeführten Bereitstellungs-Jobs ab. Die folgende Tabelle enthält Richtwerte für die ungefähre Dauer für Bereitstellungs-Jobs. Bereitstellungs-Jobs werden in Batches von bis zu fünf gleichzeitigen Servern ausgeführt, um die insgesamt erforderliche Zeit für die Bereitstellung zu verringern. Die genaue Anzahl an gleichzeitigen Jobs hängt von den verfügbaren Ressourcen ab.

Tabelle 37. Mögliche Zeitszenarios für Bereitstellungs-Jobs

Bereitstellungstyp	Ungefähre Zeit pro Bereitstellung
Nur Hypervisor	Zwischen 30 Minuten und 130 Minuten
Hypervisor- und Hardware-Profile	1 bis 4 Stunden

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 Datacenter hinzugefügt wurde oder ob eine ausstehende Bereitstellung geplant ist. Administratoren können anhand dieser Status feststellen, ob ein Server mit in einen Bereitstellungsauftrag aufgenommen werden sollte. Die möglichen Status sind:

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 ISO-Images

Voraussetzungen

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

Schritte

1. Rufen Sie die Seite support.dell.com auf.
2. Unter **Ein Produkt suchen** klicken Sie auf **Produkte anzeigen**.
3. Unter **Ein Produkt wählen** klicken Sie auf **Server, Speicher und Netzwerke**, und wählen Sie **PowerEdge**.
4. Klicken Sie auf ein Dell PowerEdge Server Modell.
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**.

13

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.

Berichterstattung und Festsetzen der Kompatibilität für vSphere Hosts

Voraussetzungen

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 installiert oder aktualisiert wurde.

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.

Info über diese Aufgabe

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:

Schritte

1. Klicken Sie in OpenManage Integration for VMware vCenter auf 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 die nicht konformen Hosts zusammen mit Host-IP-Adresse oder Hostname, Modell, Verbindungsprofil, CSIOR-Status, OMSA Status, Hypervisor- und iDRAC-Lizenz-Status 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 des Datenrasters.
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**. Weitere Informationen finden Sie unter Erstellen eines neuen Verbindungsprofils. 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 Sie OMSA entweder manuell oder über den Konformitätsassistenten, sobald der Host ausgeführt wird und wenn OMSA nicht konfiguriert ist, und führen Sie 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**.

Reparieren der iDRAC-Lizenzkonformität für vSphere-Hosts

Info über diese Aufgabe

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. Wenn der Link **Bestandsaufnahme-Job ausführen** auf der Seite **vSphere-Hosts** deaktiviert ist, sind keine vSphere-Hosts vorhanden, die aufgrund der iDRAC-Lizenz nicht konform sind.

Schritte

1. Klicken Sie in OpenManage Integration for VMware vCenter auf 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.

Verwenden von OMSA mit Servern der 11. Generation

Zur Verwaltung von Dell PowerEdge Servern der 11. Generation erfordert OMIVV, dass OMSA ausgeführt wird. Bei einem Host der 11. Generation, der durch OMIVV bereitgestellt wird, wird OMSA automatisch installiert. Für Hosts der 11. Generation, die Sie manuell bereitstellen, können Sie eine der folgenden Möglichkeiten wählen:

- Installieren und konfigurieren Sie OMSA unter Verwendung OMIVV. Siehe OMSA-Trap-Ziel einrichten.
- Installieren und konfigurieren Sie OMSA manuell. Siehe Bereitstellen von OMSA-Agent auf ESXi-System.

ANMERKUNG: Durch Bereitstellung des OMSA-Agenten unter Verwendung von OMIVV startet OMIVV den HttpClient-Dienst, aktiviert den Port 8080 und gibt ihn nach ESXi 5.0 frei, um OMSA VIB herunterzuladen und zu installieren. Sobald die OMSA-Installation abgeschlossen wurde, wird der Dienst automatisch angehalten und der Port wird 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 ESXi-System

Info über diese Aufgabe

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

Schritte

1. Falls OMSA noch nicht installiert ist, installieren Sie das vSphere-Befehlszeilentool (vSphere CLI) von **http://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 einen Neustart des Hosts nach Abschluss der Installation.

OMSA-Trap-Ziel einrichten

Info über diese Aufgabe

Auf allen Servern der 11. Generation von Hosts muss OMSA konfiguriert sein.

ANMERKUNG: OMSA ist nur auf den Dell-Servern vor Dell PowerEdge-Servern der 12. Generation erforderlich.

So richten Sie ein OMSA-Trap-Ziel ein:

Schritte

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, so dass 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 **Änderungen anwenden**.
9. Wiederholen Sie die Schritte 1 bis 8, um zusätzliche Ereignisse zu konfigurieren.

Berichterstattung und Korrektur der Konformität von Bare-Metal-Servern

Voraussetzungen

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.

Info über diese Aufgabe

Anzeigen und Korrigieren der Liste von nicht konformen Bare-Metal-Servern:

Schritte

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 das Symbol .
   d. Um die Inhalte des Datenrasters 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 des Datenrasters.
2. Zum Korrigieren nicht konformer Server klicken Sie auf **Nicht-konforme Server korrigieren** .
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 Servern erfordert, dass mindestens eine der folgenden Firmware-Komponenten aktualisiert wird:
   - iDRAC IP (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 Konformität der lizenzierten Server erneut prüfen klicken. Weitere Informationen finden Sie unter Erneute Prüfung der Bare-Metal-Server-Konformität.
   - BIOS
   - LC
5. Klicken Sie auf **Next** (Weiter).
6. Prüfen Sie die Maßnahmen, die an den Firmwarekomponenten von nicht konformen Bare-Metal-Servern durchgeführt werden, im Fenster **Zusammenfassung**.

7. Klicken Sie auf **Fertigstellen**.

Reparatur der iDRAC-Lizenzkonformität für Bare-Metal-Server

Info über diese Aufgabe

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 **Konformität der lizenzierten Server erneut prüfen** auf Seite **Bare-Metal-Server** aktiviert ist, gibt es Bare-Metal-Server, die aufgrund der iDRAC-Lizenz nicht konform sind.

Schritte

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 **Lizenzierten Server erneut prüfen**.

