Benutzerhandbuch zu iDRAC 8/7 v2.50.50.50

DELL EMC

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.

2017 - 09

Rev. A00

Inhaltsverzeichnis

1

Übersicht

iDRAC (Integrated Dell Remote Access Controller) wurde entwickelt, um die Arbeit von Serveradministratoren produktiver zu gestalten und die allgemeine Verfügbarkeit von Dell Servern zu verbessern. iDRAC weist Administratoren auf Serverprobleme hin, unterstützt Sie bei der Ausführung von Remote-Serververwaltungsaufgaben und reduziert die Notwendigkeit für den physischen Zugriff auf den Server.

iDRAC mit der Lifecycle Controller-Technologie ist Teil einer größeren Rechenzentrumslösung, die Sie dabei unterstützt, unternehmenskritische Anwendungen und Auslastungen jederzeit bereitzuhalten. Mit dieser Technologie können Administratoren Dell-Server von jedem Standort aus und ohne den Einsatz von Agenten bereitstellen, überwachen, verwalten, konfigurieren, aktualisieren, Instand setzen und Probleme auf diesen Servern beheben. Dabei ist es unerheblich, ob ein Betriebssystem oder ein Hypervisor vorhanden sind oder sie sich in einem betriebsfähigen Zustand befinden.

Verschiedene Produkte arbeiten mit dem iDRAC und dem Lifecycle-Controller zusammen, um IT-Vorgänge zu vereinfachen, darunter:

- Dell Management Plug-in für VMware vCenter
- Dell Repository Manager
- Dell Management Packs für Microsoft System Center Operations Manager (SCOM) und Microsoft System Center Configuration Manager (SCCM)
- BMC Bladelogic
- Dell OpenManage Essentials
- Dell OpenManage Power Center

Der iDRAC wird in den folgenden Varianten angeboten:

- Basic Management mit IPMI (standardmäßig für Server der 200-500 Serie verfügbar)
- iDRAC Express (standardmäßig für Rack- oder Tower-Server der 600 Serie oder höher verfügbar und für alle Blade-Server)
- iDRAC Enterprise (auf allen Servermodellen verfügbar)

Weitere Informationen finden Sie im *iDRAC Overview and Feature Guide* (iDRAC7-Überblicks- und Funktionshandbuch) unter **dell.com/support/manuals**.

Themen:

- Zugriff auf Dokumente von der Dell EMC Support-Website

Vorteile der Verwendung von iDRAC mit Lifecycle Controller

Sie können die folgenden Vorteile nutzen:

- Verbesserte Verfügbarkeit – Frühzeitige Benachrichtigungen zu potenziellen oder tatsächlichen Fehlern, die Sie dabei unterstützen, einen Server-Ausfall zu verhindern oder den zeitlichen Aufwand für die Wiederherstellung nach einem Ausfall zu reduzieren.
- Verbesserte Produktivität und geringere Gesamtbetriebskosten – Die Erweiterung des Server-Wartungsbereichs für Administratoren auf eine größere Anzahl an entfernt liegenden Servern kann Sie dabei unterstützen, die Produktivität der IT-Mitarbeiter zu erhöhen und gleichzeitig die Gesamtbetriebskosten, z. B. für Reisen, zu reduzieren.
- Sichere Umgebung – Durch die Bereitstellung eines sicheren Zugriffs auf Remote-Server können Administratoren kritische Verwaltungsaufgaben ausführen, ohne die Sicherheit von Servern und des Netzwerks zu beeinträchtigen.
- Verbesserte integrierte Verwaltung über Lifecycle-Controller – Lifecycle-Controller bietet Bereitstellungsfunktionen und vereinfacht Wartungsaufgaben durch die Lifecycle-Controller-Benutzeroberfläche für die lokale Bereitstellung und über Schnittstellen für Remote-Dienste (WS-Management) für die Remote-Bereitstellung. Außerdem bietet Lifecycle-Controller eine Integration mit Dell OpenManage Essentials und Partner-Konsolen.

Weitere Informationen zur Lifecycle-Controller-Benutzeroberfläche finden Sie im *Lifecycle Controller User's Guide* (Lifecycle-Controller-Benutzerhandbuch), Informationen zu Remote-Diensten finden Sie im *Lifecycle Controller Remote Services User's Guide* (Lifecycle-Controller-Benutzerhandbuch für Remote-Dienste), jeweils unter **dell.com/idracmanuals**.

Wichtige Funktionen

Zentrale Funktionen in iDRAC:

ANMERKUNG: Einige Funktionen sind nur mit einer iDRAC Enterprise-Lizenz verfügbar. Informationen über die verfügbaren Funktionen der verschiedenen Lizenzen finden Sie unter Lizenzverwaltung.

Bestandsaufnahme und Überwachung

- Zustand verwalteter Server anzeigen
- Netzwerkadapter zur Bestandsaufnahme und Überwachung und Speichersubsysteme (PERC und direkt angehängter Speicher) ohne Betriebssystemagenten.
- Anzeigen und Exportieren der aktuellen Bestandsliste.
- Anzeigen der Sensorinformationen wie beispielsweise Temperatur, Spannung und Eingriff.
- Überwachen des CPU-Status, automatische Prozessordrosselung und vorhergesagte Fehler.
- Anzeigen der Speicherinformation.
- Stromverbrauch überwachen und steuern
- Support für SNMPv3-GETs und Warnungen.
- Für Blade-Server: Webschnittstelle für Chassis Management Controller (CMC) starten und CMC-Informationen sowie WWN/MAC-Adressen anzeigen

ANMERKUNG: CMC ermöglicht den Zugriff auf iDRAC über das M1000E-Gehäuse-LCD-Bedienfeld und über lokale Konsolenverbindungen. Weitere Informationen finden Sie im *Benutzerhandbuch zum Chassis Management Controller* unter dell.com/support/manuals.

- Anzeigen von verfügbaren Netzwerk-Schnittstellen auf Host-Betriebssystemen.
- Anzeigen der Bestandslisten- und Überwachungsinformationen und Konfiguration der grundlegenden iDRAC-Einstellungen unter Verwendung von iDRAC Quick Sync-Funktion und einem mobilen Gerät.

Bereitstellung

- vFlash SD-Kartenpartitionen verwalten
- Anzeigeeinstellungen für das Bedienfeld auf der Vorderseite konfigurieren

- Verwalten von iDRAC-Netzwerkeinstellungen.
- Virtuelle Konsole und virtuelle Datenträger konfigurieren und verwenden
- Betriebssysteme über die Remote-Dateifreigabe, über virtuelle Datenträger und VMCLI bereitstellen
- Aktivieren Sie die automatische Ermittlung.
- Die Serverkonfiguration mit Export- oder Import-XML-Profilfunktion durch RACADM oder WS-MAN durchführen. Weitere Informationen finden Sie im *Schnellstarthandbuch zu Remote-Services mit Lifecycle Controller*.
- Konfigurieren der Richtlinie für die Persistenz von virtuellen Adressen, Initiator und Speicherzielen.
- Remote-Konfiguration von Speichergeräten, die während der Laufzeit an das System angeschlossen sind.
- Führen Sie die folgenden Operationen für Speichergeräte aus:
  - Physische Festplatten: Physische Festplatte als globales Hotspare zuweisen oder Zuweisung aufheben
  - Virtuelle Laufwerke:
    - Virtuelle Festplatten erstellen
    - Cache-Richtlinien für virtuelle Festplatten bearbeiten
    - Übereinstimmung der virtuellen Festplatte überprüfen
    - Virtuelle Festplatten initialisieren
    - Virtuelle Festplatten verschlüsseln
    - Dediziertes Hotspare zuweisen und Zuweisung aufheben
    - Virtuelle Festplatten löschen
  - Controller:
    - Controller-Eigenschaften konfigurieren
    - Fremdkonfigurationen (automatisch) importieren
    - Fremdkonfiguration löschen
    - Controller-Konfiguration zurücksetzen
    - Sicherheitsschlüssel erstellen oder ändern
  - PCIe SSD-Geräte:
    - Bestandsaufnahme und die Remote-Überwachung des Status von PCIe SSD-Geräten im Server.
    - Entfernen der PCIe SSD vorbereiten
    - Daten sicher löschen
  - Festlegen des Rückwandplatine-Modus (Unified- oder Split-Betrieb).
  - Komponenten-LEDs blinken oder Blinken beenden
  - Wenden Sie die Geräteeinstellungen sofort, beim nächsten Neustart, zu einem festgelegten Zeitpunkt oder als eine ausstehende Operation an, um sie als Stapel als Teil des einzelnen Jobs anzuwenden.

Aktualisierung

- Verwalten von iDRAC-Lizenzen.
- BIOS und Gerätefirmware für Geräte aktualisieren, die durch Lifecycle Controller unterstützt werden
- Aktualisierung oder Rollback für iDRAC-Firmware und Lifecycle-Controller-Firmware mit einem einzigen Firmware-Image.
- Verwalten gestufter Aktualisierungen.
- Serverprofil sichern und wiederherstellen
- Zugriff auf die iDRAC-Schnittstelle über direkte USB-Verbindung.
- iDRAC unter Verwendung des Server-Profiles auf dem USB-Gerät konfigurieren.

Wartung und Fehlerbehebung

- Stromversorgungsbezogene Vorgänge ausführen und Stromverbrauch überwachen
- Optimierte Systemleistung und Stromverbrauch durch Ändern der thermischen Einstellungen.
- Keine Abhängigkeit vom Open Manage Server Administrator für die Generierung von Warnmeldungen
- Ereignisdaten protokollieren: Lifecycle- und RAC-Protokolle.

- Festlegen von E-Mail-Warnungen, IPMI-Warnungen, Remote System-Protokollen, WS-Ereignisprotokollen, Redfish-Ereignissen und SNMP-Traps (v1 v2c und v3) für Ereignisse und verbesserte E-Mail-Warnungsbenachrichtigung.
- Image des letzten Systemabsturzes erfassen
- Videos zur Start- und Absturzerfassung anzeigen
- Bandexterne Überwachung und Ausgabe von Warnmeldungen an den Leistungsindex von CPU, Speicher und E/A-Modulen.
- Konfigurieren des Warnungs-Schwellenwerts für die Temperatur und Energieverbrauch.
- Verwenden Sie das iDRAC-Service-Modul zum:
  - Anzeigen von Informationen zum Betriebssystem (BS).
  - Replizieren von Lifecycle Controller-Protokollen zu den Betriebssystemprotokollen
  - Anzeigen von Optionen zur automatischen Systemwiederherstellung
  - Remote-Hardware-Zurücksetzung-iDRAC
  - Bandinterne iDRAC-SNMP-Warnungen aktivieren
  - Zugriff auf iDRAC unter Verwendung von Host-BS (experimentelle Funktion)
  - Bestücken der Windows Management Instrumentation (WMI)-Informationen
  - Integration mit SupportAssist-Erfassung Dieses Paket ist nur anwendbar, wenn Version 2.0 oder höher des iDRAC Servicemoduls installiert ist. Weitere Informationen hierzu finden Sie unter Generieren der SupportAssist-Erfassung.
  - Vorbereiten zum Entfernen der NVMe-PCIe-SSD Weitere Informationen finden Sie unter Vorbereiten auf das Entfernen von PCIe-SSDs.
- Sie können die SupportAssist-Erfassung folgendermaßen generieren:
  - Automatisch – Verwendung des iDRAC Service Module, das das Betriebssystem-Collector-Tool automatisch aufruft.
  - Manuell – Verwenden des BS-Collector-Hilfsprogramms

Dell Best Practices für iDRAC

- iDRACs sind für die Installation auf einem separaten Verwaltungsnetzwerk vorgesehen. Sie sind nicht darauf ausgelegt oder dafür gedacht, im Internet platziert oder mit dem Internet verbunden zu werden. Dies könnte das verbundene System Sicherheitsrisiken und anderen Risiken aussetzen, für die Dell nicht verantwortlich ist.
- Abgesehen von der Platzierung der iDRACs auf einem separaten Verwaltungssubnetz, sollten Benutzer das Verwaltungssubnetz/vLAN mit einer geeigneten Technologie isolieren, wie z. B. Firewalls. Außerdem sollte der Zugriff auf das Subnetz/vLAN auf Serveradministratoren mit entsprechender Berechtigung begrenzt werden.

Konnektivität absichern

Die Sicherung des Zugriffs auf kritische Netzwerkressourcen hat Priorität. iDRAC implementiert einen Bereich mit Sicherheitsfunktionen, darunter:

- Benutzerdefinierte Signaturzertifikate für Secure Socket Layer (SSL).
- Signierte Firmware-Aktualisierungen
- Benutzerauthentifizierung durch Microsoft Active Directory, generischem Lightweight Directory Access Protocol (LDAP) Directory Service oder lokal verwalteten Benutzer-IDs und Kennwörtern.
- Zweifaktorauthentifizierung über die Smart Card-Anmeldefunktion. Die Zweifaktor-Authentifizierung basiert auf der physischen Smart Card und der Smart Card-PIN.
- Authentifizierung über die einmalige Anmeldung und den öffentlichen Schlüssel
- Rollenbasierte Authentifizierung für die Konfiguration spezifischer Berechtigungen für jeden einzelnen Benutzer
- SNMPv3-Authentifizierung für Benutzerkonten, die lokal in iDRAC gespeichert sind. Es wird empfohlen, dies so zu benutzen, auch wenn die Option in den Standardeinstellungen deaktiviert ist.
- Benutzer-ID- und Kennwortkonfiguration
- Standardmäßige Anmeldekennwort-Modifikation.
- Einrichten von Kennwörtern und BIOS-Kennwörtern unter Verwendung des Einweg-Hash-Formats für verbesserte Sicherheit.
- FIPS 140-2 Ebene-1-Fähigkeit.
- Unterstützung für TLS 1.2 , 1.1 und 1.0. Um die Sicherheit zu verbessern, ist die Standardeinstellung TLS 1.1 und höher.

- SMCLP- und Webschnittstellen, die 128-Bit- und 40-Bit-Verschlüsselung unterstützen (für Länder, in denen 128-Bit nicht zulässig ist) und den TLS 1.2-Standard verwenden.

ANMERKUNG: Um eine sichere Verbindung sicherzustellen, empfiehlt Dell die Verwendung von TLS 1.1 und höher.

- Konfiguration der Sitzungszeitüberschreitung (in Sekunden)
- Konfigurierbare IP-Schnittstellen (für HTTP, HTTPS, SSH, Telnet, virtuelle Konsole und virtuelle Datenträger).

  ANMERKUNG: SSL-Verschlüsselung wird durch Telnet nicht unterstützt und ist standardmäßig deaktiviert.
- Secure Shell (SSH), die eine verschlüsselte Transportschicht für höhere Sicherheit verwendet.
- Beschränkung der Anmeldefehlschläge pro IP-Adresse, mit Anmeldeblockierung der IP-Adresse bei Überschreitung des Grenzwerts
- Beschränkter IP-Adressenbereich für Clients, die an den iDRAC angeschlossen werden
- Dedizierter Gigabit-Ethernet-Adapter auf Rack- und Tower-Servern verfügbar (ggf. zusätzliche Hardware erforderlich).

Was ist neu in dieser Version?

- Zusätzliche Unterstützung für Redfish 1.0.2, eine RESTful API, die von der Distributed Management Task Force (DMTF) standardisiert wurde. Sie bietet eine skalierbare und sichere Schnittstelle für die Systemverwaltung. Um Informationen zu IPv6 und VLAN zu erhalten, installieren Sie das iDRAC-Servicemodul (iSM).
- Zusätzlicher Support für Server-Konfigurationsprofil mithilfe der Redfish-Schnittstelle.
- Einstellungen für die IP-Blockierung wurden erweitert, um den Optionen in früheren Versionen zu entsprechen.
- Zusätzliche Option zum Aktivieren oder Deaktivieren von vMedia über die iDRAC-Webschnittstelle, RACADM und WSMan.
- AES-Verschlüsselung für vMedia hinzugefügt.
- Erweiterte AES-Verschlüsselungsunterstützung für vConsole.
- Unterstützung für TLS 1.0 für Port 5900 deaktiviert.
- Port 5900 ist geschlossen, wenn vMedia und vConsole deaktiviert sind.
- Port 5900 ist geschlossen, wenn vMedia- und vConsole-Lizenzbits deaktiviert sind.

Verwendung dieses Benutzerhandbuchs

Der Inhalt dieses Benutzerhandbuchs ermöglicht es Ihnen, die Tasks auszuführen, indem Sie Folgendes verwenden:

- iDRAC-Webschnittstelle – Hier sind nur die Task-bezogenen Informationen enthalten. Informationen zu Feldern und Optionen finden Sie in der *iDRAC-Online-Hilfe*, die Sie über die Webschnittstelle aufrufen können.
- RACADM – Hier ist der RACADM-Befehl bzw. das zu verwendende Objekt enthalten. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.
- Dienstprogramm für die iDRAC-Einstellungen – Hier sind nur die Task-bezogenen Informationen enthalten. Informationen zu den Feldern und Optionen finden Sie in der *Online-Hilfe zum Dienstprogramm für die iDRAC-Einstellungen*. Diese können Sie aufrufen, indem Sie in der GUI des Dienstprogramms auf **Help (Hilfe)** klicken (drücken Sie beim Starten die Taste <F2>, und klicken Sie dann auf der Seite **System Setup Main Menu (System-Setup – Hauptmenü)** auf **iDRAC Settings (iDRAC-Einstellungen)**.

Unterstützte Web-Browser

iDRAC wird auf folgenden Browsern unterstützt:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Eine Liste der unterstützten Versionen finden Sie in den *iDRAC Release Notes (iDRAC Versionshinweise)* unter **dell.com/idracmanuals**.

Unterstützte Betriebssysteme, Hypervisors

iDRAC wird von folgenden Betriebssystemen, Hypervisors unterstützt:

- Microsoft
- VMware
- Citrix
- RedHat
- SuSe

ANMERKUNG: Eine Liste der unterstützten Versionen finden Sie in den *iDRAC Release Notes (iDRAC Versionshinweise)* unter dell.com/idracmanuals.

Lizenzverwaltung

Die iDRAC-Funktionen richten sich nach der erworbenen Lizenz (Basisverwaltung, iDRAC Express, oder iDRAC Enterprise). Über die Schnittstellen können Sie nur auf lizenzierte Funktionen zugreifen, über die Sie iDRAC konfigurieren oder verwenden können. Dazu gehören z. B. die iDRAC-Webschnittstelle, RACADM, WS-MAN, OpenManage Server Administrator, usw. Für bestimmte Funktionen, wie z. B. die dedizierte Netzwerkschnittstellenkarte (NIC) oder vFlash, benötigen Sie iDRAC-Schnittstellenkarten, die auf Servern der 200-500-Reihe optional sind.

Die Lizenzverwaltung und die Firmware-Aktualisierungsfunktion unter iDRAC können über die iDRAC-Webschnittstelle und RACADM aufgerufen werden.

Lizenztypen

Die folgenden Lizenztypen sind verfügbar:

- 30-Tage-Testversion und Verlängerung – Diese Lizenz läuft nach 30 Tagen ab und kann um 30 weitere Tage verlängert werden. Evaluierungslizenzen sind zeitlich begrenzt und die Zeit, die für die Evaluierung zur Verfügung steht, reduziert sich sukzessive, wenn das System eingeschaltet ist.
- Dauerlizenz – Die Lizenz ist an die Service-Tag-Nummer gebunden und damit dauerhaft.

Methoden zum Erwerb von Lizenzen

Verwenden Sie zum Anfordern von Lizenzen eines der folgenden Verfahren:

- E-Mail – Die Lizenz ist an eine E-Mail angehängt, die nach der Anforderung der Lizenz durch das technische Support Center versendet wird.
- SB-Portal – Auf dem iDRAC steht ein Link zum SB-Portal zur Verfügung. Klicken Sie auf diesen Link, um im Internet das SB-Portal für Lizenzen zu öffnen. Derzeit können Sie das SB-Lizenzen-Portal nutzen, um Lizenzen abzurufen, die mit dem Server erworben wurden. Für den Kauf einer neuen Lizenz oder für die Erweiterung einer bereits bestehenden Lizenz müssen Sie entweder einen Vertriebsbeauftragten oder den technischen Support kontaktieren. Für weitere Informationen siehe die Online-Hilfe zur Seite des Selbstbedienungsportals.
- Point-of-sale – Die Lizenz wird im Rahmen der Systembestellung angefordert.

Lizenzvorgänge

Bevor Sie die Lizenzverwaltungsschritte ausführen, müssen Sie sicherstellen, dass Sie die erforderlichen Lizenzen besitzen. Weitere Informationen finden Sie im *Überblicks- und Funktionshandbuch* unter **dell.com/support/manuals**.

ANMERKUNG: Sollten Sie ein System erworben haben, auf dem sämtliche Lizenzen bereits vorinstalliert sind, ist eine Lizenzverwaltung nicht erforderlich.

Sie können die folgenden Lizenzvorgänge über iDRAC, RACADM, WS-MAN und Lifecycle-Controller-Remote-Dienste für eine 1-zu-1-Lizenzverwaltung und Dell License Manager für eine 1-zu-n-Lizenzverwaltung ausführen:

- Ansicht – Zeigen Sie die aktuellen Lizenzinformationen an.
- Importieren – Nachdem Sie die Lizenz erhalten haben, speichern Sie die Lizenz in einem lokalen Speicher und importieren Sie sie über eine unterstützte Schnittstelle nach iDRAC. Die Lizenz wird importiert, wenn Sie die Validierungsprüfungen bestanden hat.

ANMERKUNG: Bei einigen neuen Funktionen ist für die Aktivierung dieser Funktionen ein Systemneustart erforderlich.

- Exportieren – Exportieren Sie die installierte Lizenz zu Sicherungszwecken oder für eine spätere Neuinstallation im Rahmen des Austauschs der Hauptplatine auf ein externes Speichergerät. Der Dateiname und das Format der exportieren Lizenz lauten wie folgt: **<EntitlementID>.xml**.
- Löschen – Löschen Sie die Lizenz, die mit einer Komponente verknüpft ist, wenn diese Komponente nicht vorhanden ist. Nach dem Löschen der Lizenz wird diese nicht mehr auf iDRAC gespeichert und die Basisproduktfunktionen werden aktiviert.
- Ersetzen – Ersetzen Sie die Lizenz, um eine Evaluierungslizenz zu verlängern, um einen Lizenztyp zu ändern, z. B. eine Evaluierungslizenz in eine erworbene Lizenz, oder um eine abgelaufene Lizenz zu verlängern.
  - Eine Evaluierungslizenz kann durch eine umfangreichere Evaluierungslizenz oder eine erworbene Lizenz ersetzt werden.
  - Eine erworbene Lizenz kann durch eine aktualisierte Lizenz oder durch eine umfangreichere Lizenz ersetzt werden.
- Weitere Informationen – Hier finden Sie weitere Informationen zur installierten Lizenz oder zu den Lizenzen, die für eine auf dem Server installierte Komponente verfügbar sind.

ANMERKUNG: Damit die Option „Weitere Informationen“ die korrekte Seite anzeigt, stellen Sie sicher, dass Sie *.dell.com zur Liste der vertrauenswürdigen Sites in den Sicherheitseinstellungen hinterlegen. Weitere Informationen finden Sie in der Online-Dokumentation des Internet Explorers.

Bei einer 1-zu-n-Implementierung können Sie Dell License Manager verwenden. Weitere Informationen finden Sie im *Benutzerhandbuch zu Dell License Manager* unter **dell.com/support/manuals**.

Importieren der Lizenz nach Ersetzen der Hauptplatine

Sie können das Local iDRAC Enterprise License Installation Tool verwenden, wenn Sie die Hauptplatine kürzlich austauschen mussten und die iDRAC Enterprise-Lizenz lokal (ohne Netzwerkverbindung) neu installiert und die dedizierte NIC aktiviert werden muss. Dieses Dienstprogramm installiert eine 30-tägige Testversion der iDRAC Enterprise-Lizenz, womit Sie die Möglichkeit haben, den iDRAC zurückzusetzen, sodass statt der freigegebenen NIC die dedizierte NIC verwendet werden kann.

Status und Zustand von Lizenzkomponenten und verfügbare Optionen

In der folgenden Tabelle wird die Liste der verfügbaren Lizenzvorgänge auf der Basis des Status oder des Zustands der Lizenz angezeigt.

Tabelle 1. Lizenzvorgänge auf der Basis des Status oder des Zustands

Status oder Zustand von Lizenz/ Komponente	Importieren	Exportieren	„Löschen“	Ersetzen	Mehr erfahren
Nicht-Administrator-Anmeldung	Nein	Nein	Nein	Nein	Ja
Aktive Lizenz	Ja	Ja	Ja	Ja	Ja
Abgelaufene Lizenz	Nein	Ja	Ja	Ja	Ja

Status oder Zustand von Lizenz/ Komponente	Importieren	Exportieren	„Löschen“	Ersetzen	Mehr erfahren
Lizenz installiert, jedoch fehlt Komponente	Nein	Ja	Ja	Nein	Ja

ANMERKUNG: Erweitern Sie auf der iDRAC-Webschnittstelle, auf der Seite Lizenzen, das Gerät, um die Option Ersetzen im Drop-Down-Menü anzuzeigen.

Lizenzen über die iDRAC-Webschnittstelle verwalten

Um Lizenzen über die iDRAC-Webschnittstelle zu verwalten, gehen Sie zu **Übersicht** > **Server** > **Lizenzen**.

Daraufhin werden auf der Seite **Lizenzen** die Lizenzen angezeigt, die mit den Geräten verknüpft sind, oder jene Lizenzen, die zwar installiert sind, für die das entsprechende Gerät im System jedoch nicht vorhanden ist. Weitere Informationen zum Importieren, Exportieren, Löschen oder Ersetzen einer Lizenz finden Sie in der *iDRAC-Online-Hilfe*.

Lizenzen über RACADM verwalten

Um Lizenzen über RACADM zu verwalten, verwenden Sie den Unterbefehl **license**. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide* (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC) unter **dell.com/idracmanuals**.

Lizenzierte Funktionen in iDRAC7 und iDRAC8

In der folgenden Tabelle werden die iDRAC7-Funktionen aufgeführt, die gemäß der erworbenen Lizenz aktiviert sind.

Tabelle 2. Lizenzierte Funktionen in iDRAC7 und iDRAC8

Funktion	Grundlegende Verwaltung (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express für Blades	iDRAC8 Express für Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
Schnittstellen/Standards								
IPMI 2.0	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
DCMI 1.5	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Webbasierte GUI	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
RACADM-Befehlszeile (lokal/Remote)	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Redfish	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
SMASH-CLP (nur SSH)	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Telnet	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
SSH	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
WS-MAN	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Netzwerkzeitprotokoll	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja

Funktion	Grundlegende Verwaltung (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express für Blades	iDRAC8 Express für Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
Konnektivität								
Gemeinsam genutzte NIC (LOM)	Ja	Ja	Ja	Ja	k. A.	k. A.	Ja	Ja
Dedizierte NIC[1]	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja[2]
VLAN-Tagging	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
IPv4	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
IPv6	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
DHCP	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Dynamisches DNS	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
BS-Pass-Through	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
USB an der Frontblende	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Security (Sicherheit)								
Rollenbasierte Autorität	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Lokale Benutzer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
SSL-Verschlüsselung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
IP-Blockierung	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Ja
Verzeichnisdienste (AD, LDAP)	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Zwei-Faktor-Authentifizierung (Smart Card)	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Single Sign-On (Kerberos)	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja
PK-Authentifizierung (für SSH)	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Ja
Remote-Präsenz								
Stromsteuerung	Ja[4]	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Boot-Steuerung	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Seriell-über-LAN	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Virtueller Datenträger	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja
Virtuelle Ordner	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Remote-Dateifreigabe	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Virtuelle Konsole	Nein	Nein	Nein	Nein	Einzelner Benutzer	Einzelner Benutzer	Ja	6 Benutzer

Funktion	Grundlegende Verwaltung (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express für Blades	iDRAC8 Express für Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
VNC-Verbindung zum Betriebssystem	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Qualität/Bandbreiten-Kontrolle	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja
Virtuelle Konsolenzusammenarbeit (bis zu sechs Benutzer gleichzeitig)	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja
Chat über virtuelle Konsole	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Virtuelle Flash-Partitionen	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja [1,2]
Strom und thermisch								
Automatisches Einschalten nach Stromausfall	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Echtzeit-Leistungsmesser	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Stromschwellenwerte und Warnungen (mit Spielraum)	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Ja
Echtzeit-Stromdiagramme	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Historische Stromzähler	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Strombegrenzung	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Power Center-Integration	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja
Temperaturüberwachung	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Temperatur-Diagramme	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Ja
Zustandsüberwachung								
Vollständig Agentenfreie Überwachung	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Vorhergesagte Fehler-Überwachung	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja

Funktion	Grundlegende Verwaltung (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express für Blades	iDRAC8 Express für Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
Unterstützung von SNMP v1, v2 und v3 (Traps und Gets)	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
E-Mail-Warnungen	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Konfigurierbare Schwellenwerte	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Überwachung des Lüfters	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Überwachung der Stromversorgung	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Speicherüberwachung	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
CPU-Überwachung	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
RAID-Überwachung	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
NIC-Überwachung	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
HD-Überwachung (Gehäuse)	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Bandexterne Überwachung	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja
Aktualisierung								
Remote-Agentenfreie Aktualisierung	Ja [3]	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Integrierte Aktualisierung-Tools	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Synchronisierung mit Repository (geplante Aktualisierungen)	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Automatische Aktualisierung	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja
Bereitstellung und Konfiguration								
Integrierte BS-Bereitstellungs-Tools	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Integrierte Konfigurationshilfsprogra	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja

Funktion	Grundlegende Verwaltung (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express für Blades	iDRAC8 Express für Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
mme (Dienstprogramm für iDRAC-Einstellungen)								
Integrierte Konfigurationsassistenten (Lifecycle Controller-Assistenten)	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Auto-Ermittlung	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Remote BS-Bereitstellung	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Ja
Integriertes Treiberpaket	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Vollständige Konfigurationsbestandsaufnahme	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Inventar exportieren	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Remote-Konfiguration	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Berührungslose Konfiguration	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja
System Außerbetriebnahme/ Neuzuweisung	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Diagnose, Dienste und Protokolle								
Integrierte Diagnosetools	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Teilersetzung	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Backup-Server-Konfiguration	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Server-Konfiguration wiederherstellen	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Einfache Wiederherstellung (Systemkonfiguration)	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Funktionszustand-LED/LCD	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Quick-Sync (erfordert NFC-Blende)	Nein	Ja	Nein	Ja	Nein	k. A.	Nein	Ja

Funktion	Grundlegende Verwaltung (iDRAC7)	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express für Blades	iDRAC8 Express für Blades	iDRAC7 Enterprise	iDRAC8 Enterprise
iDRAC Direkt (Vordere USB-Verwaltungsschnittstelle)	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
iDRAC-Service-Moduls (iSM)	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
SupportAssist-Erfassung (integriert)	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Crash-Bildschirmaufnahme[5]	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Crash-Videoaufnahme[5]	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Start-Erfassung	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Handbuch für den iDRAC-Reset	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Virtuelles NMI	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
BS-Watchdog	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Integrierter Funktionszustand-Report	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
System-Ereignisprotokoll	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Lifecycle-Protokoll	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Arbeitsanmerkungen	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja
Remote-Syslog	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja
Lizenzverwaltung	Nein	Ja	Nein	Ja	Nein	Ja	Nein	Ja

[1] Erfordert vFlash SD-Karte.

[2] Rack- und Tower-Server der Serie 500 und niedriger erfordern eine Hardware-Karte, um diese Funktion zu aktivieren; diese Hardware wird gegen Aufpreis angeboten.

[3] Remote-Agent-Free-Update-Funktion ist nur über IPMI verfügbar.

[4] Verfügbar nur über IPMI.

[5] Erfordert den OMSA-Agenten auf Zielserver.

Schnittstellen und Protokoll für den Zugriff auf iDRAC

In der folgenden Tabelle werden die Schnittstellen für den Zugriff auf iDRAC dargestellt.

ANMERKUNG: Die gleichzeitige Verwendung von mehr als einer Schnittstelle kann zu unerwarteten Ergebnissen führen.

Tabelle 3. Schnittstellen und Protokoll für den Zugriff auf iDRAC

Schnittstelle oder Protokoll	Beschreibung
Dienstprogramm für iDRAC-Einstellungen	Verwenden Sie das Dienstprogramm für die iDRAC-Einstellungen, um Pre-OS-Vorgänge durchzuführen. Dieses Dienstprogramm bietet neben weiteren Funktionen teilweise die Funktionen, die über die iDRAC-Webschnittstelle verfügbar sind. Drücken Sie zum Zugreifen auf das Dienstprogramm für die iDRAC-Einstellungen während des Startvorgangs <F2> und klicken Sie dann auf **iDRAC Settings (iDRAC-Einstellungen)** auf der Seite **System Setup Main Menu (System-Setup – Hauptmenü)**.
iDRAC-Webschnittstelle	Über die iDRAC-Webschnittstelle können Sie iDRAC verwalten und das verwaltete System überwachen. Der Browser stellt über die HTTPS-Schnittstelle eine Verbindung mit dem Webserver her. Datenflüsse werden für Datenschutz und Integrität über die 128-Bit-SSL-Verschlüsselung verschlüsselt. Sämtliche Verbindungen zur HTTP-Schnittstelle werden auf HTTPS umgeleitet. Administratoren können ihr eigenes SSL-Zertifikat über einen SSL-CSR-Generierungsprozess hochladen, um den Webserver zu sichern. Die Standard-HTTP- und HTTPS-Schnittstelle kann geändert werden. Der Benutzerzugriff basiert auf den Benutzerberechtigungen.
RACADM	Verwenden Sie das Befehlszeilendienstprogramm für iDRAC- und Server-Verwaltungsvorgänge. Sie können RACADM lokal und remote verwenden. • Die lokale RACADM-Befehlszeilenschnittstelle wird auf verwalteten Systemen ausgeführt, auf denen Server Administrator installiert ist. Der lokale RACADM kommuniziert über die bandinterne IPMI-Host-Schnittstelle mit iDRAC. Da es auf dem lokal verwalteten System installiert ist, müssen sich Benutzer zum Ausführen dieses Dienstprogramms beim Betriebssystem anmelden. Ein Benutzer muss über umfassende Administratorrechte verfügen oder ein Root-Benutzer sein, um dieses Dienstprogramm verwenden zu können. • Remote-RACADM ist ein Client-Dienstprogramm, das auf einer Management Station ausgeführt wird. Es verwendet die bandexterne Netzwerkschnittstelle, um die RACADM-Befehle auf dem Managed System auszuführen, außerdem wird der HTTPs-Kanal verwendet. Die Option **–r** führt den RACADM-Befehl über ein Netzwerk aus. • Firmware-RACADM kann aufgerufen werden, indem Sie sich über SSH oder Telnet bei iDRAC anmelden. Sie können die Firmware-RACADM-Befehle ohne Angabe der IP-Adresse, des Benutzernamens oder des Kennworts für iDRAC ausführen. • Es ist nicht erforderlich, die IP-Adresse, den Benutzernamen oder das Kennwort für iDRAC anzugeben, um die Firmware-RACADM-Befehle auszuführen. Nachdem Sie die RACADM-Eingabeaufforderung aufgerufen haben, können Sie die Befehle ohne das Präfix „racadm“ direkt ausführen.
Server-LC-Anzeige/ Gehäuse-LC-Anzeige	Verwenden Sie die LC-Anzeige auf der Frontblende des Servers, um die folgenden Aktivitäten auszuführen: • Warnungen, IP- oder MAC-Adresse für iDRAC oder benutzerprogrammierbare Zeichenfolgen anzeigen • DHCP festlegen • Statische IP-Einstellungen für iDRAC konfigurieren Bei Blade-Servern befindet sich die LC-Anzeige auf der Frontblende des Gehäuses und wird von allen Blades gemeinsam verwendet. Um iDRAC ohne Neustart des Servers neu zu starten, halten Sie die Systemidentifikationstaste 16 Sekunden lang gedrückt.

Schnittstelle oder Protokoll	Beschreibung
CMC-Webschnittstelle	Neben der Überwachung und der Verwaltung des Gehäuses können Sie die CMC-Webschnittstelle für die folgenden Aktivitäten verwenden: • Status eines Managed System anzeigen • iDRAC-Firmware aktualisieren • iDRAC-Netzwerkeinstellungen konfigurieren • Bei der iDRAC-Webschnittstelle anmelden • Managed System starten, anhalten oder zurücksetzen • BIOS, PERC und unterstützte Netzwerkadapter aktualisieren
Lifecycle-Controller	Verwenden Sie Lifecycle Controller, um iDRAC-Konfigurationen auszuführen. Um auf Lifecycle-Controller zuzugreifen, drücken Sie <F10> während des Starts und gehen Sie zu **System Setup (System-Setup)** > **Advanced Hardware Configuration (Erweiterte Hardware-Konfiguration)** > **iDRAC Settings (iDRAC-Einstellungen)**. Weitere Informationen finden Sie im *Benutzerhandbuch zu Lifecycle Controller* unter **dell.com/idracmanuals**.
Telnet	Verwenden Sie Telnet, um auf iDRAC zuzugreifen und RACADM- und SMCLP-Befehle auszuführen. Weitere Informationen zu RACADM finden Sie im *RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC* unter **dell.com/idracmanuals**. Weitere Informationen zu SMCLP finden Sie unter SMCLP verwenden. **ANMERKUNG: Telnet ist kein sicheres Protokoll und wird standardmäßig angezeigt. Telnet überträgt alle Daten, einschließlich Kennwörter, im Textformat. Bei der Übertragung von vertraulichen Informationen verwenden Sie die SSH-Schnittstelle.**
SSH	Verwenden Sie SSH, um RACADM- und SMCLP-Befehle auszuführen. Sie bietet dieselben Fähigkeiten wie die Telnet-Konsole und verwendet eine verschlüsselte Transportschicht für höhere Sicherheit. Der SSH-Dienst ist standardmäßig auf iDRAC aktiviert. Er kann jedoch deaktiviert werden. iDRAC unterstützt ausschließlich die SSH-Version 2 mit dem RSA-Host-Schlüsselalgorithmus. Es wird ein eindeutiger 1024-Bit-RSA-Hostschüssel generiert, wenn Sie iDRAC zum ersten Mal einschalten.
IPMItool	Verwenden Sie IPMITool für den Zugriff auf die Basisverwaltungsfunktionen für das Remotesystem über iDRAC. Die Schnittstelle umfasst lokales IPMI, IPMI über LAN, IPMI über serielle Verbindungen und Serielle Verbindung über LAN. Weitere Informationen zu IPMITool finden Sie im *Benutzerhandbuch zu Dienstprogrammen des Dell OpenManage Baseboard-Verwaltungs-Controllers* unter **dell.com/idracmanuals**. **ANMERKUNG: IPMI-Version 1.5 wird nicht unterstützt.**
VMCLI	Verwenden Sie Befehlszeilenschnittstelle für virtuelle Datenträger (VMCLI) für den Zugriff auf einen Remote-Datenträger über die Managed Station und für die Bereitstellung von Betriebssystemen auf mehreren Managed Systems.
SMCLP	Verwenden Sie das SMCLP-Protokoll (Server Management Workgroup Server Management-Command Line Protocol), um Systemverwaltungsaufgaben auszuführen. Dieses Protokoll ist über SSH oder Telnet verfügbar. Weitere Informationen zu SMCLP finden Sie unter SMCLP verwenden.
WS-MAN	Der LC-Remote Service basiert auf dem WS-Management-Protokoll für 1-zu-n-Verwaltungsaufgaben. Sie müssen einen WS-MAN-Client verwenden, z. B. den WinRM-Client (Windows) oder den OpenWSMAN-Client (Linux), um die LC-Remote Services-Funktion zu verwenden. Sie können außerdem Power Shell und Python verwenden, um auf die WS-MAN-Schnittstelle zu schreiben. Web Services for Management (WS-Management) ist ein Simple Object Access Protocol (SOAP)-basiertes Protokoll, das für die Systemverwaltung verwendet wird. iDRAC verwendet WS-Management zur Übertragung von Distributed Management Task Force (DMTF) Common Information Model (CIM)-basierten Verwaltungsinformationen. Die CIM-Informationen definieren die Semantik und die Informationstypen, die in einem verwalteten System geändert werden können. Die durch WS-Management zur Verfügung gestellten Daten werden durch die iDRAC-Instrumentierungsschnittstelle bereitgestellt, die den DMTF-Profilen und den Erweiterungsprofilen zugeordnet ist.

Schnittstelle oder Protokoll	Beschreibung
	Weitere Informationen stehen zur Verfügung unter: • Lifecycle Controller-Remote Services User's Guide (Lifecycle Controller-Remote-Dienste – Benutzerhandbuch) unter **dell.com/idracmanuals**. • Lifecycle Controller Integration Best Practices Guide (Lifecycle Controller Integration Best Practices-Handbuch) unter **dell.com/support/manuals**. • Lifecycle Controller-Seite auf Dell TechCenter — **delltechcenter.com/page/Lifecycle+Controller** • Lifecycle Controller WS-Management Script Center – **delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller** • MOFs und Profile – **delltechcenter.com/page/DCIM.Library** • DMTF-Website – **dmtf.org/standards/profiles/**

iDRAC-Schnittstelleninformationen

Die folgenden Schnittstellen sind erforderlich, um auf iDRAC im Remote-Zugriff durch Firewalls zugreifen zu können. Dies sind die standardmäßigen Schnittstellen, durch die iDRAC auf Verbindungen hört. Optional können Sie die meisten Schnittstellen ändern. Informationen dazu finden Sie unter Dienste konfigurieren.

Tabelle 4. Schnittstellen, auf die iDRAC für Verbindungen wartet

Schnittstellennummer	Funktion
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
161*	SNMP
5900*	Umleitung von Tastatur und Maus für die virtuelle Konsole, für virtuelle Datenträger, für virtuelle Ordner und die Remote-Dateifreigabe
5901	VNC Wenn die VNC-Funktion aktiviert ist, wird der Port 5901 geöffnet.

* Konfigurierbare Schnittstelle

Die folgende Tabelle listet die Schnittstellen auf, die iDRAC als Client verwendet.

Tabelle 5. Schnittstellen, die iDRAC als Client verwendet

Schnittstellennummer	Funktion
25*	SMTP
53	DNS

Schnittstellennummer	Funktion
68	DHCP-zugewiesene IP-Adresse
69	TFTP
162*	SNMP-Trap
445	Common Internet File System (CIFS)
636	LDAP über SSL (LDAPS)
2049	Network File System (NFS)
123	Network Time Protocol (NTP)
3269	LDAPS für globalen Katalog (GC)

* Konfigurierbare Schnittstelle

Weitere nützliche Dokumente

Zusätzlich zu diesem Handbuch bieten die folgenden, auf der Dell Support-Website unter **dell.com/support/manuals** verfügbaren Dokumente zusätzliche Informationen über das Setup und den Betrieb von iDRAC auf Ihrem System.

- Die *iDRAC Online-Hilfe* bietet detaillierte Informationen und Beschreibungen zu den Feldern, die auf der iDRAC-Webschnittstelle angezeigt werden. Sie können nach der Installation von iDRAC auf die Online-Hilfe zugreifen.
- Das *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* enthält Informationen zu den RACADM-Unterbefehlen, den unterstützten Schnittstellen und iDRAC-Eigenschaften-Datenbankgruppen und -Objektdefinitionen.
- Die *iDRAC-RACADM-Support-Matrix* bietet eine Liste der untergeordneten Befehle und Objekte für eine bestimmte iDRAC-Version an.
- Das *Benutzerhandbuch zur Systemverwaltungsübersicht* bietet zusammengefasste Informationen zu den verschiedenen Software-Produkten, die für Systemverwaltungsaufgaben verfügbar sind.
- Im *Dell Lifecycle Controller Graphical User Interface For 12th and 13th Generation Dell PowerEdge Servers User's Guide* (Dell Lifecycle Controller grafische Benutzeroberfläche für die 12. und 13. Generation von Dell PowerEdge-Server-Benutzerhandbuch) finden Sie Informationen zur Verwendung der graphischen Benutzeroberfläche (GUI) (Graphical User Interface).
- Die *Dell Lifecycle Controller Remote Services For 12th and 13th Generation Dell PowerEdge Servers Quick Start Guide (Dell Lifecycle Controller-Remote-Dienste für die 12. und 13. Generation von Dell Poweredge-Server-Schnellstartanleitung)* enthält einen Überblick über die Fähigkeiten der Remote-Dienste, Informationen zum Einrichten der Remote-Dienste, Lifecycle Controller API und gibt Referenzen zu verschiedenen Ressourcen zum DELL Tech Center.
- Das *Dell Remote Access Configuration Tool User's Guide (Benutzerhandbuch für das Remote-Zugriffs-Konfigurationshilfsprogramm von Dell)* enthält Informationen zur Verwendung des Tools für die Ermittlung von iDRAC-IP-Adressen in Ihrem Netzwerk und zum Ausführen von 1-zu-n-Firmware-Aktualisierungen und Active Directory-Konfigurationen für die ermittelten IP-Adressen.
- Die *Dell Systems Software Support Matrix* bietet Informationen über die verschiedenen Dell-Systeme, über die von diesen Systemen unterstützten Betriebssysteme und über die Dell OpenManage-Komponenten, die auf diesen Systemen installiert werden können.
- Das *iDRAC Service Module Installation Guide (iDRAC-Servicemodul-Installationshandbuch)* enthält Informationen zum Installieren des iDRAC-Servicemoduls.
- Das *Dell OpenManage Server Administrator Installation Guide* (Dell OpenManage Server Administrator-Installationshandbuch) enthält Anleitungen zur Installation von Dell OpenManage Server Administrator.
- Das *Dell OpenManage Management Station Software-Installationshandbuch* enthält Anleitungen zur Installation der Dell OpenManage Management Station-Software, die das Baseboard Management-Dienstprogramm, DRAC Tools und Active Directory Snap-In enthält.
- Informationen zur IPMI-Schnittstelle finden Sie im *Benutzerhandbuch für Verwaltungsdienstprogramme des Dell OpenManage Baseboard-Verwaltungs-Controllers*.
- Die *Versionshinweise* geben den letzten Stand der Änderungen am System oder der Dokumentation wieder oder enthalten erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.

- Das *Glossar* enthält Informationen zu den in diesem Dokument verwendeten Begriffen.

Die folgenden Systemdokumente sind erhältlich, um weitere Informationen zur Verfügung zu stellen:

- In den mit dem System gelieferten Sicherheitshinweisen finden Sie wichtige Informationen zur Sicherheit und zu den Betriebsbestimmungen. Weitere Betriebsbestimmungen finden Sie auf der Website zur Einhaltung gesetzlicher Vorschriften unter **dell.com/regulatory_compliance**. Garantieinformationen können möglicherweise als separates Dokument beigelegt sein.
- In der zusammen mit der Rack-Lösung gelieferten *Anweisungen für die Rack-Montage* wird beschrieben, wie das System in einem Rack installiert wird.
- Das *Handbuch zum Einstieg* enthält eine Übersicht über die Systemfunktionen, die Einrichtung des Systems und technische Daten.
- Im *Benutzerhandbuch* erhalten Sie Informationen über Systemfunktionen, zur Fehlerbehebung am System und zum Installieren oder Austauschen von Systemkomponenten.

Zugehöriger Link

Kontaktaufnahme mit Dell

Zugriff auf Dokumente von der Dell EMC Support-Website

Social Media-Referenz

Wenn Sie mehr über das Produkt, Best Practices und Lösungen und Services von Dell erfahren möchten, nutzen Sie die Plattformen für soziale Medien wie z. B. Dell TechCenter. Über die iDRAC-Wiki-Seite, die unter **www.delltechcenter.com/idrac** verfügbar ist, haben Sie Zugang zu Blogs, Foren und Whitepapern, Anleitungen und mehr.

Dokumentationen zu iDRAC und zu anderer in Beziehung stehender Firmware finden Sie unter **dell.com/idracmanuals** und **dell.com/esmmanuals**.

Kontaktaufnahme mit Dell

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

Dell stellt verschiedene onlinebasierte und telefonische Support- und Serviceoptionen bereit. Da die Verfügbarkeit dieser Optionen je nach Land und Produkt variiert, stehen einige Services in Ihrer Region möglicherweise nicht zur Verfügung. So erreichen Sie den Vertrieb, den Technischen Support und den Kundendienst von Dell:

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

Zugriff auf Dokumente von der Dell EMC Support-Website

Sie können auf die Dokumente zugreifen, indem Sie die folgenden Links verwenden:

- Für Dell EMC Enterprise System-Verwaltungsdokumente – **Dell.com/SoftwareSecurityManuals**
- Für Dell EMC OpenManage-Dokumente – **Dell.com/OpenManageManuals**
- Für Dell EMC Remote-Enterprise-System-Verwaltungsdokumente – **Dell.com/esmmanuals**
- Für Dokumente zu iDRAC und Dell EMC Lifecycle Controller – **Dell.com/idracmanuals**
- Für Dell EMC OpenManage Connections Enterprise-System-Verwaltungsdokumente – **Dell.com/OMConnectionsEnterpriseSystemsManagement**
- Für Dell EMC Betriebsfähigkeits-Tools-Dokumente – **Dell.com/ServiceabilityTools**
- Für Client Command Suite-System-Verwaltungsdokumente – **Dell.com/DellClientCommandSuiteManuals**
- a Rufen Sie die Website **Dell.com/Support/Home** auf.

b Klicken Sie auf **Wählen Sie aus allen Produkten**.

c Klicken Sie im Abschnitt **Alle Produkte** auf **Software und Sicherheit**, und klicken Sie dann auf einen der folgenden Links:

- **Verwaltung von Systemen der Enterprise-Klasse**
- **Remote-Verwaltung von Systemen der Enterprise-Klasse**
- **Wartungstools**
- **Dell Client Command Suite**
- **Connections Client-Systemverwaltung**

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.