Erneute Prüfung der Bare-Metal-Server-Konformität

Info über diese Aufgabe

Bei Servern, für die Sie außerhalb des OMIVV Plug-ins die Kompatibilität hergestellt haben, führen Sie die folgende manuelle Server-Konformität-Neuprüfung durch:

Schritte

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Bereitstellung** → **Verwalten** auf **Konformität der lizenzierten Server erneut prüfen**.
2. Klicken Sie zum Aktualisieren der Liste im Fenster **Nicht konforme Server** auf **Aktualisieren**.
3. Zur Ausführung der Neuprüfung klicken Sie auf **Lizenzierten Server erneut prüfen**.

Nachdem Sie Ihr System erfolgreich korrigiert haben, wird die Liste aktualisiert und das System als **konform** aufgeführt. Ist dies nicht der Fall, wird es weiterhin als **nicht konform** aufgeführt.

14

Sicherheitsrollen und Berechtigungen

OpenManage Integration for VMware vCenter speichert Benutzeranmeldeinformationen in einem verschlüsselten Format. Es liefert keine Kennwörter an Clientanwendungen, um nicht ordnungsgemäße Anforderungen zu vermeiden. Die Datenbanksicherungen werden mithilfe benutzerdefinierter Sicherheitsausdrücke vollständig verschlüsselt, sodass die Daten nicht missbräuchlich verwendet werden können.

Als Standardeinstellung besitzen Benutzer in der Administratorgruppe alle Rechte. Die Administratoren können alle Funktionen des OpenManage Integration for VMware vCenter innerhalb von VMware vSphere Web Client verwenden. Wenn Sie wollen, dass ein Benutzer mit erforderlichen Berechtigungen das Produkt verwaltet, 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.

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.

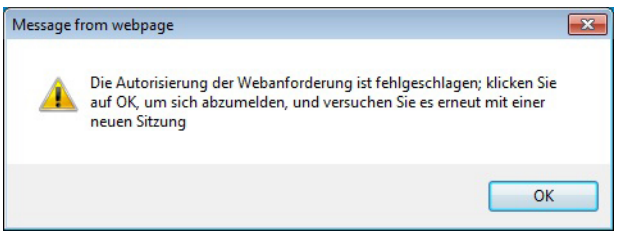

Abbildung 3. Sicherheitsfehlermeldung

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

15

Fehlerbehebung

In diesem Abschnitt finden Sie Antworten auf Fragen zur Fehlerbehebung. In diesem Abschnitt werden die folgenden Themen behandelt:

- Häufig gestellte Fragen (FAQs)
- Probleme bei der Bare-Metal-Bereitstellung

Häufig gestellte Fragen (FAQs)

In diesem Abschnitt werden einige allgemeine Fragen und Lösungen beschrieben.

Warum ist es nicht möglich, über die Schaltfläche „Alle exportieren“ CSV-Dateien in Google Chrome zu exportieren?

Nach der Registrierung eines vCenter Server gibt die Schaltfläche **Alle exportieren** einen Fehler zurück, wenn Sie einen Host hinzufügen und ein Verbindungsprofil erstellen und dann die Bestandsdetails des Hosts anzeigen. Über die Schaltfläche **Alle exportieren** werden keine Informationen in CSV-Dateien exportiert.

ANMERKUNG:
Im **Inkognito-Modus** können Sie in keinen Versionen von Google Chrome Browser Informationen mit der Schaltfläche **Alle exportieren** in eine .CSV-Datei exportieren.

Lösung: Um die Informationen mit der Schaltfläche **Alle exportieren** in eine CSV-Datei in Google Chrome zu exportieren, deaktivieren Sie den **Modus Inkognito** 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

Nach Aufhebung der Registrierung von vCenter in der früheren OMIVV-Version und Registrierung desselben vCenter mit späteren OMIVV-Versionen wird das Dell Symbol nicht mehr angezeigt.

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. Navigieren Sie im vCenter Gerät zum Ordner **/etc/vmware/Vsphere Client/VC-Pakete/Vsphere-Client-Ruhe** und prüfen Sie, ob alte Daten vorhanden sind:
   - 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

Die Einstellungen des Konfigurationsassistenten werden bei jedem Aufruf mit Standardeinstellungen überschrieben

Nachdem Sie Bestands- und Serviceabrufpläne, Ereignisse und Alarme im Erstkonfigurationsassistenten konfiguriert und den Konfigurationsassistenten erneut gestartet haben, werden die vorherigen Bestands- und Serviceabrufpläne nicht beibehalten. Die Bestands- und Servicepläne werden bei jedem Aufruf des Konfigurationsassistenten auf die Standardeinstellungen zurückgesetzt. Die Ereignisse und Alarme behalten jedoch die aktualisierten Einstellungen.

Auflösung/Problemumgehung: Replizieren Sie den vorherigen Zeitplans in den Seiten der Bestands- und Serviceabrufpläne, bevor Sie die Funktionen des Assistenten ausführen. So kann der vorherige Zeitplan nicht durch die Standardeinstellungen überschrieben werden.

Betroffene Version: 3.0 und höher

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:
  a. Weisen Sie Benutzern, die keine Administratoren sind, bei Bedarf zusätzliche Berechtigungen zu. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für Nicht-Administrator-Benutzer.
  b. Führen Sie einen Neustart des registrierten OMIVV-Geräts durch.
  c. Melden Sie sich vom Web-Client ab, und melden Sie sich dann erneut an.
- Für Administratorbenutzer:
  a. Führen Sie einen Neustart des registrierten OMIVV-Geräts durch.
  b. 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

Warum schlägt die Bestandsaufnahme bei der Durchführung einer Firmware-Aktualisierungsaufgabe auf dem ESXi 5.x-Host fehl?

Möglicherweise wird der ESXi im Host nicht mit der neuen iDRAC-IP synchronisiert, wenn Sie die nach der Registrierung eines v Center Servers die Firmware-Aktualisierungsaufgabe auf einem ESXi 5.x-Host ausführen und iDRAC als Komponente aus dem Bildschirm **Komponente auswählen** auswählen. Dies führt zu einer ungültigen im iDRAC IP für OMIVV. Das heißt, Sie können auf diesem Host keine erfolgreiche Bestandsaufnahme durchführen.

Lösung: Starten Sie den Daemon sfcdb auf dem ESXi-Host, um dieses Problem zu beheben: 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. Wie kann ich eine gültige iDRAC-IP-Adresse beziehen?

Info über diese Aufgabe

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“.

Schritte

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: Die Host-Bestandsaufnahme kann auch fehlschlagen, wenn der WBEM Dienst nicht aktiviert ist. Weitere Informationen zum WBEM-Dienst finden Sie unter Verbindungsprofil erstellen.

Bei Ausführung des Assistenten zum Beheben nicht kompatibler vSphere-Hosts wird der Status eines bestimmten Hosts als „Unbekannt“ angezeigt. Warum?

Wenn Sie den Assistenten zum Beheben nicht kompatibler vSphere-Hosts ausführen, um nicht kompatible Hosts zu korrigieren, wird der Status des entsprechenden Hosts als „Unbekannt“ angezeigt. Dies kommt vor, 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 OMIVV-Vorgänge.

Betroffene Version: 3.1

Das Dell Management Center zeigt nicht alle entsprechenden Protokolle an beim Versuch, nach einer Schweregrad-Kategorie zu filtern. Wie kann ich alle Protokolle anzeigem?

Wenn Sie eine Schweregrad-Kategorie als Filter für die Protokolldaten wählen, indem Sie **Alle Kategorien** aus dem Drop-Down - Menü wählen, werden alle Protokolle, die in eine bestimmte Kategorie gehören, genau angezeigt. Wenn Sie jedoch Filter auswählen, indem Sie **Info** aus dem Drop-Down-Menü wählen, werden die Firmware-Aktualisierungsprotokolle nicht angezeigt und nur die Aufgaben-Initiierungsprotokolle werden angezeigt.

Lösung: Zur Anzeige aller Protokolle wählen Sie im Dell Management Center **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 dem PSC aktualisiert werden. Das Skript verwendet den alten Zertifikat-Fingerabdruck als Eingabe-Argument und das neue Zertifikat wird installiert. Beim alten Zertifikat handelt es sich um das Zertifikat vor dem Austausch und beim neuen Zertifikat handelt es sich um das Zertifikat nach dem Austausch. Besuchen Sie 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 für weitere Informationen.

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 des Dienstprogramms vSphere Certificate Manager. Lesen Sie dazu Ersetzen der Zertifikate einer vCenter Windows Installation.
- 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. Lesen Sie dazu Ersetzen der Zertifikate auf dem vCenter Server-Gerät.

Die mit den genannten Verfahren abgerufene Ausgabedaten sollten jeweils `24 Services aktualisiert` und `26 Services aktualisiert` anzeigen. Wenn bei den Ausgabedaten `0 Services aktualisiert` angezeigt wird, ist der alte Zertifikat-Fingerabdruck falsch. Sie können die folgenden Schritte ausführen, um den alten Zertifikat-Fingerabdruck abzurufen. Verwenden Sie auch das folgende Verfahren zum Abrufen des alten Zertifikat-Fingerabdrucks, wenn der **vCenter Certificate Manager** nicht eingesetzt wird, um die Zertifikate zu ersetzen:

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. Lesen Sie dazu Abrufen des alten Zertifikats aus dem Managed Object Browser (MOB).
2. Extrahieren Sie den Fingerabdruck vom alten Zertifikat. Lesen Sie dazu Extrahieren des Fingerabdrucks vom alten Zertifikat.

Betroffene Version: 3.0 und höher, vCenter 6.0 und höher

Ersetzen der Zertifikate einer vCenter Windows Installation

Info über diese Aufgabe

Führen Sie die folgenden Schritte aus, wenn das Dienstprogramm vSphere Certificate Manager verwendet wird, um die Zertifikate einer vCenter Windows Installation zu ersetzen:

Schritte

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.

Nächste Schritte

OMIVV wird jetzt erfolgreich gestartet.

Ersetzen der Zertifikate auf dem vCenter Server-Gerät

Info über diese Aufgabe

Führen Sie die folgenden Schritte durch, wenn das Dienstprogramm vSphere Certificate Manager verwendet wird, um die Zertifikate eines vCenter Server-Geräts zu ersetzen:

Schritte

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.

Nächste Schritte
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.

Info über diese Aufgabe
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.

Schritte

1. Erstellen Sie auf dem PSC den Ordner **C: \Certificates** 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 Kennwort 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 den Wert des entsprechenden Felds „sslTrust“. Der Wert des Felds „sslTrust“ 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**.

Nächste Schritte

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.
- Extrahieren Sie den Fingerabdruck unter Verwendung einer Befehlszeile auf dem Gerät. Lesen Sie dazu Extrahieren des Fingerabdrucks unter Verwendung der Befehlszeile.

Extrahieren des Zertifikat-Fingerabdrucks mit dem Hilfsprogramm zur Anzeige von Zertifikaten

Info über diese Aufgabe

Führen Sie folgende Schritte durch, um den Zertifikat-Fingerabdruck zu entpacken:

Schritte

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.

Der Assistent der Firmware-Aktualisierung zeigt eine Meldung an, die besagt, dass die Bündel nicht aus dem Firmware Repository abgerufen wurden. Wie kann ich mit der Firmware-Aktualisierung fortfahren?

Wenn Sie im Web-Client den Firmware-Aktualisierungs-Assistenten für einen einzelnen Host ausführen, zeigt der Bildschirm **Komponenten auswählen** die Firmwaredetails für die Komponenten an. Wenn Sie die gewünschten Firmware-Aktualisierungen wählen und zweimal auf **Zurück** klicken, um die Seite **Willkommen** zu erreichen und dann auf **Weiter** klicken, wird eine Meldung angezeigt, die besagt, dass die Bündel nicht aus dem Firmware Repository im Bildschirm **Aktualisierungsquelle auswählen** abgerufen wurden.

Lösung: Sie können die gewünschten Firmware-Aktualisierungen auswählen und auf **Weiter** klicken, um mit der Firmware-Aktualisierung fortzufahren.

Betroffene Version: 3.0 und höher

Warum wird in der Verwaltungskonsole das Feld Aktualisierungs-Repository-Pfad nicht auf den Standardpfad gesetzt, nachdem ich das Gerät auf die werkseitigen Einstellungen zurückgesetzt habe?