2

Anmelden bei iDRAC

Sie können sich bei iDRAC als iDRAC-Benutzer, als Microsoft Active Directory-Benutzer oder als Lightweight Directory Access Protocol (LDAP)-Benutzer anmelden. Der Standardbenutzername lautet `root` und das Standardkennwort lautet `calvin`. Sie können sich auch über die einmalige Anmeldung (SSO) oder die Smart Card anmelden.

ANMERKUNG:

- Sie müssen über Berechtigungen zum Anmelden bei iDRAC verfügen, um sich bei iDRAC anzumelden.
- iDRAC-GUI unterstützt keine Browser Schaltflächen wie z. B. **Zurück**, **Vorwärts** oder **Aktualisieren**.

ANMERKUNG: Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern.

Themen:

Zugehöriger Link

Anmelden als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer bei iDRAC
Anmeldung beim CMC mit Smart Card
Bei iDRAC über die einmalige Anmeldung anmelden
Ändern des standardmäßigen Anmeldungskennworts

Anmelden als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer bei iDRAC

Stellen Sie vor der Anmeldung bei iDRAC über die Webschnittstelle sicher, dass Sie einen unterstützten Web-Browser konfiguriert haben und dass das Benutzerkonto mit den erforderlichen Berechtigungen erstellt wurde.

ANMERKUNG: Bei der Eingabe des Benutzernamens für einen Active Directory-Benutzer ist die Groß- und Kleinschreibung *nicht* relevant, beim Kennwort muss die Groß- und Kleinschreibung jedoch bei allen Benutzern beachtet werden.

ANMERKUNG: Neben Active Directory openLDAP, openDS, Novell eDir werden auch die auf Fedora basierenden Verzeichnisdienste unterstützt.

ANMERKUNG: LDAP-Authentifizierung mit OpenDS wird unterstützt. Der DH-Schlüssel muss größer sein als 768 Bit.

So melden Sie sich als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer bei iDRAC an:

1 Öffnen Sie einen unterstützten Webbrowser.

2 Geben Sie in das Feld **Adresse** `https://[iDRAC-IP-address]` ein und drücken Sie die Eingabetaste.

ANMERKUNG: Wenn die Standard-HTTPS-Schnittstellennummer (Schnittstelle 443) geändert wurde, geben Sie Folgendes ein: `https://[iDRAC-IP-address]:[port-number]`, wobei `[iDRAC-IP-address]` für die iDRAC-IPv4- oder die IPv6-Adresse und `[port-number]` für die HTTPS-Schnittstellennummer steht.

Die **Login**-Seite (Anmeldung) wird angezeigt.

3 Bei einem lokalen Benutzer:

- Geben Sie in die Felder **Benutzername** und **Kennwort** Ihre Daten für den iDRAC-Benutzernamen und das Kennwort ein.
- Wählen Sie aus dem Drop-Down-Menü **Domäne** die Option **Dieser iDRAC** aus.

4 Geben Sie für einen Active Directory-Benutzer in die Felder **Benutzername** und **Kennwort** den Active Directory-Benutzer und das zugehörige Kennwort ein. Wenn Sie den Domänennamen als Teil des Benutzernamens angegeben haben, wählen Sie **Dieser iDRAC** aus dem Drop-Down-Menü aus. Benutzernamen können in den folgenden Formaten angegeben werden: <Domäne>\<Benutzername>, <Domäne>/<Benutzername> oder <Benutzer>@<Domäne>.

Beispiele: dell.com\Markus_Bauer oder Markus_Bauer@dell.com.

Wenn die Domäne im Benutzernamen nicht angegeben ist, wählen Sie die Active Directory-Domäne aus dem Drop-Down-Menü **Domäne** aus.

5 Geben Sie für einen LDAP-Benutzer Ihren LDAP-Benutzernamen und das zugehörige Kennwort in die Felder **Benutzername** und **Kennwort** ein. Der Domänenname ist für die LDAP-Anmeldung nicht erforderlich. Standardmäßig ist **Dieser iDRAC** im Drop-Down-Menü ausgewählt.

6 Klicken Sie auf **Senden**. Sie werden mit den erforderlichen Benutzerberechtigungen bei iDRAC angemeldet.

Wenn Sie sich mit Berechtigungen „Benutzer konfigurieren“ und den standardmäßigen Kontenanmeldeinformationen anmelden und die standardmäßige Kennwortwarnungsfunktion aktiviert ist, wird Ihnen die Seite **Standardmäßige Kennwortwarnung** angezeigt, die es Ihnen ermöglicht, das Kennwort auf einfache Art und Weise zu ändern.

Zugehöriger Link

Benutzerkonten und Berechtigungen konfigurieren
Ändern des standardmäßigen Anmeldungskennworts
Konfigurieren von unterstützten Webbrowsern

Anmeldung beim CMC mit Smart Card

Sie können sich über eine Smart Card bei iDRAC anmelden. Smart Cards verfügen über eine Zweifaktor-Authentifizierung (TFA) mit Sicherheit auf zwei Ebenen:

- Physisches Smart Card-Gerät.
- Geheimcode, z. B. ein Kennwort oder eine PIN.

Benutzer müssen ihre Anmeldeinformationen über die Smart Card und die PIN überprüfen.

Zugehöriger Link

Bei iDRAC über eine Smart Card als lokaler Benutzer anmelden
Bei iDRAC über eine Smart Card als Active Directory-Benutzer anmelden

Bei iDRAC über eine Smart Card als lokaler Benutzer anmelden

Bevor Sie sich als lokaler Benutzer unter Verwendung einer Smart Card anmelden können, müssen Sie die folgenden Schritte ausführen:

- Benutzer-Smart Card-Zertifikat und vertrauenswürdiges Zertifikat der Zertifizierungsstelle nach iDRAC hochladen
- Smart Card-Anmeldung aktivieren

Die iDRAC-Webschnittstelle zeigt die Smart Card-Anmeldeseite für alle Benutzer an, die für die Verwendung der Smart Card konfiguriert wurden.

ANMERKUNG: Abhängig von den Browser-Einstellungen werden Sie aufgefordert, das Smart Card Reader-ActiveX-Plugin herunterzuladen und zu installieren, wenn Sie diese Funktion zum ersten Mal anwenden.

So melden Sie sich bei iDRAC als lokaler Benutzer über eine Smart Card an:

1 Rufen Sie die iDRAC-Web-Schnittstelle über den Link `https://[IP address]` auf.
Die **iDRAC-Anmeldeseite** wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

ANMERKUNG: Wenn die standardmäßige HTTPS-Schnittstellennummer (Schnittstelle 443) geändert wurde, geben Sie Folgendes ein: `https://[IP address]:[port number]`, wobei `[IP address]` für die IP-Adresse des iDRAC und `[port number]` für die HTTPS- Schnittstellennummer steht.

2 Legen Sie die Smart Card in das Laufwerk ein, und klicken Sie auf **Anmeldung**.
Sie werden daraufhin dazu aufgefordert, die PIN für die Smart Card einzugeben. Ein Kennwort wird nicht benötigt.

3 Geben Sie die PIN der Smart Card für lokale Smart Card-Benutzer ein.
Sie werden am iDRAC angemeldet.

ANMERKUNG: Wenn Sie ein lokaler Benutzer sind, für den die Option CRL-Prüfung für Smart Card-Anmeldung aktivieren aktiviert ist, versucht iDRAC, die Zertifikatsperrliste (CRL) herunterzuladen und überprüft die Zertifikatsperrliste (CRL) auf das Benutzerzertifikat. Die Anmeldung schlägt fehl, wenn das Zertifikat in der Zertifikatsperrliste als „Widerrufen“ gekennzeichnet ist oder wenn die Zertifikatsperrliste aus bestimmten Gründen nicht heruntergeladen werden kann.

Zugehöriger Link

Smart Card-Anmeldung aktivieren oder deaktivieren
iDRAC-Smart Card-Anmeldung für lokale Benutzer konfigurieren

Bei iDRAC über eine Smart Card als Active Directory-Benutzer anmelden

Bevor Sie sich über eine Smart Card als Active Directory-Benutzer anmelden, müssen Sie die folgenden Schritte ausführen:

- Laden Sie ein vertrauenswürdiges Zertifikat einer Zertifizierungsstelle (ein von einer Zertifizierungsstelle signiertes Active Directory-Zertifikat) nach iDRAC hoch.
- Konfigurieren Sie den DNS-Server.
- Aktivieren Sie die Active Directory-Anmeldung.
- Smart Card-Anmeldung aktivieren.

So melden Sie sich über eine Smart Card als Active Directory-Benutzer bei iDRAC an:

1 Melden Sie sich über den Link `https://[IP address]` bei iDRAC an.
Die **iDRAC-Anmelde**seite wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

ANMERKUNG: Wenn die standardmäßige HTTPS-Schnittstellennummer (Schnittstelle 443) geändert wird, geben Sie Folgendes ein: `https://[IP address]:[port number]`, wobei `[IP address]` für die iDRAC-IP-Adresse und `[port number]` für die HTTPS-Schnittstellennummer steht.

2 Legen Sie die Smart Card ein und klicken Sie auf **Anmeldung**.
Daraufhin wird das Popup-Fenster für die **PIN** angezeigt.

3 Geben Sie die PIN ein und klicken Sie auf **Senden**.

Sie sind über Ihre Active Directory-Anmeldedaten bei iDRAC angemeldet.

ANMERKUNG:

Wenn der Smart Card-Benutzer in Active Directory vorhanden ist, wird kein Active Directory-Kennwort benötigt.

Zugehöriger Link

Smart Card-Anmeldung aktivieren oder deaktivieren

iDRAC-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren

Bei iDRAC über die einmalige Anmeldung anmelden

Wenn die einmalige Anmeldung (SSO) aktiviert ist, können Sie sich ohne die Eingabe Ihrer Anmeldeinformationen für die Domänen-Benutzerauthentifizierung (also Benutzername und Kennwort) bei iDRAC anmelden.

Zugehöriger Link

iDRAC-SSO-Anmeldung für Active Directory-Benutzer konfigurieren

Bei iDRAC SSO über die iDRAC-Webschnittstelle anmelden

Bevor Sie sich über das Verfahren für die einmalige Anmeldung bei iDRAC anmelden, müssen Sie Folgendes sicherstellen:

- Sie haben sich über ein gültiges Active Directory-Benutzerkonto bei Ihrem System angemeldet.
- Die Option für die einmalige Anmeldung ist während der Active Directory-Konfiguration aktiviert.

So melden Sie sich über die Webschnittstelle bei iDRAC an:

1 Melden Sie sich unter Verwendung eines gültigen Active Directory-Kontos an der Verwaltungsstation an.

2 Geben Sie in einem Web-Browser Folgendes ein: `https://[FQDN address]`

ANMERKUNG: Wenn die standardmäßige HTTPS-Schnittstellennummer (Schnittstelle 443) geändert wurde, geben Sie Folgendes ein: `https://[FQDN address]:[port number]`, wobei `[FQDN address]` für die IP-Adresse des iDRAC und `[port number]` für die HTTPS-Schnittstellennummer steht.

ANMERKUNG: Wenn Sie die IP-Adresse statt des FQDN verwenden, schlägt die SSO fehl.

iDRAC meldet Sie mit den entsprechenden Microsoft Active Directory-Berechtigungen an und verwendet dabei die Anmeldeinformationen, die durch das Betriebssystem erfasst wurden, während Sie sich über ein gültiges Active Directory-Konto angemeldet haben.

Bei iDRAC SSO über die CMC-Webschnittstelle anmelden

Durch die Verwendung der SSO-Funktion können Sie die iDRAC-Webschnittstelle über die CMC-Web-Schnittstelle starten. Ein CMC-Benutzer verfügt über CMC-Benutzerberechtigungen, wenn er iDRAC über CMC startet. Wenn das Benutzerkonto in CMC vorhanden ist, jedoch nicht in iDRAC, kann der Benutzer iDRAC dennoch über CMC starten.

Wenn iDRAC-Netzwerk-LAN deaktiviert ist (LAN aktiviert = Nein), ist die SSO (Einzelanmeldung) nicht verfügbar.

Wenn der Server aus dem Gehäuse entfernt oder die iDRAC-IP-Adresse geändert wird, oder wenn ein Problem bei der iDRAC-Netzwerkverbindung vorliegt, wird die Option zum Starten von iDRAC in der CMC-Web-Schnittstelle ausgegraut dargestellt.

Weitere Informationen finden Sie im *Chassis Management Controller User's Guide* (Chassis Management Controller-Benutzerhandbuch) unter **dell.com/support/manuals**.

Über Remote-RACADM auf iDRAC zugreifen

Sie können Remote-RACADM für den Zugriff auf iDRAC über das RACADM-Dienstprogramm verwenden.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide* (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC) unter **dell.com/idracmanuals**.

Wenn die Management Station das iDRAC-SSL-Zertifikat nicht in ihrem Standard-Zertifikatspeicher gespeichert hat, wird eine Warnmeldung angezeigt, wenn Sie den RACADM-Befehl ausführen. Der Befehl wird jedoch erfolgreich ausgeführt.

ANMERKUNG: Bei dem iDRAC-Zertifikat handelt es sich um das Zertifikat, das iDRAC an den RACADM-Client sendet, um die sichere Sitzung aufzubauen. Dieses Zertifikat wird entweder von einer Zertifikatzertifizierungsstelle oder selbst signiert ausgegeben. Wenn die Management Station die Zertifikatzertifizierungsstelle oder die signierende Stelle nicht erkennt, wird in beiden Fällen eine Warnung angezeigt.

Zugehöriger Link

Zertifizierungsstellenzertifikat für die Verwendung von Remote-RACADM auf Linux validieren

Zertifizierungsstellenzertifikat für die Verwendung von Remote-RACADM auf Linux validieren

Bevor Sie Remote-RACADM-Befehle ausführen, validieren Sie zunächst das Zertifizierungsstellenzertifikat, das für die sichere Kommunikation verwendet wird.

So validieren Sie das Zertifikat für die Verwendung von Remote-RACADM:

1 Konvertieren Sie das Zertifikat vom DER-Format in das PEM-Format (verwenden Sie dazu das Befehlszeilen-Tool „openssl“):

```
openssl x509 -inform pem -in [yourdownloadedderformatcert.crt] -outform pem -out
[outcertfileinpemformat.pem] -text
```

2 Suchen Sie den Speicherort des Standard-Zertifizierungsstellenzertifikat-Bundle auf der Management Station. Für RHEL5 64-bit lautet es beispielsweise **/etc/pki/tls/cert.pem**.

3 Hängen Sie das PEM-formatierte CA-Zertifikat an das CA-Zertifikat der Management Station an.

Verwenden Sie beispielsweise den CAT-Befehl: `cat command: cat testcacert.pem >> cert.pem`

4 Generieren Sie das Server-Zertifikat, und laden Sie es auf iDRAC hoch.

Über lokalen RACADM auf iDRAC zugreifen

Weitere Informationen zum Zugriff auf iDRAC unter Verwendung des lokalen RACADM finden Sie unter *iDRAC RACADM Command Line Interface Reference Guide* (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC) unter **dell.com/idracmanuals**.

Über Firmware-RACADM auf iDRAC zugreifen

Sie können die SSH- oder Telnet-Schnittstellen für den Zugriff auf iDRAC und zum Ausführen der Firmware-RACADM-Befehle verwenden. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide* (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC) unter **dell.com/idracmanuals**.

Über SMCLP auf iDRAC zugreifen

SMCLP ist die Standard-Befehlszeileneingabe, wenn Sie sich über Telnet oder SSH bei iDRAC anmelden. Weitere Informationen finden Sie unter SMCLP verwenden.

Anmeldung beim iDRAC mit Authentifizierung mit öffentlichem Schlüssel

Sie können sich über SSH beim iDRAC anmelden, ohne ein Kennwort einzugeben. Sie können auch einen einzelnen RACADM-Befehl als Befehlszeilenargument an die SSH-Anwendung senden. Die Befehlszeilenoptionen verhalten sich ähnlich wie Remote-RACADM, da die Sitzung endet, nachdem der Befehl ausgeführt wurde.

Beispiel:

Anmeldung:

```
ssh username@<domain>
```

oder

```
ssh username@<IP_address>
```

wobei IP-Adresse die `IP_address` des iDRAC ist.

Senden von RACADM-Befehlen:

```
ssh username@<domain> racadm getversion
```

```
ssh username@<domain> racadm getsel
```

Zugehöriger Link

Authentifizierung von öffentlichen Schlüsseln für SSH verwenden

Mehrere iDRAC-Sitzungen

Aus der folgenden Tabelle können Sie eine Liste mit mehreren iDRAC -Sitzungen entnehmen, die durch die Verwendung der diversen Schnittstellen möglich sind.

Tabelle 6. Mehrere iDRAC-Sitzungen

Schnittstelle	Anzahl der Sitzungen
iDRAC-Web-Schnittstelle	6
Remote-RACADM	4
Firmware-RACADM/SMCLP	SSH – 2 Telnet – 2 Seriell – 1

Ändern des standardmäßigen Anmeldungskennworts

Die Warnmeldung, mithilfe der Sie das standardmäßige Anmeldungskennwort ändern können, wird angezeigt, wenn:

- MeldenSie sich bei iDRAC mit der Berechtigung „Benutzer konfigurieren“ an.
- Die Warnungsfunktion des standardmäßigen Kennworts aktiviert ist.
- Anmeldeinformationen für das derzeitig aktive Konto root/calvin lauten.

Es wird außerdem eine Warnungsmeldung angezeigt, wenn Sie sich beim iDRAC unter Verwendung von SSH, Telnet, Remote-RACADM oder Webschnittstelle anmelden. Für Webschnittstelle, SSH und Telnet wird eine einzelne Warnungsmeldung für jede Sitzung angezeigt. Für Remote-RACADM wird für jeden Befehl eine Warnungsmeldung angezeigt.

ANMERKUNG: Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern.

Zugehöriger Link

Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung

Ändern des standardmäßigen Anmeldekennworts unter Verwendung von Web-Schnittstelle

Wenn Sie sich an die iDRAC Webschnittstelle anmelden und die Seite **Standardmäßige Kennwortwarnung** angezeigt wird, können Sie das Kennwort ändern. Gehen Sie dabei folgendermaßen vor:

1 Wählen Sie die Option **Standardmäßiges Kennwort ändern**.
2 Geben Sie im Feld **Neues Kennwort** das neue Kennwort ein.

ANMERKUNG: Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern.

3 Geben Sie in dem Feld **Kennwort bestätigen** das Kennwort erneut ein.
4 Klicken Sie auf **Fortfahren**. Das neue Kennwort ist konfiguriert und Sie sind bei iDRAC angemeldet.

ANMERKUNG: Das Feld Fortfahren ist nur aktiviert, wenn die Felder Neues Kennwort und Kennwort bestätigen übereinstimmen.

Weitere Informationen zu den anderen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

Ändern eines in den Standardeinstellungen festgelegten Anmeldungskennworts unter Verwendung von RACADM

So ändern Sie ein Kennwort mithilfe der Ausführung des folgenden RACADM-Befehls:

```
racadm set iDRAC.Users.<index>.Password <Password>
```

wobei `<index>` ein Wert zwischen 1 und 16 ist (und für das Benutzerkonto steht) und `<password>` das neue benutzerdefinierte Kennwort ist.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

ANMERKUNG: Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern.

Ändern des standardmäßigen Anmeldekennworts unter Verwendung des Dienstprogramms für iDRAC-Einstellungen

So ändern Sie das standardmäßige Anmeldekennwort unter Verwendung des Dienstprogramms für iDRAC-Einstellungen:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Benutzerkonfiguration**.
Daraufhin wird die Seite **iDRAC-Einstellungen – Benutzerkonfiguration** angezeigt.
2 Geben Sie im Feld **Kennwort ändern** das neue Kennwort ein.

ANMERKUNG: **Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern.**

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Details werden gespeichert.

Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung

Sie können die Anzeige der standardmäßigen Kennwortwarnungsmeldung aktivieren oder deaktivieren. Dafür benötigen Sie jedoch die Berechtigung „Benutzer konfigurieren“.

Aktivieren oder Deaktivieren einer standardmäßigen Kennwortwarnungsmeldung unter Verwendung der Web-Schnittstelle

So aktivieren oder deaktivieren Sie die Anzeige der standardmäßigen Kennwortwarnungsmeldung nach der Anmeldung bei iDRAC:

1 Gehen Sie zu **Übersicht** > **iDRAC Einstellungen** > **Benutzerauthentifizierung** > **Lokale Benutzer**.

Die Seite **Benutzer** wird angezeigt.

2 Wählen Sie im Abschnitt **Standardmäßige Kennwortwarnung** die Option **Aktivieren** aus und klicken Sie anschließend auf **Anwenden**, um die Anzeige der Seite **Standardmäßige Kennwortwarnung** anzuzeigen, wenn Sie sich bei iDRAC anmelden. Andernfalls klicken Sie auf **Deaktivieren**.

Alternativ können Sie, wenn diese Option aktiviert ist und Sie eine Anzeige der Warnmeldung für nachfolgende Anmeldungen vermeiden wollen, erst auf die Option **Diese Warnmeldung nicht noch einmal anzeigen** auf der Seite **Standardmäßigen Kennwortwarnung** und dann auf **Anwenden** klicken.

Aktivieren oder Deaktivieren der Warnungsmeldung zum Ändern des standardmäßigen Anmeldungskennworts unter Verwendung von RACADM

Um die Anzeige der Warnmeldung zur Änderung des standardmäßigen Anmeldekennworts unter Verwendung von RACADM zu aktivieren, verwenden Sie das Objekt `idrac.tuning.DefaultCredentialWarning`.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

IP-Blockierung

Durch IP-Blockierung wird dynamisch festgestellt, wenn von einer bestimmten IP-Adresse aus aufeinanderfolgende Anmeldefehlversuche auftreten und die Adresse eine bestimmte Zeit lang blockiert bzw. daran gehindert wird, eine Anmeldung am iDRAC durchzuführen. Die IP-Blockierung enthält:

- Anzahl zulässiger Anmeldefehlschläge
- Zeitspanne in Sekunden, in der die Fehlversuche auftreten müssen
- Zeitdauer in Sekunden, innerhalb der die IP-Adresse daran gehindert wird, eine Sitzung aufzubauen, nachdem die zulässige Anzahl von Fehlschlägen überschritten wurde.

Wenn aufeinanderfolgende Anmeldefehlversuche von einer spezifischen IP-Adresse auftreten, werden sie durch einen internen Zähler festgehalten. Wenn sich der Benutzer erfolgreich anmeldet, wird die Aufzeichnung der Fehlversuche gelöscht und der interne Zähler zurückgesetzt.

ANMERKUNG: Wenn aufeinanderfolgende Anmeldeversuche von der Client-IP-Adresse abgelehnt werden, können einige SSH-Clients die folgende Meldung anzeigen:

```
ssh exchange identification: Connection closed by remote host
```

.

Tabelle 7. Eigenschaften für Einschränkungen der Anmeldewiederholungsversuche

Eigenschaft	Definition
`iDRAC.IPBlocking.BlockEnable`	Aktiviert die IP-Blockierungsfunktion. Wenn aufeinander folgende Fehlversuche (`iDRAC.IPBlocking.FailCount`) von einer einzelnen IP-Adresse aus innerhalb eines bestimmten Zeitraums (`iDRAC.IPBlocking.FailWindow`) festgestellt werden, werden alle weiteren Versuche, von dieser Adresse aus eine Sitzung aufzubauen, innerhalb einer bestimmten Zeitspanne zurückgewiesen (`iDRAC.IPBlocking.PenaltyTime`).
`iDRAC.IPBlocking.FailCount`	Legt die Anzahl der Anmeldefehler von einer bestimmten IP-Adresse fest, bevor Anmeldeversuche von dieser Adresse zurückgewiesen werden.
`iDRAC.IPBlocking.FailWindow`	Die Zeitspanne in Sekunden, während der die Fehlversuche gezählt werden. Wenn die Anzahl der Fehlversuche diesen Grenzwert überschreitet, wird der Zähler zurückgesetzt.
`iDRAC.IPBlocking.PenaltyTime`	Definiert die Zeitdauer in Sekunden, während der alle Anmeldeversuche von einer IP-Adresse mit übermäßigen Fehlern zurückgewiesen werden.

Ungültige Kennwort-Anmeldeinformationen

Zum Schutz vor nicht autorisierten Benutzern und Denial-of-Service (DoS)-Angriffen bietet iDRAC vor der Sperrung der IP und SNMP-Traps (falls aktiviert) folgendes:

- Serie von Anmeldungsfehlern und Warnungen
- Erhöhte Zeitintervalle mit jedem falschen Anmeldeversuch in Folge
- Protokolleinträge

ANMERKUNG: Die Anmeldefehler und Warnungen, das mit jedem falschen Anmeldungsversuch erhöhte Zeitintervall und die Protokolleinträge stehen unter Verwendung von allen iDRAC-Schnittstellen zur Verfügung, wie z.B. der Webschnittstelle, Telnet, SSH, Remote-RACADM, WS-MAN und VMCLI.

Tabelle 8. Verhalten der iDRAC-Webschnittstelle bei ungültigen Anmeldeversuchen

Anmeldeversuche	Sperrung (Sekunden)	Fehler wird protokolliert (USR00034)	Anzeigen einer GUI-Nachricht	SNMP-Warnung (falls aktiviert)
Erster inkorrekter Anmeldeversuch	0	Nein	Keine	Nein
Zweiter inkorrekter Anmeldeversuch	0	Nein	Keine	Nein
Dritter inkorrekter Anmeldeversuch	600	Ja	• `RAC0212: Login failed (Anmeldung fehlgeschlagen). Verify that username and password is correct. (Stellen Sie sicher, dass Benutzername und Kennwort korrekt ist.) Login delayed for 600 seconds. (Verzögerung der Anmeldung um 600 Sekunden.)` • Schaltfläche **Try again (Versuchen Sie es erneut)** wird für 600 Sekunden deaktiviert.	Ja

ANMERKUNG: Standardmäßig wird der Zähler für Anmeldefehler nach 600 Sekunden zurückgesetzt. Diese Einstellung kann individuell angepasst werden, indem Sie PenaltyTime über RACADM ändern. Verwenden Sie den Befehl *setidrac.ipblockingpenaltyTime X*.

3

Managed System und Management Station einrichten

Für die bandexterne Systemverwaltung über iDRAC müssen Sie iDRAC für die Remote-Zugriffsmöglichkeit konfigurieren, die Management Station und das Managed System einrichten und die unterstützten Web-Browser konfigurieren.

ANMERKUNG: Bei Blade-Servern müssen Sie vor der Ausführung der Konfigurationsschritte die CMC- und E/A-Module im Gehäuse und das System physisch in das Gehäuse installieren.

Sowohl iDRAC Express als auch iDRAC Enterprise werden werksseitig mit einer standardmäßigen statischen IP-Adresse ausgeliefert. Dell bietet zudem noch zwei weitere Optionen:

- **Bereitstellungsserver** – Verwenden Sie diese Option, wenn Sie einen Bereitstellungsserver in der Rechenzentrumsumgebung installiert haben. Ein Bereitstellungsserver verwaltet und automatisiert die Bereitstellung oder Aktualisierung eines Betriebssystems und die Anwendung für einen Dell PowerEdge Server. Durch Aktivieren der Bereitstellungsserveroption suchen die Server beim ersten Starten nach einem Bereitstellungsserver, der die Steuerung übernimmt und den automatisierten Bereitstellungs- oder Aktualisierungsprozess startet.
- **DHCP** – Verwenden Sie diese Option, wenn in Ihrer Rechenzentrumsumgebung ein DHCP-Server (Dynamic Host Configuration Protocol) installiert ist oder wenn Sie iDRAC Auto Config oder den Konfigurationsmanager von OpenManage Essentials für die Automatisierung der Serverbereitstellung verwenden. Der DHCP-Server weist iDRAC automatisch IP-Adresse, Gateway und Subnetzmaske zu.

Sie können den Bereitstellungsserver oder DHCP bereits bei der Bestellung des Servers kostenlos aktivieren lassen. Es ist jedoch nur eine Einstellung möglich.

Themen:

Zugehöriger Link

iDRAC-IP-Adresse einrichten
Managed System einrichten
Aktualisieren der Gerätefirmware
Rollback der Geräte-Firmware durchführen
Management Station einrichten
Konfigurieren von unterstützten Webbrowsern

iDRAC-IP-Adresse einrichten

Sie müssen die anfänglichen Netzwerkeinstellungen auf der Basis Ihrer Netzwerkinfrastruktur konfigurieren, um die bilaterale Kommunikation mit iDRAC zu aktivieren. Sie können die IP-Adresse über eine der folgenden Schnittstellen einrichten:

- Dienstprogramm für die iDRAC-Einstellungen
- Lifecycle-Controller (siehe *Lifecycle-Controller-Benutzerhandbuch*)
- Dell Deployment Toolkit (siehe *Dell Deployment Toolkit-Benutzerhandbuch*)
- LC-Anzeige auf der Gehäuse- oder Server-Frontblende (siehe das *Hardware-Benutzerhandbuch* für das System)

  ANMERKUNG: Bei Blade-Servern können Sie die Netzwerkeinstellung über die Gehäuse-LC-Anzeige auf der Frontblende nur im Rahmen der Erstkonfiguration von CMC konfigurieren. Nach der Bereitstellung des Gehäuses können Sie iDRAC nicht mehr über die Gehäuse-LC-Anzeige auf der Frontblende neu konfigurieren.
- CMC-Web-Schnittstelle (siehe *Dell Chassis Management Controller Firmware-Benutzerhandbuch)*

Bei Rack- und Tower-Servern können Sie die IP-Adresse einrichten oder die iDRAC-Standard-IP-Adresse 192.168.0.120 für die Erstkonfiguration der Netzwerkeinstellungen verwenden. Im Rahmen dieser Konfiguration können Sie auch DHCP oder die statische IP-Adresse für iDRAC einrichten.

Bei Blade-Servern wird standardmäßig die iDRAC-Netzwerkschnittstelle angezeigt.

Nach der Konfiguration der iDRAC-IP-Adresse:

- Sie müssen nach dem Einrichten der iDRAC-IP-Adresse den standardmäßigen Benutzernamen und das standardmäßige Kennwort ändern.
- Greifen Sie über die folgenden Schnittstellen auf iDRAC zu:
  - iDRAC Web-Schnittstelle unter Verwendung eines unterstützten Browsers (Internet Explorer, Firefox, Chrome oder Safari)
  - Secure Shell (SSH) – Erfordert einen Client, wie z. B. PuTTY auf Windows. SSH ist standardmäßig auf den meisten Linux-Systemen verfügbar, so dass kein Client benötigt wird.
  - Telnet (muss aktiviert werden, da es standardmäßig deaktiviert ist)
  - IPMITool (verwendet den IPMI-Befehl) oder Shell-Befehlseingabe (erfordert ein von Dell angepasstes Installationsprogramm unter Windows oder Linux, das von der *Systems Management Documentation and Tools*-DVD oder von **dell.com/support** abgerufen werden kann)

Zugehöriger Link

iDRAC-IP-Adresse über das Dienstprogramm für die iDRAC-Einstellungen einrichten
iDRAC-IP-Adresse über die CMC-Webschnittstelle einrichten
Aktivierung des Bereitstellungsservers
Konfigurieren von Servern und Serverkomponenten mithilfe der automatischen Konfiguration

iDRAC-IP-Adresse über das Dienstprogramm für die iDRAC-Einstellungen einrichten

So richten Sie die iDRAC-IP-Adresse ein:

1 Schalten Sie das verwaltete System ein.
2 Drücken Sie während des Einschaltselbsttests (POST) die Taste <F2>.
3 Klicken Sie auf der Seite **System-Setup-Hauptmenü** auf **iDRAC-Einstellungen**.
  Die Seite **iDRAC-Einstellungen** wird angezeigt.
4 Klicken Sie auf **Netzwerk**.
  Die Seite **Netzwerk** wird angezeigt.
5 Legen Sie die folgenden Einstellungen fest:

- Netzwerkeinstellungen
- Allgemeine Einstellungen
- IPv4-Einstellungen
- IPv6-Einstellungen
- IPMI-Einstellungen
- VLAN-Einstellungen

6 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Netzwerkinformationen werden gespeichert, und das System wird neu gestartet.

Zugehöriger Link

Netzwerkeinstellungen
Allgemeine Einstellungen
IPv4-Einstellungen
IPv6-Einstellungen
IPMI-Einstellungen
VLAN-Einstellungen

Netzwerkeinstellungen

So konfigurieren Sie die Netzwerkeinstellungen:

ANMERKUNG: Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

1 Wählen Sie unter **NIC aktivieren** die Option **Aktiviert** aus.

2 Wählen Sie aus dem Drop-Down-Menü **NIC-Auswahl** auf der Basis der Netzwerkanforderung eine der folgenden Schnittstellen aus:

- **Dediziert** – Wählen Sie diese Option aus, um das Remote-Zugriffsgerät zu aktivieren und die auf dem Remote-Access-Controller (RAC) verfügbare dedizierte Netzwerkschnittstelle zu verwenden. Die DRAC-Schnittstelle wird nicht an das Host-Betriebssystem freigegeben und leitet den Verwaltungsverkehr zu einem separaten physischen Netzwerk, wodurch sie vom Anwendungsverkehr getrennt werden kann.

  Diese Option impliziert, dass die dedizierte iDRAC-Netzwerkschnittstelle den Datenverkehr getrennt von den LOM- oder NIC-Schnittstellen des Servers weiterleitet. Über die Verwaltung des Netzwerkdatenverkehrs kann iDRAC über die Option „Dediziert“ im Vergleich zu den IP-Adressen, die dem Host-LOM oder den NICs zugewiesen werden, eine IP-Adresse vom gleichen Subnetz oder einem anderen Subnetz zugewiesen werden.

  ANMERKUNG: Bei Blade-Servern wird die Option "Dediziert" als Gehäuse (Dediziert) angezeigt.
- **LOM1**
- **LOM2**
- **LOM3**
- **LOM4**

ANMERKUNG: Bei Rack- und Tower-Servern sind zwei LOM-Optionen (LOM1 und LOM2) oder alle vier LOM-Optionen verfügbar. Maßgeblich dafür ist das jeweilige Server-Modell. Bei Blade-Servern mit zwei NDC-Ports sind zwei LOM-Optionen (LOM1 und LOM2) verfügbar, und auf einem Server mit vier NDC-Ports stehen alle vier LOM-Optionen zur Verfügung.

ANMERKUNG: Shared LOM wird jedoch auf den folgenden bNDCs nicht unterstützt, wenn sie in einem Server mit voller Höhe und zwei NDCs verwendet werden, weil sie keine Hardware-Arbitrierung unterstützen:

- Intel X520-k 2P bNDC 10 G
- Emulex OCM14102-N6-D-bNDC 10 GB
- Emulex OCm14102-U4-D bNDC 10 Gb
- Emulex OCm14102-U2-D bNDC 10 Gb
- QLogic QMD8262–k DP bNDC 10 G

3 Wählen Sie aus dem Drop-Down-Menü **Failover-Netzwerk** eine der verbleibenden LOMs aus. Wenn ein Netzwerk ausfällt, wird der Datenverkehr über das Failover-Netzwerk umgeleitet.

Wenn beispielsweise der iDRAC-Netzwerkverkehr über LOM2 umgeleitet werden soll, wenn LOM1 ausgefallen ist, wählen Sie **LOM1** unter **NIC-Auswahl** und **LOM2** unter **Failover-Netzwerk** aus.

ANMERKUNG: Wenn Sie in der Drop-Down-Liste NIC-Auswahl die Option Dediziert ausgewählt haben, wird diese Option ausgegraut dargestellt.

ANMERKUNG: Failover wird auf dem freigegebenen LOM für die folgenden Emulex rNDCs und bNDCs nicht unterstützt:

- Emulex OCM14104-UX-D rNDC 10 Gbx
- Emulex OCM14104-U1-D rNDC 10 Gb
- Emulex OCM14104-N1-D rNDC 10 Gb
- Emulex OCM14104B-N1-D rNDC 10 Gb
- Emulex OCM14102-U2-D bNDC 10 Gb
- Emulex OCM14102-U4-D bNDC 10 Gb
- Emulex OCM14102-N6-D bNDC 10 Gb

ANMERKUNG: Auf PowerEdge-Servern vom Typ FM120x4 und FX2 wird das Failover-Netzwerk für die Konfiguration der Gehäuseschlitten nicht unterstützt. Weitere Informationen über die Konfiguration der Gehäuseschlitten finden Sie im CMC-Benutzerhandbuch „Chassis Management Controller (CMC) User's Guide“, das unter dell.com/idracmanuals verfügbar ist.

ANMERKUNG: Stellen Sie während der Konfiguration der erweiterten Netzwerkadapterisolierung auf PowerEdge FM120x4-Servern sicher, dass LOM2 auf dem Host-System deaktiviert und bei iDRAC-NIC nicht ausgewählt ist. Weitere Informationen über die Konfiguration der Schlitten im Gehäuse finden Sie im Chassis Management Controller (CMC) Benutzerhandbuch, verfügbar unter dell.com/idracmanuals.

4 Wählen Sie unter **Automatische Verhandlung** die Option **Eingeschaltet** aus, wenn iDRAC den Duplexmodus und die Netzwerkgeschwindigkeit automatisch festlegen muss. Diese Option ist nur im dedizierten Modus verfügbar. Wenn sie aktiviert ist, legt iDRAC die Netzwerkgeschwindigkeit auf der Basis der Netzwerkgeschwindigkeit auf 10, 100 oder 1.000 MB/s fest.

5 Wählen Sie unter **Netzwerkgeschwindigkeit** entweder 10 oder 100 MB/s aus.

ANMERKUNG: Sie können die Netzwerkgeschwindigkeit nicht manuell auf 1000 MB/s setzen. Diese Option ist nur verfügbar, wenn die Option Automatische Verhandlung aktiviert ist.

6 Wählen Sie unter **Duplexmodus** die Option **Halbduplex** oder **Vollduplex** aus.

ANMERKUNG: Wenn Sie Automatische Verhandlung ausgewählt haben, wird diese Option ausgegraut dargestellt.

Allgemeine Einstellungen

Wenn die Netzwerkinfrastruktur einen DNS-Server aufweist, registrieren Sie iDRAC auf diesem DNS. Hierbei handelt es sich um die anfänglichen Einstellungsanforderungen für erweiterte Funktionen, darunter „Verzeichnisdienste – Active Directory oder LDAP“, Einmalige Anmeldung und Smart Card.

So registrieren Sie iDRAC:

1 **DRAC auf DNS registrieren** aktivieren.

2 Geben Sie den **DNS-DRAC-Namen** ein.

3 Wählen Sie **Domänennamen automatisch konfigurieren** aus, um den Domänennamen automatisch von DHCP abzurufen. Andernfall stellen Sie den **DNS-Domänennamen** bereit.

IPv4-Einstellungen

So konfigurieren Sie die IPv4-Einstellungen:

1 Wählen Sie die Option **Aktiviert** unter **IPv4 aktivieren** aus

2 Wählen Sie die Option **Aktiviert** unter **DHCP aktivieren** aus, so dass DHCP die IP-Adresse, das Gateway und die Subnetzmaske automatisch zu iDRAC zuweisen kann. Wählen Sie ansonsten die Option **Deaktiviert** aus, und geben Sie die Werte für die folgenden Elemente ein:

- Statische IP-Adresse
- Statisches Gateway
- Statische Subnetzmaske

3 Aktivieren Sie optional die Option **DHCP zum Abrufen der DNS-Server-Adresse verwenden**, so dass der DHCP-Server den **bevorzugten statsischen DNS-Server** und den **alternativen statischen DNS-Server** zuweisen kann. Geben Sie ansonsten die IP-Adressen für **Statisch Bevorzugter DNS-Server** und **Statisch Alternativer DNS-Server** ein.

IPv6-Einstellungen

Alternativ können Sie auf der Basis der Einrichtung der Infrastruktur das IPv6-Adressprotokoll verwenden.

So konfigurieren Sie die IPv6-Einstellungen:

1 Wählen Sie die Option **Aktiviert** unter **IPv6 aktivieren** aus.

2 Damit der DHCPv6-Server dem iDRAC automatisch IP-Adresse, Gateway und Subnetzmaske zuweist, aktivieren Sie die Option **Aktiviert** unter **Automatische Konfiguration aktivieren**.

ANMERKUNG: Sie können gleichzeitig statische IP-Adressen und DHCP-IP-Adressen konfigurieren.

3 Geben Sie in das Feld **Statische IP-Adresse 1** die statische IPv6-Adresse ein.

4 Geben Sie in das Feld **Statische Präfixlänge** einen Wert zwischen 0 und 128 ein.

5 Geben Sie in das Feld **Statisches Gateway** die Gateway-Adresse ein.

ANMERKUNG: Wenn Sie die statische IP konfigurieren, wird für „Aktuelle IP-Adresse 1“ „statische IP“ und für „IP-Adresse 2“ „dynamische IP“ angezeigt. Wenn Sie die Einstellungen für die statische IP löschen, wird für „Aktuelle IP-Adresse 1“ „dynamische IP“ angezeigt.

6 Wenn Sie DHCP verwenden möchten, aktivieren Sie die Option **DHCPv6 für das Abrufen von DNS-Server-Adressen einrichten**, um primäre und sekundäre DNS-Server-Adressen vom DHCPv6-Server zu erhalten. Sie können bei Bedarf die folgenden Einstellungen konfigurieren:

- Geben Sie in das Feld **Statischer bevorzugter DNS-Server** die statische DNS-Server-IPv6-Adresse ein.
- Geben Sie in das Feld **Statischer alternativer DNS-Server** den statischen alternativen DNS-Server ein.

IPMI-Einstellungen

So aktivieren Sie die IPMI-Einstellungen:

1 Wählen Sie unter **IPMI-über-LAN aktivieren Aktiviert** aus.

2 Wählen Sie unter **Berechtigungsbeschränkung des Kanals Administrator**, **Operator** oder **Benutzer** aus.

3 Geben Sie in das Feld **Verschlüsselungsschlüssel** den Verschlüsselungsschlüssel mit hexadezimalen Zeichen von 0 bis 40 ohne Leerzeichen ein. Der Standardwert sind Nullen.

VLAN-Einstellungen

Sie können iDRAC für die VLAN-Infrastruktur konfigurieren. Führen Sie zum Konfigurieren der VLAN-Einstellungen die folgenden Schritte aus:

ANMERKUNG: Bei Blade-Servern, die als Gehäuse (Dediziert) eingestellt sind, sind die VLAN-Einstellungen schreibgeschützt und können nur unter Verwendung des Gehäuseverwaltungscontrollers (CMC) geändert werden. Wenn der Server für den freigegebenen Modus eingestellt wurde, können Sie die VLAN-Einstellungen in iDRAC im freigegebenen Modus konfigurieren.

1 Wählen Sie unter **VLAN-ID aktivieren** die Option **Aktiviert** aus.
2 Geben Sie im Feld **VLAN-ID** eine gültige Zahl zwischen 1 und 4.094 ein.
3 Geben Sie in das Feld **Priorität** eine Zahl zwischen 0 und 7 ein, um die Priorität der VLAN-ID zu definieren.

ANMERKUNG: Nach der Aktivierung von VLAN ist die iDRAC-IP-Adresse eine Zeit lang nicht zugänglich.

iDRAC-IP-Adresse über die CMC-Webschnittstelle einrichten

So richten Sie die iDRAC-IP-Adresse über die CMC-Webschnittstelle ein:

ANMERKUNG: Sie müssen Administratorberechtigungen für die Gehäusekonfiguration (Chassis Configuration Administrator) besitzen, um iDRAC-Netzwerkeinstellungen über den CMC vornehmen zu können.

1 Melden Sie sich bei der CMC-Webschnittstelle an.
2 Gehen Sie zu **Server-Übersicht** > **Einrichtung** > **iDRAC**.
Die Seite **iDRAC** bereitstellen wird angezeigt.
3 Wählen Sie unter **iDRAC-Netzwerkeinstellungen** die Option **LAN aktivieren** und ggf. weitere Netzwerkparameter aus. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.
4 Für Informationen zu Blade-Server-spezifischen Netzwerkeinstellungen gehen Sie zu **Server-Übersicht** > **<Server-Name>**.
Die Seite **Serverstatus** wird angezeigt.
5 Klicken Sie auf **iDRAC starten**, und gehen Sie zu**Übersicht** > **iDRAC-Einstellungen** > **Netzwerk**.
6 Machen Sie auf der Seite **Netzwerk** Angaben zu den folgenden Aspekten:
- Netzwerkeinstellungen
- Allgemeine Einstellungen
- IPv4-Einstellungen
- IPv6-Einstellungen
- IPMI-Einstellungen
- VLAN-Einstellungen

ANMERKUNG: Weitere Informationen finden Sie in der *iDRAC Online-Hilfe*.

7 Klicken Sie zum Speichern der Netzwerkinformationen auf **Anwenden**.
Weitere Informationen finden Sie im *Chassis Management Controller User's Guide* (Chassis Management Controller-Benutzerhandbuch) unter **dell.com/support/manuals**.

Aktivierung des Bereitstellungsservers

Die Funktion des Bereitstellungsservers erlaubt neu installierten Servern, automatisch die Remote-Verwaltungskonsole zu ermitteln, die den Bereitstellungsserver hostet. Der *Bereitstellungsserver* stellt iDRAC benutzerdefinierte Administrator-Anmeldeinformationen zur Verfügung, damit der nicht bereitgestellte Server durch die Verwaltungskonsole ermittelt und verwaltet werden kann. Weitere Informationen zum Bereitstellungsserver finden Sie im *Lifecycle Controller Remote Services User's Guide* (Lifecycle Controller Remote Services-Benutzerhandbuch) unter **dell.com/idracmanuals**.

Der Bereitstellungsserver arbeitet mit einer statischen IP-Adresse. DHCP, DNS-Server oder der Standard-DNS-Host-Name ermitteln den Bereitstellungs-Server. Wenn DNS angegeben ist, wird die IP-Adresse für den Bereitstellungs-Server aus DNS abgerufen; die DHCP-Einstellungen werden nicht benötigt. Wenn der Bereitstellungs-Server angegeben ist, wird die Ermittlung übersprungen, so dass weder DHCP noch DNS erforderlich sind.

Sie können die Funktion des Bereitstellungsservers über das Dienstprogramm für die iDRAC-Einstellungen oder über Lifecycle Controller aktivieren. Weitere Informationen zur Verwendung von Lifecycle Controller finden Sie im *Lifecycle Controller User's Guide* (Lifecycle Controller-Benutzerhandbuch) unter **dell.com/idracmanuals**.

Wenn die Funktion des Bereitstellungsservers auf dem werksseitigen System nicht aktiviert ist, wird das standardmäßige Administratorkonto (Benutzername = root und Kennwort = calvin) aktiviert. Vor der Aktivierung des Bereitstellungsservers müssen Sie sicherstellen, dass Sie dieses Administratorkonto deaktivieren. Wenn die Funktion des Bereitstellungsservers in Lifecycle Controller aktiviert ist, werden alle Benutzerkonten in iDRAC deaktiviert, bis der Bereitstellungsserver *ermittelt* wird.

So aktivieren Sie den Bereitstellungsserver über das iDRAC-Einstellungsdienstprogramm:

1 Schalten Sie das verwaltete System ein.
2 Drücken Sie während des POST die Taste F2, und wechseln Sie dann zu **iDRAC-Einstellungen** > **Remote-Aktivierung**.
Daraufhin wird die Seite **iDRAC-Einstellungen – Remote-Aktivierung** angezeigt.
3 Aktivieren Sie die Auto-Ermittlung, geben Sie die IP-Adresse für den Bereitstellungs-Server ein, und klicken Sie auf **Zurück**.

ANMERKUNG: Die Angabe der IP-Adresse für den Bereitstellungs-Server ist optional. Wenn Sie diese Adresse nicht angeben, wird sie über die DHCP- oder DNS-Einstellungen ermittelt (Schritt 7).

4 Klicken Sie auf **Netzwerk**.
Die Seite **iDRAC-Einstellungen Netzwerk** wird angezeigt.
5 NIC aktivieren
6 IPv4 aktivieren

ANMERKUNG: IPv6 wird im Rahmen der Auto-Ermittlung nicht unterstützt.