Navigieren Sie nach dem Zurücksetzen des Gerät zur **Verwaltungskonsole**, und klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**. Auf der Seite **Geräteeinstellungen** wurde der **Aktualisierungs-Repository-Pfad** nicht auf den Standardpfad geändert.

Lösung: Kopieren Sie in der **Verwaltungskonsole** den Pfad aus dem Feld **Standard-Aktualisierungs-Repository** manuell in das Feld **Aktualisierungs-Repository -Pfad**.

Warum die Firmwareaktualisierung für 30 Hosts auf Cluster-Ebene fehlschlägt

VMware empfiehlt Ihnen, Cluster mit identischer Server-Hardware aufzubauen. Für die Firmware-Aktualisierung auf Cluster-Ebene befindet sich die Anzahl der Hosts nahe der Grenzwerte für einen Cluster (gemäß der Empfehlung durch VMware) oder bestehend aus verschiedenen Modellen von Dell Servern wird die Nutzung des vSphere Web-Clients empfohlen.

Warum wird der Service- und Bestandsaufnahme-Zeitplan für alle vCenter 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, können Sie ein Kontrollkästchen mit der Meldung **Für alle registrierten vCenter übernehmen** anzeigen. Wenn Sie das Kontrollkästchen auswählen und **Anwenden** drücken, wird die Einstellung für ein bestimmtes vCenter, das Sie ursprünglich ausgewählt haben, übernommen und nicht für alle vCenter. Die Meldung **Für alle registrierten vCenter übernehmen** wird nicht angewendet, wenn der Service- oder Bestandsaufnahmezeitplan von 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 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 noch einmal zurück auf die Seite „Einstellungen“ navigiere?

Wenn Sie in vSphere v5.5 im Web-Client auf eine andere Seite navigieren und danach zurück zur Seite **Einstellungen** gehen, schlägt das Laden der Seite manchmal fehl und es wird weiterhin das drehende Symbol angezeigt. 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

Warum wird der Fehler „Task kann nicht in der Vergangenheit geplant werden“ auf der Bestandsaufnahme-Zeitplan/Service-Zeitplan-Seite beim Assistenten zur Erstkonfiguration 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

Warum wird das Installationsdatum als 31.12.1969 für einige Firmwareversionen auf der Firmware-Seite angezeigt?

Das im Web-Client angezeigte Datum wird als 31.12.1969 für einige Firmwares eines Hosts auf der Firmware-Seite angezeigt. Sollte kein Firmware-Installationsdatum zur Verfügung stehen, wird dieses 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

Wiederholte globale Aktualisierungsvorgänge verursachen, dass eine Ausnahme im aktuellen Aufgabenfenster angezeigt wird. Wie kann ich den Fehler beheben?

Wenn Sie versuchen, wiederholt auf die Schaltfläche „Aktualisieren“ zu drücken, tritt möglicherweise eine Ausnahme in der VMware-Benutzeroberfläche auf.

Auflösung: Sie können diese Fehlermeldung schließen und fortfahren.

Betroffene Version: 2.2 und höher

Warum ist die Web-Client-Benutzeroberfläche für einige der Dell-Bildschirme in IE 10 verzerrt?

Es kann vorkommen, dass bei Aufruf eines Popup-Dialogfelds die Daten im Hintergrund weiß und verzerrt sind.

Lösung: Schließen Sie das Dialogfeld und der Bildschirm wird wieder normal angezeigt.

Betroffene Version: 2.2 und höher

Obwohl die Registrierung des Plug-ins im vCenter erfolgreich war, wird das OpenManage Integration-Symbol im Web-Client nicht angezeigt. Warum?

Das OpenManage Integration-System wird im Web-Client erst angezeigt, wenn die vCenter Web-Client-Dienste neu gestartet oder das Feld neu geladen wird. Bei der Registrierung des OpenManage Integration for VMware vCenter Geräts, wird das Gerät mit Desktop-Client und Web-Client registriert. Wenn Sie die Registrierung aufheben und dann dieselbe erneut oder eine neue Version des Geräts registrieren, wird sie erfolgreich mit beiden Clients registriert. Das Dell-Symbol wird jedoch möglicherweise nicht im Web-Client angezeigt. Dies liegt an einem Caching-Problem von VMware. Um das Problem zu beheben, müssen Sie den Web-Client-Dienst auf dem vCenter Server neu starten. Dann wird das Plug-in auf der Benutzeroberfläche angezeigt.

Lösung: Starten Sie den Web-Client-Dienst auf dem vCenter Server neu.

Betroffene Version: 2.2 und höher

In meinem Repository sind Bundle für das ausgewählte 11G-System hinterlegt. Warum wird bei der Firmware-Aktualisierung dennoch ausgegeben, dass keine Bundle für eine Firmware-Aktualisierung verfügbar sind?

Wenn ich im Sperrmodus einen Host in das Verbindungsprofil einfüge, wird die Bestandsaufnahme zwar gestartet, schlägt jedoch mit der Meldung fehl, dass kein Remote Access Controller gefunden wurde oder auf dem Host keine Bestandsaufnahme unterstützt wird. Sollte die Bestandsaufnahme nicht auch von Hosts im Sperrmodus unterstützt werden?

Wenn Sie den Host in den Sperrmodus versetzen oder den Sperrmodus beenden, müssen Sie 30 Minuten warten, bevor Sie den nächsten Vorgang durchführen können. Wenn Sie einen 11G Host für die Firmware-Aktualisierung verwenden, zeigt der Assistent zur Firmware-Aktualisierung keine Bundle, selbst wenn im Repository Bundle für das System vorhanden sind. Möglicherweise ist das Senden von Traps an OpenManage Integration durch OMSA auf dem 11G Host nicht konfiguriert.

Lösung: Stellen Sie die Kompatibilität des Hosts sicher. Verwenden Sie hierfür den Kompatibilitätsassistenten des OpenManage Integration-Web-Clients. Wenn er nicht kompatibel ist, beheben Sie das Problem mit der Option „Host-Konformität beheben“.

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 Aktualisierung der Intel-Netzwerkkarte von 14.5 oder 15.0 auf 16.x mit OMIVV kann aufgrund der Staging-Anforderung des DUP nicht erfolgreich durchgeführt werden.