7 Aktivieren Sie DHCP, und rufen Sie den Domänennamen, die DNS-Server-Adresse und den DNS-Domänennamen von DHCP ab.

ANMERKUNG: Schritt 7 ist optional, wenn die IP-Adresse des Bereitstellungs-Servers in Schritt 3 angegeben wurde.

Konfigurieren von Servern und Serverkomponenten mithilfe der automatischen Konfiguration

Mit der Funktion „Auto Config“ (automatische Konfiguration) wird die Konfiguration und Bereitstellung aller Komponenten in einem Server in einem einzigen Arbeitsgang vorgenommen. Diese Komponenten umfassen BIOS, iDRAC und PERC. „Auto Config“ importiert automatisch eine XML-Datei eines Server-Konfigurationsprofils (SCP), die alle konfigurierbaren Parameter enthält. Der DHCP-Server, der die IP-Adresse zuweist, stellt gleichfalls die Details zum Zugriff auf die SCP-Datei bereit.

SCP-Dateien werden durch das Konfigurieren eines „Goldkonfigurations“-Servers erstellt. Diese Konfiguration wird dann zu einem freigegebenen CIFS- oder NFS-Netzwerkspeicherort exportiert, auf den über den DHCP-Server und den iDRAC des Servers, der konfiguriert wird, zugegriffen werden kann. Der SCP-Dateiname kann auf der Service-Tag- oder auf der Modellnummer des Zielservers basieren oder einen allgemeinen Namen erhalten. Der DHCP-Server verwendet eine DHCP-Serveroption, damit der SCP-Dateiname (optional), der SCP-Dateispeicherort und die Benutzeranmeldeinformationen zum Zugriff auf das Dateiverzeichnis angegeben werden können.

Wenn der iDRAC eine IP-Adresse vom DHCP-Server erhält, der für Auto Config konfiguriert wird, verwendet iDRAC das SCP, um die Geräte des Servers zu konfigurieren. Auto Config wird erst dann aufgerufen, wenn iDRAC seine IP-Adresse vom DHCP-Server erhält. Falls keine Antwort bzw. keine IP-Adresse vom DHCP-Server eingeht, wird Auto Config nicht aufgerufen.

ANMERKUNG:

- Sie können Auto Config nur dann aktivieren, wenn die Optionen **DHCPv4** und **IPv4 aktivieren** aktiviert sind.
- Die Funktionen „Auto Config“ (Automatisch konfigurieren) und „Auto Discovery“ (Automatische Ermittlung) schließen sich gegenseitig aus. Deaktivieren Sie die automatische Ermittlung, um eine fehlerfreie Funktion für automatisches Konfigurieren zu gewährleisten.
- „Auto Config“ wird deaktiviert, nachdem ein Server einen Autokonfigurationsvorgang durchgeführt hat. Weitere Informationen zum Aktivieren von Auto Config finden Sie unter Aktivieren der Automatischen Konfiguration mithilfe von RACADM.

Wenn alle Dell PowerEdge-Server im DHCP-Serverpool den gleichen Modelltyp und die gleiche Nummer aufweisen, ist eine einzige SCP-Datei (**config.xml**) erforderlich. **config.xml** ist der Standardname für die SCP-Datei.

Sie können einzelne Server konfigurieren. Hierfür benötigen Sie unterschiedliche Konfigurationsdateien, die über einzelne Service-Tag-Nummern der Server oder Servermodelle zugeordnet werden. In einer Umgebung mit verschiedenen Servern mit spezifischen Anforderungen können Sie verschiedene SCP-Dateinamen für die Unterscheidung der einzelnen Server oder Servertypen verwenden. Wenn beispielsweise zwei Servermodelle konfiguriert werden sollen – ein PowerEdge R730s und ein PowerEdge R530s, verwenden Sie zwei SCP-Dateien, **R730-config.xml** und **R530-config.xml**.

ANMERKUNG: Wenn auf Systemen mit iDRAC-Version 2.20.20.20 oder höher der Dateinamenparameter nicht in der DHCP-Option 60 vorhanden ist, erzeugt der Konfigurationsagent des iDRAC-Servers automatisch den Konfigurationsdateinamen mithilfe der Service-Tag-Nummer des Servers, der Modellnummer oder des Standarddateinamens config.xml.

Der iDRAC-Server-Konfigurationsagent wendet die Richtlinien in der folgenden Sequenz an, um zu bestimmen, welche SCP-Datei auf der Dateifreigabe für den jeweiligen iDRAC verwendet wird:

1 Dateiname angegeben in der DHCP-Option 60.

2 **<ServiceTag>-config.xml** – Wenn in der DHCP-Option 60 kein Dateiname angegeben ist, verwenden Sie die Service-Tag-Nummer des Systems zur eindeutigen Identifizierung der SCP-Datei für das System, beispielsweise **CDVH7R1-config.xml**

3 **<Model number>-config.xml** – Wenn der Option-60-Dateiname nicht angegeben ist und die Datei **<Service Tag>-config.xml** nicht gefunden werden kann, verwenden Sie die System-Modellnummer als Grundlage für den SCP-Dateinamen, beispielsweise **R520-config.xml**.

4 **config.xml** – Wenn die Dateien auf Grundlage von Option-60-Dateiname, Service-Tag-Nummer und Modellnummer nicht verfügbar sind, verwenden Sie die Standard-Datei **config.xml**.

ANMERKUNG: Wenn sich keine dieser Dateien auf der Netzwerkfreigabe befindet, ist der Importauftrag des Serverkonfigurationsprofils als fehlgeschlagen gekennzeichnet und die Datei kann nicht gefunden werden.

Zugehöriger Link

Automatische Konfigurationssequenz
DHCP-Optionen
Aktivieren der Automatischen Konfiguration mithilfe der iDRAC-Webschnittstelle
Aktivieren der Automatischen Konfiguration mithilfe von RACADM

Automatische Konfigurationssequenz

1 Erstellen oder ändern Sie die SCP-Datei, mit der die Attribute von Dell-Servern konfiguriert werden.

2 Speichern Sie die SCP-Datei an einem freigegebenen Speicherort, der für DHCP-Server und alle Dell-Server, denen IP-Adressen vom DHCP-Server zugewiesen werden, verfügbar ist.

3 Geben Sie die SCP-Datei im Feld „vendor-option 43“ des DHCP-Servers an.

4 iDRAC meldet die Anbieterklassen-Kennung im Zuge des Abrufens der IP-Adresse an iDRAC (Option 60).

5 Der DHCP-Server vergleicht die Anbieterklasse mit der Anbieteroption in der Datei **dhcpd.conf** und sendet, falls angegeben, den Speicherort und Namen der SCP-Datei an iDRAC.

6 iDRAC verarbeitet die SCP-Datei und konfiguriert alle in der Datei aufgeführten Attribute

DHCP-Optionen

DHCPv4 ermöglicht die Weiterreichung vieler global definierter Parameter an DHCP-Clients. Die einzelnen Parameter werden als DHCP-Optionen bezeichnet. Jede Option wird mit einer Options-Tag-Nummer identifiziert, die durch einen 1-Byte-Wert dargestellt wird. Die Options-Tags 0 und 255 sind jeweils für Auffüllen und Abschließen von Optionen reserviert. Alle anderen Werte stehen für die Definition von Optionen zur Verfügung.

Die DHCP-Option 43 wird zum Senden von Informationen vom DHCP-Server an den DHCP-Client verwendet. Diese Option ist als Textzeichenfolge definiert. Diese Textzeichenfolge enthält den Namen der XML-Datei, den Freigabe-Speicherort und die Anmeldedaten für den Zugriff auf den Freigabe-Speicherort. Beispiel:

```
Option „myname“, Code 43 = Text; Subnetz 192. 168.0.0 Netzmaske 255.255.255.0 { # Option Router für das Standardgateway192.168.0.1; Option Subnetzmaske 255.255.255.0; Option nis-domain „domain.org“; Option Domänenname „domain.org“; Option Domänenname-Server 192.168.1.1; Option Zeit-Offset-18000; #Eastern Standard Time; Option Anbieterklassenkennung „iDRAC“; Anbieter-Zeichenkette festlegen = Option Anbieterklassenkennung; Option myname „-f system_config.xml -i 192.168.0.130 -u user -p password -n cifs -s 2 -d 0 -t 500“;
```

wobei -i der Speicherort der Remote-Dateifreigabe und -f zusammen mit den Anmeldeinformationen der Dateiname in der Zeichenkette für die Remote-Dateifreigabe ist.

Die DHCP-Option 60 dient der Identifizierung und Zuordnung eines DHCP-Clients zu einem bestimmten Anbieter. Für alle DHCP-Server, die Maßnahmen basierend auf einer Client-Anbieter-ID durchführen sollen, müssen die Optionen 60 und 43 konfiguriert sein. Bei Dell PowerEdge-Servern identifiziert iDRAC sich selbst mit der Hersteller-ID: *iDRAC*. Aus diesem Grund müssen Sie eine neue Anbieterklasse (Vendor Class) hinzufügen und für diese eine Bereichsoption (Scope Option) für „Code 60“ erstellen und diese Bereichsoption anschließend für den DHCP-Server aktivieren.

Zugehöriger Link

Konfigurieren der Option 43 unter Windows
Konfigurieren der Option 60 unter Windows
Konfigurieren der Optionen 43 und 60 auf Linux

Konfigurieren der Option 43 unter Windows

So konfigurieren Sie die Option 43 unter Windows:

1. Gehen Sie auf dem DHCP-Server auf **Start** > **Administrationstools** > **DHCP**, um die DHCP-Serveradministrationstools zu öffnen.
2. Gehen Sie auf den Server, und erweitern Sie alle Servereinträge.
3. Klicken Sie mit der rechten Maustaste auf **Bereichsoptionen** und wählen Sie **Optionen konfigurieren** aus.

   Daraufhin wird das Dialogfeld **Bereichsoptionen** angezeigt.
4. Führen Sie einen Bildlauf nach unten durch, und wählen Sie **043 Anbieterspezifische Informationen** aus.
5. Klicken Sie im Feld **Dateneintrag** auf eine beliebige Stelle im Bereich **ASCII**, und geben Sie die IP-Adresse des Servers mit dem freigegebenen Speicherort an, an dem sich die XML-Konfigurationsdatei befindet.

   Der Wert wird während der Eingabe sowohl unter **ASCII** angezeigt, als auch im Binärcode auf der linken Seite.
6. Klicken Sie auf **OK**, um die Konfiguration zu speichern.

Konfigurieren der Option 60 unter Windows

So konfigurieren Sie die Option 60 unter Windows:

1. Gehen Sie auf dem DHCP-Server auf **Start** > **Administrationstools** > **DHCP**, um die DHCP-Serveradministrationstools zu öffnen.
2. Gehen Sie auf den Server, und erweitern Sie die Servereinträge.
3. Klicken Sie mit der rechten Maustaste auf **IPv4**, und wählen Sie **Anbieter-Klassen definieren** aus.
4. Klicken Sie auf **Hinzufügen**.

Es wird ein Dialogfeld mit den folgenden Feldern angezeigt:

- **Anzeigename:**
- **Beschreibung:**
- **ID: Binär: ASCII:**

5 Geben Sie im Feld **Anzeigename:** `iDRAC` ein.

6 Geben Sie im Feld **Beschreibung:** `Anbieterklasse` ein.

7 Klicken Sie in den Abschnitt **ASCII:**, und geben Sie `iDRAC` ein.

8 Klicken Sie auf **OK** und anschließend auf **Schließen**.

9 Klicken Sie im DHCP-Fenster mit der rechten Maustaste auf **IPv4**, und wählen Sie **Vordefinierte Optionen festlegen** aus.

10 Wählen Sie aus dem Dropdown-Menü **Optionsklasse** die (in Schritt 4 erstellte) Option **iDRAC** aus, und klicken Sie auf **Hinzufügen**.

11 Geben Sie im Dialogfeld **Optionstyp** die folgenden Informationen ein:

- **Name** – `iDRAC`
- **Datentyp** – Zeichenfolge
- **Code** – 060
- **Beschreibung** – Dell Anbieterklassen-Kennung

12 Klicken Sie auf **OK**, um zum Fenster **DHCP** zurückzukehren.

13 Erweitern Sie alle Einträge unter dem Servernamen, klicken Sie mit der rechten Maustaste auf **Bereichsoptionen**, und wählen Sie **Optionen konfigurieren** aus.

14 Klicken Sie auf die Registerkarte **Erweitert**.

15 Wählen Sie aus dem Dropdown-Menü **Anbieterklasse** die Option **iDRAC** aus. Es wird `060 iDRAC` in der Spalte **Verfügbare Optionen** angezeigt.

16 Wählen Sie die Option **060 iDRAC** aus.

17 Geben Sie die Zeichenfolge ein, die (zusammen mit einer Standard-DHCP-IP-Adresse) an iDRAC gesendet werden muss. Die Zeichenfolge ermöglicht den Import der richtigen SCP-Datei.

Verwenden Sie für die Option **DATEN-Eintrag, Zeichenfolge-Wert** einen Text-Parameter mit den folgenden Buchstaben-Optionen und Werten:

- Dateiname (-f) Gibt den Namen der exportierten XML-Datei des Konfigurationsprofils des Servers an. Die Angabe dieses Dateinamens ist bei der iDRAC-Version 2.20.20.20 oder höher optional.

  ANMERKUNG: Weitere Informationen zu den Richtlinien von Dateinamen finden Sie unter Konfigurieren von Servern und Serverkomponenten mithilfe der automatischen Konfiguration.

- Freigabename (-n) – Gibt den Namen der Netzwerkfreigabe an.
- FreigabeTyp (-s) – Gibt den Freigabetyp an. 0 steht für NFS und 2 für CIFS.
- IPAdresse (-i) – Gibt die IP-Adresse der Dateifreigabe an.

  ANMERKUNG: Freigabename (-n), FreigabeTyp (-s) und IPAdresse (-i) sind erforderliche Attribute, die weitergereicht werden müssen.

- Benutzername (-u) – Gibt den Benutzernamen für den Zugriff auf die Netzwerkfreigabe an. Diese Informationen sind nur für CIFS erforderlich.
- Kennwort (-p) – Gibt das Kennwort für den Zugriff auf die Netzwerkfreigabe an. Diese Informationen sind nur für CIFS erforderlich.
- Typ für das Herunterfahren (-d) – Gibt den Modus für das Herunterfahren an. 0 steht für „Ordnungsgemäßes Herunterfahren“ und 1 für „Erzwungenes Herunterfahren“.

  ANMERKUNG: Die Standardeinstellung ist 0.

- Wartezeit (-t) – Gibt die Zeitspanne an, die das Host-System vor dem Herunterfahren wartet. Die Standardeinstellung liegt bei 300.
- Energiezustand des End-Hosts (-e) – Gibt den Betriebszustand des Hosts an. 0 steht für AUS und 1 für AN. Die Standardeinstellung ist 1.

  ANMERKUNG: Der Typ für das Herunterfahren (-d), die Wartezeit (-t) und der Energiezustand des End-Hosts (-e) sind optionale Attribute.

ANMERKUNG: Stellen Sie auf DHCP-Servern, auf denen Windows mit dem Betriebssystem mit iDRAC-Version vor 2.20.20.20 ausgeführt wird, sicher, dass Sie ein Leerzeichen vor (-f) setzen.

NFS: -f system_config.xml -i 192.168.1.101 -n /nfs_share -s 0 -d 1

CIFS: -f system_config.xml -i 192.168.1.101 -n cifs_share -s 2 -u <*BENUTZERNAME*> -p <*KENNWORT*> -d 1 -t 400

Konfigurieren der Optionen 43 und 60 auf Linux

Aktualisieren Sie die Datei **/etc/dhcpd.conf**. Die Schritte zur Konfiguration der Optionen ähneln den Schritten bei Windows:

1 Reservieren Sie einen Block oder Pool von Adressen, die von diesem DHCP-Server zugewiesen werden können.

2 Stellen Sie die Option 43 ein und verwenden Sie die Anbieterklassenkennung für Option 60.

```
Option „myname", Code 43 = Text; Subnetz 192.168.0.0 Netzmaske 255.255.0.0 { # Option Router
für das Standardgateway    192.168.0.1; Option Subnetzmaske    255.255.255.0; Option nis-
domain    „domain.org"; Option Domänenname    „domain.org"; Option Domänenname-Server
192.168.1.1; Option Zeit-Offset    -18000;    # Eastern Standard Time  Option
Anbieterklassenkennung „iDRAC"; Anbieter-Zeichenkette festlegen = Option
Anbieterklassenkennung; Option myname „-f system_config.xml -i 192.168.0.130 -u user -p
password -n cifs -s 2 -d 0 -t 500"; Bereich dynamisches Startprotokoll 192.168.0.128
192.168.0.254; Standard-Lease-Zeit 21600; Maximale Lease-Zeit 43200; } }
```

Im Folgenden sind die erforderlichen und optionalen Parameter angegeben, die in der Zeichenkette der Anbieterklassenkennung weitergereicht werden müssen:

- Dateiname (-f) Gibt den Namen der exportierten XML-Datei des Konfigurationsprofils des Servers an. Die Angabe des Dateinamens ist bei der iDRAC-Version 2.20.20.20 oder höher optional.

  ANMERKUNG: Weitere Informationen zu den Richtlinien von Dateinamen finden Sie unter Konfigurieren von Servern und Serverkomponenten mithilfe der automatischen Konfiguration.

- Freigabename (-n) – Gibt den Namen der Netzwerkfreigabe an.
- FreigabeTyp (-s) – Gibt den Freigabetyp an. 0 steht für NFS und 2 für CIFS.
- IPAdresse (-i) – Gibt die IP-Adresse der Dateifreigabe an.

  ANMERKUNG: Freigabename (-n), FreigabeTyp (-s) und IPAdresse (-i) sind erforderliche Attribute, die weitergereicht werden müssen.

- Benutzername (-u) – Gibt den Benutzernamen für den Zugriff auf die Netzwerkfreigabe an. Diese Informationen sind nur für CIFS erforderlich.
- Kennwort (-p) – Gibt das Kennwort für den Zugriff auf die Netzwerkfreigabe an. Diese Informationen sind nur für CIFS erforderlich.

  ANMERKUNG: Beispiel für die Freigabe bei Linux NFS und CIFS:
  - **NFS:** -f system_config.xml -i 192.168.0.130 -n /nfs -s 0 -d 0 -t 500
  - **CIFS:** -f system_config.xml -i 192.168.0.130 -n sambashare/config_files -s 2 -u user -p password -d 1 -t 400

  Stellen Sie sicher, dass Sie NFS2 oder NFS3 für die NFS-Netzwerkfreigabe verwenden.

- Typ für das Herunterfahren (-d) – Gibt den Modus für das Herunterfahren an. 0 steht für „Ordnungsgemäßes Herunterfahren" und 1 für „Erzwungenes Herunterfahren".

  ANMERKUNG: Die Standardeinstellung ist 0.

- Wartezeit (-t) – Gibt die Zeitspanne an, die das Host-System vor dem Herunterfahren wartet. Die Standardeinstellung liegt bei 300.
- Energiezustand des End-Hosts (-e) – Gibt den Betriebszustand des Hosts an. 0 steht für AUS und 1 für AN. Die Standardeinstellung ist 1.

  ANMERKUNG: Der Typ für das Herunterfahren (-d), die Wartezeit (-t) und der Energiezustand des End-Hosts (-e) sind optionale Attribute.

Es folgt ein Beispiel für eine statische DHCP-Reservierung von einer dhcpd.conf-Datei:

```
Host my_host {

Hardware Ethernet b8:2a:72:fb:e6:56;

 Feste-Adresse 192.168.0.211;

Option Host-Name „my_host“;

Option myname „ -f r630_raid.xml -i 192.168.0.1 -n /nfs -s 0 -d 0 -t 300“;

}
```

ANMERKUNG: Stellen Sie nach dem Bearbeiten der dhcpd.conf-Datei sicher, dass Sie den dhcpd-Service neu starten, um die Änderungen zu übernehmen.

Voraussetzungen vor dem Aktivieren von Auto Config

Stellen Sie vor der Aktivierung der Funktion Auto Config sicher, dass folgende Voraussetzungen bereits gegeben sind:

- Die unterstützte Netzwerkfreigabe (NFS oder CIFS) steht auf dem gleichen Subnetz wie der iDRAC- und der DHCP-Server zur Verfügung. Testen Sie die Netzwerkfreigabe, um sicherzustellen, dass darauf zugegriffen werden kann und dass die Firewall und die Benutzerberechtigungen korrekt eingerichtet wurden.
- Das Serverkonfigurationsprofil wird an die Netzwerkfreigabe exportiert. Stellen Sie außerdem sicher, dass die notwendigen Änderungen in der XML-Datei abgeschlossen sind, sodass die ordnungsgemäßen Einstellungen zur Anwendung kommen können, sobald der Autokonfigurationsvorgang initiiert wird.
- Der DHCP-Server ist eingerichtet und die DHCP-Konfiguration wird nach Bedarf für iDRAC aktualisiert, um den Server aufzurufen und die Funktion Auto Config zu initiieren.

Aktivieren der Automatischen Konfiguration mithilfe der iDRAC-Webschnittstelle

Stellen Sie sicher, dass DHCPv4 und die IPv4-Aktivierungsoptionen aktiviert und die automatische Erkennung deaktiviert ist.

So aktivieren Sie Auto Config:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk**.

Die Seite **Netzwerk** wird angezeigt.

2 Wählen Sie im Abschnitt **Auto Config** eine der folgenden Optionen aus dem Drop-Down-Menü **DHCP-Bereitstellung aktivieren** aus:

- **Einmal aktivieren** – Konfiguriert die Komponente mit einmaliger Verwendung der XML-Datei, auf die der DHCP-Server verweist. Danach wird Auto Config deaktiviert.
- **Einmal nach Reset aktivieren** – Konfiguriert nach dem iDRAC-Reset die Komponente mit einmaliger Verwendung der XML-Datei, auf die der DHCP-Server verweist. Danach wird Auto Config deaktiviert.
- **Deaktivieren** – Deaktiviert die Funktion „Auto Config“.

3 Klicken Sie auf **Anwenden,** um die Einstellung zu übernehmen.

Die Seite „Netzwerk“ wird automatisch aktualisiert.

Aktivieren der Automatischen Konfiguration mithilfe von RACADM

Verwenden Sie das Objekt `iDRAC.NIC.AutoConfig`, um die Funktion des automatischen Konfigurierens (Auto Config) unter Verwendung von RACADM zu aktivieren.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Weitere Informationen über die Funktion Auto Config finden Sie im Whitepaper *Zero-Touch Bare Metal Server Provisioning using Dell iDRAC with Lifecycle Controller Auto Config (Zero-Touch für die Bereitstellung des Bare Metal-Servers unter Verwendung von Dell iDRAC mit Lifecycle Controller Auto Config)* unter **delltechcenter.com/idrac**.

Verwenden von Hash-Kennwörtern für mehr Sicherheit

Sie können Benutzerkennwörter und BIOS-Kennwörter im Einweg-Hash-Format festlegen. Der Benutzerauthentifizierungsmechanismus ist nicht betroffen (mit Ausnahme von SNMPv3 und IPMI) und Sie können das Kennwort im Nur-Text-Format angeben.

Mit der neuen Kennwort-Hash-Funktion:

- Können Sie Ihre eigenen SHA256-Hashes erstellen, um die Kennwörter für iDRAC-Benutzer und BIOS-Kennwörter zu generieren. Damit können Sie die SHA256-Werte im Serverkonfigurations-, RACADM- und WSMAN-Profil hinterlegen. Wenn Sie die Kennwortwerte für SHA256 bereitstellen, ist eine Authentifizierung über SNMPv3 und IPMI nicht möglich.
- Sie können einen Vorlagenserver einschließlich aller iDRAC-Benutzerkonten und BIOS-Kennwörter unter Verwendung des derzeitigen Nur-Text-Mechanismus einrichten. Wenn der Server eingerichtet ist, können Sie das Serverkonfigurationsprofil mit den Kennwort-Hashwerten exportieren. Der Export umfasst die erforderlichen Hashwerte für die SNMPv3-Authentifizierung. Der Import dieses Profils führt zum Verlust der IPMI-Authentifizierung derjenigen Benutzer, für die Hash-Kennwortwerte festgelegt sind. In der F2-IDRAC-Schnittstelle wird angezeigt, dass das Benutzerkonto deaktiviert ist.
- Die anderen Schnittstellen, z. B. die IDRAC-GUI, zeigen die Benutzerkonten als aktiviert an.

ANMERKUNG: Wenn beim Herunterstufen eines Dell PowerEdge Servers der zwölften Generation von Version 2.xx.xx.xx auf1.xx.xx für den Server die Hash-Authentifizierung eingestellt wurde, können Sie sich an keiner Schnittstelle anmelden, wenn das Kennwort nicht auf die Standardeinstellung eingestellt wird.

Können Sie das Hash-Kennwort mit und ohne Salt über SHA256 generieren.

Sie müssen über eine Berechtigung zur Serversteuerung verfügen, um Hash-Kennwörter einschließen und exportieren zu können.

Wenn der Zugriff auf alle Konten verloren gegangen ist, verwenden Sie das Dienstprogramm für die iDRAC-Einstellungen oder den lokalen RACADM, und setzen Sie iDRAC auf den Standard-Task zurück.

Wenn das Kennwort für das iDRAC-Benutzerkonto nur mit dem SHA256-Kennwort-Hash und keinen anderen Hashes (SHA1v3Key oder MD5v3Key) festgelegt wurde, ist die Authentifizierung über SNMP v3 nicht verfügbar.

Hash-Kennwort unter Verwendung von RACADM

Um Hash-Kennwörter einzurichten, verwenden Sie die folgenden Objekte mit dem Befehl **set**:

- iDRAC.Users.SHA256Password
- iDRAC.Users.SHA256PasswordSalt

Verwenden Sie den folgenden Befehl, um das Hash-Kennwort im exportierten Server-Profil einzuschließen:

```
racadm get -f <file name> -l <NFS / CIFS share> -u <username> -p <password>  -t <filetype> --
includePH
```

Sie müssen das Salt-Attribut festlegen, wenn der zugeordnete Hash eingestellt wird.

ANMERKUNG: Die Attribute sind nicht für die INI-Konfigurationsdatei anwendbar.

Hash-Kennwort in Server-Konfigurationsprofil

Die neuen Hash-Kennwörter können optional in das Server-Konfigurationsprofil exportiert werden.

Beim Importieren von Server-Konfigurationsprofilen können Sie die Kommentierung des vorhandenen Kennwort-Attributs oder des neuen Kennwort-Hash-Attributs aufheben. Wenn die Kommentierung von beiden aufgehoben ist, wird ein Fehler generiert und das Kennwort wird nicht eingestellt. Eine kommentiertes Attribut wird während eines Imports nicht angewendet.

Hash-Kennwort ohne SNMPv3- und IPMI-Authentifizierung erstellen

Gehen Sie folgendermaßen vor, um das Hash-Kennwort ohne SNMPv3- und IPMI-Authentifizierung zu erstellen:

1 Bei iDRAC-Benutzerkonten müssen Sie das Kennwort mithilfe von Salt über SHA256 generieren.

Wenn Sie das Kennwort mithilfe von Salt generieren, wird eine 16-Byte-Zeichenfolge angehängt. Salt ist 16 Byte lang, falls bereitgestellt.

2 Stellen Sie den Hash-Wert und Salt im importierten Serverkonfigurationsprofil, in den RACADM-Befehlen oder in WS-MAN bereit.

3 Nach dem Festlegen des Kennworts funktioniert die normale Nur-Text-Kennwortauthentifizierung mit der Ausnahme, dass die Authentifizierung von SNMP v3 und IPMI für iDRAC-Benutzerkonten fehlschlägt, bei denen die Kennwörter mit Hash aktualisiert wurden.

Management Station einrichten

Eine Management Station ist ein Computer, der für den Zugriff auf iDRAC-Schnittstellen zur Remote-Überwachung und -Verwaltung von PowerEdge-Servern verwendet wird.

So richten Sie die Management Station ein.

1 Installieren Sie ein unterstütztes Betriebssystem. Weitere Informationen finden Sie in den Versionshinweisen.

2 Installieren und konfigurieren Sie einen unterstützten Webbrowser (Internet Explorer, Firefox, Chrome oder Safari).

3 Installieren Sie die aktuelle Java Runtime Environment (JRE) (erforderlich, wenn der Java-Plugin-Typ für den Zugriff auf iDRAC über einen Web-Browser verwendet wird).

4 Installieren Sie aus dem SYSMGMT-Ordner der *Dell Systems Management Tools and Documentation*-DVD die Komponenten „Remote-RACADM“ und „VMCLI“. Rufen Sie alternativ die **Setup**-Datei auf der DVD auf, um Remote-RACADM und weitere OpenManage-Software standardmäßig zu installieren. Weitere Informationen zu RACADM finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* unter **dell.com/idracmanuals.**.

5 Installieren Sie nach Bedarf auch die folgenden Komponenten:

- Telnet
- SSH-Client
- TFTP
- Dell OpenManage Essentials

Zugehöriger Link

VMCLI-Dienstprogramm installieren und verwenden

Konfigurieren von unterstützten Webbrowsern

Per Remote auf iDRAC zugreifen

Für den Remote-Zugriff auf die iDRAC-Webschnittstelle über eine Management Station müssen Sie sicherstellen, dass sich die Management Station auf dem gleichen Netzwerk wie iDRAC befindet. Beispiel:

- Blade-Server – Die Management Station muss sich auf dem gleichen Netzwerk wie CMC befinden. Weitere Informationen zum Isolieren des CMC-Netzwerks vom Netzwerk des Managed System finden Sie im *Chassis Management Controller User's Guide* (Chassis Management Controller-Benutzerhandbuch) unter **dell.com/support/manuals**.
- Rack- und Tower-Server – Definieren Sie iDRAC NIC-Schnittstelle auf „Dediziert“ oder LOM1, und stellen Sie sicher, dass sich die Management Station auf dem gleichen Netzwerk wie iDRAC befindet.

Verwenden Sie für den Zugriff auf die Managed System-Konsole über eine Management Station die virtuelle Konsole über die iDRAC-Webschnittstelle.

Zugehöriger Link

Virtuelle Konsole starten

Netzwerkeinstellungen

Managed System einrichten

Wenn Sie das lokale RACADM ausführen oder die Erfassung von „Bildschirm Letzter Absturz“ aktivieren möchten, installieren Sie die folgenden Komponenten von der *Dell Systems Management Tools and Documentation*-DVD:

- Lokaler RACADM
- Server Administrator

Weitere Informationen zum Server Administrator finden Sie im *Dell OpenManage* Server Administrator User's Guide (Dell OpenManage Server Administrator-Benutzerhandbuch) unter **dell.com/support/manuals**.

Zugehöriger Link

Einstellungen für lokales Administratorkonto ändern

Einstellungen für lokales Administratorkonto ändern

Nachdem Sie die iDRAC-IP-Adresse festgelegt haben, können Sie die Einstellungen für das lokale Administratorkonto (hier Benutzer 2) über das Dienstprogramm für die iDRAC-Einstellungen ändern. Gehen Sie dazu wie folgt vor:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Benutzerkonfiguration**.
Daraufhin wird die Seite **iDRAC-Einstellungen – Benutzerkonfiguration** angezeigt.

2 Geben Sie die Details für den **Benutzernamen**, die **LAN-Benutzerberechtigungen**, die **Benutzerberechtigungen für die seriellen Schnittstellen** und das **Kennwort** an.
Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
Mit diesem Schritt sind die Einstellungen für das lokale Administratorkonto konfiguriert.

Standort für das Managed System einrichten

Sie können die Standortdetails des Managed System im Rechenzentrum über die iDRAC-Webschnittstelle oder das Dienstprogramm für die iDRAC-Einstellungen festlegen.

Standort des Managed System über die Web-Schnittstelle einrichten

So legen Sie die Details für den Systemstandort fest:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Eigenschaften** > **Details**.
Die Seite **Systemdetails** wird angezeigt.

2 Geben Sie unter **Systemstandort** die Standortdetails für das Managed System im Rechenzentrum ein.
Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

3 Klicken Sie auf **Anwenden**. Daraufhin werden die Details zum Systemstandort in iDRAC gespeichert.

Standort für Managed System über RACADM einrichten

Um die Details für den Systemstandort anzugeben, verwenden Sie die Gruppenobjekte `System.Location`.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Standort für Managed System über das Dienstprogramm für die iDRAC-Einstellungen einrichten

So legen Sie die Details für den Systemstandort fest:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Systemstandort**.

Daraufhin wird die Seite **iDRAC-Einstellungen – Systemstandort** angezeigt.

2 Geben Sie die Standortdetails des Managed System im Rechenzentrum ein. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Details werden gespeichert.

Systemleistung und Stromverbrauch optimieren

Der Strom, der zur Kühlung eines Servers erforderlich ist, kann einen Großteil des Gesamtstrombedarfs eines Systems ausmachen. Unter thermischer Steuerung versteht man die aktive Verwaltung der Systemkühlung durch Steuerung der Lüfterdrehzahl und des Systemstroms, mit dem Ziel, ein zuverlässiges System bereitzustellen und gleichzeitig dessen Stromverbrauch, Luftstrom und Geräuschentwicklung zu minimieren. Sie können die Einstellungen für die thermische Steuerung anpassen und optimieren, um den Anforderungen an die Systemleistung und an die Leistung pro Watt zu entsprechen.

Unter Verwendung der iDRAC-Web-Schnittstelle, über RACADM oder über das Dienstprogramm für die iDRAC-Einstellungen können Sie die folgenden Einstellungen für die Kühlung ändern:

- Optimierung für bessere Leistung
- Optimierung für minimalen Stromverbrauch
- Einstellen der maximalen Luftauslasstemperatur
- Erhöhen des Luftstroms durch Lüfter-Offset, falls erforderlich
- Erhöhen des Luftstroms durch die minimale Lüftergeschwindigkeit

Thermische Einstellungen über die iDRAC-Webschnittstelle ändern

So ändern Sie die Standardeinstellungen:

1 Gehen Sie in der iDRAC-Webschnittstelle auf **Übersicht** > **Hardware** > **Lüfter** > **Setup**.

Die Seite **Lüfter-Setup** wird angezeigt.

2 Geben Sie folgendes an:

- **Thermisches Profil** – Wählen Sie das thermische Profil:
  - **Standard thermische Profileinstellungen** – Bedeutet, dass der thermische Algorithmus dieselben Systemprofileinstellungen verwendet, die unter der Seite **System-BIOS** > **System-BIOS-Einstellungen.Systemprofileinstellungen** definiert sind.

  Standardmäßig ist dies auf **Standardmäßige Temperaturprofileinstellungen** gesetzt. Sie können auch einen benutzerdefinierten Algorithmus auswählen, der unabhängig vom BIOS-Profil ist. Die verfügbaren Optionen sind:

- **Maximale Leistung (Leistung wird optimiert)** :
  - Geringere Wahrscheinlichkeit von Speicher- oder CPU-Drosselung.
  - Höhere Wahrscheinlichkeit der Turbo-Modus-Aktivierung.
  - Im Allgemeinen höhere Lüftergeschwindigkeiten im Leerlauf und bei Spannungsladungen.
- **Minimalstrom (optimierte Leistung pro Watt)**:
  - Optimiert für geringsten Energieverbrauch des Systems basierend auf optimalem Status des Lüfters
  - Im Allgemeinen niedrigere Lüftergeschwindigkeiten im Leerlauf und bei Spannungsladungen.

> **ANMERKUNG: Die Auswahl von Maximale Leistung oder Minimalstrom setzt die thermischen Einstellungen im Zusammenhang mit der Systemprofileinstellung auf der Seite System-BIOS > System-BIOS-Einstellungenen.Systemprofileinstellungen außer Kraft.**

- **Maximaler Ablufttemperatur-Grenzwert** – Wählen Sie im Dropdown-Menü die maximale Ablufttemperatur aus. Die Werte werden basierend auf dem System angezeigt.

  Der Standardwert ist **Standard, 70 °C (158 °F)**.

  Mit dieser Option können die Lüftergeschwindigkeiten des Systems so geändert werden, dass die Ablufttemperatur die ausgewählte Ablufttemperaturlimite nicht überschreitet. Dies kann nicht immer unter allen Systembetriebsbedingungen garantiert werden, und zwar wegen der Abhängigkeit von der Systemlade- und -kühlungsfähigkeit.
- **Offset für Lüftergeschwindigkeit** – Wenn Sie diese Option aktivieren, können Sie dem Server zusätzliche Kühlung zukommen lassen. Im Falle von hinzugefügter Hardware (z.B. neue PCIe-Karten) wird evtl. zusätzliche Kühlung benötigt. Ein Lüftergeschwindigkeits-Offset führt zur Erhöhung der Lüftergeschwindigkeiten (um den prozentualen Offset-Wert) über die Baseline-Lüftergeschwindigkeit, die mithilfe des Algorithmus für die thermische Steuerung berechnet wird. Mögliche Werte sind:
  - **Niedrige Lüftergeschwindigkeit** – Bewirkt eine moderate Lüftergeschwindigkeit.
  - **Mittlere Lüftergeschwindigkeit** – Bewirkt eine mittelschnelle Lüftergeschwindigkeit.
  - **Hohe Lüftergeschwindigkeit** – Bewirkt eine nahezu maximale Lüfterdrehzahl.
  - **Maximale Lüftergeschwindigkeit** – Bewirkt volle Lüftergeschwindigkeit.
  - **Aus** – Offset für Lüftergeschwindigkeit ist auf „Aus“ eingestellt. Dies ist der Standardwert. Wenn die Option ausgeschaltet ist, wird der Prozentsatz nicht angezeigt. Die Standard-Lüftergeschwindigkeit wird ohne Offset angewendet. Im Gegensatz dazu führt die maximale Einstellung dazu, dass alle Lüfter mit maximaler Geschwindigkeit ausgeführt werden.

  Der Lüftergeschwindigkeits-Offset ist dynamisch und basiert auf dem System. Die Lüftergeschwindigkeitserhöhung für jeden Offset wird neben jeder Option angezeigt.

  Der Lüftergeschwindigkeits-Offset erhöht die Lüftergeschwindigkeiten um denselben Prozentsatz. Die Lüftergeschwindigkeiten werden evtl. über die Offset-Geschwindigkeiten hinaus erhöht, basierend auf dem Kühlungsbedarf der einzelnen Komponenten. Der gesamte Energieverbrauch des Systems wird wahrscheinlich erhöht.

  Der Lüftergeschwindigkeit-Offset ermöglicht es Ihnen, die Lüftergeschwindigkeit des Systems mit vier Schritten zu erhöhen. Diese Schritte sind gleichmäßig zwischen der Standard-Baseline-Geschwindigkeit und der maximalen Übertragungsrate des Serversystemlüfters verteilt. Einige Hardwarekonfigurationen führen zu höheren Baseline-Lüftergeschwindigkeiten, was in einem anderen Offset als dem maximalen resultiert, um eine maximale Geschwindigkeit zu erreichen.

  Das häufigste Verwendungsszenario ist die nicht-standardmäßige PCIe-Adapterkühlung. Die Funktion kann jedoch verwendet werden, die Systemkühlung für andere Zwecke innerhalb des Systems zu verbessern.
- **Mindestlüftergeschwindigkeit in PWM (% vom Höchstwert)** – Wählen Sie diese Option zur Feinabstimmung der Lüftergeschwindigkeit aus. Mit dieser Option können Sie eine höhere Basissystemlüftergeschwindigkeit festlegen oder die Geschwindigkeit des Systemlüfters erhöhen, wenn andere benutzerdefinierte Lüftergeschwindigkeitsoptionen nicht zu den erforderlichen höheren Lüftergeschwindigkeiten führen.
  - **Standardeinstellung** – Legt die Mindestlüftergeschwindigkeit auf den Standardwert fest, der durch den Systemkühlungsalgorithmus bestimmt wird.
  - **Benutzerdefiniert** – Geben Sie den Prozentwert ein.

  Der zulässige Bereich für den Mindestlüftergeschwindigkeits-PWM ist dynamisch und basiert auf der Systemkonfiguration. Der erste Wert ist die Leerlaufgeschwindigkeit, und der zweite Wert ist die Maximalkonfiguration (die je nach Systemkonfiguration 100 % betragen kann).

Die Systemlüfter können gemäß den Temperaturanforderungen des Systems bei einer höhreren Geschwindigkeiten als dieser Geschwindigkeit laufen, jedoch nicht unterhalb der definierten Mindestgeschwindigkeit. Beispiel: Wenn Sie eine Mindestlüftergeschwindigkeit von 35 % festlegen, unterschreitet die Lüftergeschwindigkeit niemals den Wert von 35 % des PWM.

ANMERKUNG: Ein Wert von 0 % des PWM ist kein Anzeichen dafür, dass der Lüfter ausgeschaltet ist. Dies ist die niedrigste Geschwindigkeit des Lüfters, bei der der Lüfter betrieben werden kann.

Die Einstellungen sind dauerhaft, d. h., sobald diese festgelegt und angewendet wurden, werden sie während eines Systemneustarts, beim Aus- und Einschalten oder bei iDRAC- oder BIOS-Aktualisierungen nicht mehr automatisch in die Standardeinstellung geändert. Einige Dell-Server unterstützen möglicherweise einige oder alle dieser benutzerdefinierten Kühlungsoptionen nicht. Wenn die Optionen nicht unterstützt werden, werden sie nicht angezeigt, oder Sie können keinen benutzerdefinierten Wert festlegen.

3 Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

Die folgende Meldung wird angezeigt:

```
It is recommended to reboot the system when a thermal profile change has been made. This is to ensure all power and thermal settings are activated.
```

Klicken Sie auf **Jetzt neu starten** oder **Später neu starten**.

ANMERKUNG: Führen Sie einen Neustart des Systems durch, damit die Aktualisierung wirksam wird.

Thermische Einstellungen unter Verwendung von RACADM ändern

Verwenden Sie zum Ändern der thermischen Einstellungen die Objekte in der Gruppe **system.thermalsettings** mit dem untergeordneten Befehl **set**, wie in der folgenden Tabelle aufgeführt.

Tabelle 9. Temperatureinstellungen

Objekt	Beschreibung	Verwendung	Beispiel

`AirExhaustTemp`	Ermöglicht das Festlegen der maximalen Luftauslasstemperaturgrenze.	Legen Sie die Eigenschaft auf einen der folgenden Werte fest (basierend auf dem System):
		· 0 – Zeigt 40 °C an
		· 1 – Zeigt 45 °C an
		· 2 – Zeigt 50 °C an
		· 3 – Zeigt 55 °C an
		· 4 – Zeigt 60 °C an
		· 255 – Zeigt 70 °C an (Standard)
			So prüfen Sie die vorhandenen Einstellungen auf dem System:
			`racadm get system.thermalsettings.AirExhaustTemp`
			Das Ergebnis ist Folgendes:
			`AirExhaustTemp=70`
			Diese Ausgabe zeigt an, dass das System auf die Luftauslasstemperatur vion 70°C eingestellt ist.
			So stellen Sie den Auslasstemperatur-Grenzwert auf 60 °C ein:
			`racadm set system.thermalsettings.AirExhaustTemp 4`
			Das Ergebnis ist Folgendes:
			`Object value modified successfully.`
			Wenn ein System einen bestimmten Luftauslasstemperatur-Grenzwert nicht unterstützt,

Objekt	Beschreibung	Verwendung	Beispiel

			führen Sie den folgenden Befehl aus:
			`racadm set system.thermalsettings.AirExhaustTemp 0`
			Die folgende Fehlermeldung wird angezeigt:
			`ERROR: RAC947: Invalid object value specified.`
			Stellen Sie sicher, dass Sie den Wert abhängig vom Objekttyp angeben.
			Weitere Informationen dazu finden Sie in der RACADM-Hilfe.
			So legen Sie die Grenze auf den Standardwert zurück:
			`racadm set system.thermalsettings.AirExhaustTemp 255`

`FanSpeedHighOffsetVal`	• Diese Variable liest den Lüftergeschwindigkeit-Offset-Wert in %PWM für die Einstellung „Offset für hohe Lüftergeschwindigkeit“.
	• Dieser Wert richtet sich nach dem System.
	• Verwenden Sie das Objekt `FanSpeedOffset`, um diesen Wert unter Verwendung von Index-Wert 1 festzulegen.
		Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedHighOffsetVal`
			Ein numerischer Wert, zum Beispiel 66, wird ausgegeben. Dieser Wert bedeutet, dass, wenn Sie den folgenden Befehl verwenden, ein Offset für Lüftergeschwindigkeit von „Hoch“ (66% PWM) über die Drehzahl der Basislinie angewendet wird
			`racadm set system.thermalsettings FanSpeedOffset 1`

`FanSpeedLowOffsetVal`	• Diese Variable liest den Lüftergeschwindigkeit-Offset-Wert in %PWM für die Einstellung „Offset für niedrige Lüftergeschwindigkeit“.
	• Dieser Wert richtet sich nach dem System.
	• Verwenden Sie das Objekt `FanSpeedOffset`, um diesen Wert unter Verwendung von Index-Wert 0 festzulegen.
		Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedLowOffsetVal`
			Dies gibt einen Wert wie „23“ zurück. Das bedeutet, dass, wenn Sie den folgenden Befehl verwenden, ein Offset für Lüftergeschwindigkeit auf niedrig (23% PWM) über die Drehzahl der Basislinie angewendet wird.
			`racadm set system.thermalsettings FanSpeedOffset 0`

`FanSpeedMaxOffsetVal`	• Diese Variable liest den Lüftergeschwindigkeit-Offset-Wert in %PWM für die Einstellung „Offset für maximale Lüftergeschwindigkeit“.	Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedMaxOffsetVal`

Objekt	Beschreibung	Verwendung	Beispiel
	• Dieser Wert richtet sich nach dem System. • Verwenden Sie das Objekt `FanSpeedOffset`, um diesen Wert unter Verwendung von Index-Wert 3 festzulegen.		Dies gibt einen Wert wie „100“ aus. Dies bedeutet, dass, wenn Sie den folgenden Befehl verwenden, ein Lüfterdrehzahlversatz des Werts „Max“ angewendet wird (d. h. volle Geschwindigkeit, 100 % PWM). Normalerweise resultiert dieser Versatz der Lüfterdrehzahlerhöhung in der Höchstgeschwindigkeit. `racadm set system.thermalsettings FanSpeedOffset 3`

`FanSpeedMediumOffsetVal`	• Diese Variable liest den Lüftergeschwindigkeit-Offset-Wert in %PWM für die Einstellung „Offset für mittlere Lüftergeschwindigkeit“.
	• Dieser Wert richtet sich nach dem System.
	• Verwenden Sie das Objekt `FanSpeedOffset`, um diesen Wert unter Verwendung von Index-Wert 2 festzulegen.
		Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedMediumOffsetVal`
			Dies gibt einen Wert wie „47“ zurück. Das bedeutet, dass, wenn Sie den folgenden Befehl verwenden, ein Offset für Lüftergeschwindigkeit auf mittel (47% PWM) über die Drehzahl der Basislinie angewendet wird.
			`racadm set system.thermalsettings FanSpeedOffset 2`

`FanSpeedOffset`	• Das Verwenden dieses Objekts mit dem Get-Befehl zeigt den vorhandenen Lüfterdrehzahl-Offset-Wert an.
	• Das Verwenden dieses Objekts mit dem Get-Befehl ermöglicht die Einstellung des erforderlichen Lüfterdrehzahl-Offset-Werts.
	• Der Indexwert entscheidet über den Versatz, der angewendet wird, und die Objekte `FanSpeedLowOffsetVal`, `FanSpeedMaxOffsetVal` `FanSpeedHighOffsetVal` und `FanSpeedMediumOffsetVal` (zuvor definiert) sind die Werte, bei denen der Versatz angewendet wird.
		Mögliche Werte sind:
		• 0 – für niedrige Lüfterdrehzahl
		• 1 – für hohe Lüfterdrehzahl
		• 2 – für mittlere Lüfterdrehzahl
		• 3 – für maximale Lüfterdrehzahl
		• 255 – Keine
			So zeigen Sie die vorhandene Einstellung an:
			`racadm get system.thermalsettings. FanSpeedOffset`
			So legen Sie den Lüfterdrehzahl-Offset-Wert (wie definiert in `FanSpeedHighOffsetVal` auf Hoch
			`racadm set system.thermalsettings. FanSpeedOffset 1`

`MFSMaximumLimit`	Maximalwerte für MFS lesen	Werte von 1 – 100	So zeigen Sie den höchsten Wert an, der mithilfe der Option `MinimumFanSpeed` eigestellt werden kann: `racadm get system.thermalsettings. MFSMaximumLimit`

Objekt	Beschreibung	Verwendung	Beispiel
`MFSMinimumLimit`	Minimalwerte für MFS lesen	Werte von 0 bis `MFSMaximumLimit` Der Standardwert ist 255 (das bedeutet Keine)	So zeigen Sie den niedrigsten Wert an, der mithilfe der Option `MinimumFanSpeed` eigestellt werden kann: `racadm get system.thermalsettings.MFSMinimumLimit`
`MinimumFanSpeed`	• Ermöglicht die Konfiguration der Mindest-Lüftergeschwindigkeit, die erforderlich ist, damit das System betrieben werden kann. • Sie definiert den Basiswert für die Lüftergeschwindigkeit und versetzt Lüfter in die Lage, diesen Wert für die Lüftergeschwindigkeit zu unterschreiten. • Dieser Wert ist der PWM-Wert für die Lüftergeschwindigkeit, angegeben in Prozent.	Werte von `MFSMinimumLimit` bis `MFSMaximumLimit` Wenn der Befehl 255 meldet, bedeutet dies, dass der benutzerdefinierte Versatz nicht angewendet wurde.	Gehen Sie wie folgt vor, um sicherzustellen, dass die Systemmindestgeschwindigkeit nicht unter 45 % des PWM fällt (45 muss ein Wert zwischen `MFSMinimumLimit` und `MFSMaximumLimit` sein): `racadm set system.thermalsettings.MinimumFanSpeed 45`

`ThermalProfile`	• Ermöglicht die Angabe des thermischen Base-Algorithmus.
	• Ermöglicht das Festlegen des Systemprofils für thermisches Verhalten, das dem Profil zugeordnet ist.
		Werte:
		• 0 – Auto
		• 1 – Maximale Leistung
		• 2: Minimale Stromversorgung
			So zeigen Sie die vorhandene thermische Profileinstellung an:
			
			`racadm get system.thermalsettings.ThermalProfile`
			
			So legen Sie das thermische Profil auf maximale Leistung fest:
			
			`racadm set system.thermalsettings.ThermalProfile 1`

`ThirdPartyPCIFanResponse`	• Thermische Überschreibungen für PCI-Karten von Drittanbietern. • Ermöglicht das Deaktivieren oder Aktivieren der Lüfterreaktion des Standardsystems für erkannte PCI-Karten von Drittanbietern. • Sie können die Existenz der PCI-Karte von Drittanbietern durch das Anzeigen der Meldungs-ID PCI3018 im Lifecycle Controller-Protokoll bestätigen.	Werte: • 1 – Aktiviert • 0 – Deaktiviert **ANMERKUNG: Der Standardwert ist 1.**	So deaktivieren Sie jegliche eingestellte Standard-Lüftergeschwindigkeitsreaktion für eine erkannte PCI-Karte von Drittanbietern: `racadm set system.thermalsettings.ThirdPartyPCIFanResponse 0`

Thermische Einstellungen unter Verwendung vom Dienstprogramm für die iDRAC-Einstellungen ändern

So ändern Sie die Standardeinstellungen:

1 Gehen Sie im Dienstprogramm für die iDRAC -Einstellungen zu **Thermisch**.
Die Seite **iDRAC-Einstellungen Thermisch** wird angezeigt.

2 Geben Sie folgendes an:
- Thermisches Profil
- Maximaler Ablufttemperatur-Grenzwert
- Offset für Lüftergeschwindigkeit
- Minimale Lüftergeschwindigkeit

Weitere Informationen zu den Feldern finden Sie unter Ändern der thermischen Einstellungen unter Verwendung der Webschnittstelle.

Die Einstellungen sind dauerhaft, d. h., sobald diese festgelegt und angewendet wurden, werden sie während eines Systemneustarts, beim Aus- und Einschalten oder bei iDRAC- oder BIOS-Aktualisierungen nicht mehr automatisch in die Standardeinstellung geändert. Einige Dell-Server unterstützen möglicherweise einige oder alle dieser benutzerdefinierten Kühlungsoptionen nicht. Wenn die Optionen nicht unterstützt werden, werden sie nicht angezeigt, oder Sie können keinen benutzerdefinierten Wert festlegen.

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
Die Konfiguration der Temperatureinstellungen ist damit abgeschlossen.

Konfigurieren von unterstützten Webbrowsern

ANMERKUNG: Informationen zu den unterstützten Browsern und deren Versionen finden Sie in *Release Notes (Versionshinweisen)* unter dell.com/idracmanuals.

Auf die meisten Funktionen der iDRAC-Webschnittstelle kann zugegriffen werden, indem diese Browser mit den Standardeinstellungen verwendet werden. Damit bestimmte Funktionen ordnungsgemäß funktionieren, müssen Sie einige Einstellungen ändern. Diese Einstellungen umfassen das Deaktivieren von Popup-Blockern, das Aktivieren von Java-, ActiveX- oder HTML5-Plug-in-Support usw.

Wenn Sie von einer Management Station aus, die über einen Proxyserver mit dem Internet verbunden ist, eine Verbindung zur iDRAC-Webschnittstelle herstellen, konfigurieren Sie den Webbrowser so, dass er von diesem Server aus auf das Internet zugreifen kann.

ANMERKUNG: Wenn Sie den Internet Explorer oder Firefox zum Zugriff auf die iDRAC-Webschnittstelle verwenden, müssen Sie möglicherweise bestimmte Einstellungen, wie in diesem Abschnitt beschrieben, konfigurieren. Sie können andere unterstützte Browser mit ihren Standardeinstellungen verwenden.

Zugehöriger Link

Lokalisierte Versionen der Webschnittstelle anzeigen
Hinzufügen von iDRAC-IP zur Liste vertrauenswürdiger Webseiten
Weiße Liste-Funktion in Firefox deaktivieren

Internet Explorer konfigurieren

Dieser Abschnitt enthält Details zur Konfiguration von Internet Explorer (IE), um sicherzustellen, dass Sie Zugriff auf alle Funktionen der iDRAC-Webschnittstelle haben und diese verwenden können. Diese Einstellungen umfassen:

- Zurücksetzen der Sicherheitseinstellungen
- Hinzufügen von iDRAC-IP zu vertrauenswürdigen Sites

- IE für die Aktivierung von Active Directory SSO konfigurieren

Internet Explorer-Sicherheitseinstellungen zurücksetzen

Stellen Sie sicher, dass Internet Explorer- (IE) Einstellungen auf die von Microsoft empfohlenen Standardeinstellungen eingestellt sind und passen Sie die Einstellungen, wie in diesem Abschnitt beschrieben, an.

1 Öffnen Sie IE als Administrator oder unter Verwendung eines Administratorkontos.
2 Klicken Sie auf **Extras Internetoptionen Sicherheit Lokales Netzwerk** oder **Lokales Intranet**.
3 Klicken Sie auf **Stufe anpassen**, wählen Sie **Mittelniedrig** und klicken Sie auf **Zurücksetzen**. Klicken Sie zur Bestätigung auf **OK**.

Hinzufügen von iDRAC-IP zur Liste vertrauenswürdiger Webseiten

Wenn Sie auf die iDRAC-Web-Schnittstelle zugreifen, werden Sie dazu aufgefordert, die iDRAC-IP-Adresse zur Liste der vertrauenswürdigen Domänen hinzuzufügen, wenn die IP-Adresse nicht in der Liste enthalten ist. Wenn Sie fertig sind, klicken Sie auf **Aktualisieren** oder starten den Webbrowser neu, um eine Verbindung zur iDRAC- Web-Schnittstelle aufzubauen. Wenn Sie nicht aufgefordert werden, die IP hinzuzufügen, wird empfohlen, dass Sie die IP-manuell zur Liste vertrauenswürdiger Seiten hinzufügen.

ANMERKUNG: Wenn Sie sich an der iDRAC-Webschnittstelle mit einem Zertifikat anmelden wollen, dem der Browser nicht vertraut, wird die Zertifikatfehlerwarnung des Browsers nach dem Bestätigen der ersten Meldung möglicherweise ein zweites Mal angezeigt.

So fügen Sie iDRAC-IP-Adresse der Liste vertrauenswürdiger Websites hinzu:

1 Klicken Sie auf **Extras** > **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Sites** > **Sites**.
2 Geben Sie die IP-Adresse des iDRAC in das Feld **Diese Website zur Zone hinzufügen** ein.
3 Klicken Sie auf **Hinzufügen**, dann auf **OK** und schließlich auf **Schließen**.
4 Klicken Sie auf **OK** und aktualisieren Sie dann den Browser.

Internet Explorer für die Aktivierung von Active Directory SSO konfigurieren

So konfigurieren Sie die Browser-Einstellungen für Internet Explorer:

1 Navigieren Sie im Internet Explorer zu **Lokales Intranet**, und klicken Sie dann auf **Sites**.
2 Wählen Sie nur die folgenden Optionen aus:
   - Schließen Sie alle lokalen (Intranet-) Sites ein, die nicht auf anderen Zonen aufgeführt sind.
   - Schließen Sie alle Sites ein, die den Proxy-Server umgehen.
3 Klicken Sie auf **Erweitert**.
4 Fügen Sie alle betreffenden Domänennamen ein, die für iDRAC-Instanzen, die Teil der SSO-Konfiguration sind, verwendet werden (z. B. **myhost.example.com**.)
5 Klicken Sie auf **Schließen** und anschließend auf **OK** zweimal.

Konfiguration von Mozilla Firefox

Dieser Abschnitt enthält Details zur Konfiguration von Firefox, um sicherzustellen, dass Sie Zugriff auf alle Funktionen der iDRAC-Webschnittstelle haben und diese verwenden können. Diese Einstellungen umfassen:

- Weiße Liste-Funktion deaktivieren
- Firefox für die Aktivierung von Active Directory SSO konfigurieren

Weiße Liste-Funktion in Firefox deaktivieren

Firefox verfügt über eine „Weiße Liste"-Sicherheitsfunktion, die eine Benutzerberechtigung zum Installieren von Plugins für jede Site erfordert, die ein Plugin hostet. Ist die Weiße Liste-Funktion aktiviert, ist die Installation eines Virtuelle Konsole-Viewers für jeden besuchten iDRAC erforderlich, obwohl die Viewer-Versionen identisch sind.

Führen Sie folgende Schritte aus, um die Funktion „Weiße Liste" zu deaktivieren und unnötige Plug-in-Installationen zu vermeiden:

1 Öffnen Sie ein Internet-Browser-Fenster in Firefox.

2 Geben Sie in das Adressfeld `about:config` ein und drücken Sie auf <Eingabe>.

3 Machen Sie in der Spalte **Einstellungsname** den Eintrag **xpinstall.whitelist.required** ausfindig und doppelklicken Sie darauf.

Die Werte für **Einstellungsname**, **Status**, **Typ** und **Wert** ändern sich zu fett gedrucktem Text. Der Wert **Status** ändert sich zu Vom Benutzer festgelegt, und der **Wert** ändert sich zu false (falsch).

4 Machen Sie in der Spalte **Einstellungs**name den Eintrag xpinstall.enabled ausfindig.

Stellen Sie sicher, dass der **Wert true** (wahr) ist. Ist dies nicht der Fall, doppelklicken Sie auf **xpinstall.enabled**, um den **Wert** auf **true** (wahr) zu setzen.

Firefox für die Aktivierung von Active Directory SSO konfigurieren

So konfigurieren Sie die Browser-Einstellungen für Firefox:

1 Geben Sie in die Firefox-Adresszeile `about:config` ein.

2 Geben Sie unter **Filter** `network.negotiate` ein.

3 Fügen Sie den Domänen-Namen zu network.negotiate-auth.trusted-uris (kommaseparierte Liste verwenden) hinzu.

4 Fügen Sie den Domänen-Namen zu network.negotiate-auth.delegation-uris (kommaseparierte Liste verwenden) hinzu.

Web-Browser für die Verwendung der virtuellen Konsole konfigurieren

So verwenden Sie die virtuelle Konsole auf Ihrer Management Station:

1 Stellen Sie sicher, dass eine unterstützte Browserversion installiert ist (Internet Explorer (Windows) oder Mozilla Firefox (Windows oder Linux), Google Chrome, Safari).

Weitere Informationen zu den unterstützten Browserversionen finden Sie in *Release Notes* (Versionshinweisen) unter **dell.com/idracmanuals**.

2 Wenn Sie Internet Explorer verwenden, setzen Sie IE auf **Als Administrator ausführen**.

3 Konfigurieren Sie den Web-Browser für die Verwendung des ActiveX-, Java- oder HTML5-Plugin.

Der ActiveX-Viewer wird nur unter Internet Explorer unterstützt. HTML5 oder ein Java-Viewer werden auf jedem Browser unterstützt.

4 Importieren Sie die Stammzertifikate auf das Managed System, um Popup-Fenster zu unterbinden, die Sie zur Überprüfung der Zertifikate auffordern.

5 Installieren Sie das verknüpfte Paket **compat-libstdc++-33-3.2.3-61**.

ANMERKUNG: Unter Windows ist das verknüpfte Paket „compat-libstdc++-33-3.2.3-61" möglicherweise im .NET Framework-Paket oder im Betriebssystempaket enthalten.

6 Wenn Sie ein MAC-Betriebssystem nutzen, wählen Sie die Option **Zugriff für Hilfsgeräte aktivieren** im Fenster **Universeller Zugriff**.

Weitere Informationen finden Sie in der Dokumentation des MAC-Betriebssystems.

Zugehöriger Link

Internet Explorer zur Verwendung des HTML-5-basierten Plug-In konfigurieren
Web-Browser für die Verwendung des Java-Plugin konfigurieren
IE für die Verwendung des ActiveX-Plugin konfigurieren
Zertifizierungsstellenzertifikate auf die Management Station importieren

Internet Explorer zur Verwendung des HTML-5-basierten Plug-In konfigurieren

Die APIs für die virtuelle HTML5-Konsole und virtuelle Datenträger wurden unter Verwendung der HTML5-Technologie erstellt. Diese bietet die folgenden Vorteile:

- Auf der Client Workstation ist keine Installation erforderlich.
- Die Kompatibilität basiert auf dem Browser und nicht auf dem Betriebssystem oder den installierten Komponenten.
- Kompatibel mit den meisten des Desktops und mobilen Plattformen.
- Schnelle Bereitstellung und Herunterladen des Clients als Teil einer Webseite.

Sie müssen Einstellungen des Internet Explorer (IE) konfigurieren, bevor Sie HTML 5-basierte Anwendungen der virtuellen Konsole und des virtuellen Datenträgers starten und ausführen. So konfigurieren Sie die Browser-Einstellungen:

1 Deaktivieren Sie den Popupblocker. Klicken Sie dazu auf**Extras** > **Internetoptionen** > **Datenschutz**, und deaktivieren Sie das Kontrollkästchen **Popupblocker einschalten**.
2 Starten Sie die virtuelle HTML5-Konsole unter Verwendung von einer der folgenden Methoden:
   - Klicken Sie in IE auf **Extras** > **Einstellungen der Kompatibilitätsansicht**, und entfernen Sie die Markierung bei **Intranetsites in Kompatibilitätsansicht anzeigen**.
   - Modifizieren Sie bei Verwendung einer IPv6-Adresse diese Adresse in IE wie folgt:
     ```
     https://[fe80::d267:e5ff:fef4:2fe9]/ to https://fe80--d267-e5ff-fef4-2fe9.ipv6-literal.net/
     ```
   - Direkte virtuelle HTML5-Konsole. Modifizieren Sie bei Verwendung einer IPv6-Adresse diese Adresse in IE wie folgt:
     ```
     https://[fe80::d267:e5ff:fef4:2fe9]/console to https://fe80--d267-e5ff-fef4-2fe9.ipv6-literal.net/console
     ```
3 Wechseln Sie zum Anzeigen der Titelleisteninformationen in IE zu**Systemsteuerung** > **Darstellung und Anpassung** > **Anpassung** > **Windows – klassisch**.

Web-Browser für die Verwendung des Java-Plugin konfigurieren

Installieren Sie eine Java Runtime Environment (JRE), wenn Sie Firefox oder IE verwenden und den Java Viewer verwenden möchten.

ANMERKUNG: Installieren Sie eine 32-Bit- oder 64-Bit-JRE-Version auf einem 64-Bit-Betriebssystem oder eine 32-Bit-JRE-Version auf einem 32-Bit-Betriebssystem.

So konfigurieren Sie IE für die Verwendung des Java-Plugin:

- Deaktivieren Sie die automatische Anforderung von Datei-Downloads im Internet Explorer.
- Deaktivieren Sie die Option *Verstärkter Sicherheitsmodus* im Internet Explorer.

Zugehöriger Link

Virtuelle Konsole konfigurieren

IE für die Verwendung des ActiveX-Plugin konfigurieren

Sie müssen die Internet Explorer-Einstellungen konfigurieren, bevor Sie die ActiveX-basierten Anwendungen der virtuellen Konsole und des virtuellen Datenträgers starten und ausführen. Die ActiveX-Anwendungen werden als signierte CAB-Dateien vom iDRAC-Server bereitgestellt. Wenn der Plug-In-Typ in der virtuellen Konsole auf den Native-ActiveX-Typ gesetzt ist und Sie versuchen, die virtuelle

Konsole zu starten, wird die CAB-Datei auf das Client-System heruntergeladen, und die ActiveX-basierte virtuelle Konsole wird gestartet. Internet Explorer fordert bei einigen Konfigurationen, diese ActiveX-basierten Anwendungen herunterzuladen, zu installieren oder auszuführen.

Internet Explorer ist sowohl in 32-Bit- als auch in 64-Bit-Versionen auf 64-Bit-Browsern verfügbar. Sie können eine beliebige Version verwenden, aber wenn Sie das Plug-In in den 64-Bit-Browser installieren und dann versuchen, das Anzeigeprogramm in einem 32-Bit-Browser auszuführen, müssen Sie das Plug-In erneut installieren.

ANMERKUNG: Sie können das ActiveX-Plugin nur mit Internet Explorer verwenden.

ANMERKUNG: Um das ActiveX-Plugin auf Systemen mit Internet Explorer 9 zu verwenden, stellen Sie vor dem Konfigurieren von Internet Explorer sicher, dass Sie den erweiterten Sicherheitsmodus in Internet Explorer oder im Server-Manager in den Betriebssystemen von Windows Server deaktivieren.

Bei ActiveX-Anwendungen in Windows 2003, Windows XP, Windows Vista, Windows 7 und Windows 2008 müssen Sie die folgenden Internet Explorer-Einstellungen konfigurieren, um das ActiveX-Plug-in verwenden zu können:

1. Leeren Sie den Browser-Cache.
2. Fügen Sie die iDRAC-IP-Adresse oder den Host-Namen zur Liste **Vertrauenswürdige Sites** hinzu.
3. Setzen Sie die benutzerdefinierten Einstellungen auf **Mittelhoch (Standard)** zurück, oder ändern Sie die Einstellungen, um die Installation von signierten ActiveX-Plugins zu ermöglichen.
4. Aktivieren Sie den Browser für das Herunterladen von verschlüsselten Inhalten, und aktivieren Sie Drittanbieter-Browser-Erweiterungen. Gehen Sie dazu zu **Extras** > **Internetoptionen** > **Erweitert**, deaktivieren Sie die Option **Verschlüsselte Sites nicht auf dem Datenträger speichern**, und aktivieren Sie die Option **Browsererweiterungen von Drittanbietern aktivieren**.

   ANMERKUNG: Starten Sie Internet Explorer neu, damit die Einstellung „Browsererweiterungen von Drittanbietern aktivieren“ aktiviert wird.
5. Gehen Sie zu **Extras** > **Internetoptionen** > **Sicherheit**, und wählen Sie die Zone aus, in der Sie die Anwendung ausführen möchten.
6. Klicken Sie auf **Stufe anpassen**. Führen Sie im Fenster **Sicherheitseinstellungen** die folgenden Schritte aus:
   - Wählen Sie die Option **Aktivieren** für **Automatische Eingabeaufforderung für ActiveX-Steuerelemente** aus.
   - Wählen Sie die Option **Auffordern** für **Signierte ActiveX-Steuerelemente herunterladen** aus.
   - Wählen Sie die Option **Aktivieren** oder **Auffordern** für **ActiveX-Steuerelemente und -Plugins ausführen** aus.
   - Wählen Sie die Option **Aktivieren** oder **Auffordern** für **Script-ActiveX-Steuerelemente, die für das Scripting als sicher gekennzeichnet wurden** aus.
7. Klicken Sie auf **OK**, um das Fenster **Sicherheitseinstellungen** zu schließen.
8. Klicken Sie auf **OK**, um das Fenster **Internetoptionen** zu schließen.

   ANMERKUNG: Stellen Sie auf Systemen mit Internet Explorer 11 sicher, dass Sie die iDRAC-IP-Adresse hinzufügen, indem Sie auf Extras > Einstellungen der Kompatibilitätsansicht klicken.

   ANMERKUNG:
   - Die unterschiedlichen Versionen von Internet Explorer geben **Internetoptionen** frei. Nachdem Sie also den Server zur Liste der *vertrauenswürdigen Websites* für einen Browser hinzugefügt haben, verwendet der andere Browser die gleiche Einstellung.
   - Vor der Installation des ActiveX-Steuerelements zeigt Internet Explorer möglicherweise eine Sicherheitswarnung an. Um die Installation für die ActiveX-Steuerung abzuschließen, akzeptieren Sie das ActiveX-Steuerelement, wenn Internet Explorer Sie mit einer Sicherheitswarnung dazu auffordert.

Zugehöriger Link

Browser-Cache leeren

Zusätzliche Einstellungen für Windows Vista oder neuere Microsoft-Betriebssysteme

Zusätzliche Einstellungen für Windows Vista oder neuere Microsoft-Betriebssysteme

Die Internet Explorer-Browser in Windows Vista oder neueren Betriebssystemen weisen eine zusätzliche Sicherheitsfunktion mit der Bezeichnung *Schutzmodus* auf.

Um ActiveX-Anwendungen in Internet Explorer-Browsern mit dem *Schutzmodus* zu starten und auszuführen:

1 Führen Sie IE als Administrator aus.
2 Gehen Sie zu **Extras** > **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Sites**.
3 Stellen Sie sicher, dass die Option **Schutzmodus aktivieren** für vertrauenswürdige Sites nicht aktiviert ist. Alternativ dazu können Sie die iDRAC-Adresse den Sites in der Intranetzone hinzufügen. Standardmäßig ist der Schutzmodus für Sites in der Intranetzone und in der Zone für vertrauenswürdige Sites ausgeschaltet.
4 Klicken Sie auf **Sites**.
5 Geben Sie in das Feld **Diese Website zur Zone hinzufügen** die Adresse des iDRAC ein, und klicken Sie auf **Hinzufügen**.
6 Klicken Sie auf **Schließen** und dann auf **OK**.
7 Schließen Sie den Browser und starten Sie ihn neu, damit die Einstellungen wirksam werden.

Browser-Cache leeren

Wenn beim Betrieb der virtuellen Konsole Probleme auftreten (Fehler des Typs Außerhalb des Bereichs, Synchronisierungsprobleme usw.) löschen Sie den Browser-Cache, um alte Viewer-Versionen zu entfernen oder zu löschen, die auf dem System gespeichert sein könnten, und wiederholen Sie den Vorgang.

ANMERKUNG: Um den Browser-Cache löschen zu können, müssen Sie über Administratorrechte verfügen.

Frühere Java-Versionen löschen

So löschen Sie ältere Versionen von Java-Viewer in Windows oder Linux:

1 Führen Sie bei der Eingabeaufforderung `javaws-viewer` oder `javaws-uninstall` aus.
Der **Java Cache-Viewer** wird angezeigt.
2 Löschen Sie die Elemente mit der Bezeichnung *Client der virtuellen iDRAC-Konsole*.

Zertifizierungsstellenzertifikate auf die Management Station importieren

Wenn Sie die virtuelle Konsole oder den virtuellen Datenträger starten, werden Sie über Abfragen dazu aufgefordert, die Zertifikate zu überprüfen. Wenn Sie über Web Server-Zertifikate verfügen, können Sie diese Abfragen durch das Importieren der Zertifizierungsstellenzertifikate in den vertrauenswürdigen Java- oder ActiveX-Store umgehen.

Zugehöriger Link

Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige Java-Zertifikate importieren
Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige ActiveX-Zertifikate importieren

Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige Java-Zertifikate importieren

So importieren Sie das Zertifizierungsstellenzertifikat in den vertrauenswürdigen Java-Speicher:

1 Starten Sie das **Java-Systemsteuerung**.
2 Klicken Sie auf die Registerkarte **Sicherheit** und dann auf **Zertifikate**.
Das Dialogfeld **Zertifikate** wird angezeigt.
3 Wählen Sie aus dem Drop-Down-Menü „Zertifikattyp“ die Option **Vertrauenswürdige Zertifikate** aus.
4 Klicken Sie auf **Importieren**, browsen Sie zum gewünschten Zertifizierungsstellenzertifikat (im in Base64-verschlüsselten Format), wählen Sie es aus, und klicken Sie dann auf **Öffnen**.
Das ausgewählte Zertifikat wird in den vertrauenswürdigen, web-basierten Zertifikatspeicher importiert.
5 Klicken Sie auf **Schließen** und dann auf **OK**. Daraufhin wird das Fenster **Java-Systemsteuerung** geschlossen.

Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige ActiveX-Zertifikate importieren

Sie müssen das OpenSSL-Befehlszeilen-Tool verwenden, um das Zertifikat-Hash über den Secure Hash Algorithm (SHA) zu erstellen. Es wird empfohlen, das OpenSSL-Tool ab Version 1.0.x zu verwenden, da es SHA standardmäßig verwendet. Das Zertifizierungsstellenzertifikat muss im Base64-verschlüsselten PEM-Format vorliegen. Dies ist ein einmaliger Prozess für den Import jedes einzelnen Zertifizierungsstellenzertifikats.

So importieren Sie das Zertifizierungsstellenzertifikat in den vertrauenswürdigen ActiveX-Speicher:

1 Öffnen Sie die OpenSSL-Befehlseingabe.

2 Führen Sie einen 8-Byte-Hash auf dem Zertifizierungsstellenzertifikat aus, das derzeit auf der Management Station verwendet wird. Verwenden Sie dazu den folgenden Befehl: `openssl x509 -in (name of CA cert) -noout -hash`

   Daraufhin wird eine Ausgabedatei generiert. Wenn der Dateiname des Zertifizierungsstellenzertifikats beispielsweise **cacert.pem** lautet, lautet der Befehl wie folgt:

   ```
   openssl x509 -in cacert.pem -noout -hash
   ```

   Es wird eine Ausgabedatei generiert, die dem folgenden Beispiel ähnelt: „431db322“.

3 Nennen Sie die Datei für das Zertifizierungsstellenzertifikat in den Namen der Ausgabedatei um, und fügen Sie die Erweiterung „.0“ hinzu. Beispiel: 431db322.0.

4 Kopieren Sie das umbenannte Zertifizierungsstellenzertifikat in Ihr Home-Verzeichnis. Beispiel für das Verzeichnis: **C:\Domumente und Einstellungen\<Benutzer>**.

Lokalisierte Versionen der Webschnittstelle anzeigen

Die iDRAC-Webschnittstelle wird in den folgenden Sprachen unterstützt:

- Englisch (en-us)
- Französisch (fr)
- Deutsch (de)
- Spanisch (es)
- Japanisch (ja)
- Vereinfachtes Chinesisch (zh-cn)

Die ISO-Sprachcodes in den runden Klammern kennzeichnen die unterstützten Sprachvarianten. Bei einigen unterstützten Sprachen ist es erforderlich, das Browserfenster auf eine Breite von 1024 Pixel einzustellen, um alle Funktionen anzuzeigen.

Die iDRAC-Webschnittstelle wurde für den Einsatz mit den jeweiligen Tastaturbelegungen für die unterstützten Sprachvarianten entwickelt. Einige Funktionen der iDRAC-Webschnittstelle, wie z. B. Virtuelle Konsole, können zusätzliche Schritte für den Zugriff auf bestimmte Funktionen/Buchstaben erfordern. Andere Tastaturen werden nicht unterstützt und können ggf. unerwartete Probleme verursachen.

ANMERKUNG: Lesen Sie in der Dokumentation zum Browser nach, wie verschiedene Sprachen konfiguriert und eingerichtet werden, und lassen Sie sich lokalisierte Versionen der iDRAC-Webschnittstelle anzeigen.

Aktualisieren der Gerätefirmware

Mithilfe von iDRAC können Sie die Firmware von iDRAC, BIOS und sämtlichen unterstützten Geräten aktualisieren, indem Sie eine Lifecycle Controller-Aktualisierung verwenden, z. B.:

- Fibre Channel (FC)-Karten
- Diagnose
- Treiberpaket des Betriebssystems
- Netzwerkschnittstellenkarte (NIC)

- RAID-Controller
- Netzteileinheit (PSU)
- NVMe PCIe-Geräte
- SAS-/SATA-Festplatten
- Rückwandplatinenaktualisierung für interne und externe Gehäuse
- BS-Collector

VORSICHT: Die PSU-Firmware-Aktualisierung kann je nach Systemkonfiguration und PSU-Modell mehrere Minuten dauern. Um einen Schaden am PSU zu vermeiden, unterbrechen Sie den Aktualisierungsvorgang oder die Stromversorgung des Systems während der PSU-Firmware-Aktualisierung nicht.

Die benötigte Firmware muss zu iDRAC hochgeladen werden. Nach dem Hochladen wird die aktuelle Version der Firmware, die auf dem Gerät installiert wurde, und die verwendete Version angezeigt. Wenn die hochgeladene Firmwareversion nicht gültig ist, wird eine Fehlermeldung angezeigt. Aktualisierungen, bei denen kein Neustart erforderlich ist, werden sofort angewendet. Aktualisierungen, bei denen ein Neustart des Systems erforderlich ist, werden gestuft und beim nächsten Systemneustart ausgeführt. Es ist nur ein Systemneustart erforderlich, um alle Aktualisierungen durchzuführen.

Nachdem die Firmware aktualisiert wurde, zeigt die Seite **System-Bestandsaufnahme** die aktualisierte Firmwareversion und aufgezeichnete Protokolle an.

Die unterstützten Firmware-Image-Dateitypen sind:

- **.exe** – Windows-basiertes Dell Update Package (DUP)
- **.d7** – Enthält iDRAC und Lifecycle Controller-Firmware.

Für Dateien mit der Erweiterung **.exe** müssen Sie über die Berechtigung zur Systemsteuerung verfügen. Die lizenzierte Remote-Firmwareaktualisierungsfunktion und Lifecycle Controller müssen aktiviert sein.

Für Dateien mit der Erweiterung **.d7** müssen Sie über die Berechtigung zur Konfiguration verfügen.

ANMERKUNG: Möglicherweise stellen Sie nach Aktualisierung der iDRAC-Firmware Unterschiede im Zeitstempel des Lifecycle Controller-Protokolls fest, bis die iDRAC-Zeit mit NTP zurückgesetzt wird. Das Lifecycle-Protokoll zeigt bis zum Zurücksetzen der iDRAC-Zeit die BIOS-Zeit an.

Sie können Firmware-Aktualisierungen mithilfe der folgenden Methoden ausführen:

- Hochladen eines unterstützten Imagetyps einer nach dem anderen von einem lokalen System oder einer Netzwerkfreigabe.
- Verbindung zu einer FTP-, TFTP- oder HTTP-Seite oder zu einem Netzwerk-Repository, das Windows-DUPs und eine entsprechende Katalogdatei enthält.

  Mithilfe von Dell Repository Manager können Sie benutzerdefinierte Repositorys erstellen. Weitere Informationen finden Sie im *Benutzerhandbuch zum Dell Repository Manager Data Center*. iDRAC kann einen Bericht mit Unterschieden zwischen dem BIOS und der installierten Firmware auf dem System und den im Repository verfügbaren Aktualisierungen bereitstellen. Alle im Repository enthaltenen verfügbaren Aktualisierungen werden auf das System angewandt. Für diese Funktion ist eine iDRAC Enterprise-Lizenz erforderlich.
- Das Planen wiederkehrender, automatischer Firmware-Aktualisierungen mithilfe der Katalogdatei und benutzerdefiniertem Repository.

Es gibt mehrere Tools und Schnittstellen, die verwendet werden können, um die iDRAC-Firmware zu aktualisieren. Die folgende Tabelle gilt nur für die iDRAC-Firmware. In der folgenden Tabelle werden die unterstützten Schnittstellen, Image-Dateitypen aufgelistet und es wird auch aufgelistet, ob sich Lifecycle Controller im aktivierten Zustand befinden muss, damit die Firmware aktualisiert werden kann.

Tabelle 10. Abbilddateitypen und Abhängigkeiten

	.D7-Image		iDRAC DUP (iDRAC-IP)	
Schnittstelle	**Unterstützt**	**Erfordert, dass LC aktiviert ist**	**Unterstützt**	**Erfordert, dass LC aktiviert ist**
BMCFW64.exe-Dienstprogramm	Ja	Nein	Nein	k. A.
Racadm FWUpdate (alt)	Ja	Nein	Nein	k. A.
Racadm-Aktualisierung (neu)	Ja	Ja	Ja	Ja
iDRAC UI (iDRAC-IP)	Ja	Ja	Ja	Ja
WSMAN	Ja	Ja	Ja	Ja
Bandintern BS-DUP	Nein	k. A.	Ja	Nein

Die folgende Tabelle enthält Informationen dazu, ob ein Neustart des Systems erforderlich ist, wenn die Firmware für eine bestimmte Komponente aktualisiert wird:

ANMERKUNG: Wenn mehrere Firmware-Aktualisierungen durch bandexterne Methoden angewendet werden, werden die Aktualisierungen in möglichst effizienter Weise gereiht, um unnötige Systemneustarts zu vermeiden.

Tabelle 11. Firmware-Aktualisierung

Komponentenname	Firmware-Rollback unterstützt? (Ja oder Nein)	Bandextern – Systemneustart erforderlich?	Bandintern – Systemneustart erforderlich?	Lifecycle Controller-GUI – Neustart erforderlich?
Diagnose	Nein	Nein	Nein	Nein
BS-Treiberpaket	Nein	Nein	Nein	Nein
iDRAC mit Lifecycle Controller	Ja	Nein	**Nein*	Ja
BIOS	Ja	Ja	Ja	Ja
RAID-Controller	Ja	Ja	Ja	Ja
Rückwandplatinen	Ja	Ja	Ja	Ja
Gehäuse	Ja	Ja	Nein	Ja
NIC	Ja	Ja	Ja	Ja
Netzteil	Ja	Ja	Ja	Ja
CPLD	Nein	Ja	Ja	Ja
FC-Karten	Ja	Ja	Ja	Ja
NVMe PCIe SSD-Laufwerke (nur Dell PowerEdge-Server der 13. Generation)	Ja	Nein	Nein	Nein
SAS-/SATA-Festplatten	Nein	Ja	Ja	Nein
CMC (auf PowerEdge FX2-Servern)	Nein	Ja	Ja	Ja
BS-Collector	Nein	Nein	Nein	Nein

* Zeigt an, dass obgleich ein Neustart des Systems nicht erforderlich ist, iDRAC neu gestartet werden muss, um die Aktualisierungen anzuwenden. iDRAC-Kommunikation und -Überwachung werden vorübergehend unterbrochen.

** Bei der iDRAC-Aktualisierung von Version 1.30.30 oder später ist ein Neustart des Systems nicht erforderlich. Bei iDRAC-Firmwareversionen vor 1.30.30 ist jedoch ein Neustart des Systems erforderlich, wenn die Aktualisierung unter Verwendung der bandexternen Schnittstellen angewendet wird.

ANMERKUNG: Konfigurationsänderungen und Firmware-Aktualisierungen, die innerhalb des Betriebssystems erfolgen, werden möglicherweise erst nach einem Serverneustart richtig in der Bestandsaufnahme angezeigt.

Wenn Sie nach Aktualisierungen suchen, weist die Version, die als **Verfügbar** gekennzeichnet ist, nicht unbedingt darauf hin, dass es die neueste verfügbare Version ist. Bevor Sie die Aktualisierung installieren, stellen Sie sicher, dass die Version, die Sie installieren möchten, neuer als die derzeit installierte Version ist. Wenn Sie steuern möchten, welche Version von iDRAC ermittelt wird, erstellen Sie ein benutzerdefiniertes Repository unter Verwendung des Dell Repository Managers (DRM) und konfigurieren Sie iDRAC für die Verwendung dieses Repository, um nach Aktualisierungen zu suchen.

Zugehöriger Link

Einzelgeräte-Firmware aktualisieren
Aktualisieren der Firmware mithilfe eines Repository
Firmware-Aktualisierung über FTP, TFTP oder HTTP
Aktualisieren der Gerätefirmware über RACADM
Planung automatischer Firmware-Aktualisierungen
Firmware über die CMC-Web-Schnittstelle aktualisieren
Firmware über DUP aktualisieren
Firmware über Remote-RACADM aktualisieren
Firmware über die Lifecycle-Controller-Remote-Dienste aktualisieren

Firmware über die iDRAC-Webschnittstelle aktualisieren

Sie können zur Aktualisierung der Geräte-Firmware Firmware-Images vom lokalen System, von einem Repository auf einer Netzwerkfreigabe (CIFS oder NFS) oder von FTP verwenden.

Einzelgeräte-Firmware aktualisieren

Vor der Aktualisierung der Firmware mithilfe der Einzelgeräte-Aktualisierung stellen Sie sicher, dass das Firmware-Abbild an einen Speicherort auf dem lokalen System heruntergeladen ist.

ANMERKUNG: Stellen Sie sicher, dass der Dateiname der Einzelkomponenten-DUPs keine Leerzeichen enthält.

So aktualisieren Sie die Gerätefirmware eines einzelnen Gerätes mithilfe der iDRAC-Webschnittstelle:

1 Gehen Sie zu **Übersicht** > **iDRAC Einstellungen** > **Aktualisieren und Zurücksetzen**.
Die Seite **Firmware-Aktualisierung** wird angezeigt.
2 Wählen Sie auf der Registerkarte **Aktualisieren** die Option **Lokal** als Dateispeicherort aus.
3 Klicken Sie auf **Durchsuchen**, wählen Sie die Firmware-Image-Datei für die gewünschte Komponente aus und klicken Sie dann auf **Hochladen**.
4 Nachdem der Hochladevorgang abgeschlossen ist, wird im Abschnitt **Aktualisierungsdetails** jede auf iDRAC hochgeladene Firmware-Datei mit ihrem Status angezeigt.
Wenn die Firmware-Imagedatei gültig ist und erfolgreich hochgeladen wurde, wird in der Spalte **Inhalte** ein Pluszeichen (+) neben dem Dateinamen des Firmware-Images angezeigt. Erweitern Sie den Namen, um Informationen zum **Gerätenamen** zur **derzeitigen** und zur **verfügbaren** Firmware-Version anzuzeigen.
5 Wählen Sie die erforderliche Firmware-Datei aus und führen Sie einen der folgenden Schritte aus:

- Klicken Sie bei Firmware-Abbildern, bei denen kein Neustart des Host-Systems erforderlich ist, auf **Installieren**, z. B. iDRAC-Firmwaredatei.
- Für Firmwareimages, bei denen ein Neustart des Hostsystems erforderlich ist, klicken Sie auf **Installieren und Neustart** oder **Beim nächsten Systemstart installieren**.
- Um die Aktualisierung der Firmware abzubrechen, klicken Sie auf **Abbrechen**.

Wenn Sie auf **Installieren**, **Installieren und Neustart** oder **Beim nächsten Neustart installieren** klicken, wird die Meldung `Updating Job Queue` angezeigt.

6 Zur Anzeige der Seite **Job-Warteschlange** klicken Sie auf **Job-Warteschlange**. Verwenden Sie diese Seite, um die bereitgestellten Firmware-Aktualisierungen anzuzeigen und zu verwalten oder klicken Sie auf **OK**, um die aktuelle Seite zu aktualisieren und den Status der Firmware-Aktualisierung anzuzeigen.

ANMERKUNG: Wenn Sie die Seite verlassen, ohne die Aktualisierungen zu speichern, wird eine Fehlermeldung angezeigt und der gesamte hochgeladene Inhalt geht verloren.

Zugehöriger Link

Aktualisieren der Gerätefirmware

Anzeigen und Verwalten von gestuften Aktualisierungen

Aktualisieren der Firmware mithilfe eines Repository

Ein Repository ist ein Speicherort, an dem Sie Aktualisierungspakete speichern und auf diese zugreifen können. Dell Repository Manager (DRM) ermöglicht Ihnen die Erstellung und Verwaltung eines Repository, das iDRAC auf Aktualisierungen überprüfen kann. Die Erstellung und Verwendung benutzerdefinierter Repositorys für Firmwareaktualisierungen bietet mehrere Vorteile, da Sie vollständige Kontrolle darüber haben, welche Geräte oder Komponenten aktualisiert werden. Mit iDRAC können Sie eine Repository-Aktualisierung entweder im beaufsichtigten oder vollständig beaufsichtigten Modus durchführen.

ANMERKUNG: Es wird empfohlen, den Dell Repository Manager zum Durchführen von Aktualisierungen auf Ihrem System zu verwenden, und nicht die Firmware direkt auf der Dell Website herunterzuladen und sie zu aktualisieren.

DRM kann Folgendes verwenden, um das Repository zu erstellen:

- Neuer Dell-Online-Katalog
- Vorheriger Dell Katalog, den Sie verwendet haben
- Lokale Quelle Repository
- Ein benutzerdefiniertes Repository

ANMERKUNG: Weitere Informationen über DRM finden Sie unter delltechcenter.com/repositorymanager.

ANMERKUNG: Der Lifecycle Controller muss aktiviert sein und Sie müssen über die Berechtigung zur Serversteuerung verfügen, um Firmware für andere Geräte als iDRAC zu aktualisieren.

So aktualisieren Sie Geräte-Firmware mithilfe eines Repository:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Aktualisierung und Rollback**.
Die Seite **Firmware-Aktualisierung** wird angezeigt.

2 Wählen Sie auf der Registerkarte **Aktualisieren** die **Netzwerkfreigabe** als **Datei-Speicherort** aus.

3 Geben Sie im Abschnitt **Speicherort des Katalogs** die Details der Netzwerkeinstellungen ein.
Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen. Weitere Informationen finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern.

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

4 Klicken Sie auf **Nach Aktualisierungen suchen**.
Im Abschnitt **Aktualisierungsdetails** wird ein Vergleichsbericht mit der aktuellen Firmware-Version und den im Repository verfügbaren Firmware-Versionen angezeigt.

ANMERKUNG: Aktualisierungen, die nicht unterstützt oder nicht für das System oder die installierte Hardware gelten, sind im Vergleichsbericht nicht enthalten.

5 Wählen Sie die erforderlichen Aktualisierungen aus und führen Sie einen der folgenden Schritte aus:

ANMERKUNG: Eine Version, die als „Verfügbar“ markiert ist, weist nicht immer darauf hin, dass es ist die neueste verfügbare Version oder aktueller als die bereits installierte Version ist.

- Für Firmware-Images, bei denen kein Neustart des Hostsystems erforderlich ist, klicken Sie auf **Install (Installieren)**. Zum Beispiel **.d7**-Firmwaredatei.
- Für Firmware-Images, bei denen ein Neustart des Hostsystems erforderlich ist, klicken Sie auf **Installieren und Neustart** oder **Beim nächsten Systemstart installieren**.
- Um die Aktualisierung der Firmware abzubrechen, klicken Sie auf **Abbrechen**.

Wenn Sie auf **Install (Installieren)**, **Install and Reboot (Installieren und Neustart)** oder **Install Next Reboot (Beim nächsten Neustart installieren)** klicken, wird die Meldung `Updating Job Queue` angezeigt.

6 Klicken Sie auf **Jobwarteschlange**, um die Seite **Jobwarteschlange** anzuzeigen, wo Sie die gestuften Firmware-Aktualisierungen verwalten oder auf **OK** klicken können, um die aktuelle Seite neu zu laden und den Status der Firmwareaktualisierung anzuzeigen.

Zugehöriger Link

Aktualisieren der Gerätefirmware
Anzeigen und Verwalten von gestuften Aktualisierungen
Planung automatischer Firmware-Aktualisierungen

Firmware-Aktualisierung über FTP, TFTP oder HTTP

Sie können einen FTP-, TFTP- oder HTTP-Server einrichten und iDRAC konfigurieren, um dies für die Ausführung von Firmware-Aktualisierungen zu verwenden. Sie können die Windows-basierenden Update-Pakete (DUPs) und eine Katalogdatei verwenden.

ANMERKUNG: Der Lifecycle Controller muss aktiviert sein und Sie müssen über die Berechtigung zur Server-Steuerung verfügen, um Firmware für andere Geräte als iDRAC zu aktualisieren.

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Aktualisierung und Rollback**.

Die Seite **Firmware-Aktualisierung** wird angezeigt.

2 Wählen Sie im Register **Aktualisierung** die gewünschte Option in **Dateispeicherort** aus – **FTP**, **TFTP** oder **HTTP**.

3 Geben Sie die erforderlichen Details in die angezeigten Felder ein.

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

4 Klicken Sie auf die Option **Auf Aktualisierungen prüfen**.

5 Nach vollständiger Aktualisierung wird im Abschnitt **Aktualisierungsdetails** ein Vergleichsbericht mit der aktuellen Firmware-Version und den im Repository verfügbaren Firmware-Versionen angezeigt.

ANMERKUNG: Aktualisierungen, die nicht unterstützt werden oder nicht für das System zutreffend sind, oder installierte Hardware sind im Vergleichsbericht nicht enthalten.

6 Wählen Sie die erforderlichen Aktualisierungen aus, und führen Sie einen der folgenden Schritte aus:

- Für Firmware-Images, bei denen kein Neustart des Hostsystems erforderlich ist, klicken Sie auf **Installieren**. Zum Beispiel: **.d7**-Firmwaredatei.
- Für Firmware-Images, bei denen ein Neustart des Hostsystems erforderlich ist, klicken Sie auf **Installieren und Neustart** oder **Beim nächsten Systemstart installieren**.
- Um die Aktualisierung der Firmware abzubrechen, klicken Sie auf **Abbrechen**.

Wenn Sie auf **Installieren**, **Installieren und Neustart** oder **Beim nächsten Neustart installieren** klicken, wird die Meldung `Updating Job Queue` angezeigt.

7 Zur Anzeige der Seite **Job-Warteschlange** klicken Sie auf **Job-Warteschlange**. Auf dieser Seite können Sie die bereitgestellten Firmware-Aktualisierungen anzeigen und verwalten. Klicken Sie auf **OK** um die aktuelle Seite zu aktualisieren und den Status der Firmware-Aktualisierung anzuzeigen.

Zugehöriger Link

Aktualisieren der Gerätefirmware
Anzeigen und Verwalten von gestuften Aktualisierungen
Planung automatischer Firmware-Aktualisierungen

Aktualisieren der Gerätefirmware über RACADM

Um die Gerätefirmware unter Verwendung von RACADM zu aktualisieren, verwenden Sie den Unterbefehl **update**. Weitere Informationen finden Sie im *RACADM Reference Guide for iDRAC and CMC* (RACADM Referenzhandbuch für iDRAC und CMC) unter **dell.com/idracmanuals**.

Beispiele:

- So erstellen Sie einen Vergleichsreport mit einem Update-Repository:
  ```
  racadm update -f catalog.xml -l //192.168.1.1 -u test -p passwd --verifycatalog
  ```
- So führen Sie alle verfügbaren Aktualisierungen aus dem Update-Repository mit **myfile.xml** als Katalogdatei sowie einen ordentlichen Neustart durch:
  ```
  racadm update -f "myfile.xml" -b "graceful" -l //192.168.1.1 -u test -p passwd
  ```
- So führen Sie alle verfügbaren Aktualisierungen von einem FTP-Update-Repository mit **Catalog.xml** als Katalogdatei durch:
  ```
  racadm update -f "Catalog.xml" -t FTP -e 192.168.1.20/Repository/Catalog
  ```

Planung automatischer Firmware-Aktualisierungen

Sie können für iDRAC einen Zeitplan zur regelmäßigen Prüfung auf Firmware-Aktualisierungen erstellen. iDRAC nimmt dann gemäß geplanten Datums und Zeit Verbindung mit dem angegebenen Ziel auf, prüft ob neue Aktualisierungen vorliegen und führt alle anwendbaren Aktualisierungen durch bzw. stellt diese bereit. Es wird eine Protokolldatei auf dem Remote-Server erstellt, die Informationen über den Server-Zugriff und die bereitgestellten Firmware-Updates enthält.

Es wird empfohlen, dass Sie ein Repository unter Verwendung des Dell Repository Managers (DRM) erstellen und Sie iDRAC so konfigurieren, dass dieses Repository für die Überprüfung und Durchführung der Firmware-Aktualisierungen verwendet wird. Unter Verwendung eines internen Repository können Sie für iDRAC verfügbare Firmware und verfügbare Versionen steuern; dies trägt zur Vermeidung unbeabsichtigter Firmware-Änderungen bei.

ANMERKUNG: Weitere Informationen über DRM finden Sie unter delltechcenter.com/repositorymanager.

Die iDRAC Enterprise-Lizenz ist erforderlich, um automatische Aktualisierungen zu planen.

Sie können automatische Firmware-Aktualisierungen mithilfe der iDRAC-Webschnittstelle oder mit RACADM planen.

ANMERKUNG: Die IPv6-Adresse wird bei der Planung automatischer Firmware-Aktualisierungen nicht unterstützt.

Zugehöriger Link

Aktualisieren der Gerätefirmware
Anzeigen und Verwalten von gestuften Aktualisierungen

Planen der automatischen Firmware-Aktualisierung mithilfe der Webschnittstelle

So erstellen Sie einen Zeitplan für die automatische Aktualisierung der Firmware mithilfe der Webschnittstelle:

ANMERKUNG: Wenn bereits ein Job geplant ist, erstellen Sie keine weitere geplante automatische Aktualisierung, da hierdurch sonst der aktuell geplante Job überschrieben wird.