Dies ist ein bekanntes Problem bei NIC 14.5 und 15.0. Stellen Sie sicher, dass Sie vor der Aktualisierung der Firmware auf 16.x den benutzerdefinierter Katalog für die Aktualisierung auf 15.5.0 verwenden.

Betroffene Version: Alle

Nach einer Firmware-Aktualisierung mit einem ungültigen DUP wird als Status der Hardwareaktualisierung in der vCenter Konsole kein Fehler und auch nach mehreren Stunden keine Zeitüberschreitung gemeldet. In den LC-Aufforderungen wird der Status der Aufgabe jedoch als „Fehlgeschlagen“ gemeldet. Warum?

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 Administration-Portal nicht erreichbare Speicherorte für Aktualisierungs-Repositorys an?

Wenn Sie einen nicht erreichbaren Pfad für das Aktualisierungs-Repository angeben, wird oben in der Ansicht „Geräteaktualisierung“ die Fehlermeldung „Fehler bei der Verbindung mit der URL ...“ angezeigt. Der Pfad für das Aktualisierungs-Repository wird jedoch nicht auf den Wert vor der Aktualisierung gelöscht.

Lösung: Bewegen Sie sich von dieser Seite auf eine andere Seite und aktualisieren Sie sie.

Betroffene Version: Alle

Warum wurde mein System bei der Durchführung einer 1:n-Firmware-Aktualisierung nicht in den Wartungsmodus gesetzt?

Einige Firmware-Aktualisierungen können auch ohne Neustart des Hosts ausgeführt werden. In diesem Fall wird die Firmware-Aktualisierung durchgeführt, ohne dass der Host in den Wartungsmodus wechselt.

Warum wird der globale Funktionszustand des Gehäuses noch als funktionsfähig angezeigt, obwohl der Status einiger Netzteile als kritisch gemeldet wird?

Der globale Funktionszustand des Gehäuses im Bezug auf die Stromversorgung basiert auf den Redundanzrichtlinien und richtet sich außerdem danach, ob der Strombedarf des Gehäuses über die Netzteile, die noch online und funktionsfähig sind, gedeckt wird. Selbst wenn also einige Netzteile nicht funktionieren, kann der Strombedarf des Gehäuses insgesamt gedeckt sein. Der globale Funktionszustand wird dann als funktionsfähig ausgeben. Weitere Informationen zu Stromversorgung und der Energieverwaltung finden Sie im Benutzerhandbuch zur Dell PowerEdge M1000e Chassis Management Controller-Firmware.

Warum wird auf der Seite „Systemüberblick“ in der Ansicht „Prozessor“ als Prozessorversion „nicht verfügbar“ angezeigt?

In PowerEdge Dell Servern der 12. Generation und neueren Generationen wird die Version des Prozessors in der Spalte „Marke“ angezeigt. In früheren Generationen wird die Prozessorversion in der Spalte „Version“ angezeigt.

Warum wird eine Ausnahme zurückgegeben, wenn ich nach der Bearbeitung des Verbindungsprofils auf dem Web-Client auf „Fertigstellen“ klicke?

Dies kann vorkommen, wenn der vCenter Server nicht über FDQN, sondern über IP am Gerät registriert wird. Das Verbindungsprofil kann über den Web-Client bearbeitet werden.

Lösung: Die Neuregistrierung des vCenter-Servers am selben Gerät kann das Problem nicht beheben. Der Server muss neu eingerichtet und mit FDQN registriert werden.

Warum werden die Verbindungsprofile, denen der Host zugeordnet ist, bei Erstellung/ Bearbeitung eines Verbindungsprofils auf der Web-Benutzeroberfläche nicht angezeigt?

Dies kann vorkommen, wenn der vCenter Server nicht über FDQN, sondern über IP am Gerät registriert wird. Das Neuregistrieren des vCenter Servers am selben Gerät kann das Problem nicht beheben. Der Server muss neu eingerichtet und mit FDQN registriert werden.

Warum ist das Feld „Hostfenster auswählen“ auf der Web-Benutzeroberfläche bei der Bearbeitung von Verbindungsprofilen leer?

Dies kann vorkommen, wenn der vCenter Server nicht über FDQN, sondern über IP am Gerät registriert wird. Das Neuregistrieren des vCenter Servers am selben Gerät kann das Problem nicht beheben. Der Server muss neu eingerichtet und mit FDQN registriert werden.

Warum wird eine Fehlermeldung angezeigt, wenn ich auf den Firmware-Link klicke?

Info über diese Aufgabe

Wenn Ihre Netzwerkverbindung langsam ist (9.600 Bit/s), kann es vorkommen, dass Sie eine Kommunikationsfehlermeldung erhalten. wenn Sie im vSphere-Client für OpenManage Integration for VMware vCenter auf den Firmware-Link klicken. Das liegt daran, dass das Zeitlimit für die Verbindung abläuft, während Sie versuchen, die Softwarebestandsliste abzurufen. Der Timeout wird von Microsoft Internet Explorer initiiert. Für die Versionen 9 und 10 von Microsoft Internet Explorer liegt der Standardwert für die Zeitüberschreitung bei eingehenden Daten bei 10 Sekunden. Gehen Sie wie folgt vor, um das Problem zu beheben:

Abbildung 4. Firmware-Link-Kommunikationsfehler

Schritte

1. Öffnen Sie den Microsoft- Registrierungs-Editor (Regedit).
2. Navigieren Sie zum folgenden Ort in der Registrierung:
   KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
3. Fügen Sie einen DWORD-Wert für die Zeitüberschreitung beim Empfangen (ReceiveTimeout) hinzu.
4. Stellen Sie den Wert auf 30 Sekunden (30000) ein.
   In Ihrer Umgebung muss der Wert höher sein.
5. Beenden Sie Regedit.
6. Starten Sie Internet Explorer neu.

ANMERKUNG: Es reicht nicht aus, ein neues Internet Explorer-Fenster zu öffnen. Starten Sie den Internet Explorer-Browser komplett neu.

Welche Generation von Dell Servern konfiguriert und unterstützt OMIVV für SNMP-Traps?

OMIVV unterstützt OMSA SNMP-Traps auf Servern, die älter sind als die 12. Generation, und iDRAC-Traps auf Servern der 12. Generation.

Welche vCenter Server werden von OMIVV verwaltet?