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Aktualisierung und Rollback**.

Die Seite **Firmware-Aktualisierung** wird angezeigt.

2 Klicken Sie auf die Registerkarte **Automatische Aktualisierung**.

3 Wählen Sie die Option **Automatische Aktualisierung aktivieren** aus.

4 Wählen Sie eine der folgenden Optionen aus, um anzugeben, ob ein Systemneustart erforderlich ist, nachdem die Aktualisierungen bereitgestellt wurden:

- **Aktualisierungen planen** – Stellt die Firmware-Aktualisierungen bereit, führt aber keinen Serverneustart aus.
- **Aktualisierungen planen und Server neu starten** – Initiiert einen Server-Neustart, nachdem die Firmware-Aktualisierungen bereitgestellt wurden.

5 Wählen Sie eine der folgenden Optionen, um den Speicherort der Firmware-Abbilder anzugeben:

- **Netzwerk** – Verwenden Sie die Katalogdatei einer Netzwerkfreigabe (CIFS oder NFS). Geben Sie die Details zur Netzwerkfreigabe ein.

  ANMERKUNG: Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen.

- **FTP** – Verwenden Sie den Katalogdatei vom FTP-Standort. Geben Sie die Details zum FTP-Standort ein.

6 Geben Sie anhand der Auswahl in Schritt 5 die Netzwerkeinstellungen oder die FTP-Einstellungen ein.

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

7 Geben Sie im Abschnitt **Aktualisierungszeitplan** die Startzeit für die Firmware-Aktualisierung und die Häufigkeit der Aktualisierung (täglich, wöchentlich oder monatlich) ein.

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

8 Klicken Sie auf **Aktualisierung planen**.

Der nächste geplante Job wird in der Job-Warteschlange erstellt. Fünf Minuten, nachdem die erste Instanz des wiederkehrenden Jobs begonnen hat, wird der Job für den nächsten Zeitraum erstellt.

Planen der automatischen Firmware-Aktualisierung mithilfe von RACADM

Verwenden Sie zum Erstellen von Zeitplänen für die automatische Firmware-Aktualisierung die folgenden Befehle:

- Für die Aktivierung der automatischen Firmware-Aktualisierung:

```
racadm set lifecycleController.lcattributes.AutoUpdate.Enable 1
```

- Zum Anzeigen des Status der automatischen Firmware-Aktualisierung:

```
racadm get lifecycleController.lcattributes.AutoUpdate
```

- Zum Planen der Startzeit und Häufigkeit der Firmware-Aktualisierung:

```
racadm AutoUpdateScheduler create -u username -p password -l <location> [-f catalogfilename -pu <proxyuser> -pp<proxypassword> -po <proxy port> -pt <proxytype>] -time < hh:mm> [-dom < 1 - 28,L,’*’> -wom <1-4,L,’*’> -dow <sun-sat,’*’>] -rp <1-366> -a <applyserverReboot (1-enabled | 0-disabled)>
```

Beispiel:

- Für die automatische Aktualisierung der Firmware mithilfe einer CIFS-Freigabe:

```
racadm AutoUpdateScheduler create -u admin -p pwd -l //1.2.3.4/CIFS-share -f cat.xml -time 14:30 -wom 1 -dow sun -rp 5 -a 1
```

- Für die automatische Aktualisierung der Firmware mithilfe von FTP:

```
racadm AutoUpdateScheduler create -u admin -p pwd -l ftp.mytest.com -pu puser -pp puser -po 8080 -pt http -f cat.xml -time 14:30 -wom 1 -dow sun -rp 5 -a 1
```

- Zum Anzeigen des aktuellen Zeitplans der Firmware-Aktualisierung:

```
racadm AutoUpdateScheduler view
```

- Zum Deaktivieren der automatischen Firmware-Aktualisierung:

```
racadm set lifecycleController.lcattributes.AutoUpdate.Enable 0
```

- Zum Löschen der Einzelheiten der Zeitpläne:
  ```
  racadm AutoUpdateScheduler clear
  ```

Firmware über die CMC-Web-Schnittstelle aktualisieren

Sie können die iDRAC-Firmware für Blade-Server über die CMC-Webschnittstelle aktualisieren.

So aktualisieren Sie die iDRAC-Firmware über die CMC-Webschnittstelle:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Gehen Sie zu **Server** > **Übersicht** > **<Servername>** .
   Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf **iDRAC-Web-Schnittstelle starten**, und führen Sie dann die **iDRAC-Firmware-Aktualisierung** aus.

Zugehöriger Link

Aktualisieren der Gerätefirmware

Firmware über die iDRAC-Webschnittstelle aktualisieren

Firmware über DUP aktualisieren

Bevor Sie die Firmware über das Dell Update Package (DUP) aktualisieren, müssen Sie Folgendes sicherstellen:

- Installieren und aktivieren Sie die IPMI und die Treiber des verwalteten Systems.
- Aktivieren und starten Sie den Windows-Verwaltungsinstrumentationsdienst (WMI), wenn Ihr System auf einem Windows-Betriebssystem läuft.

  ANMERKUNG: Während Sie die iDRAC-Firmware über das DUP-Dienstprogramm für Linux aktualisieren und Fehlermeldungen wie `usb 5-2: device descriptor read/64, error -71` auf der Konsole angezeigt werden, können Sie diese Fehlermeldungen ignorieren.
- Wenn auf dem System der ESX-Hypervisor installiert ist, müssen Sie für das Ausführen der DUP-Datei sicherstellen, dass der Dienst „usbarbitrator“ über den folgenden Befehl angehalten wird: `service usbarbitrator stop`

So aktualisieren Sie iDRAC über DUP:

1. Laden Sie das DUP-Dienstprogramm auf der Basis des installierten Betriebssystems herunter, und führen Sie es auf dem Managed System aus.
2. Führen Sie DUP aus.
   Die Firmware wurde aktualisiert. Ein Systemneustart ist nicht erforderlich, nachdem die Firmware-Aktualisierung abgeschlossen ist.

Firmware über Remote-RACADM aktualisieren

1. Laden Sie das Firmware-Image auf den TFTP oder einen FTP-Server herunter. Beispiel: C:\downloads\firmimg.d7
2. Führen Sie den folgenden RACADM-Befehl aus:
   TFTP-Server:
   - Unter Verwendung des Befehls **fwupdate**:
     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate -g -u -a <path>
     ```
     path der Speicherort auf dem TFTP-Server, auf dem **firmimg.d7** gespeichert ist.
   - Unter Verwendung des Befehls **update**:
     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
     ```

   FTP-Server

- Unter Verwendung des Befehls **fwupdate**:

```
racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate -f <ftpserver IP>
<ftpserver username> <ftpserver password> -d <path>
```

path der Speicherort auf dem FTP-Server, auf dem **firmimg.d7** gespeichert ist.

- Unter Verwendung des Befehls **update**:

```
racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
```

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Firmware über die Lifecycle-Controller-Remote-Dienste aktualisieren

Für Informationen zur Aktualisierung der Firmware unter Verwendung von Lifecycle Controller–Remote-Dienste siehe *Lifecycle Controller Remote Services Quick Start Guide* (Lifecycle-Controller Remote-Dienste –Schnellstarthandbuch) unter **dell.com/idracmanuals**.

Aktualisieren der CMC-Firmware über iDRAC

Bei PowerEdge FX2-/FX2s-Gehäusen können Sie die Firmware für den Chassis Management Controller und alle Komponenten aktualisieren, die von CMC aktualisiert und über die Server von iDRAC aus freigegeben werden können.

Bevor Sie die Aktualisierung anwenden, stellen Sie Folgendes sicher:

- Server dürfen nicht durch CMC eingeschaltet werden.
- Gehäuse mit LCD müssen die folgende Meldung anzeigen: „Die Aktualisierung von <Name der Komponente> läuft“.
- Gehäuse ohne LCD müssen den Aktualisierungsvorgang durch Blinken eines LED-Musters anzeigen.
- Während der Aktualisierung sind die Gehäuse-Aktionsstrombefehle deaktiviert.

Die Aktualisierungen für Komponenten wie Programmable System-on-Chip (PSoC) von EAM, die erfordern, dass alle Server im Ruhezustand sind, werden beim nächsten Aus- und Einschaltvorgang des Gehäuses angewandt.

CMC-Einstellungen zur Aktualisierung der iDRAC-Firmware über iDRAC

Führen Sie bei PowerEdge FX2-/FX2s-Gehäusen vor der Firmware-Aktualisierung über iDRAC für CMC und dessen freigegebenen Komponenten die folgenden Schritte aus:

1 Starten der CMC-Webschnittstelle
2 Wechseln Sie zu **Gehäuseübersicht** > **Setup** > **Allgemeines**.
3 Wählen Sie aus dem Dropdown-Menü **Chassis Management in Servermodus** den Eintrag **Verwalten und Überwachen** aus und klicken Sie auf **Anwenden**.

iDRAC-Einstellungen zur Aktualisierung der CMC-Firmware

Nehmen Sie bei FX2-/FX2s-Gehäusen vor der Aktualisierung der Firmware für CMS und dessen freigegebener Komponenten über iDRAC die folgenden Einstellungen in iDRAC vor:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Aktualisieren und Rollback** > **Einstellungen**
Daraufhin wird die Seite **Firmware-Aktualisierungseinstellungen für den Chassis Management Controller** angezeigt.
2 Wählen Sie für **CMC-Aktualisierungen über das BS und Lifecycle Controller zulassen**, und wählen Sie **Aktiviert** aus, um die CMC-Firmware-Aktualisierung über iDRAC zu aktivieren.

3 Stellen Sie unter **Aktuelle CMC-Einstellung** sicher, dass die Option **Gehäuseverwaltung im Servermodus Verwalten und überwachen** anzeigt. Sie können dies im CMC ändern.

Anzeigen und Verwalten von gestuften Aktualisierungen

Sie können die geplanten Aufgaben anzeigen und löschen, einschließlich der Konfiguration und Aktualisierung von Aufgaben. Dies ist eine lizenzierte Funktion. Alle Aufgaben, die in der Warteschlange sind und während des nächsten Neustarts ausgeführt werden sollen, können gelöscht werden.

Zugehöriger Link

Aktualisieren der Gerätefirmware

Anzeigen und Verwalten gestufter Aktualisierungen unter Verwendung der iDRAC Webschnittstelle

Zum Anzeigen der geplanten Aufgaben unter Verwendung der iDRAC Webschnittstelle, gehen Sie zu **Übersicht** > **Server** > **Job-Warteschlange**. Die Seite **Job-Warteschlange** zeigt den Status der Jobs in der Job-Warteschlange des Lifecycle Controllers an. Für mehr Informationen zu den angezeigten Feldern siehe die *iDRAC Online-Hilfe*.

Um einen oder mehrere Jobs zu löschen, wählen Sie einen oder mehrere Jobs aus und klicken Sie auf **Löschen**. Die Seite wird neu geladen und der ausgewählte Job wird aus der Jobwarteschleife von Lifecycle Controller entfernt. Sie können alle Jobs in der Warteschleife löschen, die während des nächsten Systemstarts ausgeführt werden sollen. Sie können keine aktiven Jobs mit dem Status *Wird ausgeführt* oder *Wird heruntergeladen* löschen.

Sie müssen die Berechtigung „Serversteuerung“ besitzen, um Jobs löschen zu können.

Anzeigen und Verwalten gestufter Aktualisierungen unter Verwendung von RACADM

Zur Anzeige der gestuften Aktualisierungen unter Verwendung von RACADM verwenden Sie den Unterbefehl **jobqueue**. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)*, das unter **dell.com/idracmanuals** verfügbar ist.

Rollback der Geräte-Firmware durchführen

Sie können die Firmware für iDRAC oder für ein anderes von Lifecycle Controller unterstütztes Gerät zurücksetzen, auch wenn die Aktualisierung zuvor über eine andere Schnittstelle durchgeführt wurde. Beispiel: Wenn die Aktualisierung über die GUI von Lifecycle Controller durchgeführt wurde, können Sie ein Rollback der Firmware über die iDRAC-Webschnittstelle zurücksetzen. Sie können die Firmware für mehrere Geräte gleichzeitig im Rahmen eines Systemneustarts zurücksetzen.

Auf Dell PowerEdge-Servern der 13. Generation, die über einen einzelnen iDRAC und Lifecycle Controller-Firmware verfügen, wird beim Zurücksetzen der iDRAC-Firmware außerdem ein Rollback der Lifecycle Controller-Firmware durchgeführt. Auf einem PowerEdge-Server der 12. Generation mit der Firmware Version 2.*xx.xx.xx* wird durch ein Rollback von iDRAC auf eine frühere Version wie z. B. 1.*xx.xx* kein Rollback der Lifecycle-Controller-Firmware-Version durchgeführt. Es wird empfohlen, dass Sie nach dem Zurücksetzen des iDRAC ein Rollback auf eine frühere Version des Lifecycle Controllers durchführen.

ANMERKUNG: Auf einem PowerEdge-Server der 12. Generation mit der Firmware Version 2.10.10.10 kann ohne Zurücksetzen des iDRAC kein Rollback des Lifecycle Controllers auf1.*xx.xx* durchgeführt werden. Setzen Sie den iDRAC zuerst auf die Version 1.*xx.xx* zurück; erst dann können Sie ein Rollback des Lifecycle Controllers durchführen.

Es wird empfohlen, die Firmware auf dem neuesten Stand zu halten, um sicherzustellen, dass Sie über die neuesten Funktionen und Sicherheitsaktualisierungen verfügen. Sie müssen eventuell ein Rollback eines Updates durchführen oder eine frühere Version installieren, falls nach einer Aktualisierung Probleme auftreten. Um eine frühere Version zu installieren, verwenden Sie Lifecycle Controller, um nach Aktualisierungen zu suchen und die Version auszuwählen, die installiert werden soll.

Sie können die Firmware der folgenden Komponenten zurücksetzen:

- iDRAC mit Lifecycle Controller
- BIOS
- Netzwerkschnittstellenkarte (NIC)
- Netzteileinheit (PSU)
- RAID-Controller
- Rückwandplatine

ANMERKUNG: Für das Diagnoseprogramm, Treiberpakete und CPLD kann die Firmware nicht zurückgesetzt werden.

Stellen Sie vor dem Zurücksetzen der Firmware Folgendes sicher:

- Sie verfügen über Konfigurationsberechtigungen zum Zurücksetzen der iDRAC-Firmware.
- Sie verfügen über Serversteuerungsberechtigungen und haben Lifecycle Controller für das Zurücksetzen der Firmware für andere Geräte als den iDRAC aktiviert.
- Ändern Sie den NIC-Modus auf **Dediziert**, wenn der Modus als **Gemeinsam genutztes LOM** eingestellt wurde.

Sie können ein Rollback der Firmware auf die zuvor installierte Version über eines der folgenden Verfahren ausführen:

- iDRAC-Web-Schnittstelle
- CMC-Webschnittstelle
- RACADM CLI – iDRAC und CMC
- Lifecycle-Controller-GUI
- Lifecycle Controller-Remote-Dienste

Zugehöriger Link

Rollback für die Firmware über die iDRAC-Webschnittstelle durchführen
Rollback der Firmware über die CMC-Web-Schnittstelle durchführen
Rollback der Firmware über RACADM durchführen
Rollback der Firmware über Lifecycle-Controller durchführen
Rollback der Firmware über die Remote-Dienste für den Lifecycle Controller durchführen

Rollback für die Firmware über die iDRAC-Webschnittstelle durchführen

So führen Sie einen Rollback der Geräte-Firmware aus:

1. Wechseln Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Aktualisierung und Rollback** > **Rollback**.
   Alle Geräte, deren Firmware zurückgesetzt werden kann, werden auf der Seite **Rollback** angezeigt. Sie können den Gerätenamen, die zugehörigen Geräte, die derzeit installierte Firmware-Version und die verfügbare Firmware-Version, auf die zurückgesetzt werden soll, anzeigen.
2. Wählen Sie eines oder mehrere Geräte aus, für die Sie einen Firmware-Rollback ausführen möchten.
3. Auf Grundlage der ausgewählten Geräten klicken Sie auf **Installieren und neu starten** oder auf **Beim nächsten Systemstart installieren**. Wenn nur iDRAC ausgewählt ist, klicken Sie auf **Installieren**.
   Wenn Sie auf **Installieren und Neustart** oder **Beim nächsten Systemstart installieren** klicken, wird die Meldung „Aktualisierung der Jobwarteschlange“ angezeigt.
4. Klicken Sie auf **Job-Warteschlange**.

Die Seite **Job-Warteschlangen** wird angezeigt, auf der Sie die bereitgestellten Firmware-Aktualisierungen anzeigen und verwalten können.

ANMERKUNG:

- Wenn Sie sich im Rollback-Modus befinden, wird der Rollback-Vorgang auch dann im Hintergrund fortgesetzt, wenn Sie zu einer anderen Seite wechseln.

In folgenden Fällen wird eine Fehlermeldung angezeigt:

- Sie verfügen nicht über die erforderliche Serversteuerungsberechtigung zum Zurücksetzen der Firmware für andere Geräte als den iDRAC, oder Sie verfügen nicht über die erforderliche Konfigurationsberechtigung zum Zurücksetzen der iDRAC-Firmware.
- Die Firmware wird bereits in einer anderen Sitzung zurückgesetzt.
- Es wurden Aktualisierungen zur Ausführung bereitgestellt oder sie werden bereits ausgeführt.

Wenn Lifecycle Controller deaktiviert ist oder sich im Wiederherstellungszustand befindet und Sie versuchen, die Firmware für ein anderes Gerät als iDRAC zurückzusetzen, wird eine Warnmeldung mit Hinweisen zum Aktivieren von Lifecycle-Controller angezeigt.

Rollback der Firmware über die CMC-Web-Schnittstelle durchführen

So führen Sie ein Rollback über die CMC-Web-Schnittstelle durch:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Gehen Sie zu **Server-Übersicht** > **<Server-Name>**.
   Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf **iDRAC starten**, und führen Sie den Geräte-Firmware-Rollback gemäß Abschnitt Rollback für die Firmware über die iDRAC-Webschnittstelle durchführen aus.

Rollback der Firmware über RACADM durchführen

1. Überprüfen Sie den Status von Rollback-Vorgang und FQDD mit dem Befehl `swinventory`:
   ```
   racadm swinventory
   ```
   Für das Gerät, für das Sie den Firmware-Rollback ausführen möchten, muss die `Rollback Version` den Status `Available` (Verfügbar) aufweisen. Notieren Sie gleichfalls die FQDD.
2. Führen Sie den Rollback der Geräte-Firmware mithilfe des folgenden Befehls aus:
   ```
   racadm rollback <FQDD>
   ```
   Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* unter **dell.com/idracmanuals**.

Rollback der Firmware über Lifecycle-Controller durchführen

Weitere Informationen finden Sie im *Lifecycle-Controller User's Guide* (Lifecycle-Controller Benutzerhandbuch) unter **dell.com/idracmanuals**.

Rollback der Firmware über die Remote-Dienste für den Lifecycle Controller durchführen

Informationen finden Sie im *Lifecycle Controller Remote Services Quick Start Guide* (Lifecycle-Controller Remote-Dienste – Schnellstarthandbuch) unter **dell.com/idracmanuals**.

iDRAC wiederherstellen

iDRAC unterstützt zwei Betriebssystem-Images, um ein startfähiges iDRAC sicherzustellen. Gehen Sie bei einem nicht vorhersehbaren Fehler mit schwerwiegenden Folgen und dem Verlust der beiden Startpfade wie folgt vor:

- Der iDRAC-Bootloader erkennt, dass kein startfähiges Image vorhanden ist.
- Die Systemzustands- und Identifizierungs-LED leuchtet etwa im Halbsekundentakt auf. (Die LED befindet sich auf der Rückseite von Rack- und Tower-Systemen sowie auf der Vorderseite eines Blade-Servers.)
- Der Bootloader fragt den SD-Kartensteckplatz ab.
- Formatieren Sie eine SD-Karte mit FAT über ein Windows-Betriebssystem oder EXT3 über ein Linux-Betriebssystem.
- Kopieren Sie das Image **firmimg.d7** auf die SD-Karte.
- Legen Sie die SD-Karte in den Server ein.
- Bootloader erkennt die SD-Karte, schaltet die blinkende LED auf eine dauerhaft gelbe Anzeige, liest das Image „firmimg.d7“, programmiert iDRAC um und startet iDRAC neu.

TFTP-Server verwenden

Sie können den Trivial File Transfer Protocol (TFTP)-Server zum Hoch- und Herunterstufen der iDRAC-Firmware oder zum Installieren von Zertifikaten verwenden. Er wird in den SM-CLP and RACADM-Befehlszeilenschnittstellen verwendet, um Dateien von und nach iDRAC zu übertragen. Der Zugriff auf den TFTP-Server muss über eine iDRAC-IP-Adresse oder einen DNS-Namen aktiviert werden.

ANMERKUNG: Wenn Sie die iDRAC-Webschnittstelle zum Übertragen von Zertifikaten und zum Aktualisieren der Firmware verwenden, wird der TFTP-Server nicht benötigt.

Sie können den Befehl `netstat -a` auf Windows- oder Linux-Betriebssystemen verwenden, um zu ermitteln, ob ein TFTP-Server ausgeführt wird. Die Standardschnittstelle für TFTP ist 69. Wenn der TFTP-Server nicht ausgeführt wird, führen Sie einen der folgenden Schritte aus:

- Suchen Sie im Netzwerk, in dem ein TFTP-Dienst ausgeführt wird, einen anderen Computer.
- Installieren Sie einen TFTP-Server auf dem Betriebssystem.

Sichern von Serverprofilen

Sie können die Systemkonfiguration, einschließlich der installierten Firmware-Images auf verschiedenen Komponenten wie BIOS, RAID, NIC, iDRAC, Lifecycle Controller und Network Daughter Cards (NDCs) sowie die Konfigurationseinstellungen dieser Komponenten sichern. Der Sicherungsvorgang umfasst außerdem die Konfigurationsdaten von Festplatte, Hauptplatine und Ersatzteilen. Die Sicherung erstellt eine einzelne Datei, die Sie auf einer vFlash-SD-Karte oder auf der Netzwerkfreigabe (CIFS oder NFS) speichern können.

Sie haben außerdem die Möglichkeit, periodische Backups der Firmware und der Serverkonfiguration auf täglicher, wöchentlicher oder monatlicher Basis zu aktivieren und zu planen.

Die Backup-Funktion ist lizenziert und mit der iDRAC Enterprise-Lizenz verfügbar.

ANMERKUNG: Bei Servern der 13. Generation ist diese Funktion automatisch aktiviert.

Stellen Sie vor Durchführen eines Sicherungsvorgang Folgendes sicher:

- Die Option zur Systembestandsaufnahme bei Neustart (Collect Inventory On Restart, CSIOR) ist aktiviert. Wenn Sie einen Backup-Vorgang einleiten, während CSIOR deaktiviert ist, wird die folgende Meldung angezeigt:

  ```
  System Inventory with iDRAC may be stale,start CSIOR for updated inventory
  ```
- So führen Sie eine Sicherung auf einer vFlash-SD-Karte aus:
  - Die vFlash-SD-Karte ist eingelegt, aktiviert und initialisiert.
  - Die vFlash-SD-Karte verfügt über mindestens 100 MB freien Speicherplatz zur Speicherung der Sicherungsdatei.

Die Sicherungsdatei enthält verschlüsselte, sensible Benutzerdaten, Konfigurationsinformationen und Firmware-Abbilder, die Sie für den Serverprofil-Import nutzen können.

Backup-Ereignisse werden im Lifecycle-Protokoll aufgezeichnet.

Zugehöriger Link

Planen der automatischen Server-Profil-Sicherung
Importieren von Serverprofilen

Sichern des Serverprofils unter Verwendung der iDRAC-Webschnittstelle

So sichern Sie das Serverprofil mithilfe der iDRAC-Webschnittstelle:

1 Gehen Sie zu **Übersicht** > **iDRAC-Einstellungen** > **Serverprofile**.

Die Seite **Backup und Exportieren eines Serverprofils** wird angezeigt.

2 Wählen Sie eine der folgenden Optionen aus, um das Sicherungsdatei-Image zu speichern:
- **Netzwerk**, um das Sicherungsdatei-Abbild auf einer CIFS- oder NFS-Freigabe zu speichern.
- **vFlash** zum Speichern der Sicherungs-Abbild-Datei auf der vFlash-Karte.

3 Geben Sie Name und Verschlüsselungspassphrase (optional) der Sicherungsdatei ein.

4 Wenn als Speicherort der Datei **Netzwerk** ausgewählt wird, geben Sie die Netzwerkeinstellungen ein.

> **ANMERKUNG: Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen.**

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

5 Klicken Sie auf **Jetzt sichern**.

Der Backup-Vorgang wird initiiert und Sie können den Status auf der Seite **Job-Warteschlange** anzeigen. Nach einem erfolgreichen Vorgang wird die Sicherungsdatei am angegebenen Ort gespeichert.

Sichern des Serverprofils unter Verwendung von RACADM

Um das Serverprofil mithilfe von RACADM zu sichern, verwenden Sie den Befehl **systemconfig backup**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Planen der automatischen Server-Profil-Sicherung

Sie haben die Möglichkeit, periodische Backups der Firmware und der Serverkonfiguration auf täglicher, wöchentlicher oder monatlicher Basis zu aktivieren und zu planen.

Bevor Sie automatische Sicherungen von Serverprofilen planen, stellen Sie Folgendes sicher:

- Die Optionen Lifecycle Controller und Collect System Inventory On Reboot (CSIOR) sind aktiviert.
- Network Time Protocol (NTP, Netzwerkzeitprotokoll) ist aktiviert, so dass Zeitverschiebungen keine Auswirkung auf die tatsächlichen Zeiten geplanter Jobs und auf den Erstellungszeitpunkt des nächsten geplanten Jobs haben.
- So führen Sie eine Sicherung auf einer vFlash-SD-Karte aus:
  - Eine von Dell unterstützte vFlash-SD-Karte ist eingelegt und initialisiert.
  - Die vFlash-SD-Karte verfügt über ausreichend Speicherplatz zur Speicherung der Sicherungsdatei.

ANMERKUNG: Die IPv6-Adresse wird bei der Planung automatischer Serverprofil-Sicherungen nicht unterstützt.

Planung automatischer Backup-Server-Profile mithilfe der Webschnittstelle

So planen Sie eine automatische Sicherung des Serverprofils:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Serverprofil**.
   Die Seite **Backup und Exportieren eines Serverprofils** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Automatische Sicherung**.
3. Wählen Sie die Option **Automatische Sicherung aktivieren** aus.
4. Wählen Sie eine der folgenden Optionen aus, um das Sicherungsdatei-Image zu speichern:
   - **Netzwerk**, um das Sicherungsdatei-Abbild auf einer CIFS- oder NFS-Freigabe zu speichern.
   - **vFlash** zum Speichern der Sicherungs-Abbild-Datei auf der vFlash-Karte.
5. Geben Sie Name und Verschlüsselungspassphrase (optional) der Sicherungsdatei ein.
6. Wenn als Speicherort der Datei **Netzwerk** ausgewählt wird, geben Sie die Netzwerkeinstellungen ein.

   ANMERKUNG: Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen.

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
7. Geben Sie im Bereich **Sicherungszeitplan** die Startzeit für die Sicherung und die Häufigkeit der Sicherung (täglich, wöchentlich oder monatlich) ein.
   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
8. Klicken Sie auf **Sicherung planen**.
   Ein wiederkehrender Job wird in der Job-Warteschlange mit Startdatum und Uhrzeit des nächsten geplanten Sicherungsvorgangs dargestellt. Fünf Minuten, nachdem die erste Instanz des wiederkehrenden Jobs begonnen hat, wird der Job für den nächsten Zeitraum erstellt. Der Sicherungsvorgang des Serverprofils wird zum geplanten Datum und Uhrzeit ausgeführt.

Planung automatischen Backup-Server-Profile unter Verwendung von RACADM

Verwenden Sie zum Aktivieren automatischer Sicherungen den folgenden Befehl:

```
racadm set lifecyclecontroller.lcattributes.autobackup Enabled
```

So planen Sie eine Sicherung des Serverprofils:

```
racadm systemconfig backup -f <filename> <target> [-n <passphrase>] -time <hh:mm> -dom
<1-28,L,'*'> -dow<*,Sun-Sat> -wom <1-4, L,'*'> -rp  <1-366>-mb <Max Backups>
```

So zeigen Sie den aktuellen Backup-Plan an:

```
racadm systemconfig getbackupscheduler
```

Verwenden Sie zum Deaktivieren automatischer Sicherungen den folgenden Befehl:

```
racadm set LifeCycleController.lcattributes.autobackup Disabled
```

So löschen Sie den Sicherungszeitplan:

```
racadm systemconfig clearbackupscheduler
```

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Importieren von Serverprofilen

Sie können die Backup-Imagedatei zum Importieren (oder Wiederherstellen) der Konfiguration und Firmware für denselben Server verwenden, ohne den Server neu zu starten.

Importfunktion ist nicht lizenziert.

ANMERKUNG: Für den Wiederherstellungsvorgang müssen der Service-Tag und der Service-Tag in der Sicherungsdatei identisch sein. Der Wiederherstellungsvorgang gilt für alle Systemkomponenten, die gleich sind und sich am gleichen Ort oder Steckplatz, wie in der Sicherungsdatei festgehalten, befinden. Wenn sich Komponenten unterscheiden oder sich nicht am gleichen Ort befinden, werden sie nicht modifiziert und im Lifecycle-Protokoll werden Wiederherstellungsfehler protokolliert.

Vor der Ausführung eines Importvorgangs achten Sie darauf, dass Lifecycle Controller aktiviert ist. Falls Lifecycle Controller deaktiviert ist und Sie einen Importvorgang starten, wird die folgende Meldung angezeigt:

```
Lifecycle Controller is not enabled, cannot create Configuration job.
```

Sollte bereits ein Import durchgeführt und gleichzeitig ein neuer Importvorgang gestartet werden, wird die folgende Fehlermeldung angezeigt:

```
Restore is already running
```

Importereignisse werden im Lifecycle-Protokoll aufgezeichnet.

Easy Restore (Einfache Wiederherstellung)

ANMERKUNG: Einfache Wiederherstellung steht nur auf PowerEdge-Servern der 13. Generation zur Verfügung, die mit Easy Restore Flash-Speicher ausgestattet sind. Einfache Wiederherstellung ist nicht verfügbar auf PowerEdge R930.

Nach dem Ersetzen der Hauptplatine auf Ihrem Server ermöglicht Easy Restore (einfache Wiederherstellung) Ihnen die automatische Wiederherstellung der folgenden Daten:

- System-Service-Tag-Nummer
- Lizenzdaten
- UEFI Diagnoseanwendung
- Systemkonfigurationseinstellungen-– BIOS, iDRAC und NIC

Einfache Wiederherstellung verwendet den Easy Restore Flash-Speicher, um die Daten zu sichern. Wenn Sie die Hauptplatine ersetzen und das System einschalten, fragt das BIOS die iDRAC ab und fordert Sie zur Wiederherstellung der gesicherten Daten auf. Der erste BIOS-Bildschirm fordert Sie dazu auf, die Service-Tag -Nummer, Lizenzen und UEFI-Diagnose-Anwendung wiederherzustellen. Der zweite BIOS-Bildschirm fordert Sie dazu auf, Systemkonfigurationseinstellungen wiederherzustellen. Wenn Sie sich dazu entscheiden, im ersten BIOS-Bildschirm keine Daten wiederherzustellen, und wenn Sie die Service-Tag-Nummer nicht durch eine andere Methode einstellen, wird der erste BIOS-Bildschirm wieder angezeigt. Der zweite BIOS-Bildschirm wird nur einmal angezeigt.

ANMERKUNG:

- Systemkonfigurationseinstellungen werden nur gesichert, wenn CSIOR aktiviert ist. Stellen Sie sicher, dass Lifecycle Controller und CSIOR aktiviert sind.
- Löschen des Systems löscht nicht die Daten aus dem Easy Restore Flash-Speicher.
- Einfache Wiederherstellung sichert keine anderen Daten als die Firmware-Images, vFlash-Daten oder Add-In-Karten Daten.

Zugehöriger Link

Sequenz für den Wiederherstellungsvorgang

Importieren des Serverprofils mithilfe der iDRAC-Webschnittstelle

So importieren Sie das Serverprofil mithilfe der iDRAC-Webschnittstelle:

1 Gehen Sie zu **Übersicht** > **iDRAC-Einstellungen** > **Serverprofil** > **Import**.

Die Seite **Serverprofil importieren** wird angezeigt.

2 Wählen Sie eine der folgenden Optionen, um den Speicherort der Sicherungsdatei anzugeben:

- **Netzwerk**
- **vFlash**

3 Geben Sie Name und Entschlüsselungspassphrase (optional) der Sicherungsdatei ein.

4 Wenn als Speicherort der Datei **Netzwerk** ausgewählt wird, geben Sie die Netzwerkeinstellungen ein.

ANMERKUNG: Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen.

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

5 Wählen Sie eine der folgenden Optionen für die **Konfiguration der virtuellen Laufwerke und Festplatten-Daten**:

- **Bewahren** - Bewahrt die RAID-Ebene, virtuelle Laufwerke, Controller-Attribute und Festplattendaten im System auf und bringt das System mit Hilfe der Backup-Abbild-Datei auf einen zuvor bekannten Zustand zurück.
- **Löschen und ersetzen** - Löscht die RAID-Stufe, virtuelle Laufwerke, Controller-Attribute und Festplattenkonfigurationsdaten im System und ersetzt sie durch die Daten aus der Backup-Abbild-Datei.

6 Klicken Sie auf **Importieren**.

Der Import von Serverprofilen wird gestartet.

Wiederherstellen des Serverprofils unter Verwendung von RACADM

Zum Importieren des Serverprofils mithilfe von RACADM verwenden Sie den den Befehl **systemconfig restore**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Sequenz für den Wiederherstellungsvorgang

Die Sequenz für den Wiederherstellungsvorgang sieht wie folgt aus:

1 Das Host-System fährt herunter.

2 Die Informationen aus der Sicherheitsdatei werden zur Wiederherstellung des Lifecycle-Controllers verwendet.

3 Das Host-System wird eingeschaltet.

4 Der Wiederherstellungsprozess von Firmware und Konfiguration für das Gerät wird abgeschlossen.
5 Das Host-System fährt herunter.
6 Der Wiederherstellungsprozess von iDRAC-Firmware und Konfiguration wird abgeschlossen.
7 Der iDRAC startet neu.
8 Das wiederhergestellte Host-System wird eingeschaltet, um den Normalbetrieb wiederaufzunehmen.

iDRAC über andere Systemverwaltungs-Tools überwachen

Sie können iDRAC über Dell Management Console und Dell OpenManage Essentials entdecken und überwachen. Sie können außerdem das Dell Remote Access Configuration Tool (DRACT) verwenden, um iDRACs zu entdecken, die Firmware zu aktualisieren und Active Directory einzurichten. Weitere Informationen finden Sie in den jeweiligen Benutzerhandbüchern.

4

iDRAC konfigurieren

Mit iDRAC können Sie iDRAC-Eigenschaften konfigurieren, Benutzer einrichten und Warnungen für die Ausführung von Remote-Verwaltungsaufgaben einrichten.

Stellen Sie vor der Konfiguration von iDRAC sicher, dass die iDRAC-Netzwerkeinstellungen und ein unterstützter Browser konfiguriert und die erforderlichen Lizenzen aktualisiert sind. Weitere Informationen zu den lizenzierbaren Funktionen in iDRAC finden Sie unter Lizenzen verwalten.

Sie können iDRAC über die folgenden Komponenten konfigurieren:

- iDRAC-Web-Schnittstelle
- RACADM
- Remote-Dienste (siehe *Dell Lifecycle Controller Remote Services-Benutzerhandbuch*)
- IPMITool (siehe *Benutzerhandbuch zu den Dienstprogrammen des Dell OpenManage Baseboard Management Controller*)

So konfigurieren Sie iDRAC:

1 Melden Sie sich bei iDRAC an.
2 Ändern der Netzwerkeinstellungen falls erforderlich.

> **ANMERKUNG: Wenn Sie die iDRAC-Netzwerkeinstellungen während der Einrichtung der iDRAC-IP-Adresse über das Dienstprogramm für die iDRAC-Einstellungen konfiguriert haben, können Sie diesen Schritt übergehen.**

3 Konfigurieren Sie Schnittstellen für den Zugriff auf iDRAC.
4 Konfigurieren Sie die Anzeige auf der Frontblende.
5 Konfigurieren Sie ggf. den Systemstandort.
6 Konfigurieren Sie ggf. Zeitzone und Network Time Protocol (NTP).
7 Bauen Sie eine der folgenden alternativen Verfahren für die Kommunikation mit iDRAC auf:
   - Serielle IPMI- oder RAC-Verbindung
   - Serielle IPMI-Verbindung über LAN
   - IPMI über LAN
   - SSH- oder Telnet-Client
8 Erforderliche Zertifikate abrufen.
9 Hinzufügen und Konfiguration von iDRAC-Benutzern mit Berechtigungen.
10 Konfigurieren und aktivieren Sie E-Mail-Warnungen, SNMP-Traps oder IPMI-Warnungen.
11 Einrichten der Strombegrenzungsrichtlinie falls erforderlich.
12 Bildschirm des letzten Systemabsturzes anzeigen
13 Konfigurieren Sie ggf. die virtuelle Konsole und die virtuellen Datenträger.
14 Konfigurieren Sie ggf. die vFlash SD-Karte.
15 Richten Sie ggf. das erste Startlaufwerk ein.
16 Stellen Sie das Betriebssystem ggf. auf iDRAC-Passthrough.

Themen:

- Modus FIPS (Konfiguration)
- Dienste konfigurieren
- Verwenden des VNC-Client für die Remote-Server-Verwaltung
- Anzeige auf der Frontblende konfigurieren
- Das Konfigurieren von Zeitzone und NTP
- Erstes Startlaufwerk einstellen
- Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough
- Zertifikate abrufen
- Mehrere iDRACs über RACADM konfigurieren
- Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen auf einem Host-System deaktivieren

Zugehöriger Link

Anmelden bei iDRAC
Netzwerkeinstellungen ändern
Dienste konfigurieren
Anzeige auf der Frontblende konfigurieren
Standort für das Managed System einrichten
Das Konfigurieren von Zeitzone und NTP
Einrichten der iDRAC-Kommunikation
Benutzerkonten und Berechtigungen konfigurieren
Stromversorgung überwachen und verwalten
Bildschirm „Letzter Absturz“ aktivieren
Virtuelle Konsole konfigurieren und verwenden
Virtuelle Datenträger verwalten
vFlash SD-Karte verwalten
Erstes Startlaufwerk einstellen
Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough
iDRAC für das Versenden von Warnungen konfigurieren

iDRAC-Informationen anzeigen

Sie können die iDRAC-Basiseigenschaften anzeigen.

iDRAC-Informationen über die Webschnittstelle anzeigen

Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Eigenschaften**, um die folgenden Informationen in Bezug auf iDRAC anzuzeigen. Weitere Informationen zu den Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

- Hardware- und Firmware-Version
- Letzte Firmware-Aktualisierung
- RAC-Uhrzeit
- IPMI-Version
- Informationen über die Benutzerschnittstelle in der Titelleiste
- Netzwerkeinstellungen
- IPv4-Einstellungen
- IPv6-Einstellungen

iDRAC-Informationen über RACADM anzeigen

Weitere Informationen zum Anzeigen von iDRAC-Informationen über RACADM finden Sie in den Unterbefehlen `getsysinfo` oder `get` im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Netzwerkeinstellungen ändern

Nach der Konfiguration der iDRAC7-Netzwerkeinstellungen über das Dienstprogramm für die iDRAC-Einstellungen können Sie auch die Einstellungen über die iDRAC-Web-Schnittstelle, über RACADM, über den Lifecycle-Controller, über das Dell Deployment Toolkit und (nach dem Starten des Betriebssystems) über Server Administrator ändern. Weitere Informationen zu den Tools und den Berechtigungseinstellungen finden Sie in den entsprechenden Benutzerhandbüchern.

Zum Ändern der Netzwerkeinstellungen über die iDRAC-Web-Schnittstelle oder RACADM müssen Sie über Berechtigungen zum **Konfigurieren** verfügen.

ANMERKUNG: Durch das Ändern der Netzwerkeinstellungen werden möglicherweise die aktuellen Netzwerkverbindungen mit iDRAC beendet.

Netzwerkeinstellungen über die Web-Schnittstelle ändern

So ändern Sie die iDRAC-Netzwerkeinstellungen:

1 Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk**.
Die Seite **Netzwerk** wird angezeigt.

2 Geben Sie Netzwerkeinstellungen, allgemeine Einstellungen, IPv4, IPv6, IPMI und/oder VLAN-Einstellungen je nach Bedarf an und klicken Sie auf **Anwenden**.
Wenn Sie **Automatisch dedizierte NIC** unter **Netzwerkeinstellungen** auswählen, ändert iDRAC seine NIC-Auswahl zur Verwendung der dedizierte NIC, wenn bei ihm die NIC-Auswahl als freigegebenes LOM (1, 2, 3 oder 4) angegeben ist und ein Link auf der dedizierten NIC des iDRAC erkannt wird. Wird kein Link auf der dedizierten NIC erkannt, verwendet iDRAC das freigegebene LOM. Der Wechsel von freigegebener zu dedizierter Zeitüberschreitung dauert fünf Sekunden und von dedizierter zu freigegebener 30 Sekunden. Sie können diesen Zeitüberschreitungswert mithilfe von RACADM oder WS-MAN konfigurieren.

Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

Netzwerkeinstellungen über einen lokalen RACADM ändern

Um eine Liste verfügbarer Netzwerkeigenschaften zu erstellen, verwenden Sie den Befehl

```
racadm get iDRAC.Nic
```

Wenn DHCP zur Ermittlung einer IP-Adresse verwendet werden soll, kann der folgende Befehl zum Schreiben des Objekts DHCPEnable und zum Aktivieren dieser Funktion verwendet werden.

```
racadm set iDRAC.IPv4.DHCPEnable 1
```

Das folgende Beispiel zeigt, wie der Befehl zur Konfiguration benötigter LAN-Netzwerkeigenschaften verwendet werden kann:

```
racadm set iDRAC.Nic.Enable 1
racadm set iDRAC.IPv4.Address 192.168.0.120
racadm set iDRAC.IPv4.Netmask 255.255.255.0
racadm set iDRAC.IPv4.Gateway 192.168.0.120
```

```
racadm set iDRAC.IPv4.DHCPEnable 0
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNS1 192.168.0.5
racadm set iDRAC.IPv4.DNS2 192.168.0.6
racadm set iDRAC.Nic.DNSRegister 1
racadm set iDRAC.Nic.DNSRacName RAC-EK00002
racadm set iDRAC.Nic.DNSDomainFromDHCP 0
racadm set iDRAC.Nic.DNSDomainName MYDOMAIN
```

ANMERKUNG: Wenn iDRAC.Nic.Enable auf 0 gesetzt ist, wird das iDRAC-LAN selbst dann deaktiviert, wenn DHCP aktiviert ist.

IP-Filterung konfigurieren

Verwenden Sie neben der Benutzerauthentifizierung die folgenden Optionen für zusätzliche Sicherheit, während Sie auf iDRAC zugreifen:

- IP-Filterung beschränkt den IP-Adressbereich der Clients, die auf iDRAC zugreifen. Dabei wird die IP-Adresse einer eingehenden Anmeldung mit dem angegebenen Bereich verglichen, und der Zugang zu iDRAC wird nur über eine Management Station genehmigt, deren IP-Adresse sich innerhalb dieses Bereichs befindet. Alle anderen Anmeldeanfragen werden abgelehnt.
- Wenn fehlgeschlagene Anmeldeversuche von einer bestimmten IP-Adresse wiederholt auftreten, wird die Adresse für eine vorgewählte Zeitspanne daran gehindert, sich bei iDRAC anzumelden. Wenn Ihre Anmeldeversuche bis zu zwei Mal nicht erfolgreich sind, können Sie sich erst nach 30 Sekunden erneut anmelden. Wenn Ihre Anmeldeversuche mehr als zwei Mal nicht erfolgreich sind, können Sie sich erst nach 60 Sekunden erneut anmelden.

Wenn sich Anmeldefehler von einer spezifischen IP-Adresse aus ansammeln, werden sie durch einen internen Zähler registriert. Wenn sich der Benutzer erfolgreich anmeldet, wird die Aufzeichnung der Fehlversuche gelöscht und der interne Zähler zurückgesetzt.

ANMERKUNG: Wenn Anmeldeversuche von der Client-IP-Adresse abgelehnt werden, können einige SSH-Clients die Meldung anzeigen: `ssh exchange identification: Connection closed by remote host`.

ANMERKUNG: Wenn Sie das Dell Deployment Toolkit (DTK) verwenden, finden Sie weitere Informationen zu den Berechtigungen im *Dell Deployment Toolkit-Benutzerhandbuch*.

IP-Filterung über die iDRAC-Webschnittstelle konfigurieren

Sie müssen über Berechtigungen zum Konfigurieren verfügen, um diese Schritte auszuführen.

So konfigurieren Sie die IP-Filterung:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Netzwerk**.
   Die Seite **Netzwerk** wird angezeigt.
2. Klicken Sie auf **Erweiterte Einstellungen**.
   Die Seite **Netzwerksicherheit** wird angezeigt.
3. Geben Sie die IP-Filterungseinstellungen an.
   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

#IP-Filterung über RACADM konfigurieren

Sie müssen über Berechtigungen zum Konfigurieren verfügen, um diese Schritte auszuführen.

Verwenden Sie zum Konfigurieren der IP-Filterung die folgenden RACADM-Objekte in der Gruppe **iDRAC.IPBlocking**:

- RangeEnable
- RangeAddr
- RangeMask

Die Eigenschaft **RangeMask** wird sowohl auf die eingehende IP-Adresse als auch auf die **RangeAddr**-Eigenschaften angewendet. Sind die Ergebnisse identisch, wird für die eingehende Anmeldeaufforderung der Zugriff auf den iDRAC zugelassen. Anmeldung von IP-Adressen außerhalb dieses Bereichs führen zu einer Fehlermeldung.

Die Anmeldung wird fortgeführt, wenn der folgende Ausdruck Null entspricht:

```
RangeMask & (<incoming-IP-address> ^ RangeAddr)
```

&	Bitweise UND der Mengen
^	Bitweise ausschließliche ODER

Beispiele für die IP-Filterung

Die folgenden RACADM-Befehle blockieren alle IP-Adressen außer 192.168.0.57:

```
racadm set iDRAC.IPBlocking.RangeEnable 1
racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.57
racadm set iDRAC.IPBlocking.RangeMask 255.255.255.255
```

Zur Beschränkung von Anmeldungen auf einen Satz von vier angrenzenden IP-Adressen (z. B. 192.168.0.212 bis 192.168.0.215) wählen Sie alle außer den niederwertigsten zwei Bits in der Maske aus:

```
racadm set iDRAC.IPBlocking.RangeEnable 1
racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.212
racadm set iDRAC.IPBlocking.RangeMask 255.255.255.252
```

Das letzte Byte der Bereichsmaske ist auf 252 eingestellt, das Dezimaläquivalent von 11111100b.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Modus FIPS (Konfiguration)

FIPS ist ein Computer-Sicherheitsstandard, den USA-Regierungsbehörden und Vertragspartner verwenden müssen. Ab Version 2.40.40.40 iDRAC unterstützt iDRAC das Aktivieren des FIPS-Modus.

iDRAC wird offiziell zertifiziert zur Unterstützung des FIPS-Modus in der Zukunft.

Unterschied zwischen FIPS-Modus-unterstützt und FIPS-validiert

Software, die durch das Durchführen des „Cryptographic Module Validation Program“ (Kryptographisches Modul Validierungsprogramm) validiert wurde, bezeichnet man als FIPS-validiert. Aufgrund der Zeit, die für eine vollständige FIPS-Validierung benötigt wird, sind nicht alle Versionen von iDRAC bestätigt. Informationen zum aktuellen Status der FIPS-Validierung für iDRAC finden Sie auf der Seite „Cryptographic Module Validation Program“ (Kryptographisches Modul Validierungsprogramm) auf der NIST-Webseite.

FIPS-Modus aktivieren

VORSICHT: Das Aktivieren des FIPS-Modus setzt iDRAC auf die standardmäßigen Werkseinstellungen zurück. Wenn Sie die Einstellungen wiederherstellen möchten, sichern Sie das Server-Konfigurationsprofil (SCP) vor dem Aktivieren des FIPS-Modus und stellen das SCP nach dem Neustart von iDRAC wieder her.

ANMERKUNG: Wenn Sie Sie iDRAC-Firmware erneut installieren oder aktualisieren, wird der FIPS-Modus deaktiviert.