OMIVV verwaltet nur registrierte vCenter Server im verknüpften oder nicht verknüpften Modus.

Unterstützt OMIVV vCenter im verknüpften Modus?

Ja, OMIVV unterstützt bis zu 10 vCenter Server entweder im verknüpften oder im nicht verknüpften Modus. Weitere Informationen darüber, wie OMIVV im verknüpften Modus arbeitet, finden Sie im Whitepaper *OpenManage Integration for VMware vCenter: Working in Linked Mode* unter www.dell.com.

Welche Porteinstellungen sind für OMIVV erforderlich?

ANMERKUNG: Wenn Sie den OMSA-Agenten in OMIVV über den Link Nicht kompatible vSphere Hosts beheben im Fenster Kompatibilität bereitstellen, startet OMIVV den HTTP-Client-Dienst und aktiviert auf Versionen ab ESXi 5.0 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. Ports für virtuelle Geräte

Portnummer	Protokolle	Port-Typ	Max. Verschlüsselungsebene	Richtung	Verwendung	Konfigurierbar
21	FTP	TCP	Keine	Ausgang	FTP-Befehls-Client	Nein
53	DNS	TCP	Keine	Ausgang	DNS-Client	Nein
80	HTTP	TCP	Keine	Ausgang	Dell Online-Datenzugriff	Nein
80	HTTP	TCP	Keine	Eingang	Verwaltungskonsole	Nein
162	SNMP-Agent	UDP	Keine	Eingang	SNMP-Agent (Server)	Nein
11620	SNMP-Agent	UDP	Keine	Eingang	SNMP-Agent (Server)	Nein
443	HTTPS	TCP	128–Bit	Eingang	HTTPS-Server	Nein
443	WSMAN	TCP	128–Bit	Ein/Aus	iDRAC/OMSA-Kommunikation	Nein
4433	HTTPS	TCP	128–Bit	Eingang	Automatische Ermittlung	Nein
2049	NFS	UDP	Keine	Ein/Aus	Öffentliche Freigabe	Nein
4001–4004	NFS	UDP	Keine	Ein/Aus	Öffentliche Freigabe	Nein
11620	SNMP-Agent	UDP	Keine	Eingang	SNMP-Agent (Server)	Nein

Tabelle 44. Verwaltete Knoten

Portnummer	Protokolle	Port-Typ	Max. Verschlüsselungsebene	Richtung	Verwendung	Konfigurierbar
162, 11620	SNMP	UDP	Keine	Ausgang	Hardware-Ereignisse	Nein
443	WSMAN	TCP	128–Bit	Eingang	iDRAC/OMSA-Kommunikation	Nein
4433	HTTPS	TCP	128–Bit	Ausgang	Automatische Ermittlung	Nein
2049	NFS	UDP	Keine	Ein/Aus	Öffentliche Freigabe	Nein
4001–4004	NFS	UDP	Keine	Ein/Aus	Öffentliche Freigabe	Nein
443	HTTPS	TCP	128–Bit	Eingang	HTTPS-Server	Nein
8080	HTTP	TCP		Eingang	HTTP-Server; lädt den OMSA VIB herunter und behebt nicht konforme vSphere-Hosts	Nein

Portnummer	Protokolle	Port-Typ	Max. Verschlüsselungsebene	Richtung	Verwendung	Konfigurierbar
50	RMCP	UDP/TCP	128–Bit	Ausgang	Remote Mail Check Protocol	Nein
51	IMP	UDP/TCP	k. A.	k. A.	IMP Logical Address Maintenance	Nein
5353	mDNS	UDP/TCP		Ein/Aus	Multicast DNS	Nein
631	IPP	UDP/TCP	Keine	Ausgang	Internet Printing Protocol (IPP)	Nein
69	TFTP	UDP	128–Bit	Ein/Aus	Trivial File Transfer (Einfache Dateiübertragung)	Nein
111	NFS	UDP/TCP	128–Bit	Eingang	SUN Remote Procedure Call (Portmap)	Nein
68	BOOTP	UDP	Keine	Ausgang	Bootstrap Protocol Client	Nein

Welche Mindestanforderungen gelten für die erfolgreiche Installation und den erfolgreichen Betrieb des virtuellen Geräts?

Die folgenden Einstellungen stellen die Mindestanforderungen für das Gerät dar:

- Google Chrome, Version 28 und höher
- Microsoft Internet Explorer, Version 9 und 10
- Mozilla Firefox ,Version 22 und später
- Reservierter Speicher: 2 GB

  ANMERKUNG: Für optimale Leistung empfiehlt Dell 3 GB.
- Laufwerk: 44 GB
- CPU: 2 virtuelle CPUs

Das Kennwort des für die Bare-Metal-Erkennung verwendeten Benutzers wurde nicht geändert, obwohl das Hardwareprofil für den selben Benutzer erfolgreich angewendet wurde, dessen Anmeldeinformationen in der iDRAC-Benutzerliste geändert wurden. Warum

Das Kennwort des von Discovery verwendeten Benutzers wird nicht gemäß den neuen Anmeldeinformationen geändert, wenn für die Bereitstellung nur die Hardwareprofilvorlage ausgewählt wird. Dieses Verhalten ist beabsichtigt, damit das Plug-in mit dem iDRAC kommunizieren kann, und in zukünftigen Bereitstellungen verwendbar ist.

Warum kann ich die auf den vCenter Hosts und Clusterseiten aufgeführten Details zur neuen iDRAC-Version nicht anzeigen?

Lösung: Aktualisieren Sie nach erfolgreicher Fertigstellung einer Firmware-Aktualisierungsaufgabe im vSphere-Web-Client die Seite **Firmware-Aktualisierung** und überprüfen Sie die Firmware-Versionen. Wenn auf der Seite die alten Versionen angezeigt werden, navigieren Sie in OpenManage Integration for VMware vCenter zur Seite **Hostkompatibilität** und prüfen Sie den CSIOR-Status des Hosts. Wenn CSIOR nicht aktiviert ist, aktivieren Sie CSIOR und starten Sie den Host neu. Wenn CSIOR bereits aktiviert ist, melden

Sie sich an der iDRAC-Konsole an, setzen Sie iDRAC zurück, warten Sie einige Minuten und aktualisieren Sie dann die Seite **Firmware-Aktualisierung**.