Aktivieren des FIPS-Modus unter Verwendung des Internets

1 Navigieren Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk**.
2 Klicken Sie auf **Erweiterte Einstellungen** neben **Optionen**.
3 Unter **FIPS-Modus** wählen Sie **Aktiviert** und klicken auf **Anwenden**.
4 Es wird eine Meldung angezeigt, in der Sie aufgefordert werden, die Änderung zu bestätigen. Klicken Sie auf **OK**.
iDRAC startet im FIPS-Modus neu. Warten Sie mindestens 60 Sekunden, bevor Sie erneut eine Verbindung zu iDRAC herstellen.
5 Installieren Sie ein vertrauenswürdiges Zertifikat für iDRAC.

ANMERKUNG: Das Standard-SSL-Zertifikat ist nicht zulässig im FIPS-Modus.

ANMERKUNG: Einige iDRAC-Schnittstellen, wie z. B. die standardmäßig konformen Implementierungen von IPMI und SNMP unterstützen keine FIPS-Übereinstimmung.

FIPS-Modus über RACADM aktivieren

Verwenden Sie RACADM-CLI, um den folgenden Befehl auszuführen:

```
racadm set iDRAC.Security.FIPSMode <Enable>
```

Deaktivieren des FIPS-Modus

Zum Deaktivieren des FIPS-Modus müssen Sie einen Reset von iDRAC auf die werksseitigen Voreinstellungen durchführen.

Dienste konfigurieren

Sie können die folgenden Dienste auf iDRAC konfigurieren und aktivieren:

Lokale Konfiguration	Deaktivieren Sie den Zugriff auf die iDRAC-Konfiguration (vom Host-System) über den lokalen RACADM und das Dienstprogramm für iDRAC-Einstellungen.
Webserver	Aktivieren Sie den Zugang zur iDRAC-Webschnittstelle. Wenn Sie die Webschnittstelle deaktivieren, wird auch Remote-RACADM deaktiviert. Verwenden Sie lokalen RACADM, um den Web-Server wieder und Remote-RACADM erneut zu aktivieren.
SSH	Greifen Sie über die Firmware-RACADM auf iDRAC zu.
Telnet	Greifen Sie über die Firmware-RACADM auf iDRAC zu.
Remote-RACADM	Greifen Sie remote auf iDRAC zu.
Redfish	Aktiviert Unterstützung für Redfish RESTful-API.
SNMP-Agent	Aktiviert Unterstützung für SNMP-Anfragen (GET-, GETNEXT- und GETBULK-Vorgänge) in iDRAC.
Automatisierte Systemwiederherstellung/Agent	Aktivieren Sie den Bildschirm „Letzter Systemabsturz“.
VNC-Server	Aktivieren Sie VNC-Server mit oder ohne SSL-Verschlüsselung.

Services unter Verwendung der Webschnittstelle konfigurieren

Dienste über die iDRAC-Web-Schnittstelle konfigurieren:

1 Gehen Sie in der iDRAC-Web-Schnittstelle zu**Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Dienste**.
Die Seite **Dienste** wird angezeigt.

2 Geben Sie die erforderlichen Informationen ein und klicken Sie auf **Anwenden**.
Weitere Informationen zu den verschiedenen Einstellungen finden Sie in der *iDRAC-Online-Hilfe*.

ANMERKUNG: Aktivieren Sie nicht das Kontrollkästchen Verhindern, dass diese Seite zusätzliche Dialoge erstellt. Die Auswahl dieser Option verhindert, dass Sie Dienste konfigurieren können.

Dienste über RACADM konfigurieren

Um Dienste über RACADM zu aktivieren und konfigurieren, verwenden Sie den Befehl **set** mit den Objekten in den folgenden Objektgruppen:

- iDRAC.LocalSecurity
- iDRAC.LocalSecurity
- iDRAC.SSH
- iDRAC.Webserver
- iDRAC.Telnet
- iDRAC.Racadm
- iDRAC.SNMP

Weitere Informationen zu diesen Objekten finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Aktivieren oder Deaktivieren der HTTPS-Umleitung

Wenn Sie aufgrund des Zertifikatwarnungs-Problems mit Standard- iDRAC-Zertifikat oder zur vorübergehenden Einstellung für den Debug-Modus nicht möchten, dass die automatische HTTP-zu-HTTPS-Umleitung erfolgt, können Sie iDRAC so konfigurieren, dass die Umleitung vom http-Port (Standardeinstellung 80) zum https-Port (Standardeinstellung 443) deaktiviert ist. Standardmäßig ist die Umleitung aktiviert. Sie müssen sich von iDRAC ab- und wieder anmelden, damit diese Einstellung wirksam wird. Wenn Sie diese Funktion deaktivieren, wird eine Warnmeldung angezeigt.

Sie müssen über die Berechtigung zum Konfigurieren von iDRAC verfügen, damit Sie die HTTPS-Umleitung aktivieren oder deaktivieren können.

Beim Aktivieren oder Deaktivieren dieser Funktion wird ein Ereignis in der Lifecycle Controller-Protokolldatei aufgezeichnet.

So deaktivieren Sie die HTTP-zu-HTTPS-Umleitung:

```
racadm set iDRAC.Webserver.HttpsRedirection Disabled
```

So aktivieren Sie die HTTP-zu-HTTPS-Umleitung:

```
racadm set iDRAC.Webserver.HttpsRedirection Enabled
```

So zeigen Sie den Status der HTTP-zu-HTTPS-Umleitung an:

```
racadm get iDRAC.Webserver.HttpsRedirection
```

Konfigurieren von TLS

Standardmäßig ist der iDRAC so konfiguriert, dass er TLS 1.1 und höher verwendet. Sie können iDRAC so konfigurieren, dass eines des Folgenden verwendet wird:

- TLS 1.0 und höher
- TLS 1.1 und höher
- Nur TLS 1.2

ANMERKUNG: Um eine sichere Verbindung sicherzustellen, empfiehlt Dell die Verwendung von TLS 1.1 und höher.

TLS mittels Webschnittstelle konfigurieren

1 Wechseln Sie zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk**.
2 Klicken Sie auf die Registerkarte **Dienste** und klicken Sie dann auf **Web Server**.
3 In der Dropdown-Liste **TLS-Protokolle** wählen Sie die TLS-Version und klicken auf **Anwenden**.

Konfigurieren von TLS unter Verwendung von RACADM

Zum Überprüfen der konfigurierten Version von TLS:

```
racadm get idrac.webserver.tlsprotocol
```

So stellen Sie die Version von TLS ein:

```
racadm set idrac.webserver.tlsprotocol <n>
```

<n>=0	TLS 1.0 und höher
<n>=1	TLS 1.1 und höher
<n>=2	Nur TLS 1.2

Verwenden des VNC-Client für die Remote-Server-Verwaltung

Sie können einen offenen Standard-VNC-Client zur Remote-Server-Verwaltung mithilfe von Desktop- und mobilen Geräten, wie z. B. Dell Wyse PocketCloud verwenden. Wenn Server in Rechenzentren nicht mehr funktionieren, sendet iDRAC oder das Betriebssystem eine Warnung an die Konsole der Management Station. Die Konsole sendet dann eine E-Mail oder eine SMS mit den erforderlichen Informationen an ein mobiles Gerät und startet die VNC Viewer-Anwendung auf der Management Station. Der VNC Viewer kann eine Verbindung mit Betriebssystem/Hypervisor auf dem Server herstellen und ermöglicht den Zugriff auf Tastatur, Anzeige und Maus auf dem Hostserver zwecks Fehlerbehebung. Aktivieren Sie vor dem Ausführen des VNC-Client den VNC-Server und konfigurieren Sie in iDRAC die VNC-Servereinstellungen wie Kennwort, VNC-Portnummer, SSL-Verschlüsselung und Timeout-Wert. Sie können diese Einstellungen über die iDRAC-Webschnittstelle oder RACADM konfigurieren.

ANMERKUNG: Die VNC-Funktion ist lizenziert und ist im Rahmen der iDRAC Enterprise-Lizenz erhältlich.

Sie können zwischen vielen VNC-Anwendungen oder Desktop-Clients beispielsweise von RealVNC oder Dell Wyse PocketCloud auswählen.

Es kann jeweils nur eine VNC-Client-Sitzung gleichzeitig aktiv sein.

Wenn eine VNC-Sitzung aktiv ist, können Sie den virtuellen Datenträger nur über die Option „Virtuelle Konsole starten“ starten, und nicht über den Viewer der virtuellen Konsole.

Wenn die Videoverschlüsselung deaktiviert ist, beginnt der VNC-Client direkt mit RFB-Handshake, wobei SSL-Handshake nicht erforderlich ist. Ist während des VNC-Client-Handshakes (RFB oder SSL) eine andere VNC-Sitzung aktiv oder eine Sitzung der virtuellen Konsole geöffnet, so wird die neue VNC-Client-Sitzung abgelehnt. Nach Abschluss des anfänglichen Handshakes deaktiviert VNC-Server die virtuelle Konsole und lässt lediglich virtuelle Datenträger zu. Nach Beendigung der VNC-Sitzung stellt VNC-Server den ursprünglichen Zustand der virtuellen Konsole (aktiviert oder deaktiviert) wieder her.

ANMERKUNG:

- Wenn sich die iDRAC-NIC im freigegebenen Modus befindet und das Hostsystem aus- und wieder eingeschaltet wird, geht die Netzwerkverbindung für einige Sekunden verloren. Wenn Sie während dieser Zeit eine Aktion auf dem aktiven VNC-Client ausführen, wird die VNC-Sitzung möglicherweise geschlossen. Sie müssen die Zeitüberschreitung (der Wert, der auf der Seite **Services** in der iDRAC-Webschnittstelle für die VNC-Servereinstellungen festgelegt wurde) abwarten und anschließend die VNC-Verbindung erneut herstellen.
- Wenn das VNC-Client-Fenster für mehr als 60 Sekunden minimiert wird, wird das Client-Fenster geschlossen. Sie müssen eine neue VNC-Sitzung öffnen. Wenn Sie das VNC-Client-Fenster innerhalb von 60 Sekunden maximieren, können Sie es weiterhin verwenden.

Konfigurieren von VNC-Server unter Verwendung der iDRAC-Webschnittstelle

So konfigurieren Sie die VNC-Servereinstellungen:

1 Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Dienste**.

Die Seite **Dienste** wird angezeigt.

2 Aktivieren Sie im Abschnitt **VNC-Server** den VNC-Server, geben Sie das Kennwort und die Portnummer ein, und aktivieren oder deaktivieren Sie die SSL-Verschlüsselung.

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

3 Klicken Sie auf **Anwenden**.

Der VNC-Server ist konfiguriert.

VNC-Server unter Verwendung von RACADM konfigurieren

Verwenden Sie zum Konfigurieren des VNC-Servers den Befehl `set` mit den Objekten in `VNCserver`.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Einrichten von VNC Viewer mit SSL-Verschlüsselung

Während der Konfiguration der VNC-Server-Einstellungen in iDRAC muss die SSL-Tunnelanwendung zusammen mit dem VNC-Viewer verwendet werden, um die verschlüsselte SSL-Verbindung mit dem iDRAC-VNC-Server herzustellen, falls die Option **SSL-Verschlüsselung** aktiviert ist.

ANMERKUNG: Die meisten VNC-Clients haben keinen integrierten SSL-Verschlüsselungs-Support.

So konfigurieren Sie die SSL-Tunnel-Anwendung:

1 Konfigurieren Sie SSL-Tunnel, um die Verbindung auf `<localhost>:<localport number>` zu akzeptieren. Beispielsweise 127.0.0.1:5930.

2 Konfigurieren Sie SSL-Tunnel, um die Verbindung mit `<iDRAC IP address>:<VNC server port Number>` herzustellen, beispielsweise 192.168.0.120:5901.

3 Starten Sie die Tunnelanwendung.

Um eine Verbindung zum iDRAC-VNC-Server über den verschlüsselten SSL-Kanal herzustellen, verbinden Sie den VNC-Viewer mit dem localhost (Link-Local-IP-Adresse) und der lokalen Schnittstellennummer (127.0.0.1: <lokale Schnittstellennummer>).

Einrichten von VNC Viewer ohne SSL-Verschlüsselung

Im Allgemeinen müssen alle mit Remote-Frame Buffer (RFB) kompatiblen VNC Viewer Verbindung mit dem VNC-Server über die iDRAC-IP-Adresse und die Anschlussnummer aufnehmen, die für die VNC-Server konfiguriert ist. Wenn die Option für die SSL-Verschlüsselung deaktiviert ist, wenn die VNC-Servereinstellungen in iDRAC konfiguriert werden, dann führen Sie zur Verbindungsherstellung mit dem VNC Viewer folgende Schritte aus:

Geben Sie im Dialogfeld **VNC Viewer** die iDRAC-IP-Adresse und die VNC-Schnittstellennummer in das Feld **VNC-Server** ein.

Das Format lautet `<iDRAC IP address:VNC port number>`

Beispiel: Wenn die iDRAC-IP-Adresse 192.168.0.120 und die VNC-Schnittstellennummer 5901 ist, dann geben Sie `192.168.0.120:5901` ein.

Anzeige auf der Frontblende konfigurieren

Sie können die Anzeige der LC- und LE-Anzeigen auf der Frontblende des Managed System konfigurieren.

Bei Rack- und Tower-Servern sind zwei Frontblendentypen verfügbar:

- LC-Anzeige auf der Frontblende und System-ID-LED
- LE-Anzeige auf der Frontblende und System-ID-LED

Bei Blade-Servern ist nur die System-ID-LED auf der Frontblende des Servers verfügbar, da das Blade-Gehäuse mit einer LC-Anzeige ausgerüstet ist.

Zugehöriger Link

LCD-Einstellung konfigurieren
LED-Einstellung für die System-ID konfigurieren

LCD-Einstellung konfigurieren

Sie können eine Standardzeichenkette, wie z. B. den iDRAC-Namen, die IP-Adresse, usw. oder eine benutzerdefinierte Zeichenkette auf der LC-Anzeige auf der Frontblende des Managed System definieren und anzeigen.

Einstellungen für die LC-Anzeige über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die LC-Anzeige auf der Frontblende eines Servers:

1 Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **Hardware** > **Frontblende**.
2 Wählen Sie im Abschnitt **Einstellungen für LC-Anzeige** über das Drop-Down-Menü **Nachricht auf der Startseite einrichten** einen der folgenden Aspekte aus:
   - Service-Tag-Nummer (Standardeinstellung)
   - Systemkennnummer
   - DRAC-MAC-Adresse
   - DRAC-IPv4-Adresse
   - DRAC-IPv6-Adresse
   - Systemstrom
   - Umgebungstemperatur

- Systemmodell
- Host-Name
- Benutzerdefiniert
- Keine

  Wenn Sie **Benutzerdefiniert** auswählen, geben Sie die erforderliche Nachricht in das Textfeld ein.

  Wenn Sie **Keine** auswählen, wird die Nachricht auf der Startseite nicht auf der LC-Anzeige auf der Frontblende angezeigt.

3 Aktivieren Sie die Anzeige der virtuellen Konsole (optional). Bei Aktivierung zeigen der Abschnitt Live-Status an der Frontblende und die LCD-Anzeige am Server die Meldung `Virtual console session active` an, wenn es eine aktive Sitzung der virtuellen Konsole gibt.

4 Klicken Sie auf **Anwenden**.

Die LC-Anzeige auf der Frontblende des Servers zeigt die konfigurierte Nachricht für die Startseite an.

LCD-Einstellungen über RACADM konfigurieren

Um die Server-LCD-Frontblendenanzeige zu konfigurieren, verwenden Sie die Objekte in der Gruppe System.LCD.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

LCD-Einstellungen über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

So konfigurieren Sie die LC-Anzeige auf der Frontblende eines Servers:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Frontblendensicherheit**.

Die Seite **iDRAC-Einstellungen.Frontblendensicherheit** wird angezeigt.

2 Aktivieren oder deaktivieren Sie den Netzschalter.

3 Geben Sie folgendes an:

- Zugang zur Frontblende
- LCD-Meldungszeichenkette
- Systemstromeinheiten, Umgebungstemperatureinheiten und Fehleranzeige

4 Aktivieren oder deaktivieren Sie die Anzeige der virtuellen Konsole.

Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

5 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

LED-Einstellung für die System-ID konfigurieren

Aktivieren oder deaktivieren Sie für die Identifizierung eines Servers das Blinken der System-ID-LED auf dem Managed System.

LED-Einstellung für die System-ID über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die LE-Anzeige für die System-ID:

1 Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **Hardware** > **Frontblende**. Daraufhin wird die Seite **Frontblende** angezeigt.

2 Wählen Sie im Abschnitt **LED-Einstellungen für die System-ID** beliebige der folgenden Optionen aus, um das Blinken der LED zu aktivieren oder zu deaktivieren:

- Blinken ausgeschaltet

- Blinken eingeschaltet
- Blinken einschalten bei Zeitüberschreitung von einem Tag
- Blinken einschalten bei Zeitüberschreitung von einer Woche
- Blinken einschalten bei Zeitüberschreitung von einem Monat

3 Klicken Sie auf **Anwenden**.

Das Blinken der LED auf der Frontblende ist konfiguriert.

LED-Einstellung der System-ID über RACADM konfigurieren

Um die System-ID-LED zu konfigurieren, verwenden Sie den Befehl **setled**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Das Konfigurieren von Zeitzone und NTP

Sie können die Zeitzone in iDRAC konfigurieren und die iDRAC-Zeit synchronisieren, indem Sie das Network Time Protocol (NTP) anstelle von BIOS oder Host-Systemzeiten verwenden.

Sie müssen über die Berechtigung zur Konfiguration verfügen, um die Zeitzone oder NTP-Einstellungen zu konfigurieren.

Konfigurieren von Zeitzone und NTP unter Verwendung der iDRAC- Web-Schnittstelle

So konfigurieren Sie Zeitzone und NTP mithilfe der iDRAC-Web-Schnittstelle:

1 Gehen Sie zu **Übersicht** > **iDRAC-Einstellungen** > **Eigenschaften** > **Einstellungen**.

Die Seite **Zeitzone und NTP** wird angezeigt.

2 Um die Zeitzone zu konfigurieren, wählen Sie im Drop-Down-Menü **Zeitzone** die gewünschte Zeitzone aus und klicken dann auf **Anwenden**.

3 Um NTP zu konfiguriere, aktivieren Sie NTP, geben Sie die NTP-Serveradressen ein und klicken Sie dann auf **Anwenden**.

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

Konfigurieren von Zeitzone und NTP unter Verwendung von RACADM

Um Zeitzone und NTP zu konfigurieren, verwenden Sie den Befehl **set** mit den Objekten in der Gruppe **iDRAC.Time** und **iDRAC.NTPConfigGroup**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Erstes Startlaufwerk einstellen

Sie können das erste Startlaufwerk nur für den nächsten Startvorgang oder für alle nachfolgenden Neustarts festlegen. Wenn Sie festlegen, dass das Gerät für alle nachfolgenden Bootvorgänge verwendet werden soll, verbleibt es als das erste Startgerät in der BIOS-Startreihenfolge, bis eine erneute Änderung entweder über die iDRAC-Webschnittstelle oder von der BIOS-Startreihenfolge aus erfolgt.

Sie können das erste Startgerät auf einen der folgenden Punkte einstellen:

- Normaler Start
- PXE
- BIOS-Setup
- Lokale Floppy/Primäre Wechselmedien
- Lokale CD/DVD
- Festplattenlaufwerk
- Virtuelle Diskette
- Virtuelle CD/DVD/ISO
- Lokale SD-Karte
- vFlash
- Lifecycle-Controller
- BIOS Boot Manager
- UEFI-Gerätepfad

ANMERKUNG:

- BIOS-Setup (F2), Lifecycle Controller (F10) und BIOS Boot Manager (F11) können nicht als permanentes Startgerät eingestellt werden.
- Die Einstellungen für das erste Startgerät in der iDRAC-Webschnittstelle überschreiben die Starteinstellungen im System-BIOS.
- Verwenden Sie die Redfish-Schnittstelle zum Festlegen des Wertes für den UEFI-Gerätepfad. Starten zum UEFI-Gerätepfad wird nur auf Dell 13. Generation oder neueren Servern unterstützt.

Erstes Startgerät über die Web-Schnittstelle einrichten

So richten Sie das erste Startgerät über die iDRAC-Webschnittstelle ein:

1 Gehen Sie zu **Übersicht** > **Server** > **Einrichtung** > **Erstes Startgerät**.

Der Bildschirm **Erstes Startgerät** wird angezeigt.

2 Wählen Sie das gewünschte erste Startgerät aus der Drop-Down-Liste aus, und klicken Sie dann auf **Anwenden**.

Das System startet bei den nachfolgenden Neustarts vom ausgewählten Gerät.

3 Um den Startvorgang vom ausgewählten Startgerät beim nächsten Starten nur einmal auszuführen, wählen Sie **Einmalstart** aus. Daraufhin startet das System vom ersten Startgerät gemäß der BIOS-Startreihenfolge.

Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Erstes Startgerät über RACADM festlegen

- Um das erste Startlaufwerk festzulegen, verwenden Sie das Objekt **iDRAC.ServerBoot.FirstBootDevice**.
- Um den einmaligen Start für ein Gerät zu aktivieren, verwenden Sie das Objekt **iDRAC.ServerBoot.BootOnce**.

Weitere Informationen zu diesen Objekten finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* unter **dell.com/idracmanuals**.

Einstellen des ersten Startgeräts unter Verwendung der virtuellen Konsole

Sie können das Gerät, von dem aus gestartet werden soll, auswählen, während der Server im Viewer für die virtuelle Konsole angezeigt wird, bevor er seine Startsequenz durchläuft. Sie können bei allen unterstützten Geräten, die unter Erstes Startgerät einstellen aufgelistet sind, einen Einmalstart durchführen.

So stellen Sie das erste Startgerät mithilfe der virtuellen Konsole ein:

1 Starten Sie die virtuelle Konsole.
2 Stellen Sie im Viewer der virtuellen Konsole im Menü **Nächster Start** das gewünschte Gerät als erstes Startgerät ein.

Bildschirm „Letzter Absturz“ aktivieren

Um den Grund für den Absturz unter einem Managed System zu beheben, können Sie das Image des Systemabsturzes über iDRAC erfassen.

ANMERKUNG: Informationen über Server Administrator finden Sie im *Dell OpenManage Server Administrator-Installationshandbuch* unter dell.com/support/manuals. Weitere Informationen zu iSM finden Sie unter Verwenden des iDRAC Service Module.

1 Von der DVD *Dell Systems Management Tools and Documentation* oder von der Dell-Support-Website, installieren Sie Server Administrator oder das iDRAC-Service-Module (iSM) auf das Managed System.
2 Stellen Sie im Fenster „Starten und Wiederherstellen“ unter **Windows** sicher, dass die Option für den automatischen Neustart nicht ausgewählt ist.

   Nähere Informationen erhalten Sie in der Windows Dokumentation.
3 Verwenden Sie Server Administrator, um den Zeitgeber für die **automatische Wiederherstellung** zu aktivieren, stellen Sie die automatische Wiederherstellung auf **Zurücksetzen**, **Ausschalten** oder **Aus- und einschalten** ein und stellen Sie den Zeitgeber in Sekunden ein (ein Wert zwischen 60 und 480).
4 Aktivieren Sie die Option **Automatisches Herunterfahren und Wiederherstellen** (ASR) über eine der folgenden Komponenten:
   - Server Administrator - Schlagen Sie im *Dell OpenManage Server Administrator User's Guide* (Benutzerhandbuch für Dell OpenManage Server Administrator) nach.
   - Lokaler RACADM - Verwenden Sie den Befehl `racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1`
5 Aktivieren Sie **Automatischer System-Wiederherstellungsagent**. Gehen Sie dazu zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Dienste**, wählen Sie **Aktivieren** aus, und klicken Sie auf **Anwenden**.

Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough

Bei Servern, die Network-Daughter-Card- (NDC) oder integrierte LAN-On-Motherboard- (LOM) Geräte aufweisen, können Sie die Funktion Betriebssystem-zu-iDRAC-Passthrough aktivieren. Diese Funktion stellt eine bidirektionale bandinterne Hochgeschwindigkeitskommunikation zwischen iDRAC und dem Host-Betriebssystem mittels eines freigegebenen LOM (Rack- oder Tower-Server), einer dedizierten NIC (Rack-, Tower- oder Blade-Server) oder der USB-NIC bereit. Diese Funktion ist mit der iDRAC Enterprise-Lizenz verfügbar.

ANMERKUNG: iDRAC- Service-Modul (iSM) enthält weitere Funktionen zum Verwalten von iDRAC über das Betriebssystem. Weitere Informationen erhalten Sie im *iDRAC Service Module Installation Guide (iDRAC-Servicemodul-Installationshandbuch)*, das unter dell.com/support/manuals verfügbar ist.

Wenn der Browser durch eine dedizierte NIC aktiviert wurde, kann dieser im Host-Betriebssystem gestartet werden und dann auf die iDRAC-Web-Schnittstelle zugreifen. Die dedizierte NIC für die Blade-Server findet sich im Chassis Management Controller.

Das Wechseln zwischen dedizierter NIC und freigegebenem LOM erfordert keinen Neustart oder Reset des Host-Betriebssystems oder des iDRAC.

Der Kanal kann folgendermaßen aktiviert werden:

- iDRAC-Web-Schnittstelle
- RACADM oder WS-MAN (Nachbetriebssystemumgebung)
- Dienstprogramm für iDRAC-Einstellungen (Vorbetriebssystemumgebung)

Wenn die Netzwerkkonfiguration durch die iDRAC-Web-Schnittstelle geändert wird, müssen Sie mindestens 10 Sekunden warten, bevor das Betriebssystem zu iDRAC-Passthrough aktiviert wird.

Wenn Sie die XML-Konfigurationsdatei über RACADM oder WS-MAN verwenden und wenn die Netzwerkeinstellungen in dieser Datei geändert wurden, dann müssen Sie 15 Sekunden warten, um entweder die Funktion des Betriebssystems zum iDRAC-Passthrough zu aktivieren oder die IP-Adresse des Host-Betriebssystems einzustellen.

Vor Aktivierung des Betriebssystems zum iDRAC-Passthrough stellen Sie Folgendes sicher:

- iDRAC wurde zur Verwendung von dedizierten NIC oder dem gemeinsamen Modus konfiguriert (das heißt, die NIC-Auswahl wird einer der LOMs zugewiesen).
- Host-Betriebssystem und iDRAC befinden sich auf dem gleichen Subnetz und auf dem gleichen VLAN.
- Die IP-Adresse des Host-Betriebssystems ist konfiguriert.
- Eine Karte ist installiert, die Betriebssystem-zu-iDRAC-Passthrough-Funktion unterstützt.
- Sie verfügen über die Berechtigung zum Konfigurieren.

Wenn Sie diese Funktion aktivieren:

- Im freigegebenen Modus wird die IP-Adresse des Host-Betriebssystems verwendet.
- Im dedizierten Modus müssen Sie eine gültige IP-Adresse des Host-Betriebssystems angeben. Wenn mehr als ein LOM aktiv ist, geben Sie die IP-Adresse des ersten LOM ein.

Falls die Funktion „Betriebssystem-zu-iDRAC-Passthrough“ nach der Aktivierung nicht funktioniert, überprüfen Sie Folgendes:

- Das für iDRAC dedizierte NIC-Kabel ist richtig angeschlossen.
- Es ist mindestens ein LOM aktiv.

ANMERKUNG: Verwenden Sie die Standard-IP-Adresse. Stellen Sie sicher, dass die IP-Adresse der USB-NIC-Schnittstelle sich nicht in demselben Netzwerk-Subnetz wie die iDRAC- oder Host-BS-IP-Adressen befindet. Wenn jedoch ein Konflikt dieser IP-Adresse mit anderen Schnittstellen des Host-Systems oder des lokalen Netzwerks vorliegt, müssen Sie sie ändern.

ANMERKUNG: Verwenden Sie nicht die IP-Adressen 169.254.0.3 und 169.254.0.4. Diese IP-Adressen sind für die USB-NIC-Schnittstelle an der Vorderseite reserviert, wenn ein A/A-Kabel verwendet wird.

Zugehöriger Link

Unterstützte Karten für Betriebssystem-zu-iDRAC-Passthrough
Unterstützte Betriebssysteme für USB-NIC
Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung der Web-Schnittstelle
Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung von RACADM
Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung des Dienstprogramms für iDRAC-Einstellungen

Unterstützte Karten für Betriebssystem-zu-iDRAC-Passthrough

Die folgende Tabelle zeigt eine Liste der Karten, die die Funktion von Betriebssystem-zu-iDRAC-Passthrough mithilfe von LOM unterstützen.

Tabelle 12. Betriebssystem-zu-iDRAC-Passthrough mithilfe von LOM

Kategorie	Hersteller	Typ
NDC	Broadcom	• 5720 QP rNDC 1G BASE-T • 57810S DP bNDC KR • 57800S QP rNDC (10G BASE-T + 1G BASE-T)

Kategorie	Hersteller	Typ
		• 57800S QP rNDC (10G SFP+ + 1G BASE-T) • 57840 4x10G KR • 57840 rNDC
	Intel	• i540 QP rNDC (10G BASE-T + 1G BASE-T) • i350 QP rNDC 1G BASE-T • x520/i350 rNDC 1GB
	QLogic	QMD8262 Blade NDC

Integrierte LOM-Karten unterstützen ebenfalls die Betriebssystem-zu-iDRAC-Passthrough-Funktion.

Die folgenden Karten unterstützen nicht die Funktion von Betriebssystem zu iDRAC-Passthrough:

- Intel 10 GB NDC.
- Intel rNDC (Elk Flat rNDC) mit zwei Controllern – 10G-Controller unterstützen diese Funktion nicht.
- Qlogic bNDC
- PCIe, Mezzanine, Netzwerk-Schnittstellenkarten.

Unterstützte Betriebssysteme für USB-NIC

Die unterstützten Betriebssysteme für USB-NIC sind:

- Windows Server 2008 R2 mit SP1
- Windows Server 2008 SP2 (64-Bit)
- Windows Server 2012
- Windows Server 2012 R2
- SUSE Linux Enterprise Server 10 SP4 (64-Bit)
- SUSE Linux Enterprise Server 11 SP2 (64-Bit)
- SUSE Linux Enterprise Server 11 SP4
- RHEL 5.9 (32-Bit und 64-Bit)
- RHEL 6.4
- RHEL 6.7
- vSphere v5.0 U2 ESXi
- vSphere v5.1 U3
- vSphere 5.1 U1 ESXi
- vSphere v5.5 ESXi
- vSphere v5.5 U3
- vSphere 6.0
- vSphere 6.0 U1
- CentOS 6.5
- CentOS 7.0
- Ubuntu 14.04.1 LTS
- Ubuntu 12.04.04 LTS
- Debian 7.6 (Wheezy)
- Debian 8.0

Auf Servern mit Windows 2008 SP2 (64 Bit) wird das virtuelle iDRAC-CD-USB-Gerät nicht automatisch erkannt (oder aktiviert). Sie müssen es manuell aktivieren. Weitere Informationen finden Sie unter den von Microsoft vorgeschlagenen Schritten zur manuellen Aktualisierung des RNDIS-Treibers (Remote Network Driver Interface Specification) für dieses Gerät.

Für Linux-Betriebssysteme müssen Sie vor dem Aktivieren der USB-NIC die USB-NIC als DHCP auf dem Host-Betriebssystem konfigurieren.

Wenn das Betriebssystem auf dem Host SUSE Linux Enterprise Server 11, CentOS 6.5, CentOS 7.0, Ubuntu 14.04.1 LTS oder Ubuntu 12.04.4 LTS ist, müssen Sie nach dem Aktivieren der USB-NIC in iDRAC den DHCP-Client auf dem Hostbetriebssystem manuell aktivieren. Weitere Informationen zum Aktivieren von DHCP finden Sie in der Dokumentation zu SUSE Linux Enterprise Server, CentOS und Ubuntu-Betriebssystemen.

Für vSphere müssen Sie vor dem Aktivieren von USB-NIC die VIB-Datei installieren.

Für die folgenden Betriebssysteme können Sie, wenn Sie die Avahi- und nss-mdns-Pakete installieren, den Link **https://idrac.local** zum Starten von iDRAC vom Hostbetriebssystem aus verwenden. Wenn diese Pakete nicht installiert sind, verwenden Sie **https://169.254.0.1** zum Starten von iDRAC.

Tabelle 13. Betriebssysteminformationen für USB-NIC

Betriebssystem	Firewall-Status	Avahi-Paket	nss-mdns-Paket
RHEL 5.9 32-Bit	Disable (Deaktivieren)	Installieren als separates Paket (**avahi-0.6.16-10.el5_6.i386.rpm**)	Installieren als separates Paket (**nss-mdns-0.10-4.el5.i386.rpm**)
RHEL 6.4 64-Bit	Disable (Deaktivieren)	Installieren als separates Paket (**avahi-0.6.25-12.el6.x86_64.rpm**)	Installieren als separates Paket (**nss-mdns-0.10-8.el6.x86_64.rpm**)
SLES 11 SP3 64-Bit	Disable (Deaktivieren)	Das Avahi-Paket ist Bestandteil der Betriebssystem-DVD	nss-mdns wird während der Installation von Avahi installiert

Auf dem Hostsystem ist der USB-NIC-Pass-Through-Modus während der Installation des Betriebssystems RHEL 5.9 deaktiviert. Wenn diese Funktion nach Abschluss der Installation aktiviert wird, ist das der Netzwerkschnittstelle entsprechende USB-NIC-Gerät nicht automatisch aktiv. Sie können einen der folgenden Schritte ausführen, um das USB-NIC-Gerät zu aktivieren:

- Konfigurieren Sie die USB-NIC-Schnittstelle mithilfe des Network Manager-Tools. Navigieren Sie zu **System** > **Administrator** > **Network (Netzwerk)** > **Devices (Geräte)** > **New (Neu)** > **Ethernet Connection (Ethernet-Verbindung)** und wählen Sie **Dell computer corp.iDRAC Virtual NIC USB Device (Dell Computer corp.iDRAC Virtuelles NIC-USB-Gerät)**. Klicken Sie auf das Aktivierungssymbol, um das Gerät zu aktivieren. Weitere Information finden Sie in der Dokumentation zu RHEL 5.9.
- Erstellen Sie die entsprechende Schnittstellen-Konfigurationsdatei **ifcfg-ethX** im Verzeichnis **/etc/sysconfig/network-script/**. Fügen Sie die Basiseinträge DEVICE, BOOTPROTO, HWADDR und ONBOOT hinzu. Fügen Sie TYPE in der Datei **ifcfg-ethX** hinzu und starten Sie die Netzwerkdienste neu, indem Sie den Befehl `service network restart` verwenden.
- Starten Sie das System neu.
- Schalten Sie das System aus und wieder ein.

Bei Systemen mit RHEL 5.9 ist das USB-NIC-Gerät nicht automatisch aktiv, wenn es deaktiviert wurde und Sie das System ausschalten oder umgekehrt, wenn das System eingeschaltet und das USB-NIC-Gerät aktiviert ist. Prüfen Sie zum Aktivieren, ob die Datei **ifcfg-ethX.bak** im Verzeichnis **/etc/sysconfig/network-script** für die USB-NIC-Schnittstelle verfügbar ist. Wenn dies der Fall ist, benennen Sie die Datei in **ifcfg-ethX** um und verwenden Sie dann den Befehl `ifup ethX`.

Zugehöriger Link

Installieren der VIB-Datei

Installieren der VIB-Datei

Für vSphere-Betriebssystemen muss vor der Aktivierung des USB-NIC die VIB-Datei installiert werden.

So installieren Sie die VIB-Datei:

1 Kopieren Sie mit Win SCP die VIB-Datei in den Ordner **/tmp/** des ESX-i-Host-Betriebssystems.

2 Wechseln Sie zur ESXi-Eingabeaufforderung, und führen Sie den folgenden Befehl aus:

```
esxcli software vib install -v /tmp/ iDRAC_USB_NIC-1.0.0-799733X03.vib --no-sig-check
```

Das Ergebnis ist Folgendes:

```
Message: The update completed successfully, but the system needs to be rebooted for the
changes to be effective. Reboot Required: true VIBs Installed:
Dell_bootbank_iDRAC_USB_NIC_1.0.0-799733X03 VIBs Removed: VIBs Skipped:
```

3 Starten Sie den Server neu.

4 Geben Sie in der ESXi-Eingabeaufforderung den folgenden Befehl ein: `esxcfg-vmknic -l`.

Die Ausgabe zeigt den usb0-Eintrag.

Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung der Web-Schnittstelle

So aktivieren Sie das Betriebssystem zum iDRAC-Passthrough mithilfe der Web-Schnittstelle:

1 Gehen Sie zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Betriebssystem zu iDRAC-Passthrough**.

Die Seite **Betriebssystem zu iDRAC-Passthrough** wird angezeigt.

2 Wählen Sie eine der folgenden Optionen, um Betriebssystem-zu-iDRAC-Passthrough zu aktivieren:

- **LOM** – Der BS zu iDRAC PassThrough-Link zwischen dem iDRAC und dem Host-Betriebssystem wird über das LOM oder die NDC hergestellt.
- **USB-NIC** – Der BS zu iDRAC PassThrough-Link zwischen dem iDRAC und dem Host-Betriebssystem wird über den internen USB hergestellt.

Zum Deaktivieren der Funktion klicken Sie auf **Deaktiviert**.

3 Wenn Sie **LOM** als PassThrough-Konfiguration auswählen und wenn der Server über den dedizierten Modus verbunden ist, geben Sie die IPv4-Adresse des Betriebssystems ein.

> **ANMERKUNG: Wenn der Server im freigegebenen LOM-Modus verbunden ist, ist das Feld Betriebssystem-IP-Adresse deaktiviert.**

4 Wenn Sie die Option **USB-NIC** als Passthrough-Konfiguration auswählen, geben Sie die IP-Adresse des USB-NIC ein.

Der Standardwert lautet 169.254.0.1. Es wird empfohlen, die Standard-IP-Adresse zu verwenden. Wenn jedoch ein Konflikt dieser IP-Adresse mit anderen Schnittstellen des Host-Systems oder des lokalen Netzwerks vorliegt, müssen Sie sie ändern.

Geben Sie nicht die 169.254.0.3 und 169.254.0.4 IP-Adressen ein. Diese IP-Adressen sind für den USB-NIC-Anschluss an der Vorderseite, wenn ein A/A-Kabel verwendet wird, reserviert.

5 Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

6 Klicken Sie auf **Netzwerkkonfiguration testen**, um zu überprüfen ob die IP zugreifbar ist und die Verbindung zwischen dem iDRAC und dem Host-Betriebssystem hergestellt ist.

Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung von RACADM

Um das Betriebssystem zum iDRAC-Passthrough unter Verwendung von RACADM zu aktivieren oder deaktivieren, verwenden Sie die Objekte in der Gruppe **iDRAC.OS-BMC**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung des Dienstprogramms für iDRAC-Einstellungen

So aktivieren oder deaktivieren Sie das Betriebssystem zum iDRAC-Passthrough mithilfe des Dienstprogramms für iDRAC-Einstellungen:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Kommunikationsberechtigungen**.

Die Seite **iDRAC-Einstellungen.Kommunikationsberechtigungen** wird angezeigt.

2 Wählen Sie eine der folgenden Optionen, um Betriebssystem-zu-iDRAC-Passthrough zu aktivieren:

- **LOM** – Der BS zu iDRAC PassThrough-Link zwischen dem iDRAC und dem Host-Betriebssystem wird über das LOM oder die NDC hergestellt.
- **USB-NIC** – Der BS zu iDRAC PassThrough-Link zwischen dem iDRAC und dem Host-Betriebssystem wird über den internen USB hergestellt.

Zum Deaktivieren der Funktion klicken Sie auf **Deaktiviert**.

> **ANMERKUNG: Die LOM-Option kann nur ausgewählt werden, wenn eine der installierten Karten das Durchreichen vom Betriebssystem zum iDRAC unterstützt. Andernfalls ist die Option ausgegraut.**

3 Wenn Sie **LOM** als PassThrough-Konfiguration auswählen und wenn der Server über den dedizierten Modus verbunden ist, geben Sie die IPv4-Adresse des Betriebssystems ein.

> **ANMERKUNG: Wenn der Server im freigegebenen LOM-Modus verbunden ist, ist das Feld Betriebssystem-IP-Adresse deaktiviert.**

4 Wenn Sie die Option **USB-NIC** als Passthrough-Konfiguration auswählen, geben Sie die IP-Adresse des USB-NIC ein.

Der Standardwert lautet 169.254.0.1. Wenn jedoch ein Konflikt dieser IP-Adresse mit einer IP-Adresse von anderen Schnittstellen des Host-Systems oder des lokalen Netzwerks vorliegt, müssen Sie sie ändern. Geben Sie die IP-Adressen 169.254.0.3 und 169.254.0.4 nicht ein. Diese IP-Adressen sind für die USB-NIC-Schnittstelle an der Frontblende reserviert, wenn ein A/A-Kabel verwendet wird.

5 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Details werden gespeichert.

Zertifikate abrufen

In der folgenden Tabelle werden die Zertifikattypen auf der Basis des Anmeldetyps aufgelistet.

Tabelle 14. Zertifikattypen auf der Basis des Anmeldetyps

Anmeldetyp	Zertifikattyp	Abrufmöglichkeit
Einmalige Anmeldung über Active Directory	Vertrauenswürdiges Zertifizierungsstellenzertifikat	Zertifikatsignierungsanforderung (CSR) generieren und diese von einer Zertifizierungsstelle signieren lassen SHA-2-Zertifikate werden ebenfalls unterstützt.
Smart Card-Anmeldung als lokaler oder Active Directory-Benutzer	• Benutzerzertifikat • Vertrauenswürdiges Zertifizierungsstellenzertifikat	• Benutzerzertifikat – Smart Card-Benutzerzertifikat als Base64-kodierte Datei unter Verwendung der Kartenverwaltungssoftware exportieren, die durch den Smart Card-Anbieter bereitgestellt wird. • Vertrauenswürdiges Zertifizierungsstellenzertifikat – Dieses Zertifikat wird von einer Zertifizierungsstelle ausgegeben. SHA-2-Zertifikate werden ebenfalls unterstützt.
Active Directory-Benutzeranmeldung	Vertrauenswürdiges Zertifizierungsstellenzertifikat	Dieses Zertifikat wird durch eine Zertifizierungsstelle ausgegeben. SHA-2-Zertifikate werden ebenfalls unterstützt.
Lokale Benutzeranmeldung	SSL-Zertifikat	Zertifikatsignierungsanforderung (CSR) generieren und diese von einer vertrauenswürdigen Zertifizierungsstelle signieren lassen **ANMERKUNG: iDRAC wird mit einem standardmäßigen selbstsignierten SSL-Serverzertifikat geliefert. Dieses Zertifikat wird vom iDRAC Webserver, von virtuellen Datenträgern und der virtuellen Konsole verwendet.** SHA-2-Zertifikate werden ebenfalls unterstützt.

Zugehöriger Link

SSL-Serverzertifikate

Neue Zertifikatsignierungsanforderung erstellen

SSL-Serverzertifikate

iDRAC umfasst einen Webserver, der für das zum Branchenstandard gehörende SSL-Sicherheitsprotokoll konfiguriert ist, um über das Netzwerk verschlüsselte Daten zu übermitteln. Eine SSL-Verschlüsselungsoption dient zum Deaktivieren von schwachen Chiffrierschlüsseln. Auf der Basis einer asymmetrischen Verschlüsselungstechnologie wird SSL als eine allgemein akzeptierte Methode für die Bereitstellung einer authentifizierten und verschlüsselten Kommunikation zwischen Clients und Servern betrachtet, um unbefugtes Abhören in einem Netzwerk zu vermeiden.

Ein SSL-aktiviertes System kann die folgenden Aufgaben ausführen:

- Sich an einem SSL-aktivierten Client authentifizieren
- Beiden Systemen gestatten, eine verschlüsselte Verbindung herzustellen

ANMERKUNG: Wenn die SSL-Verschlüsselung auf 256 Bit oder höher festgelegt ist, erfordern die Kryptografie-Einstellungen für die Umgebung Ihrer virtuellen Maschine (JVM, IcedTea) möglicherweise eine Installation der Richtliniendateien Unlimited Strength Java Cryptography Extension, um die Verwendung von iDRAC-Plugins wie der vConsole mit dieser Verschlüsselungsebene zuzulassen. Weitere Informationen über das Installieren der Richtliniendateien finden Sie in der Dokumentation zu Java.

iDRAC Webserver verfügt standardmäßig über ein von Dell selbst signiertes, eindeutiges digitales SSL-Zertifikat. Sie können das standardmäßige SSL-Zertifikat durch ein von einer bekannten Zertifizierungsstelle signiertes Zertifikat ersetzen. Eine Zertifizierungsstelle ist ein Unternehmen, das in der IT-Industrie dafür anerkannt ist, hohe Ansprüche bezüglich des zuverlässigen Screenings, der Identifizierung und anderen wichtigen Sicherheitskriterien zu erfüllen. Beispiele für Zertifizierungsstellen sind Thawte und VeriSign. Um den Prozess des Abrufens signierter Zertifikate zu initiieren, verwenden Sie entweder die iDRAC-Web-Schnittstelle oder die RACADM-Schnittstelle. Über diese Schnittstellen können Sie eine Zertifikatsignierungsanforderung (CSR) mit den Daten für Ihr Unternehmen generieren. Übermitteln Sie anschließend die generierte Zertifikatsignierungsanforderung (CSR) an eine Zertifizierungsstelle wie VeriSign oder Thawte. Bei einer Zertifizierungsstelle kann es sich um eine Stammzertifizierungsstelle oder um eine Zwischenzertifizierungsstelle handeln. Nachdem Sie das von der Zertifizierungsstelle signierte SSL-Zertifikat erhalten haben, laden Sie es in iDRAC hoch.

Für jeden iDRAC, dem die Management Station vertrauen soll, muss das jeweilige iDRAC-SSL-Zertifikat im Zertifikatspeicher der Management Station platziert werden. Wenn das SSL-Zertifikat auf den Management Stations installiert ist, können unterstützte Browser auf iDRAC ohne Zertifikatswarnungen zugreifen.

Sie können zur Signierung des SSL-Zertifikats auch ein benutzerdefiniertes Signaturzertifikat hochladen, anstatt des Standardsignaturzertifikats für diese Funktion. Durch den Import eines benutzerdefinierten Signaturzertifikats in alle Management Stations werden alle iDRACs als vertrauenswürdig gekennzeichnet, die dieses benutzerdefinierte Signaturzertifikat verwenden. Falls ein benutzerdefiniertes Signaturzertifikat hochgeladen wird, wenn ein anderes benutzerdefiniertes SSL-Zertifikat bereits verwendet wird, wird das benutzerdefinierte SSL-Zertifikat deaktiviert und ein einmaliges, automatisch generiertes SSL-Zertifikat verwendet, das mit dem benutzerdefinierten Signaturzertifikat signiert ist. Sie können das benutzerdefinierte Signaturzertifikat (ohne den privaten Schlüssel) herunterladen. Sie können auch das vorhandenen Signaturzertifikat löschen. Nach Löschen des benutzerdefinierten Signaturzertifikats setzt iDRAC dieses zurück und generiert automatisch ein neues, selbst signiertes SSL-Zertifikat. Wenn ein selbst signiertes Zertifikat erneut generiert wird, muss die Vertrauensstellung zwischen iDRAC und der Management Workstation erneut konfiguriert werden. Automatisch generierte SSL-Zertifikate sind selbst signiert und haben ein Ablaufdatum von sieben Jahren und einem Tag; das Startdatum liegt einen Tag zurück (wegen verschiedener Zeitzoneneinstellungen für die Management Stations und iDRAC).

Das SSL-Zertifikat für iDRAC-Webserver unterstützt Sternchen (*) als Teil der am weitesten links stehenden Komponente des allgemeinen Namens im Rahmen der Generierung einer Zertifikatsignierungsanforderung (CSR). Zum Beispiel *.qa.com oder *.company.qa.com. Dies wird als Platzhalterzertifikat bezeichnet. Wenn eine Zertifikatsignierungsanforderung mit Platzhaltern außerhalb von iDRAC generiert wird, können Sie ein einzelnes signiertes SSL-Zertifikat mit Platzhaltern für mehrere iDRACs hochladen. Alle iDRACs gelten für unterstützte Browser als vertrauenswürdig. Beim Herstellen einer Verbindung zur iDRAC Webschnittstelle unter Verwendung eines unterstützten Browsers, das ein Platzhalterzertifikat unterstützt, gilt iDRAC für den Browser als vertrauenswürdig. Beim Starten der Ansichten gelten die iDRACs für die Anzeigeclients als vertrauenswürdig.

Zugehöriger Link

Neue Zertifikatsignierungsanforderung erstellen
Serverzertifikat hochladen
Serverzertifikat anzeigen
Hochladen eines benutzerdefinierten Signaturzertifikats
Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen
Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat löschen

Neue Zertifikatsignierungsanforderung erstellen

Eine CSR ist eine digitale Anforderung eines SSL-Serverzertifikats von einer Zertifizierungsstelle (CA). SSL-Serverzertifikate ermöglichen Clients des Servers, die Identität des Servers als vertrauenswürdig einzustufen und eine verschlüsselte Sitzung mit dem Server auszuhandeln.