Wie teste ich Ereigniseinstellungen, indem ich mit OMSA Temperaturfehler an der Hardware simuliere?

Info über diese Aufgabe

Um sicherzustellen, dass die Ereignisse korrekt funktionieren, führen Sie folgende Schritte durch:

Schritte

1. Navigieren Sie in der OMSA-Benutzeroberfläche zu **Warnungsverwaltung** → **Plattformereignisse**.
2. Aktivieren Sie das Kontrollkästchen **Warnungen zu Plattformereignisfiltern aktivieren**.
3. Führen Sie einen Bildlauf bis ganz nach unten durch, und klicken Sie auf **Änderungen anwenden**.
4. Um sicherzugehen, dass ein bestimmtes Ereignis, etwas die Temperaturwarnung aktiviert ist, wählen Sie aus der Struktur auf der linken Seite die Option **Hauptsystemgehäuse** aus.
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, der direkt unter dem aktuell aufgeführten Messwert liegt.

    Beispiel: Wenn der aktuelle Messwert 27 lautet, stellen Sie den Schwellenwert auf **25** ein.
12. Nach Auswahl von **Änderungen anwenden** wird das Temperaturwarnungsereignis generiert.

    Um ein weiteres Ereignis auszulösen, stellen Sie die ursprünglichen Einstellungen wieder her. Verwenden Sie dafür dieselbe Option **Auf Werte setzen**. Ereignisse werden als Warnungen generiert und dann auf einen normalen Zustand gesetzt. Wenn alles ordnungsgemäß abläuft, navigieren Sie zur Ansicht **Aufgaben und Ereignisse in vCenter**. Hier sollte ein Ereignis für Temperatursondenwarnungen angezeigt werden.

    ANMERKUNG: Es gibt einen Filter für doppelte Ereignisse. Wenn Sie versuchen, dasselbe Ereignis zu oft hintereinander auszulösen, erhalten Sie nur ein Ereignis. Um alle Ereignisse anzuzeigen, müssen Sie mindestens 30 Sekunden zwischen dem Auslösen der Ereignisse warten.

OMSA-Agent ist auf dem OMIVV Hostsystem installiert. Trotzdem erhalte ich Fehlermeldungen, die darauf hinweisen, dass OMSA nicht installiert ist. Wie kann ich das Problem beheben?

Info über diese Aufgabe

Um dieses Problem auf einem Server der 11. Generation zu beheben:

Schritte

1. Installieren Sie den **OMSA** mit der Komponente **Remote-Aktivierung** auf dem Hostsystem.
2. Wenn Sie OMSA über die Befehlszeile installieren, stellen Sie sicher, dass Sie die **Option -c** angeben. Falls OMSA bereits installiert ist, installieren Sie OMSA mit der Option -c und starten Sie den Dienst neu:

   ```
   srvadmin-install.sh -c
   srvadmin-services.sh restart
   ```

   Bei einem ESXi-Host müssen Sie **OMSA VIB** mit dem Tool **VMware-Remote-CLI** installieren, und das System neu starten.

Unterstützt OMIVV ESXi auch bei aktiviertem Sperrmodus?

Ja, der Sperrmodus wird auf dieser Version auf Host der Version ESXi 5.0 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.

Welche Einstellung sollte ich für UserVars.CIMoeMProviderEnable mit ESXi 4.1 U1 verwenden?

Stellen Sie **UserVars.CIMoemProviderEnabled** auf 1 ein.

Wie gehe ich vor, wenn die Erstellung des Hardwareprofils bei Verwendung von Referenzservern fehlschlägt?

Überprüfen Sie, ob die empfohlenen Mindestversionen der iDRAC- und Lifecycle-Controller-Firmware sowie des BIOS installiert sind.

Um sicherzustellen, 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.

Warum schlägt die Bereitstellung von ESXi auf Blade Server fehl?

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 kann auch auf eine interne RIPS SD-Karte installiert werden.

Warum schlagen Hypervisor-Bereitstellungen auf PowerEdge R210-II-Maschinen fehl?

Ein Zeitüberschreitungsproblem auf PowerEdge R210-II-Systemen verursacht einen Hypervisor-Bereitstellungsfehler, da das BIOS nicht vom zugehörigen ISO starten kann.

Lösung: Installieren Sie den Hypervisor manuell auf der Maschine.

Warum werden automatisch ermittelte Systeme im Bereitstellungsassistent ohne Modellinformationen angezeigt?

Dies weist in der Regel davon hin, dass die auf dem System installierte Firmware-Version die empfohlenen Mindestanforderungen nicht erfüllt. In manchen Fällen wurde möglicherweise eine Firmware-Aktualisierung nicht auf dem System registriert.

Lösung: Führen Sie einen Kaltstart des Systems durch oder setzen Sie das Blade erneut ein. Das neu aktivierte Konto auf dem iDRAC muss deaktiviert und die automatische Erkennung 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.

Info über diese Aufgabe

Gehen Sie folgendermaßen vor, um die Lösung zu finden:

Schritte

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.

Wie kann ich die Entfernung des virtuellen Geräts erzwingen?

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 ein und klicken Sie anschließend auf **Methode aufrufen**.
7. Geben Sie den Erweiterungsschlüssel zur Deregistrierung von com.dell.plugin.openManage_integration_for_VMware_vCenter_WebClient ein und klicken Sie anschließend auf **Methode aufrufen**.
8. 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.

Wie gehe ich vor, wenn eine Firmware-Aktualisierung fehlschlägt?

Prüfen Sie in den Protokollen der virtuellen Geräte, ob bei der Aufgabe ein Timeout aufgetreten ist. Falls ja, muss iDRAC durch einen Kaltstart zurückgesetzt werden. Nachdem das System hochgefahren wurde und ausgeführt wird, überprüfen Sie, ob die Aktualisierung erfolgreich war. Führen Sie entweder eine Bestandsaufnahme durch oder verwenden Sie die Registerkarte **Firmware**.

Wie gehe ich vor, wenn die vCenter-Registrierung fehlgeschlagen ist?