Nachdem die Zertifizierungsstelle eine Zertifikatssignierungsanforderung erhalten hat, werden die in der CSR enthaltenen Informationen eingesehen und überprüft. Wenn der Bewerber die Sicherheitsstandards der Zertifizierungsstelle erfüllt, erteilt die Zertifikatzertifizierungsstelle ein digital signiertes SSL-Serverzertifikat, das den Server des Anmeldenden beim Aufbau von SSL-Verbindungen über Browser, die auf Management Stations ausgeführt werden, eindeutig identifiziert.

Nach der Genehmigung der Zertifikatsignierungsanforderung (CSR) und der Ausgabe des Serverzertifikats durch die Zertifikatzertifizierungsstelle kann die CSR auf iDRAC hochgeladen werden. Die Informationen, die zum Generieren der CSR verwendet und auf der iDRAC-Firmware gespeichert werden, müssen mit den Informationen auf dem SSL-Serverzertifikat übereinstimmen, dies bedeutet, dass das Zertifikat mithilfe der durch iDRAC erstellte CSR generiert worden sein muss.

Zugehöriger Link

SSL-Serverzertifikate

CSR unter Verwendung der Webschnittstelle erstellen

Um neue CSR zu erstellen:

ANMERKUNG: Jede neue Zertifikatsignierungsanforderung überschreibt alle vorangegangenen, in der Firmware gespeicherten Daten. Die Informationen in der Zertifikatsignierungsanforderung müssen den Informationen im Zertifikat entsprechen. Andernfalls akzeptiert der iDRAC nicht das Zertifikat.

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **SSL**, wählen Sie **Eine neue Zertifikatsignierungsanforderung erstellen (CSR)** aus, und klicken Sie auf **Weiter**.

   Daraufhin wird die Seite **Ein neues Zertifikat erstellen** angezeigt.
2. Geben Sie einen Wert für jedes CSR-Attribut ein.

   Weitere Informationen finden Sie in der *iDRAC Online-Hilfe*.
3. Klicken Sie auf **Erstellen**.

   Es wird eine neue CSR erzeugt. Speichern Sie sie in der Management Station.

CSR über RACADM generieren

Um eine CSR unter Verwendung von RACADM zu erzeugen, verwenden Sie den Befehl **set** mit den Objekten in der Gruppe **iDRAC.Security** und verwenden dann den Befehl **sslcsrgen**, um die CSR zu generieren

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Serverzertifikat hochladen

Nach der Generierung einer Zertifikatsignierungsanforderung (CSR) können Sie das signierte SSL-Serverzertifikat auf die iDRAC-Firmware hochladen. iDRAC muss zurückgesetzt werden, um das Zertifikat anzuwenden. iDRAC akzeptiert nur X509- und Base 64-kodierte Webserver-Zertifikate. SHA-2-Zertifikate werden ebenfalls unterstützt.

VORSICHT: Während des Resets ist iDRAC für einige Minuten nicht verfügbar.

Zugehöriger Link

SSL-Serverzertifikate

Serverzertifikat über die Web-Schnittstelle hochladen

So laden Sie das SSL-Serverzertifikat hoch:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **SSL**, wählen Sie **Serverzertifikat hochladen** aus, und klicken Sie dann auf **Weiter**.

   Die Seite **Zertifikat hochladen** wird angezeigt.
2. Klicken Sie unter **Dateipfad** auf **Durchsuchen**, und wählen Sie dann das Zertifikat auf der Management Station aus.
3. Klicken Sie auf **Anwenden**.

   Das SSL-Serverzertifikat wird auf iDRAC hochgeladen.
4. Ein Fenster öffnet sich, in dem Sie aufgefordert werden, iDRAC sofort oder zu einem späteren Zeitpunkt zurückzusetzen. Klicken Sie nach Bedarf auf **iDRAC zurücksetzen** oder **iDRAC später zurücksetzen**.

   iDRAC wird zurückgesetzt, und das neue Zertifikat wird angewendet. Während des Resets ist iDRAC für einige Minuten nicht verfügbar.

   ANMERKUNG: Sie müssen iDRAC zurücksetzen, um das neue Zertifikat anzuwenden. Bis iDRAC zurückgesetzt wird, ist das vorhandene Zertifikat gültig.

Serverzertifikat über RACADM hochladen

Um das SSL-Serverzertifikat hochzuladen, verwenden Sie den Befehl **sslcertupload**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC) unter **dell.com/idracmanuals**.

Wenn die CSR außerhalb von iDRAC mit einem verfügbaren privaten Schlüssel erstellt wird, laden Sie das Zertifikat wie folgt auf iDRAC hoch:

1. Senden Sie die CSR zu einer bekannten Zertifizierungsstelle. Diese unterzeichnet die CSR, wodurch aus der CSR ein gültiges Zertifikat wird.
2. Laden Sie den privaten Schlüssel mithilfe des Remote-RACADM-Befehls `sslkeyupload` hoch.
3. Laden Sie das signierte Zertifikat mithilfe des Remote-RACADM-Befehls `sslcertupload` auf iDRAC hoch.

   Das neue Zertifikat wurde für iDRAC hochgeladen. Eine Meldung wird angezeigt, in der Sie aufgefordert werden, iDRAC zurückzusetzen.
4. Führen Sie den Befehl racadm **racreset** aus, um iDRAC zurückzusetzen.

   iDRAC wird zurückgesetzt, und das neue Zertifikat wird angewendet. Während des Resets ist iDRAC für einige Minuten nicht verfügbar.

   ANMERKUNG: Sie müssen iDRAC zurücksetzen, um das neue Zertifikat anzuwenden. Bis iDRAC zurückgesetzt wird, ist das vorhandene Zertifikat gültig.

Serverzertifikat anzeigen

Sie können das SSL-Serverzertifikat, das derzeit in iDRAC verwendet wird, anzeigen.

Zugehöriger Link

SSL-Serverzertifikate

Serverzertifikat über die Web-Schnittstelle anzeigen

Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **SSL**. Die Seite **SSL** zeigt oben auf der Seite das SSL-Serverzertifikat an, das derzeit verwendet wird.

Serverzertifikat über RACADM anzeigen

Um das SSL-Serverzertifikat anzuzeigen, verwenden Sie den Befehl **sslcertview**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Hochladen eines benutzerdefinierten Signaturzertifikats

Sie können ein benutzerdefiniertes Signaturzertifikat zum Signieren des SSL-Zertifikats hochladen. SHA-2-Zertifikate werden ebenfalls unterstützt.

Hochladen von benutzerdefinierten Signaturzertifikaten mithilfe der Web-Schnittstelle

So laden Sie ein benutzerdefiniertes Signaturzertifikat mithilfe der iDRAC-Webschnittstelle hoch:

1. Gehen Sie zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **SSL**.
   Die Seite **SSL** wird angezeigt.
2. Wählen Sie unter **Benutzerdefiniertes SSL-Zeritfikatssignaturzertifikat Benutzerdefiniertes SSL-Zeritfikatssignaturzertifikat hochladen** aus und klicken Sie auf **Weiter**.
   Die Seite **Benutzerdefiniertes SSL-Zeritfikatssignaturzertifikat hochladen** wird angezeigt.
3. Klicken Sie auf **Durchsuchen** und wählen Sie das benutzerspezifische SSL-Zertifikat Signierungszertifikatdatei aus.
   Es werden nur Zertifikate, die mit Public-Key Cryptography Standards #12 (PKCS #12) konform sind, unterstützt.
4. Wenn das Zertifikat kennwortgeschützt ist, geben Sie in das Feld **PKCS#12 Kennwort** das Kennwort ein.
5. Klicken Sie auf **Anwenden**.
   Das Zertifikat wird auf iDRAC hochgeladen.
6. Ein Fenster öffnet sich, in dem Sie aufgefordert werden, iDRAC sofort oder zu einem späteren Zeitpunkt zurückzusetzen. Klicken Sie nach Bedarf auf **iDRAC zurücksetzen** oder **iDRAC später zurücksetzen**.
   Nachdem iDRAC zurückgesetzt wurde, werden die neuen Zertifikats angewendet. Während des Zurücksetzens ist iDRAC für einige Minuten nicht verfügbar.

   ANMERKUNG: Sie müssen iDRAC zurücksetzen, um das neue Zertifikat anzuwenden. Bis iDRAC zurückgesetzt wird, ist das vorhandene Zertifikat gültig.

Hochladen eines benutzerdefinierten SSL-Zeritfikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Zertifikatsignaturzertifikat mit RACADM hochzuladen, verwenden Sie den Befehl **sslcertupload** und dann den Befehl **racreset**, um iDRAC zurückzusetzen.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **www.dell.com/idracmanuals**.

Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen

Sie können das benutzerdefinierte Signaturzertifikat mithilfe der iDRAC-Webschnittstelle oder RACADM herunterladen.

Benutzerdefiniertes Signierungszertifikat herunterladen

So laden Sie Benutzerdefinierte Signierungszertifikate unter Verwendung der iDRAC Webschnittstelle herunter:

1 Gehen Sie zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **SSL**.
Die Seite **SSL** wird angezeigt.

2 Wählen Sie unter **Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat** die Option **Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen** und klicken Sie auf **Weiter**.
Ein Fenster öffnet sich, über das Sie das benutzerdefinierte Signierungszertifikat an den Speicherort Ihrer Wahl speichern können.

Herunterladen eines benutzerdefinierten SSL-Zeritfikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Zeritfikatssignaturzertifikat herunterzuladen, verwenden Sie den Unterbefehl **sslcertdownload**. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide* (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC) unter **dell.com/idracmanuals**.

Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat löschen

Sie können ein bestehendes benutzerdefiniertes Signierungszertifikat auch unter Verwendung der iDRAC Webschnittstelle oder RACADM löschen.

Löschen von benutzerdefinierten Signaturzertifikaten mithilfe der iDRAC-Webschnittstelle

So löschen Sie ein benutzerdefiniertes Signaturzertifikat mithilfe der iDRAC-Webschnittstelle:

1 Gehen Sie zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **SSL**.
Die Seite **SSL** wird angezeigt.

2 Wählen Sie unter **Benutzerdefiniertes SSL-Zeritfikatssignaturzertifikat Benutzerdefiniertes SSL-Zeritfikatssignaturzertifikat löschen** aus und klicken Sie auf **Weiter**.

3 Ein Fenster öffnet sich, in dem Sie aufgefordert werden, iDRAC sofort oder zu einem späteren Zeitpunkt zurückzusetzen. Klicken Sie nach Bedarf auf **iDRAC zurücksetzen** oder **iDRAC später zurücksetzen**.
Nachdem iDRAC zurückgesetzt wird, wird ein neues selbstsigniertes Zertifikat generiert.

Löschen eines benutzerdefinierten SSL-Zeritfikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Zertifikatsignaturzertifikat unter Verwendung von RACADM zu löschen, verwenden Sie den Unterbefehl **sslcertdelete**. Verwenden Sie dann den Befehl **racreset**, um iDRAC zurückzusetzen.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **www.dell.com/idracmanuals**.

Mehrere iDRACs über RACADM konfigurieren

Sie können einen oder mehrere iDRACs mit identischen Eigenschaften über RACADM konfigurieren. Wenn Sie einen spezifischen iDRAC über seine Gruppen-ID und die Objekt-ID abfragen, erstellt RACADM eine Konfigurationsdatei .cfg aus den abgerufenen Informationen. Importieren Sie die Datei für identische Konfigurationen auf andere iDRACs.

ANMERKUNG:

- Die Konfigurationsdatei enthält Informationen, die für den bestimmten Server anwendbar sind. Diese Informationen sind unter verschiedenen Objekt-Gruppen organisiert.
- Einige Konfigurationsdateien enthalten eindeutige iDRAC-Informationen (z. B. die statische IP-Adresse), die Sie ändern müssen, bevor Sie die Datei auf andere iDRACs importieren.

Sie können auch das Systemkonfigurationsprofil verwenden, um mehrere iDRACs mit RACADM zu konfigurieren. Die XML-Datei der Systemkonfiguration enthält die Informationen zur Komponentenkonfiguration. Sie können diese Datei verwenden, um die Konfiguration für BIOS, iDRAC, RAID und NIC anzuwenden, indem die Datei in ein Zielsystem importiert wird. Weitere Informationen finden Sie im Whitepaper *XML Configuration Workflow*, das unter **dell.com/support/manuals** oder im Dell Tech Center verfügbar ist.

So konfigurieren Sie mehrere iDRACs unter Verwendung der Konfigurationsdatei:

1 Rufen Sie den Ziel-iDRAC ab, der die erforderliche Konfiguration enthält, indem Sie den folgenden Befehl verwenden:

```
racadm get -f <file_name>.xml -t xml
```

Der Befehl fordert die iDRAC-Konfiguration an und generiert die Konfigurationsdatei.

ANMERKUNG: Das Umleiten der iDRAC-Konfiguration zu einer Datei unter Verwendung von `get -f` wird nur bei den lokalen und Remote-RACADM-Schnittstellen unterstützt.

ANMERKUNG: Die erstellte Konfigurationsdatei enthält keine Benutzerkennwörter.

Der Befehl **get** zeigt alle Konfigurationseigenschaften in einer Gruppe (angegeben nach Gruppenname und Index) und alle Konfigurationseigenschaften für einen Benutzer an.

2 Ändern Sie falls erforderlich die Konfigurationsdatei mit einem einfachen Texteditor.

ANMERKUNG: Es wird empfohlen, diese Datei mit einem einfachen Texteditor zu bearbeiten. Das RACADM-Dienstprogramm verwendet einen ASCII-Text-Parser. Jede Formatierung verursacht Störungen bei der Analyse und kann die RACADM-Datenbank beschädigen.

3 Auf dem Ziel-iDRAC verwenden Sie den folgenden Befehl zum Ändern der Einstellungen:

```
racadm set -f <file_name>.xml -t xml
```

Durch diesen Befehl werden die Informationen in den anderen iDRAC geladen. Sie können den Befehl **set** verwenden, um die Benutzer- und Kennwortdatenbank mit Server Administrator zu synchronisieren.

4 Setzen Sie den Ziel-iDRAC über den folgenden Befehl zurück: `racadm racreset`

iDRAC-Konfigurationsdatei erstellen

Die Konfigurationsdatei kann über folgenden Zustand verfügen:

- Erstellt.
- Erhalten unter Verwendung des Befehls `racadm get -f <file_name>.xml -t xml`.
- Erhalten unter Verwendung von `racadm get -f <file_name>.xml -t xml` und dann bearbeitet.

  Informationen zum Befehl **get** finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)*, der unter **dell.com/idracmanuals** verfügbar ist.

Die Konfigurationsdatei wird zunächst analysiert, um zu überprüfen, dass gültige Gruppen- und Objektnamen vorhanden sind und die grundlegenden Syntaxregeln befolgt werden. Fehler werden mit der Zeilennummer markiert, wo der Fehler ermittelt wurde, und eine Meldung beschreibt das Problem. Die gesamte Datei wird auf Richtigkeit analysiert und alle Fehler werden angezeigt. Schreibbefehle werden nicht zu iDRAC übertragen, wenn in der Datei ein Fehler gefunden wird. Sie müssen alle Fehler korrigieren, bevor Sie die Datei verwenden, um iDRAC zu konfigurieren.

VORSICHT: Verwenden Sie den Befehl `racresetcfg`, um die Datenbank und die iDRAC-NIC-Einstellungen auf die Standardeinstellungen zurückzusetzen und alle Benutzer und Benutzerkonfigurationen zu entfernen. Während der Stammbenutzer verfügbar ist, werden die Einstellungen anderer Benutzer ebenfalls auf die Standardeinstellungen zurückgesetzt.

Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen auf einem Host-System deaktivieren

Sie können den Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen über einen lokalen RACADM oder ein Dienstprogramm für iDRAC-Einstellungen deaktivieren. Außerdem können Sie diese Konfigurationseinstellungen anzeigen. Gehen Sie dazu wie folgt vor:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Dienste**.
2. Wählen eine oder beide der folgenden Maßnahmen aus:
   - **Lokale iDRAC-Konfiguration unter Verwendung der iDRAC-Einstellungen deaktivieren** – Deaktiviert den Zugriff zum Ändern der Konfigurationseinstellungen im Dienstprogramm für die iDRAC-Einstellungen.
   - **Lokale iDRAC-Konfiguration unter Verwendung von RACADM deaktivieren** – Deaktiviert den Zugriff zum Ändern der Konfigurationseinstellungen im lokalen RACADM.
3. Klicken Sie auf **Anwenden**.

ANMERKUNG: Wenn der Zugriff zum Ändern deaktiviert ist, können Sie Server Administrator oder IPMITool nicht zum Ändern der iDRAC-Konfigurationen verwenden. Sie können jedoch IPMI-über-LAN verwenden

5

Anzeigen von Informationen zu iDRAC und zum Managed System

Sie können den Zustand und die Eigenschaften für iDRAC und das Managed System, außerdem die Bestandsliste zu Hardware und Firmware, den Zustand des Sensors, die Speichergeräte und die Netzwerkgeräte anzeigen. Darüber hinaus können Sie Benutzersitzungen anzeigen und beenden. Bei Blade-Servern können Sie außerdem Informationen zur Flex-Adresse anzeigen.

Themen:

Zugehöriger Link

Zustand und Eigenschaften des Managed System anzeigen

Wenn Sie sich bei der iDRAC-Webschnittstelle anmelden, können Sie auf der Seite **Systemzusammenfassung** den Zustand des Managed System und Basis-iDRAC-Informationen anzeigen, eine Vorschau auf die virtuelle Konsole abrufen, Arbeitsnotizen hinzufügen und anzeigen und Aufgaben schnell starten, wie z. B. Aus- und Einschalten, Protokolle anzeigen, Firmware aktualisieren und Firmware-Rollback durchführen, die LED an der Frontblende ein- oder ausschalten und iDRAC zurücksetzen.

Gehen Sie zum Aufrufen der Seite **Systemzusammenfassung** zu **Übersicht** > **Server** > **Eigenschaften** > **Zusammenfassung**. Daraufhin wird die Seite **Systemzusammenfassung** angezeigt. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Außerdem können Sie die Basis-Systemzusammenfassungsinformationen über das Dienstprogramm für die iDRAC-Einstellungen anzeigen. Gehen Sie dazu im Dienstprogramm für die iDRAC-Einstellungen zu **Systemzusammenfassung**. Daraufhin wird die Seite **iDRAC-**

Einstellungen – Systemzusammenfassung angezeigt. Weitere Informationen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

System-Bestandsaufnahme anzeigen

Sie können die Informationen zu den auf dem Managed System installierten Hardware- und Firmware-Komponenten anzeigen. Gehen Sie dazu in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Eigenschaften** > **System-Bestandsaufnahme**. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

Der Abschnitt Hardware-Bestandsaufnahme zeigt die Informationen für die folgenden Komponenten an, die auf dem Managed System verfügbar sind:

- iDRAC
- RAID-Controller
- Batterien
- CPUs
- DIMMs
- HDDs
- Rückwandplatinen
- Netzwerk-Schnittstellenkarten (integrierte und eingebettete)
- Videokarte
- SD-Karte
- Netzteile
- Lüfter
- Fibre-Channel-HBAs
- USB
- NVMe PCIe SSD-Geräte

Der Abschnitt Firmware-Bestandsaufnahme zeigt die Firmware-Version für die folgenden Komponenten:

- BIOS
- Lifecycle-Controller
- iDRAC
- BS-Treiberpaket
- 32-Bit Diagnose
- System CPLD
- PERC-Controller
- Batterien
- Physische Laufwerke
- Netzteil
- NIC
- Fibre-Channel
- Rückwandplatine
- Gehäuse
- PCIe-SSD-Laufwerke

ANMERKUNG: In der Software-Bestandsaufnahme werden nur die letzten 4 Byte der Firmware-Version angezeigt. Beispiel: Wenn die Firmware-Version FLVDL06 lautet, wird in der Bestandsliste DL06 angezeigt.

ANMERKUNG: Auf Dell PowerEdge FX2-/FX2s-Servern unterscheidet sich die Namenskonvention der CMC-Version in der iDRAC-GUI von der Version in der CMC-GUI. Die Version muss jedoch unverändert bleibt.

Wenn Sie Hardware-Komponente ersetzen oder die Firmware-Versionen aktualisieren, müssen Sie sicherstellen, dass Sie die Option **System-Bestandsaufnahme beim Neustart erstellen** (CSIOR) aktivieren und ausführen, um eine System-Bestandsaufnahme beim

Neustart zu erstellen. Melden Sie sich nach einigen Minuten bei iDRAC an, und navigieren Sie zur Seite **System-Bestandsaufnahme**, um die Details anzuzeigen. Es kann in Abhängigkeit von der auf dem Server installierten Hardware bis zu fünf Minuten dauern, bis die Informationen angezeigt werden.

ANMERKUNG: CSIOR-Option ist standardmäßig aktiviert.

ANMERKUNG: Konfigurationsänderungen und Firmware-Aktualisierungen, die innerhalb des Betriebssystems erfolgen, werden möglicherweise erst nach einem Serverneustart richtig in der Bestandsaufnahme angezeigt.

Klicken Sie auf **Exportieren**, um die Hardware-Bestandsaufnahme in ein XML-Format zu exportieren und speichern Sie sie an einen Speicherplatz Ihrer Wahl.

Sensorinformationen anzeigen

Die folgenden Sensoren unterstützen Sie bei der Überwachung des Zustands des verwalteten Systems:

- **Batterien** – Bietet Informationen zu den Batterien auf dem Hauptplatinen-CMOS und dem Speicher-RAID auf der Hauptplatine (ROMB).

  ANMERKUNG: Die Einstellungen für Speicher-ROMB-Batterien sind nur verfügbar, wenn das System einen ROMB mit einer Batterie aufweist.
- **Lüfter** (nur für Rack- und Tower-Server verfügbar) – Bietet Informationen zu Lüftern in Systemen – Lüfterredundanz und Lüfterliste, in der die Lüftergeschwindigkeit und die Schwellenwerte angezeigt werden.
- **CPU** – Zeigt den Zustand und den Status der CPUs im verwalteten System an. Zeigt Informationen zur automatischen Prozessordrosselung an und vorhergesagte Fehler.
- **Speicher** – Zeigt den Funktionszustand und den allgemeinen Zustand der im Managed System vorhandenen Speichermodule mit zwei Kontaktanschlussreihen (Dual In-line Memory Module, DIMM) an.
- **Eingriff** – Zeigt Informationen über das Gehäuse an.
- **Netzteil** (nur für Tack- und Tower-Server) – Bietet Informationen zu den Netzteilen und dem Status der Netzteilredundanz.

  ANMERKUNG: Wenn das System nur ein Netzteil aufweist, ist die Netzteilredundanz deaktiviert.
- **Entfernbarer Flash-Datenträger** – Bietet Informationen zu den internen SD-Modulen, vFlash und Internal Dual SD Module (IDSDM).
  - Wenn IDSDM-Redundanz aktiviert ist, werden die folgenden IDSDM-Sensorstatus angezeigt: IDSDM-Redundanzstatus , IDSDM SD1 und IDSDM SD2. Wenn Redundanz deaktiviert ist, wird nur IDSDM SD1 angezeigt.
  - Wenn IDSDM-Redundanz beim Einschalten des Systems oder nach dem Zurücksetzen von iDRAC deaktiviert wird, wird der IDSDM SD1-Sensorstatus nur angezeigt, wenn eine Karte eingesetzt wird.
  - Wenn IDSDM-Redundanz aktiviert ist, während zwei SD-Karten im IDSDM vorhanden sind, und sich eine SD-Karte im Online-Modus befindet, während sich die andere Karte im Offline-Modus befindet. Es ist ein Neustart des Systems erforderlich, um die Redundanz zwischen den beiden SD-Karten im IDSDM wiederherzustellen. Nach der Wiederherstellung der Redundanz befinden sich beide SD-Karten im IDSDM wieder im Online-Modus.
  - Während der Wiederherstellung der Redundanz zwischen zwei SD-Karten, die sich im IDSDM befinden, wird der IDSDM-Status nicht angezeigt, da die IDSDM-Sensoren ausgeschaltet sind.

    ANMERKUNG: Wenn das Hostsystem während der IDSDM-Wiederherstellung neu gestartet wird, zeigt iDRAC die IDSDM-Informationen nicht an. Um dieses Problem zu beheben, erstellen Sie das IDSDM neu oder setzen Sie iDRAC zurück.

    ANMERKUNG: Auf Dell PowerEdge-Servern der 13. Generation wird der Vorgang zum Neugenerieren von IDSDM im Hintergrund ausgeführt und das System während des Wiederaufbauvorgangs nicht angehalten. Sie können die Lifecycle Controller-Protokolle überprüfen, um den Status des Wiederherstellungsvorgangs anzuzeigen. Auf einem Dell PowerEdge-Server der 12. Generation wird das System angehalten, während der Wiederherstellungsvorgang durchgeführt wird.
  - Die Systemereignisprotokolle (SEL) für eine schreibgeschützte oder beschädigte SD-Karte im IDSDM-Modul werden erst wiederholt, nachdem sie durch das Ersetzen der SD-Karte durch eine beschreibbare und funktionsfähige SD-Karte gelöscht wurden.
- **Temperatur** – Bietet Informationen zu den Lufteintritts- und Luftaustrittstemperaturen auf der Systemplatine (nur bei Rack-Servern). Die Temperaturmessung zeigt an, ob sich der Status des Messgeräts innerhalb des vordefinierten Warnwerts oder des kritischen Schwellenwerts befindet.
- **Spannung** – Zeigt den Status und die Messwerte des Spannungssensors für verschiedene Systemkomponenten an.

Die folgende Tabelle enthält Informationen über das Anzeigen der Sensorinformationen unter Verwendung der iDRAC-Webschnittstelle und RACADM. Weitere Informationen zu den in der Webschnittstelle angezeigten Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

ANMERKUNG: Die Seite „Hardware-Übersicht“ zeigt nur Daten für Sensoren an, die auf Ihrem System vorhanden sind.

Tabelle 15. Abrufen von Sensorinformationen über die Web-Schnittstelle und RACADM

Sensorinformationen anzeigen für	über die Web-Schnittstelle	RACADM verwenden
Batterien	**Übersicht** > **Hardware** > **Batterien**	Verwenden Sie den Befehl **getsensorinfo**. Bei Netzteilen können Sie außerdem den Befehl **System.Power.Supply** mit dem Unterbefehl **get** verwenden. Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.
Lüfter	**Übersicht** > **Hardware** > **Lüfter**	
CPU	**Übersicht** > **Hardware** > **CPU**	
Speicher	**Übersicht** > **Hardware** > **Speicher**	
Eingriff	**Übersicht** > **Server** > **Eingriff**	
Netzteile	**Übersicht** > **Hardware** > **Netzteile**	
Wechselbarer Flash-Datenträger	**Übersicht** > **Hardware** > **Wechselbarer Flash-Datenträger**	
Temperatur	**Übersicht** > **Server** > **Energie/Thermisch** > **Temperaturen** **Übersicht** > **Server** > **Energie/Thermisch** > **Spannungen**	

Überwachen des Leistungsindex für CPU-, Speicher- und E/A-Module

Auf Dell PowerEdge-Servern der 13 Generation unterstützt Intel ME die CUPS-Funktionalität (Compute Usage Per Second, Rechenleistung pro Sekunde). Die CUPS-Funktionalität bietet die Echtzeitüberwachung von CPU-, Speicher- und E/A-Auslastung und Systemebenen-Auslastungsindex für das System. Intel ME ermöglicht Out-of-Band (OOB)-Leistungsüberwachung und verwendet keine CPU-Ressourcen. Intel ME hat einen CUPS-Sensor, der Rechen-, Speicher- und E/A-Ressourcenauslastungswerte als CUPS-Index bereitstellt. iDRAC überwacht diesen CUPS-Index für die gesamte Systemauslastung und überwacht auch den unmittelbaren Auslastungsindex von CPU, Speicher und E/A.

ANMERKUNG: Diese Funktion wird nicht auf PowerEdge R930-Servern unterstützt.

Die CPU und der Chipsatz verfügen über dedizierte Ressourcenüberwachungsindikatoren (RMC). Die Daten von diesen RMCs werden abgefragt, um Auslastungsinformationen zu Systemressourcen abzurufen. Die Daten von RMCs werden durch den Knoten-Manager aggregiert, um die kumulative Auslastung der einzelnen Systemressourcen zu ermitteln, die von iDRAC über die vorhandenen interkommunikativen Mechanismen eingelesen werden, um Daten über bandexterne Verwaltungsschnittstellen bereitzustellen.

Die Darstellung von Intel-Sensoren für Leistungsparameter und Indexwerte beziehen sich auf das gesamte physische System. Daher bezieht sich die Darstellung von Leistungsdaten auf den Schnittstellen auf das gesamte physische System, selbst wenn das System virtualisiert ist und mehrere virtuelle Hosts enthält.

Zum Anzeigen der Leistungsparameter müssen die unterstützten Sensoren auf dem Server vorhanden sein.

Die vier Systemauslastungsparameter sind:

- **CPU-Auslastung** – Daten von RMCs für jeden einzelnen CPU-Kern werden aggregiert, um eine kumulative Auslastung aller Kerne im System bereitzustellen. Diese Auslastung basiert auf der aufgewendeten Zeit in aktiven und inaktiven Zuständen. Alle sechs Sekunden werden RMC-Beispieldaten abgerufen.
- **Speicherauslastung** – RMCs messen Speicherdatenverkehr auf den einzelnen Speicherkanälen oder Speichercontrollerinstanzen. Daten von diesen RMCs werden aggregiert, um den kumulativen Speicherdatenverkehr auf allen Speicherkanälen im System zu messen. Dies ist eine Messung des Speicherbandbreitenbedarfs und keine Speichergrößenauslastung. iDRAC aggregiert dies für eine Minute, sodass sie der Speicherauslastung, die von anderen BS-Tools, wie z. B. **top** unter Linux gezeigt werden, entsprechen können. Speicherbandbreitenauslastung, die iDRAC anzeigt, ist ein Anzeichen dafür, ob eine Arbeitsauslastung speicherintensiv ist.
- **E/A-Auslastung** – Es gibt ein RMC pro Root-Port auf dem PCI Express Root Complex, um den PCI Express-Datenverkehr zu messen, der dem unteren Segment und dem Root-Port entspringt oder dahin dirigiert wird. Daten von diesen RMCs werden aggregiert, um PCI Express-Datenverkehr für alle PCI Express-Segmente zu messen, die diesem Paket entspringen. Dies ist eine Messung für E/A-Bandbreitenauslastung für das System.
- **CUPS-Index auf Systemebene** – Der CUPS-Index wird berechnet, indem der CPU-, Speicher- und E/A-Index unter Berücksichtigung eines vordefinierten Auslastungsfaktors für jede Systemressource aggregiert wird. Der Auslastungsfaktor hängt von der Art der Arbeitsauslastung auf dem System ab. CUPS-Index repräsentiert die Messung der auf dem Server verfügbaren Berechnungsaussteuerungsreserve. Wenn das System über einen großen CUPS-Index verfügt, steht auf diesem System begrenzte Aussteuerungsreserve bereit, um mehr Arbeitsauslastung auf diesem System zu platzieren. Mit abnehmender Ressourcenauslastung reduziert sich auch der CUPS-Index. Ein niedriger CUPS-Index gibt an, dass eine große Berechnungsaussteuerungsreserve vorliegt und der Server neue Arbeitsauslastungen empfangen kann und der Server über einen niedrigeren Stromzustand verfügt, um den Stromverbrauch zu reduzieren. Arbeitsauslastungsüberwachung kann dann auf das gesamte Rechenzentrum angewendet werden, um eine allgemeine und ganzheitliche Sicht auf die Arbeitsauslastung des Rechenzentrums bereitzustellen, wodurch eine dynamische Lösung für das Rechenzentrum bereitgestellt wird.

ANMERKUNG: Die Indizes für die CPU-, Speicher- und E/A-Auslastung werden über einen Zeitraum von einer Minute zusammengefasst. Wenn es unmittelbare Spitzen in diesen Indizes gibt, werden sie möglicherweise unterdrückt. Diese sind ein Anzeichen für Arbeitslastmuster, nicht aber für die Menge der Ressourcennutzung.

Die IPMI-, SEL- und SNMP-Traps werden generiert, wenn die Schwellenwerte für die Auslastungsindizes erreicht und die Sensorereignisse aktiviert sind. Die Sensorereigniskennzeichnungen sind standardmäßig deaktiviert. Sie können jedoch über die Standard-IPMI-Schnittstelle aktiviert werden.

Im Folgenden werden die erforderlichen Berechtigungen aufgeführt:

- Anmeldeberechtigung für die Überwachung der Leistungsdaten
- Konfigurationsberechtigung für das Einstellen der Warnungsschwellenwerte und das Zurücksetzen der Verlaufsspitzen
- Anmeldeberechtigung und eine Enterprise-Lizenz sind erforderlich, um historische Statistikdaten zu lesen.

Überwachen des Leistungsindex für CPU-, Speicher- und E/A-Module über die Webschnittstelle

Um den Leistungsindex von CPU, Speicher und E/A-Modulen zu überwachen, gehen Sie in der iDRAC-Webschnittstelle zu **Overview (Übersicht)** > **Hardware**. Auf der Seite **Hardware Overview (Hardware-Übersicht)** wird Folgendes angezeigt:

- Abschnitt **Hardware** – Klicken Sie auf den erforderlichen Link, um den Zustand der Komponente anzuzeigen.
- Abschnitt **Systemleistung** – Zeigt den aktuellen Messwert und den Warnungsmesswert für den CPU-, Speicher- und E/A-Auslastungsindex sowie den CUPS-Index auf Systemebene in einer grafischen Ansicht an.
- Abschnitt **Historische Daten der Systemleistung**:
  - Stellt Statistiken zur CPU-, Speicher und zur E/A-Auslastung sowie zum CUPS-Index auf Systemebene bereit. Wenn das Host-System ausgeschaltet ist, zeigt das Diagramm die Zeile für die ausgeschaltete Stromversorgung unter „0 Prozent“ an.
  - Sie können die maximale Auslastung für einen bestimmten Sensor zurücksetzen. Klicken Sie auf **Reset Historical Peak (Historischen Spitzenwert zurücksetzen)**. Sie müssen über die Berechtigung zur Konfiguration verfügen, um den Spitzenwert zurückzusetzen.
- Abschnitt **Leistungskennzahlen**:

- Zeigt den Status an und präsentiert Messwerte .
- Warnungsschwellenwert für die Auslastungsgrenze anzeigen oder festlegen. Sie müssen über Berechtigungen zum Konfigurieren des Servers verfügen, um die Schwellenwerte festlegen zu können.

ANMERKUNG: Die angezeigten Informationen auf dieser Seite hängen von den Sensoren ab, die von Ihrem Server unterstützt werden. Alle Dell PowerEdge Server der 12. Generation und bestimmte Dell Power Server der 13. Generation zeigen die Abschnitte System Performance (Systemleistung), System Performance Historical Data (Historische Daten der Systemleistung) und Performance Metrics (Leistungsmetriken) nicht an.

Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

Überwachen des Leistungsindex für CPU-, Speicher- und E/A-Module über RACADM

Verwenden Sie den Unterbefehl **SystemPerfStatistics** zur Überwachung des Leistungsindex für CPU-, Speicher- und E/A-Module. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Das System auf Frischlufttauglichkeit prüfen

Die Frischluftkühlung kühlt die Systeme im Datenzentrum direkt mit Außenluft. Frischlufttaugliche Systeme können oberhalb ihres normalen Betriebstemperaturbereichs betrieben werden (Temperaturen bis zu 113 °F (45 °C)).

ANMERKUNG: Einige Server oder bestimmte Konfigurationen eines Servers sind nicht frischlufttauglich. Weitere Informationen zu den Details für die Frischluftkompatibilität finden Sie im jeweiligen Serverhandbuch, oder wenden Sie sich an Dell, um weitere Informationen zu erhalten.

So prüfen Sie das System auf Frischlufttauglichkeit:

1 Gehen Sie in der iDRAC-Weboberfläche zu **Übersicht** > **Server** > **Leistung/Wärme** > **Temperaturen**.
Die **Temperatur**-Seite wird angezeigt.
2 Im Bereich **Frischluft** wird angezeigt, ob das System frischlufttauglich ist oder nicht.

Temperaturverlaufsdaten anzeigen

Sie können den Prozentsatz der Zeit überwachen, in der das System bei einer Umgebungstemperatur betrieben wurde, die oberhalb des normalerweise unterstützten Temperaturschwellenwertes für Frischluft liegt. Der Messwert des Temperatursensors der Systemplatine wird über einen gewissen Zeitraum erfasst, um die Temperatur zu überwachen. Die Datenerfassung beginnt beim ersten Einschalten nach dem Versand aus dem Werk. Die Daten werden erfasst und angezeigt, während das System eingeschaltet ist. Sie können die überwachte Temperatur für die vergangenen sieben Jahre nachverfolgen und speichern.

ANMERKUNG: Sie können den Verlauf der Temperatur auch für Systeme verfolgen, die nicht Fresh-Air-kompatibel sind. Die grenzwert- und frischluftbezogenen Warnungen basieren jedoch auf Grenzwerten für die Frischluftunterstützung. Die Grenzwerte liegen bei 42 °C für Warnungen und bei 47 °C für kritische Warnungen. Diese Werte entsprechen Frischluftgrenzwerten von 40 °C und 45 °C mit einer Genauigkeitsmarge von 2 °C.

Es werden zwei feste Temperaturbereiche erfasst, die mit Grenzwerten für Frischluftkühlung verknüpft sind:

- Warnbereich: besteht aus der Zeitdauer, während derer ein System oberhalb des Temperatursensor-Warnschwellenwerts (42 °C) betrieben wurde. Das System darf in zwölf Monaten 10 % der Zeit im Warnbereich betrieben werden.
- Kritischer Bereich: besteht aus der Zeitdauer, während derer ein System oberhalb des kritischen Temperatursensor-Schwellenwerts (47 °C) betrieben wurde. Das System darf in zwölf Monaten 1 % der Zeit im kritischen Bereich betrieben werden, wozu auch die Zeit im Warnbereich zählt.

Die erfassten Daten werden in einem grafischen Format dargestellt, um die Werte von 10 % und 1 % nachzuverfolgen. Die protokollierten Temperaturdaten können nur vor der Auslieferung vom Werk gelöscht werden.

Ein Ereignis wird erstellt, wenn das System weiterhin über dem normalerweise unterstützten Temperaturschwellwert während einer angegebenen Betriebszeit betrieben wird. Entspricht die Durchschnittstemperatur während der angegebenen Betriebszeit der Warnungsebene (> 8 %) oder der kritischen Ebene (> 0,8 %) bzw. liegt sie darüber, wird im Lifecycle-Protokoll ein Ereignis protokolliert und die entsprechende SNMP-Trap erstellt. Es gibt folgende Ereignisse:

- Warnereignis, wenn die Temperatur während 8 % oder mehr der vergangenen zwölf Monate oberhalb des Warnschwellenwertes lag.
- Kritisches Ereignis, wenn die Temperatur während 10 % oder mehr der vergangenen zwölf Monate oberhalb des Warnschwellenwertes lag.
- Warnereignis, wenn die Temperatur während 0,8 % oder mehr der vergangenen zwölf Monate oberhalb des kritischen Schwellenwertes lag.
- Kritisches Ereignis, wenn die Einlasstemperatur während 1 % oder mehr der vergangenen zwölf Monate oberhalb des kritischen Schwellenwertes lag.

Sie können iDRAC auch so konfigurieren, dass weitere Ereignisse erzeugt werden. Weitere Informationen finden Sie im Abschnitt Alarmwiederholungsereignis einrichten.

Anzeigen der Temperaturverlaufsdaten über die iDRAC-Webschnittstelle

So zeigen Sie den Verlauf der Temperaturdaten an:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Leistung/Wärme** > **Temperaturen**.

Die **Temperatur**-Seite wird angezeigt.

2 Im Bereich **Verlauf der Systemplatinentemperatur** wird in einem grafischen Schaubild die gespeicherte Temperatur (Durchschnitts- und Spitzenwerte) für den letzten Tag, die letzten 30 Tage und das letzte Jahr angezeigt.

Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

ANMERKUNG: Nach einer Aktualisierung der iDRAC-Firmware oder einem Reset des iDRAC werden manche Temperaturdaten möglicherweise nicht mehr im Schaubild angezeigt.

Temperaturverlaufsdaten über RACADM anzeigen

Um den Datenverlauf unter Verwendung von RACADM anzuzeigen, verwenden Sie den Befehl **inlettemphistory**.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Konfigurieren des Warnungsschwellenwerts für die Einlasstemperatur

Sie können die minimalen und maximalen Warnungsschwellenwerte für den Einlasstemperatursensor ändern. Wenn Sie den Vorgang zum Zurücksetzen auf die Standardwerte ausführen, werden die Warnungsschwellenwerte für die Temperatursonden auf die Standardwerte eingestellt. Sie müssen die Benutzerberechtigung zum Festlegen von Warnungsschwellenwerten für die Einlasstemperatursensor haben.

Konfigurieren der Warnschwelle für die Einlasstemperatur über die Webschnittstelle

So konfigurieren Sie den Warnungsschwellenwert für die Einlasstemperatur:

1 Gehen Sie in der iDRAC-Webschnittstelle auf **Übersicht** > **Server** > **Leistung/Thermisch** > **Temperaturen**.

Die **Temperatur**-Seite wird angezeigt.

2 Geben Sie im Abschnitt **Temperatursonden** für die **Systemplatineneinlasstemperatur** die Mindest- und Höchstwerte für die **Warnschwelle** in Celsius oder Fahrenheit an. Wenn Sie den Wert in Celsius eingeben, berechnet das System automatisch den Wert in Fahrenheit und zeigt ihn an. Ebenso gilt: Wenn Sie Fahrenheit eingeben, wird der Wert in Celsius angezeigt.

3 Klicken Sie auf **Anwenden**.

Die Werte werden konfiguriert.

ANMERKUNG: Änderungen an den Standardschwellenwerten werden im Diagramm mit den historischen Daten nicht dargestellt, da sich die Diagrammgrenzwerte nur auf Werte für Frischluft beziehen. Die Warnungen in Bezug auf die Überschreitung der benutzerdefinierten Schwellenwerte weichen von der Warnung zur Überschreitung der Frischluftgrenzwerte ab.

Anzeigen der auf dem Host-Betriebssystem verfügbaren Netzwerkschnittstellen

Sie können die Informationen über alle verfügbaren Netzwerkschnittstellen auf dem Host-Betriebssystem anzeigen, wie z. B. die IP-Adressen, die dem Server zugewiesen sind. Das iDRAC-Servicemodul stellt iDRAC diese Informationen bereit. Die Informationen umfassen die IP-Adresse des Betriebssystems, die IPv4- und IPv6-Adressen, MAC-Adresse, Subnetz-Maske bzw. Präfix-Länge, die FQDD des Netzwerkgeräts, Netzwerkschnittstellenbezeichnung, Beschreibung der Netzwerkschnittstelle, den Status der Netzwerkschnittstelle, Netzwerkschnittstellentyp (Ethernet, Tunnel, Loopback usw.), Gateway-Adresse, DNS-Server-Adresse und DHCP-Serveradresse.

ANMERKUNG: Diese Funktion ist mit den iDRAC Express- und Enterprise-Lizenzen erhältlich.

Zum Anzeigen der Informationen zum Betriebssystem, stellen Sie Folgendes sicher:

- Sie verfügen über die Berechtigung zur Anmeldung.
- Das iDRAC-Service-Modul ist auf dem Host-Betriebssystem installiert und wird ausgeführt.
- Die Option für die BS-Informationen ist auf der Seite **Übersicht** > **Server** > **Service-Modul** aktiviert.

iDRAC kann die IPv4- und IPv6-Adressen für alle Schnittstellen anzeigen, die auf dem Host-Betriebssystem konfiguriert sind.

Je nach vom Host-Betriebssystem für die Ermittlung des DHCP-Servers verwendeter Methode kann die zugehörige IPv4- oder IPv6-DHCP-Server-Adresse möglicherweise nicht angezeigt werden.

Anzeigen von verfügbaren Netzwerkschnittstellen auf dem Host-Betriebssystem über die Webschnittstelle

So zeigen Sie die Netzwerkschnittstellen auf dem Host-Betriebssystem über die Webschnittstelle an:

1 Wechseln Sie zu **Übersicht** > **Host-Betriebssystem** > **Netzwerkschnittstellen**.

Die Seite **Netzwerkschnittstellen** zeigt alle Netzwerkschnittstellen an, die auf dem Host-Betriebssystem verfügbar sind.

2 Um die Liste der Netzwerkschnittstellen anzuzeigen, die mit einem Netzwerkgerät verknüpft sind, wählen Sie ein Netzwerkgerät aus dem Drop-Down-Menü **Netzwerkgeräte-FQDD** aus, und klicken Sie dann auf **Anwenden**.

Die Betriebssystem-IP-Details werden im Abschnitt **Host-BS-Netzwerkschnittstellen** angezeigt.

3 Klicken Sie in der Spalte **Geräte-FQDD** auf den Link für das Netzwerkgerät.

Die entsprechende Geräteseite wird im Abschnitt **Hardware** > **Network Devices (Netzwerkgeräte)** angezeigt, auf der Sie die Gerätedetails anzeigen können. Weitere Informationen zu den Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

4 Klicken Sie auf das Symbol +, um weitere Informationen zu erhalten.

In ähnlicher Weise können Sie die Informationen zur Hostbetriebssystem-Netzwerkschnittstelle anzeigen, die mit einem Netzwerkgerät verknüpft sind. Diese Informationen befinden sich auf der Seite **Hardware** > **Network Devices (Netzwerkgeräte)**. Klicken Sie auf **View Host OS Network Interfaces (Host-BS-Netzwerkschnittstellen anzeigen)**.

ANMERKUNG: Ab Version 2.3.0 des iDRAC-Servicemoduls wird für das ESXi-Host-BS die Spalte Beschreibung in der Liste Zusätzliche Details in folgendem Format angezeigt:

```
<List-of-Uplinks-Configured-on-the-vSwitch>/<Port-Group>/<Interface-name>
```

Anzeigen der auf dem Host-Betriebssystem verfügbaren Netzwerke über RACADM

Verwenden Sie den Befehl **gethostnetworkinterfaces**, um die Netzwerkschnittstellen auf Hostbetriebssystemen über RACADM anzuzeigen. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Verbindungen der FlexAddress-Mezzanine-Kartenarchitektur anzeigen

In Blade Servern ermöglicht FlexAddress die Verwendung von beständigen, dem Gehäuse zugewiesenen World-Wide-Namen und MAC-Adressen (WWN/MAC) für jede verwaltete Server-Anschlussverbindung.

Sie können die folgenden Informationen für jede installierte eingebettete Ethernet- und optionalen Mezzanine-Kartenschnittstelle anzeigen:

- Strukturen, mit denen die Karten verbunden sind
- Strukturtyp
- MAC-Adressen, die Servern, Gehäusen oder remote zugewiesen sind

Um Flex-Adressinformationen in iDRAC anzuzeigen, konfigurieren und aktivieren Sie die FlexAddress-Funktion über den Chassis Management Controller (CMC). Weitere Informationen finden Sie im *Dell Chassis Management Controller User Guide* (Dell Chassis Management Controller-Benutzerhandbuch) unter **dell.com/support/manuals**. Alle aktiven Sitzungen für die virtuelle Konsole oder virtuellen Datenträger werden beendet, wenn die FlexAddress-Einstellung aktiviert oder deaktiviert ist.

ANMERKUNG: Um Fehler zu vermeiden, die zu einer Stromunterversorgung auf dem verwalteten System führen können, *muss* der richtige Mezzanine-Kartentyp für jede Anschluss- und Architekturverbindung installiert sein.

Die FlexAddress-Funktion ersetzt die Server-zugewiesenen MAC-Adressen durch Gehäuse-zugewiesene MAC-Adressen und wird für den iDRAC zusammen mit Blade-LOMs, Mezzanine-Karten und E/A-Modulen eingesetzt. Die Funktion FlexAddress des iDRAC unterstützt die Bewahrung der steckplatzspezifischen MAC-Adressen für iDRACs in einem Gehäuse. Die Gehäuse-zugewiesene MAC-Adresse wird im permanenten CMC-Speicher abgelegt und bei einem iDRAC-Start oder einer Aktivierung der CMC-FlexAddress an den iDRAC gesendet.

Wenn CMC Gehäusen zugewiesene MAC-Adressen aktiviert, zeigt iDRAC die **MAC-Adresse** auf den folgenden Seiten an:

- **Übersicht** > **Server** > **Eigenschaften Details** > **iDRAC-Informationen**.
- **Übersicht** > **Server** > **Eigenschaften WWN/MAC**.
- **Übersicht** > **iDRAC-Einstellungen** > **EigenschaftenIDRAC-Informationen** > **Derzeitige Netzwerkeinstellungen**.
- **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Netzwerkeinstellungen**.

VORSICHT: Wenn Sie bei aktivierter FlexAddress zwischen Server-zugewiesener MAC-Adresse und Gehäuse-zugewiesener MAC-Adresse umschalten oder umgekehrt, ändert sich auch die iDRAC-IP-Adresse.