Die vCenter Registrierung kann aufgrund von Kommunikationsproblemen fehlschlagen. Probleme dieser Art können Sie mithilfe einer statischen IP-Adresse beheben. Um eine statische IP-Adresse zu verwenden, wählen Sie in OpenManage Integration for VMware vCenter auf der Registerkarte „Konsole“ die Optionen **Netzwerk konfigurieren** → **Geräte bearbeiten** und geben Sie das richtige **Gateway** und den richtigen **FQDN** (Fully Qualified Domain Name) ein. Geben Sie den Namen des DNS-Servers unter „DNS-Konfiguration bearbeiten“ ein.

ANMERKUNG: Stellen Sie sicher, dass das virtuelle Gerät den eingegebenen DNS-Server auflösen kann.

Die Leistung ist während des Tests der Anmeldeinformationen im Verbindungsprofils langsam oder und die Anwendung reagiert nicht.

Info über diese Aufgabe

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:

Schritte

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 das VMware vCenter Server-Gerät?

Ja, OMIVV unterstützt das VMware vCenter Server-Gerät seit v2.1.

Ich habe eine Firmware-Aktualisierung mit der Option „Beim nächsten Neustart anwenden“ ausgeführt und das System neu gestartet. Warum wurde die Firmware-Version nicht aktualisiert?

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.

Warum wird der Host auch nach seiner Entfernung aus der vCenter-Struktur weiterhin unterhalb des Gehäuses angezeigt?

Die dem Gehäuse untergeordneten Hosts werden als Teil des Gehäusebestands erkannt. Nach einer erfolgreichen Bestandsaufnahme des Gehäuses wird die Liste der dem Gehäuse untergeordneten Hosts aktualisiert. Daher wird der Host bis zur nächsten Gehäuse-Bestandsaufnahme weiterhin unterhalb des Gehäuses angezeigt, auch wenn er bereits aus der vCenter-Struktur entfernt wurde.

Warum wird in der Verwaltungskonsole das Feld Aktualisierungs-Repository-Pfad nicht auf den Standardpfad gesetzt, nachdem ich das Gerät auf die werkseitigen Einstellungen zurückgesetzt habe?

Navigieren Sie nach dem Zurücksetzen des Gerät zur **Verwaltungskonsole**, und klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**. Auf der Seite **Geräteeinstellungen** wurde der **Aktualisierungs-Repository-Pfad** nicht auf den Standardpfad geändert.

Lösung: Kopieren Sie in der **Verwaltungskonsole** den Pfad aus dem Feld **Standard-Aktualisierungs-Repository** manuell in das Feld **Aktualisierungs-Repository -Pfad**.

Warum werden die Alarm-Einstellungen nach Sicherung und Wiederherstellung von OMIVV nicht wiederhergestellt?

Bei der der Wiederherstellung der gesicherten OMIVV-Geräte werden nicht alle Alarmeinstellungen wiederhergestellt. In OpenManage Integration for VMware-GUI werden die wiederhergestellten Einstellungen jedoch im Feld **Alarme und Ereignisse** angezeigt.

Lösung: Ändern Sie in OpenManage Integration for VMware-GUI auf der Registerkarte**Einstellungen** → **verwalten** die Einstellungen für **Ereignisse und Alarme** manuell.

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

Info über diese Aufgabe

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:

Schritte

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
   ```

16

Zugehörige Dokumentation

Zusätzlich zu diesem Handbuch können Sie auf die anderen Handbücher unter **Dell.com/support/manuals** zugreifen. Klicken Sie auf der Seite „Handbücher“ auf **Produkte anzeigen** unter der Kategorie **Ein Produkt suchen**. Klicken Sie im Abschnitt **Ein Produkt wählen** auf **Software und Sicherheit** → **Virtualisierungslösungen**. Klicken Sie auf **OpenManage Integration for VMware vCenter 4.0**, um auf die folgenden Dokumente zuzugreifen:

- *OpenManage Integration for VMware vCenter Version 4.0 Web-Client-Benutzerhandbuch*
- *OpenManage Integration for VMware vCenter Version 4.0-Versionshinweise*
- *OpenManage Integration for VMware vCenter Version 4.0-Kompatibilitäts-Matrix*

Sie finden Sie die technischen Artefakte einschließlich Whitepapers unter **www.delltechcenter.com**. Klicken Sie auf der Dell TechCenter Wiki-Startseite auf **Systemverwaltung** → **OpenManage Integration for VMware vCenter**, um auf die Artikel zuzugreifen.

Zugriff auf Dokumente der Dell Support-Website

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

- Verwendung der folgenden Links:
  - Für alle Enterprise-System-Verwaltungsdokumente – **Dell.com/SoftwareSecurityManuals**
  - Für OpenManage-Dokumente – **Dell.com/OpenManageManuals**
  - Für Remote-Enterprise-System-Verwaltungsdokumente – **Dell.com/esmmanuals**
  - Für Dokumente zu iDRAC und Lifecycle Controller – **Dell.com/idracmanuals**
  - Für OpenManage Connections Enterprise-System-Verwaltungsdokumente – **Dell.com/OMConnectionsEnterpriseSystemsManagement**
  - Für Betriebsfähigkeits-Tools-Dokumente – **Dell.com/ServiceabilityTools**
  - Für Client Command Suite-System-Verwaltungsdokumente – **Dell.com/DellClientCommandSuiteManuals**
  - Für Dokumente zu OpenManage-Virtualisierungslösungen – **Dell.com/VirtualizationSolutions**
- Gehen Sie auf der Dell Support-Website folgendermaßen vor:
  a. Rufen Sie die Website **Dell.com/Support/Home** auf.
  b. Klicken Sie auf **Produkte anzeigen** und unter **Wählen Sie ein Produkt** auf **Software und Sicherheit**.
  c. Klicken Sie im Gruppenfeld **Software & Sicherheit** auf einen der folgenden Links:
     - **Enterprise-Systemverwaltung**
     - **Remote Enterprise-Systemverwaltung**
     - **Tools für die Betriebsfähigkeit**
     - **Dell Client Command Suite**
     - **Connections Client-Systemverwaltung**
     - **Virtualisierungslösungen**
  d. Um ein Dokument anzuzeigen, klicken Sie auf die jeweilige Produktversion.

- Verwendung von Suchmaschinen:
  - Geben Sie den Namen und die Version des Dokuments in das Kästchen „Suchen“ ein.