Anzeigen und Beenden von iDRAC-Sitzungen

Sie können die Anzahl der Benutzer anzeigen, die derzeit bei iDRAC angemeldet sind, und die Benutzersitzungen beenden.

Beenden der iDRAC-Sitzungen über die Webschnittstelle

Benutzer ohne Administratorberechtigungen benötigen eine Berechtigung zum Konfigurieren von iDRAC, um iDRAC-Sitzungen über die iDRAC-Webschnittstelle beenden zu können.

So zeigen Sie die iDRAC-Sitzungen an und beenden sie:

1 Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Sitzungen**.

Daraufhin werden auf der Seite **Sitzungen** die Sitzungs-ID, der Benutzername, die IP-Adresse und der Sitzungstyp angezeigt. Weitere Informationen zu diesen Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

2 Klicken Sie zum Beenden der Sitzung in der Spalte **Beenden** auf das Papierkorbsymbol für eine Sitzung.

Beenden von iDRAC-Sitzungen über RACADM

Sie benötigen Administratorberechtigungen, um iDRAC-Sitzungen über RACADM beenden zu können.

Verwenden Sie zum Anzeigen der aktuellen Benutzersitzungen den Befehl **getssninfo**.

Verwenden Sie zum Beenden einer Benutzersitzung den Befehl **closessn**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

6

Einrichten der iDRAC-Kommunikation

Sie können über eine der folgenden Modi mit iDRAC kommunizieren:

- iDRAC-Web-Schnittstelle
- Serielle Verbindung mithilfe eines DB9-Kabels (serielle RAC-Verbindung oder serielle IPMI-Verbindung) – nur für Rack- und Tower-Server
- Serielle IPMI-Verbindung über LAN
- IPMI über LAN
- Remote-RACADM
- Lokaler RACADM
- Remote-Dienste

ANMERKUNG: Um sicherzustellen, dass lokale RACADM Import- oder Exportbefehle ordnungsgemäß funktionieren, vergewissern Sie sich, dass der USB-Massenspeicherhost im Betriebssystem aktiviert ist. Informationen zum Aktivieren des USB-Speicherhosts finden Sie in der Dokumentation Ihres Betriebssystems.

Die folgende Tabelle enthält eine Übersicht der unterstützten Protokolle und Befehle sowie die Voraussetzungen:

Tabelle 16. Kommunikationsmodi – Übersicht

Kommunikationsmodus	Unterstütztes Protokoll	Unterstützte Befehle	Voraussetzung
iDRAC-Web-Schnittstelle	Internet-Protokolle (https)	k. A.	Webserver
Serielle Verbindung über Null-Modem-DB9-Kabel	Protokoll für serielle Verbindung	RACADM	Teil der iDRAC-Firmware
		SMCLP	Serielle RAC- oder IPMI-Verbindungen ist aktiviert
		IPMI	
Serielle IPMI-Verbindung über LAN	Intelligent Platform Management Bus-Protokoll	IPMI	IPMITool ist installiert, und die serielle IPMI-Verbindung über LAN ist aktiviert
	SSH		
	Telnet		
IPMI über LAN	Intelligent Platform Management Bus-Protokoll	IPMI	IPMITool ist installiert und die IPMI-Einstellungen sind aktiviert
SMCLP	SSH	SMCLP	SSH oder Telnet auf iDRAC ist aktiviert
	Telnet		
Remote-RACADM	HTTPS	Remote-RACADM	Remote-RACADM ist installiert und aktiviert
Firmware RACADM	SSH	Firmware RACADM	Firmware-RACADM ist installiert und aktiviert.
	Telnet		
Lokaler RACADM	IPMI	Lokaler RACADM	Lokaler RACADM ist installiert

Kommunikationsmodus	Unterstütztes Protokoll	Unterstützte Befehle	Voraussetzung
Remote-Dienste [1]	WS-MAN	WinRM (Windows) OpenWSMAN (Linux)	WinRM ist installiert (Windows), oder OpenWSMAN ist installiert (Linux)
	Redfish	Verschiedene Browser-Plug-ins, CURL (Windows und Linux), Python-Aufforderung und JSON-Module	Plug-ins, CURL, Python Module sind installiert

[1] Weitere Informationen finden Sie im *Lifecycle Controller Remote Services User's Guide* (Dell Lifecycle Controller Remote Services-Benutzerhandbuch) unter **dell.com/idracmanuals**

Themen:

Zugehöriger Link

Mit iDRAC über eine serielle Verbindung über ein DB9-Kabel kommunizieren
Von der seriellen RAC-Verbindung auf die serielle Konsolenverbindung bei Verwendung eines DB9-Kabels umschalten
Mit iDRAC über IPMI SOL kommunizieren
Mit iDRAC über IPMI über LAN kommunizieren
Remote-RACADM aktivieren oder deaktivieren
Lokalen RACADM deaktivieren
IPMI auf Managed System aktivieren
Linux während des Starts für die serielle Konsole konfigurieren
Unterstützte SSH-Verschlüsselungssysteme

Mit iDRAC über eine serielle Verbindung über ein DB9-Kabel kommunizieren

Sie können jede der folgenden Kommunikationsmethoden verwenden, um Systemverwaltungsaufgaben über eine serielle Verbindung auf den Rack- und Tower-Servern durchzuführen:

- Serielle RAC-Verbindung
- Serielle IPMI-Verbindung – Grundlegender Modus „Direktverbindung“ und Terminalmodus „Direktverbindung“

ANMERKUNG: Bei Blade-Servern wird die serielle Verbindung über das Gehäuse aufgebaut. Weitere Informationen finden Sie im *Chassis Management Controller User's Guide (Chassis Management Controller-Benutzerhandbuch)* unter dell.com/support/manuals.

So bauen Sie eine serielle Verbindung auf:

1 Konfigurieren Sie das BIOS, um die serielle Verbindung zu aktivieren.
2 Verbinden Sie das Null-Modem-DB9-Kabel von der seriellen Schnittstelle auf der Management Station mit dem externen seriellen Konnektor auf dem verwalteten System.

3 Stellen Sie sicher, dass die Terminal-Emulations-Software der Management Station für jede serielle Verbindung über eine der folgenden Methoden konfiguriert ist:

- Linux Minicom in einem Xterm
- Hilgraeve HyperTerminal Private Edition (Version 6.3)

Je nachdem, an welcher Stelle des Startvorgangs sich das verwaltete System derzeit befindet, wird entweder der POST-Bildschirm oder der Betriebssystembildschirm angezeigt. Die Anzeige richtet sich nach der Konfiguration: SAC für Windows und Linux-Textmodusbildschirme für Linux.

4 Aktivieren Sie serielle RAC- oder IPMI-Verbindungen auf iDRAC.

Zugehöriger Link

BIOS für serielle Verbindung konfigurieren
Serielle RAC-Verbindung aktivieren
Grundlegenden seriellen IPMI-Verbindungs- und -Terminalmodus aktivieren

BIOS für serielle Verbindung konfigurieren

So konfigurieren Sie das BIOS für serielle Verbindungen:

ANMERKUNG: Dies gilt nur für iDRAC auf Rack- und Tower-Servern.

1 Schalten Sie das System ein oder starten Sie es neu.
2 Klicken Sie auf F2.
3 Gehen Sie zu **System-BIOS-Einstellungen** > **Serielle Kommunikation**.
4 Wählen Sie **Externer serieller Konnektor** auf **Remote-Zugriffsgerät** aus.
5 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
6 Drücken Sie auf die Esc-Taste, um das **System-Setup**-Programm zu beenden.

Serielle RAC-Verbindung aktivieren

Nach der Konfiguration der seriellen Verbindung im BIOS aktivieren Sie die serielle RAC-Verbindung in iDRAC.

ANMERKUNG: Dies gilt nur für iDRAC auf Rack- und Tower-Servern.

Serielle RAC-Verbindungen über die Web-Schnittstelle aktivieren

So aktivieren Sie die serielle RAC-Verbindung:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Serielle Verbindung**.
Die Seite **Serielle Verbindung** wird angezeigt.
2 Wählen Sie unter **Serielle RAC-Verbindung** die Option **Aktiviert** aus, und legen Sie die Attributwerte fest.
3 Klicken Sie auf **Anwenden**.
Damit werden die seriellen RAC-Einstellungen konfiguriert.

Serielle RAC-Verbindung über RACADM aktivieren

Um die serielle RAC-Verbindung über RACADM zu aktivieren, verwenden Sie den Befehl **set** mit dem Objekt in der Gruppe **iDRAC.Serial**.

Grundlegenden seriellen IPMI-Verbindungs- und -Terminalmodus aktivieren

Konfigurieren Sie zum Aktivieren der seriellen IPMI-Weiterleitung des BIOS an iDRAC die serielle IPMI-Verbindung in den folgenden iDRAC-Modi:

ANMERKUNG: Dies gilt nur für iDRAC auf Rack- und Tower-Servern.

- Grundlegender IPMI-Modus - Unterstützt eine binäre Schnittstelle für Programmzugriff, z. B. die IPMI-Shell (ipmish), die zum Lieferumfang des Baseboard-Verwaltungsdienstprogramms (BMU) gehört. Beispiel: Führen Sie zum Ausdrucken des Systemereignisprotokolls mittels ipmish über den grundlegenden IPMI-Modus den folgenden Befehl aus:

  ```
  ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
  ```

- IPMI-Terminalmodus – Unterstützt ASCII-Befehle, die von einem seriellen Terminal gesendet werden. Dieser Modus unterstützt eine begrenzte Anzahl von Befehlen (einschließlich der Stromsteuerung) und Raw-IPMI-Befehle, die als hexadezimale ASCII-Zeichen eingegeben werden. Mit dieser Funktion können Sie die Startsequenzen für das Betriebssystem bis zum BIOS anzeigen, wenn Sie sich bei iDRAC über SSH oder Telnet anmelden.

Zugehöriger Link

BIOS für serielle Verbindung konfigurieren

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus

Serielle Verbindung über die Web-Schnittstelle aktivieren

Stellen Sie sicher, dass Sie die serielle RAC-Schnittstelle für die Aktivierung der seriellen IPMI-Verbindung deaktivieren.

So konfigurieren Sie die Einstellungen für serielle IPMI-Verbindungen:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Serielle Verbindung**.
2. Legen Sie unter **Serielle IPMI-Verbindung** die Werte für die Attribute fest. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**.

IPMI-Modus für die serielle Verbindung über RACADM aktivieren

Um den IPMI-Modus zu konfigurieren, deaktivieren Sie die serielle RAC-Schnittstelle und aktivieren dann den IPMI-Modus.

```
racadm set iDRAC.Serial.Enable 0
racadm set iDRAC.IPMISerial.ConnectionMode <n>
```

n=0 - Terminalmodus

n=1 - Grundlegender Modus

Einstellungen für serielle IPMI-Verbindung über RACADM aktivieren

1. Ändern Sie den Modus für die serielle IPMI-Verbindung über den folgenden Befehl auf die gewünschte Einstellung.

   ```
   racadm set iDRAC.Serial.Enable 0
   ```

2. Stellen Sie die serielle Baudrate für IPMI über den folgenden Befehl ein.

   ```
   racadm set iDRAC.IPMISerial.BaudRate <baud_rate>
   ```

Parameter	Zulässige Werte (in bps)
<baud_rate>	9600, 19200, 38400, 57600 und 115200.

3 Aktivieren Sie die Hardware-Datenflusssteuerung der seriellen IPMI-Hardware über den folgenden Befehl.

```
racadm set iDRAC.IPMISerial.FlowContro 1
```

4 Stellen Sie die Mindestberechtigungsebene des seriellen IPMI-Kanals unter Verwendung des Befehls ein.

```
racadm set iDRAC.IPMISerial.ChanPrivLimit <level>
```

Parameter	Berechtigungsstufe
<level> = 2	Benutzer
<level> = 3	Operator
<level> = 4	Administrator

5 Stellen Sie sicher, dass der serielle MUX (externer serieller Konnektor) über das BIOS-Setup-Programm ordnungsgemäß für das Remote-Zugriffsgerät eingestellt ist, um das BIOS für die serielle Verbindung zu konfigurieren.

Weitere Informationen über diese Eigenschaften finden Sie in der IPMI 2.0-Spezifikation.

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus

In diesem Abschnitt finden Sie zusätzliche Konfigurationseinstellungen für den seriellen IPMI-Terminalmodus.

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus über die Web-Schnittstelle konfigurieren

So legen Sie die Terminalmoduseinstellungen fest:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Seriell**

Die Seite **Serial** wird angezeigt.

2 Aktivieren Sie „Serielle IPMI-Verbindung“.

3 Klicken Sie auf **Terminalmoduseinstellungen** .

Daraufhin wird die Seite **Terminalmoduseinstellungen** angezeigt.

4 Legen Sie die folgenden Werte fest:

- Zeilenbearbeitung
- Löschsteuerung
- Echo-Steuerung
- Handshaking-Steuerung
- Neue Zeilenreihenfolge
- Neue Zeilenfolgen eingeben

Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

5 Klicken Sie auf **Anwenden**.

Die Terminalmoduseinstellungen werden konfiguriert.

6 Stellen Sie sicher, dass der serielle MUX (externer serieller Konnektor) über das BIOS-Setup-Programm ordnungsgemäß für das Remote-Zugriffsgerät eingestellt ist, um das BIOS für die serielle Verbindung zu konfigurieren.

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus über RACADM konfigurieren

Um die Terminalmoduseinstellungen zu konfigurieren, verwenden Sie den Befehl **set** mit den Objekten in der Gruppe **idrac.ipmiserial**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Von der seriellen RAC-Verbindung auf die serielle Konsolenverbindung bei Verwendung eines DB9-Kabels umschalten

iDRAC unterstützt Escape-Tastensequenzen, mit denen Sie zwischen der seriellen RAC-Schnittstellenkommunikation und der seriellen Konsole auf den Rack- und Tower-Servern umschalten können.

Von der seriellen Konsole auf die serielle RAC-Verbindung umschalten

Um zum Kommunikationsmodus „Serielle RAC-Schnittstelle“ umzuschalten, wenn Sie sich im Modus „Serielle Konsole“ befinden, betätigen Sie Esc+Umschalttaste, 9.

Mit der obigen Tastenfolge rufen Sie entweder die `iDRAC Login` auf (wenn der iDRAC auf den seriellen RAC-Modus gesetzt ist) oder den seriellen Anschlussmodus, in dem Terminalbefehle abgeben werden können (wenn der iDRAC auf den seriellen IPMI-Terminalmodus bei Direktverbindung eingestellt ist).

Von der seriellen RAC-Verbindung auf die serielle Konsole umschalten

Um auf den Modus „Serielle Konsole“ umzuschalten, wenn Sie sich im Kommunikationsmodus „Serielle RAC-Schnittstelle“ befinden, betätigen Sie Esc+Umschalttaste, Q.

Betätigen Sie im Terminalmodus zum Umschalten der Verbindung zum Modus „Serielle Konsole“ Esc+Umschalttaste, Q.

Um zum Terminalmodus zurückzukehren, wenn Sie über den Modus „Serielle Konsole“ verbunden sind, betätigen sie Esc+Umschalttaste, 9.:

Mit iDRAC über IPMI SOL kommunizieren

Mit der seriellen IPMI über LAN-Verbindung kann die textbasierte Konsole eines Managed System serielle Daten über das dedizierte oder freigegebene bandexterne Ethernet-Verwaltungsnetzwerk von iDRAC umleiten. Mit der Verwendung von SOL können Sie Folgendes ausführen:

- Ohne zeitliche Beschränkung remote auf Betriebssysteme zugreifen.
- Hostsysteme auf Emergency Management Services (EMS) oder Special Administrator Console (SAC) für Windows oder Linux-Shell diagnostizieren.
- Fortschritt eines Servers während des POST (Einschalt-Selbsttest) anzeigen und das BIOS-Setup-Programm neu konfigurieren

So richten Sie den SOL-Kommunikationsmodus ein:

1 Konfigurieren Sie das BIOS für die serielle Verbindung.
2 Konfigurieren Sie iDRAC für die Verwendung von SOL.
3 Aktivieren Sie ein unterstütztes Protokoll (SSH, Telnet, IPMItool).

Zugehöriger Link

BIOS für serielle Verbindung konfigurieren
iDRAC für die Verwendung von SOL konfigurieren
Unterstütztes Protokoll aktivieren

BIOS für serielle Verbindung konfigurieren

ANMERKUNG: Dies gilt nur für iDRAC auf Rack- und Tower-Servern.

1 Schalten Sie das System ein oder starten Sie es neu.
2 Klicken Sie auf F2.
3 Gehen Sie zu **System-BIOS-Einstellungen** > **Serielle Kommunikation**.
4 Legen Sie die folgenden Werte fest:
   - Serielle Kommunikation – Eingeschaltet mit Konsolenumleitung
   - Adresse der seriellen Schnittstelle – COM2

     ANMERKUNG: Sie können die serielle Kommunikation auf Eingeschaltet mit serieller Umleitung über COM1 einstellen, wenn das Adressfeld des seriellen Anschlusses, Serielles Gerät2, auch auf COM1 eingestellt ist.
   - Externer serieller Anschluss - Serielles Gerät2
   - Failsafe-Baud-Rate – 115.200
   - Remote-Terminaltyp... vt100/vt220
   - Umleitung nach Start – Aktiviert
5 Klicken Sie auf **Zurück** und dann auf **Fertigstellen**.
6 Klicken Sie auf **Ja**, um die Änderungen zu speichern.
7 Drücken Sie auf die Esc-Taste, um das **System-Setup**-Programm zu beenden.

ANMERKUNG: BIOS sendet dem Bildschirm serielle Daten im 25 x 80-Format. Das SSH-Fenster, das dazu verwendet wird, den Befehl `console com2` aufzurufen, muss auf 25 x 80 eingestellt sein. Dann wird der umgeleitete Bildschirm korrekt angezeigt.

ANMERKUNG: Wenn der Bootloader oder das Betriebssystem serielle Umleitung wie GRUB oder Linux bereitstellt, muss die BIOS-Einstellung Umleitung nach dem Start deaktiviert sein. Dadurch soll potenzielle Racebedingung mehrerer Komponenten, die auf die serielle Schnittstelle zugreifen, vermieden werden.

iDRAC für die Verwendung von SOL konfigurieren

Sie können die SOL-Einstellungen in iDRAC über die Webschnittstelle, über RACADM oder über das Dienstprogramm für die iDRAC-Einstellungen festlegen.

iDRAC für die Verwendung von SOL über die iDRAC-Webschnittstelle konfigurieren

Um IPMI Seriell über LAN (SOL) zu konfigurieren:

1 Gehen Sie in der iDRAC-Webschnittstelle nach **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Serielle Verbindung über LAN**.
   Die Seite **Seriell über LAN** wird angezeigt.
2 Aktivieren Sie SOL, geben Sie die Werte ein, und klicken Sie dann auf **Anwenden**.
   Die IPMI-SOL-Einstellungen werden konfiguriert.
3 Um das Intervall der Zeichenakkumulation und den Schwellenwert für die gesendeten Zeichen festzulegen, wählen Sie **Erweiterte Einstellungen** aus.

Die Seite **Seriell über LAN - Erweiterte Einstellungen** wird angezeigt.

4 Geben Sie die Werte für die Attribute ein, und klicken Sie auf **Anwenden**.
Die erweiterten Einstellungen für IPMI SOL sind damit konfiguriert. Diese Werte unterstützen Sie bei der Verbesserung der Leistung.

Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

iDRAC für die Verwendung von SOL über RACADM konfigurieren

Um IPMI Seriell über LAN (SOL) zu konfigurieren:

1 Aktivieren Sie unter Verwendung des Befehls „Seriell über LAN“.

```
racadm set iDRAC.IPMISol.Enable 1
```

2 Aktualisieren Sie die IPMI-SOL-Mindestberechtigungsebene unter Verwendung des Befehls.

```
racadm set iDRAC.IPMISol.MinPrivilege <level>
```

Parameter	Berechtigungsstufe
<level> = 2	Benutzer
<level> = 3	Operator
<level> = 4	Administrator

ANMERKUNG: Die Mindestberechtigungsebene für IPMI SOL bestimmt die Mindestberechtigung für die Aktivierung von IPMI SOL. Weitere Informationen finden Sie in den technischen Daten zu IPMI 2.0.

3 Aktualisieren Sie die IPMI-SOL-Baudrate unter Verwendung des Befehls.

```
racadm set iDRAC.IPMISol.BaudRate <baud_rate>
```

ANMERKUNG: Um die serielle Konsole über LAN umzuleiten, stellen Sie sicher, dass die SOL-Baudrate mit der Baudrate des verwalteten Systems übereinstimmt.

Parameter	Zulässige Werte (in bps)
<baud_rate>	9600, 19200, 38400, 57600 und 115200.

4 Aktivieren Sie SOL für jeden Benutzer unter Verwendung des Befehls.

```
racadm set iDRAC.Users.<id>.SolEnable 2
```

Parameter	Beschreibung
<id>	Eindeutige ID des Benutzers

ANMERKUNG: Um die serielle Konsole über LAN umzuleiten, ist sicherzustellen, dass die SOL-Baudrate mit der Baudrate des Managed System identisch ist.

Unterstütztes Protokoll aktivieren

Die unterstützten Protokolle sind IPMI, SSH und Telnet.

Unterstütztes Protokoll über die Web-Schnittstelle aktivieren

Um SSH oder Telnet zu aktivieren, gehen Sie zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Dienste**, und wählen Sie die Option **Aktiviert** für SSH oder Telnet aus.

Gehen Sie zum Aktivieren von IPMI zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk**, und wählen Sie **IPMI über LAN aktivieren** aus. Stellen Sie außerdem sicher, dass der Wert für den **Verschlüsselungsschlüssel** vollständig aus Nullen besteht, oder drücken Sie auf die Rückschritttaste, um den Wert so zu ändern, dass er ausschließlich Nullen enthält.

Unterstütztes Protokoll über RACADM aktivieren

Zum Aktivieren von SSH oder Telnet, führen Sie die folgenden Befehle aus.

- Telnet

  ```
  racadm set iDRAC.Telnet.Enable 1
  ```

- SSH

  ```
  racadm set iDRAC.SSH.Enable 1
  ```

  So ändern Sie den SSH-Port

  ```
  racadm set iDRAC.SSH.Port <port number>
  ```

Sie können u. a. die folgenden Tools verwenden:

- IPMItool zur Verwendung des IPMI-Protokolls
- Putty/OpenSSH zur Verwendung der SSH- oder Telnet-Protokolle

Zugehöriger Link

SOL über das IPMI-Protokoll
SOL unter Verwendung der SSH- oder Telnet-Protokolle

SOL über das IPMI-Protokoll

Das IPMI-basierte SOL-Dienstprogramm, IPMItool, verwendet RMCP+, das unter Verwendung von UDP-Datengrammen an Anschluss 623 geliefert wird. RMCP+ bietet verbesserte Authentifizierung, Datenintegritätsprüfungen und Verschlüsselung sowie die Fähigkeit, verschiedene Arten von Nutzlasten zu tragen. Weitere Informationen finden Sie unter **http://ipmitool.sourceforge.net/manpage.html**.

RMCP+ verwendet für die Authentifizierung einen Verschlüsselungsschlüssel mit einer Hexadezimal-Zeichenkette aus 40 Zeichen (mit den Zeichen 0-9, a-f und A-F). Der Standardwert ist eine Zeichenkette mit 40 Nullen.

Eine RMCP+-Verbindung zu iDRAC muss über den Verschlüsselungsschlüssel (Schlüsselgenerator-Schlüssel) verschlüsselt werden. Sie können den Verschlüsselungsschlüssel über die iDRAC-Web-Schnittstelle oder das Dienstprogramm für die iDRAC-Einstellungen konfigurieren.

So starten Sie eine SOL-Sitzung mithilfe von IPMItool von einer Management Station aus:

ANMERKUNG: Falls erforderlich, können Sie die Standard-SOL-Zeitüberschreitung unter Übersicht > iDRAC-Einstellungen > Netzwerk > Dienste ändern.

1 Installieren Sie IPMITool über die *Dell Systems Management Tools and Documentation*-DVD.
Weitere Anweisungen finden Sie im *Software-Schnellinstallationshandbuch*.

2 In der Eingabeaufforderung (Windows oder Linux) führen Sie den folgenden Befehl aus, um SOL über iDRAC zu starten:

```
ipmitool -H <iDRAC-ip-address> -I lanplus -U <login name> -P <login password> sol activate
```

Mit diesem Befehl wurde eine Verbindung von der Management Station zur seriellen Schnittstelle des Managed System hergestellt.

3 Zum Beenden einer SOL-Sitzung über IPMItool betätigen Sie „~“ und anschließend „.“ (Punkt).

ANMERKUNG: Wenn sich eine SOL-Sitzung nicht beenden lässt, setzen Sie iDRAC zurück, und warten Sie etwa zwei Minuten, bis der Startvorgang vollständig abgeschlossen ist.

SOL unter Verwendung der SSH- oder Telnet-Protokolle

Secure Shell (SSH) sind Netzwerkprotokolle, die zum Ausführen der Kommunikation über Befehlszeilen mit iDRAC verwendet werden. Sie können Remote-RACADM- und SMCLP-Befehle über eine dieser Schnittstellen parsen.

SSH bietet im Vergleich zu Telnet die größere Sicherheit. iDRAC unterstützt nur die SSH-Version 2 mit Kennwortauthentifizierung. Diese Funktion ist standardmäßig aktiviert. iDRAC unterstützt bis zu zwei SSH-Sitzungen und zwei Telnet-Sitzungen gleichzeitig. Aus Sicherheitsgründen wird empfohlen, SSH zu verwenden, da es sich bei Telnet nicht um ein sicheres Protokoll handelt. Sie müssen Telnet nur dann verwenden, wenn Sie den SSH-Client nicht installieren können oder davon ausgehen, dass Ihre Netzwerkinfrastruktur sicher ist.

Verwenden Sie Open Source-Programme, wie z. B. PuTTY oder OpenSSH, die SSH- und Telnet-Netzwerkprotokolle auf einer Management Station unterstützen, um die Verbindung zu iDRAC herzustellen.

ANMERKUNG: Führen Sie `OpenSSH` über einen VT100- oder ANSI-Terminalemulator auf Windows aus. Wenn Sie `OpenSSH` an der Windows-Befehlseingabe ausführen, können Sie nicht auf den vollen Funktionsumfang zugreifen (einige Tasten reagieren nicht, und einige Grafiken werden nicht angezeigt).

Bevor Sie SSH oder Telnet für die Kommunikation mit iDRAC verwenden, müssen Sie die folgenden Schritte ausführen:

1 BIOS für die Aktivierung der seriellen Konsole konfigurieren
2 SOL in iDRAC konfigurieren
3 SSH oder Telnet über die iDRAC-Webschnittstelle oder RACADM aktivieren

Client für Telnet (Schnittstelle 23)/SSH (Schnittstelle 22) <--> WAN-Verbindung <--> iDRAC

Durch das IPMI-basierte SOL, das das SSH- oder Telnet-Protokoll verwendet, erübrigt sich die Verwendung eines zusätzlichen Dienstprogramms, da die Seriell-auf-Netzwerk-Umsetzung innerhalb von iDRAC erfolgt. Die von Ihnen verwendete SSH- oder Telnet-Konsole muss in der Lage sein, die von der seriellen Schnittstelle des verwalteten Systems eingehenden Daten zu interpretieren und darauf zu reagieren. Die serielle Schnittstelle hängt sich in der Regel an eine Shell, die ein ANSI- oder VT100/VT220-Terminal simuliert. Die serielle Konsole wird automatisch auf die SSH- oder Telnet-Konsole umgeleitet.

Zugehöriger Link

SOL über PuTTY auf Windows verwenden
SOL über OpenSSH oder Telnet auf Linux verwenden

SOL über PuTTY auf Windows verwenden

ANMERKUNG: Falls erforderlich, können Sie die Standardeinstellung für Zeitüberschreitungen für SSH oder Telnet über Übersicht > iDRAC-Einstellungen > Netzwerk > Dienste ändern.

So starten Sie IPMI SOL über PuTTY auf einer Windows-Management Station:

1 Führen Sie den folgenden Befehl aus, um eine Verbindung zu iDRAC herzustellen

```
putty.exe [-ssh | -telnet] <login name>@<iDRAC-ip-address> <port number>
```

ANMERKUNG: Die Angabe der Schnittstellennummer ist optional. Sie wird nur dann benötigt, wenn die Schnittstellennummer neu zugewiesen wird.

2 Führen Sie den Befehl `console com2` oder den Befehl `connect` aus, um SOL zu starten und das verwaltete System zu starten.

Es wird eine SOL-Sitzung von der Management Station zum verwalteten System unter Verwendung des SSH- oder des Telnet-Protokolls geöffnet. Folgen Sie zum Aufrufen der iDRAC-Befehlszeilenkonsole der ESC-Tastensequenz. Verhaltensweisen von PuTTY und SOL-Verbindungen:

- Während Sie im Rahmen des POST auf das verwaltete System zugreifen, falls die Funktionstasten und Keypad-Option unter PuTTY wie folgt eingestellt sind:
  - VT100+ – F2 erfolgreich, F12 nicht erfolgreich
  - ESC[n~ – F12 erfolgreich, F2 jedoch nicht erfolgreich
- Wenn unter Windows die Emergency Management System (EMS)-Konsole unmittelbar nach dem Neustart eines Hosts geöffnet wird, wird das Special Admin Console (SAC)-Terminal möglicherweise beschädigt. Beenden Sie die SOL-Sitzung, schließen Sie das Terminal, öffnen Sie ein anderes Terminal, und starten Sie die SOL-Sitzung über den gleichen Befehl.

Zugehöriger Link

Trennen der Verbindung zur SOL-Sitzung in der iDRAC-Befehlszeilenkonsole

SOL über OpenSSH oder Telnet auf Linux verwenden

So verwenden Sie SOL über OpenSSH oder Telnet auf einer Linux-Management Station:

ANMERKUNG: Falls erforderlich, können Sie die Standardzeitüberschreitung für SSH- oder Telnet-Sitzungen unter Overview (Übersicht) > iDRAC Settings (iDRAC-Einstellungen) > Network (Netzwerk) > Services (Dienste)ändern.

1 Starten Sie eine Shell.

2 Stellen Sie eine Verbindung zu iDRAC über den folgenden Befehl her:

- SSH: ssh *<iDRAC-IP-Adresse>* -l *<Anmeldename>*
- Telnet: telnet *<iDRAC-IP-Adresse>*

ANMERKUNG: Wenn Sie die Standardanschlussnummer für den Telnet-Dienst (Anschluss 23) geändert haben, fügen Sie die Anschlussnummer am Ende des Telnet-Befehls hinzu.

3 Geben Sie zum Starten von SOL an der Befehlseingabeaufforderung einen der folgenden Befehle ein:

- `connect`
- `console com2`

Mit diesen Befehlen wird iDRAC mit der SOL-Schnittstelle des verwalteten Systems verbunden. Sobald eine SOL-Sitzung aufgebaut wurde, steht die iDRAC-Befehlszeilenkonsole nicht mehr zur Verfügung. Führen Sie die Escape-Sequenz ordnungsgemäß aus, um die iDRAC-Befehlszeilenkonsole zu öffnen. Die Escape-Sequenz wird außerdem auf dem Bildschirm angezeigt, sobald eine SOL-Sitzung aufgebaut wurde. Wenn das verwaltete System ausgeschaltet ist, kann der Aufbau der SOL-Sitzung einen Moment dauern.

ANMERKUNG: Sie können entweder Konsole com1 oder Konsole com2 verwenden, um SOL zu starten. Starten Sie den Server neu, um die Verbindung herzustellen.

Der Befehl `console -h com2` zeigt den Inhalt des seriellen Verlaufspuffers an, bevor er auf Eingaben über die Tastatur oder neue Zeichen vom seriellen Anschluss wartet.

Die Standardgröße (bzw. maximale Größe) des Verlaufspuffers beträgt 8 192 Zeichen. Sie können diese Zahl auf einen kleineren Wert einstellen, indem Sie den folgenden Befehl verwenden:

```
racadm set iDRAC.Serial.HistorySize <number>
```

4 Beenden Sie die SOL-Sitzung, um eine aktive SOL-Sitzung zu schließen.

Zugehöriger Link

Virtuelle Telnet-Konsole verwenden
Die Rücktaste für die Telnet-Sitzung konfigurieren
Trennen der Verbindung zur SOL-Sitzung in der iDRAC-Befehlszeilenkonsole

Virtuelle Telnet-Konsole verwenden

Einige Telnet-Clients auf Microsoft-Betriebssystemen zeigen den BIOS-Setup-Bildschirm eventuell nicht richtig an, wenn die virtuelle BIOS-Konsole auf die VT100/VT220-Emulation eingestellt ist. Wenn dieses Problem auftritt, können Sie die Anzeige aktualisieren, indem Sie die BIOS-Konsolenumleitung auf ANSI-Modus ändern. Um dieses Verfahren im BIOS-Setup-Menü auszuführen, wählen Sie **Virtuelle Konsole** > **Remote-Terminaltyp** > **ANSI** aus.

Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete virtuelle Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine ordnungsgemäße Textanzeige sicherzustellen. Andernfalls werden einige Textanzeigen möglicherweise nicht richtig dargestellt.

So verwenden Sie virtuelle Telnet-Konsole:

1 Aktivieren Sie **Telnet** in den **Windows-Komponentendiensten**.

2 Stellen Sie unter Verwendung des folgenden Befehls eine Verbindung zu iDRAC her

```
telnet <IP address>:<port number>
```

Parameter	Beschreibung
`<IP address>`	IP-Adresse für iDRAC
`<port number>`	Telnet-Port-Nummer (falls Sie einen neuen Port verwenden)

Die Rücktaste für die Telnet-Sitzung konfigurieren

Je nach verwendetem Telnet-Client kann die Verwendung der Rücktaste zu unerwarteten Ergebnissen führen. Die Sitzung kann beispielsweise ein `^h`-Echo verursachen. Die meisten Microsoft- und Linux-Telnet-Clients können jedoch für die Verwendung der Rücktaste konfiguriert werden.

Um eine Linux Telnet-Sitzung für die Verwendung der Rückschritttaste zu konfigurieren, öffnen Sie eine Befehlseingabe, und geben Sie den Befehl `stty erase ^h` ein. Geben Sie an der Eingabeaufforderung den Befehl `telnet` ein.

So konfigurieren Sie Microsoft-Telnet-Clients zur Verwendung der Rücktaste:

1. Öffnen Sie ein Eingabeaufforderungsfenster (falls erforderlich).
2. Wenn Sie keine Telnet-Sitzung ausführen, geben Sie `telnet` ein. Wenn Sie hingegen eine Telnet-Sitzung ausführen, drücken Sie auf die Tastenkombination Ctrl+].
3. Geben Sie an der Eingabeaufforderung den Befehl `set bsasdel` ein.

   Daraufhin wird die Meldung `Backspace will be sent as delete` angezeigt.

Trennen der Verbindung zur SOL-Sitzung in der iDRAC-Befehlszeilenkonsole

Die Befehle zum Trennen einer SOL-Sitzung basieren auf dem Dienstprogramm. Sie können das Dienstprogramm nur dann beenden, wenn eine SOL-Sitzung vollständig beendet wurde.

Beenden Sie zum Abbrechen einer SOL-Sitzung die SOL-Sitzung über die iDRAC-Befehlszeilenkonsole.

- Um die SOL-Umleitung zu beenden, betätigen Sie Eingabetaste, Esc, T.

  Die SOL-Sitzung wird geschlossen.
- Zum Beenden einer SOL-Sitzung von Telnet unter Linux drücken und halten Sie Strg+].

  Eine Telnet-Eingabeaufforderung wird angezeigt. Geben Sie `quit` ein, um Telnet zu beenden.

Wenn eine SOL-Sitzung im Dienstprogramm nicht vollständig beendet wurde, sind andere SOL-Sitzungen möglicherweise nicht verfügbar. Um dieses Problem zu lösen, beenden Sie die Befehlszeilenkonsole in der Web-Schnittstelle unter **Übersicht** > **iDRAC-Einstellungen** > **Sitzungen**.

Mit iDRAC über IPMI über LAN kommunizieren

Sie müssen IPMI über LAN für iDRAC konfigurieren, um IPMI-Befehle über LAN-Kanäle auf beliebigen externen Systemen zu aktivieren oder zu deaktivieren. Wenn IPMI über LAN nicht konfiguriert ist, können die externen Systeme nicht über die IPMI-Befehle mit dem iDRAC-Server kommunizieren.

ANMERKUNG: Ab iDRAC-Version 2.30.30.30 unterstützt IPMI auch das IPv6-Adressprotokoll für Linux-basierte Betriebssysteme.

IPMI über LAN mithilfe der Web-Schnittstelle konfigurieren

So konfigurieren Sie IPMI über LAN:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk**.

   Die Seite **Netzwerk** wird angezeigt.
2. Geben Sie unter **IPMI-Einstellungen** die Attributwerte an, und klicken Sie dann auf **Anwenden**.

   Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Die IPMI über LAN-Einstellungen werden konfiguriert.

IPMI über LAN mithilfe des Dienstprogramms für die iDRAC-Einstellungen konfigurieren

So konfigurieren Sie IPMI über LAN:

1 Gehen Sie im **Dienstprogramm für die iDRAC-Einstellungen** zu **Netzwerk**.
Die Seite **iDRAC-Netzwerkeinstellungen** wird angezeigt.

2 Geben Sie die erforderlichen Werte für die **IPMI-Einstellungen** ein.
Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
Die IPMI über LAN-Einstellungen werden konfiguriert.

IPMI über LAN mithilfe von RACADM konfigurieren

1 IPMI-über-LAN aktivieren

```
racadm set iDRAC.IPMILan.Enable 1
```

ANMERKUNG: Diese Einstellung bestimmt die IPMI-Befehle, die von der IPMI-über-LAN-Schnittstelle ausgeführt werden können. Weitere Informationen finden Sie in den IPMI 2.0-Angaben unter intel.com.

2 Aktualisieren Sie die IPMI-Kanalberechtigungen.

```
racadm set iDRAC.IPMILan.PrivLimit <level>
```

Parameter	Berechtigungsstufe
<level> = 2	Benutzer
<level> = 3	Operator
<level> = 4	Administrator

3 Stellen Sie den IPMI-LAN-Kanalverschlüsselungsschlüssel ein, falls erforderlich.

```
racadm set iDRAC.IPMILan.EncryptionKey <key>
```

Parameter	Beschreibung
<key>	20-Zeichen-Verschlüsselungsschlüssel in einem gültigen Hexadezimalformat.

ANMERKUNG: Die iDRAC-IPMI unterstützt das RMCP+-Protokoll. Weitere Informationen finden Sie in den IPMI 2.0-Angaben unter intel.com.

Remote-RACADM aktivieren oder deaktivieren

Sie können Remote-RACADM über die iDRAC-Webschnittstelle oder RACADM aktivieren oder deaktivieren. Sie können bis zu fünf Remote-RACADM-Sitzungen gleichzeitig ausführen.

ANMERKUNG: Remote-RACADM ist standardmäßig aktiviert.

Remote-RACADM über die Web-Schnittstelle aktivieren oder deaktivieren

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Dienste**.
2 Wählen Sie unter **Remote-RACADM** die gewünschte Option aus und klicken Sie auf **Anwenden**.
Entsprechend Ihrer Auswahl ist Remote-RACADM damit aktiviert oder deaktiviert.

Remote-RACADM über RACADM aktivieren oder deaktivieren

ANMERKUNG: Es wird empfohlen, diese Befehle auf Ihrem lokalen System auszuführen.

- So deaktivieren Sie Remote-RACADM:
```
racadm set iDRAC.Racadm.Enable 0
```
- So aktivieren Sie Remote-RACADM:
```
racadm set iDRAC.Racadm.Enable 1
```

Lokalen RACADM deaktivieren

Der lokale RACADM ist standardmäßig aktiviert. Weitere Informationen zum Deaktivieren finden Sie unter Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen auf dem Host-System deaktivieren.

IPMI auf Managed System aktivieren

Verwenden Sie auf einem Managed System Dell Open Manage Server Administrator, um IPMI zu aktivieren oder zu deaktivieren. Weitere Informationen finden Sie im *Dell Open Manage Server Administrator's User Guide* (Dell Open Manage Server Administrator-Benutzerhandbuch) unter **dell.com/support/manuals**.

ANMERKUNG: Ab iDRAC-Version 2.30.30.30 unterstützt IPMI das IPv6-Adressprotokoll für Linux-basierte Betriebssysteme.

Linux während des Starts für die serielle Konsole konfigurieren

Die folgenden Schritte beziehen sich speziell auf den Linux Grand Unified Bootloader (GRUB). Ähnliche Änderungen sind erforderlich, um einen anderen Bootloader zu verwenden.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete virtuelle Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine ordnungsgemäße Textanzeige sicherzustellen. Andernfalls werden einige Textanzeigen möglicherweise nicht richtig dargestellt.

Bearbeiten Sie die Datei **/etc/grub.conf** wie folgt:

1 Suchen Sie in der Datei die Abschnitte zur allgemeinen Einstellung und fügen Sie Folgendes hinzu:
```
serial --unit=1 --speed=57600 terminal --timeout=10 serial
```
2 Hängen Sie zwei Optionen an die Kernel-Zeile an:
```
kernel ............. console=ttyS1,115200n8r console=tty1
```
3 Deaktivieren Sie die grafische GRUB-Schnittstelle und verwenden Sie die textbasierte Schnittstelle. Andernfalls wird der GRUB-Bildschirm nicht in der virtuellen RAC-Konsole angezeigt. Zum Deaktivieren der grafischen Schnittstelle kommentieren Sie die Zeile aus, die mit `splashimage` beginnt.

Das folgende Beispiel enthält ein Beispiel einer **/etc/grub.conf**-Datei, die die in diesem Verfahren beschriebenen Änderungen zeigt.

```
# grub.conf generated by anaconda
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You do not have a /boot partition. This means that all
# kernel and initrd paths are relative to /, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sda1
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0
console=ttyS1,115200n8r
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
initrd /boot/initrd-2.4.9-e.3.im
```

4 Um mehreren GRUB-Optionen das Starten von Sitzungen der virtuellen Konsole über die serielle RAC-Verbindung zu ermöglichen, fügen Sie die folgende Zeile allen Optionen hinzu:

```
console=ttyS1,115200n8r console=tty1
```

Das Beispiel zeigt, dass `console=ttyS1,57600` zur ersten Option hinzugefügt wurde.

ANMERKUNG: Wenn der Bootloader oder das Betriebssystem serielle Umleitung wie GRUB oder Linux bereitstellt, muss die BIOS-Einstellung Umleitung nach dem Start deaktiviert sein. Dadurch soll potenzielle Racebedingung mehrerer Komponenten, die auf die serielle Schnittstelle zugreifen, vermieden werden.

Anmeldung an der virtuellen Konsole nach dem Start aktivieren

Fügen Sie in der Datei **/etc/inittab** eine neue Zeile hinzu, um `agetty` auf der seriellen COM2-Schnittstelle zu konfigurieren:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

Das folgende Beispiel zeigt eine Beispieldatei mit der neuen Zeile.

```
#inittab This file describes how the INIT process should set up #the system in a certain run-
level. #Author:Miquel van Smoorenburg #Modified for RHS Linux by Marc Ewing and Donnie Barnes
#Default runlevel. The runlevels used by RHS are: #0 - halt (Do NOT set initdefault to this) #1
- Single user mode #2 - Multiuser, without NFS (The same as 3, if you do not have #networking)
#3 - Full multiuser mode #4 - unused #5 - X11 #6 - reboot (Do NOT set initdefault to this) id:
3:initdefault: #System initialization. si::sysinit:/etc/rc.d/rc.sysinit l0:0:wait:/etc/rc.d/rc
0 l1:1:wait:/etc/rc.d/rc 1 l2:2:wait:/etc/rc.d/rc 2 l3:3:wait:/etc/rc.d/rc 3 l4:4:wait:/etc/
rc.d/rc 4 l5:5:wait:/etc/rc.d/rc 5 l6:6:wait:/etc/rc.d/rc 6 #Things to run in every runlevel.
ud::once:/sbin/update ud::once:/sbin/update #Trap CTRL-ALT-DELETE ca::ctrlaltdel:/sbin/shutdown
-t3 -r now #When our UPS tells us power has failed, assume we have a few #minutes of power
left. Schedule a shutdown for 2 minutes from now. #This does, of course, assume you have power
installed and your #UPS is connected and working correctly. pf::powerfail:/sbin/shutdown -f -h
+2 "Power Failure; System Shutting Down" #If power was restored before the shutdown kicked in,
cancel it. pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
#Run gettys in standard runlevels co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1 2:2345:respawn:/sbin/mingetty tty2 3:2345:respawn:/sbin/
mingetty tty3 4:2345:respawn:/sbin/mingetty tty4 5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6 #Run xdm in runlevel 5 #xdm is now a separate service x:
5:respawn:/etc/X11/prefdm -nodaemon
```

Fügen Sie in der Datei **/etc/securetty** eine neue Zeile mit dem Namen der seriellen tty für COM2 hinzu:

```
ttyS1
```

Das folgende Beispiel zeigt eine Beispieldatei mit der neuen Zeile.

ANMERKUNG: Verwenden Sie die Sequenz der Untbr-Taste (~B), um auf einer seriellen Konsole mithilfe des IPMI-Hilfsprogramms die Befehle der magischen Linux S-Abf-Taste auszuführen.

```
vc/1 vc/2 vc/3 vc/4 vc/5 vc/6 vc/7 vc/8 vc/9 vc/10 vc/11 tty1 tty2 tty3 tty4 tty5 tty6 tty7
tty8 tty9 tty10 tty11 ttyS1
```

Unterstützte SSH-Verschlüsselungssysteme

Um mit iDRAC über das SSH-Protokoll zu kommunizieren, unterstützt es verschiedene Verschlüsselungsschemas, die in der folgenden Tabelle aufgelistet sind.

Tabelle 17. SSH-Verschlüsselungsschemas

Schematyp	Algorithmen
Asymmetrische Verschlüsselung	
Öffentlicher Schlüssel	ssh-rsa
	ecdsa-sha2-nistp256
Symmetrische Verschlüsselung	
Schlüsselaustausch	curve25519-sha256@libssh.org
	ecdh-sha2-nistp256
	ecdh-sha2-nistp384
	ecdh-sha2-nistp521
	diffie-hellman-group-exchange-sha256
	diffie-hellman-group14-sha1
Verschlüsselung	chacha20-poly1305@openssh.com
	aes128-ctr
	aes192-ctr
	aes256-ctr
	aes128-gcm@openssh.com
	aes256-gcm@openssh.com
MAC	hmac-sha1
	hmac-ripemd160
	umac-64@openssh.com
Compression (Komprimierung)	Keine

ANMERKUNG: Wenn Sie OpenSSH 7.0 oder höher aktivieren, wird Unterstützung für öffentliche DSA-Schlüssel auf „Disabled“ (Deaktiviert) gesetzt. Um bessere Sicherheit für iDRAC zu garantieren, empfiehlt Dell, die Unterstützung für öffentliche DSA-Schlüssel nicht zu aktivieren.

Authentifizierung von öffentlichen Schlüsseln für SSH verwenden

iDRAC unterstützt die Authentifizierung mit öffentlichem Schlüssel (PKA) über SSH. Das ist eine lizenzierte Funktion. Wenn PKA über SSH eingerichtet ist und korrekt verwendet wird, müssen Sie bei der Anmeldung am iDRAC keinen Benutzernamen eingeben. Das ist sehr nützlich für automatisierte Skripts zur Durchführung verschiedener Funktionen. Die hochgeladenen Schlüssel müssen im RFC 4716- oder OpenSSH-Format sein. Wenn sie dieses Format nicht aufweisen, müssen die Schlüssel in dieses Format konvertiert werden.

ANMERKUNG: Wenn Sie OpenSSH 7.0 oder höher aktivieren, wird Unterstützung für öffentliche DSA-Schlüssel auf „Disabled“ (Deaktiviert) gesetzt. Um bessere Sicherheit für iDRAC zu garantieren, empfiehlt Dell, die Unterstützung für öffentliche DSA-Schlüssel nicht zu aktivieren.

In allen Szenarios muss ein Paar aus einem privaten und einem öffentlichen Schlüssel auf der Management Station generiert werden. Der öffentliche Schlüssel wird auf den lokalen iDRAC7-Benutzer hochgeladen, und der private Schlüssel wird durch den SSH-Client verwendet, um eine vertrauenswürdige Beziehung zwischen der Management Station und iDRAC aufzubauen.

Sie können das Paar aus einem öffentlichen und einem privaten Schlüssel über die folgenden Verfahren generieren:

- *PuTTY-Schlüsselgenerator*-Anwendung für Clients, die auf Windows ausgeführt werden
- *ssh-keygen*-Befehlszeilenschnittstelle für Clients, die unter Linux ausgeführt werden

VORSICHT: Diese Berechtigung ist im Normalfall für Benutzer reserviert, die Mitglieder der Administratorbenutzergruppe auf iDRAC sind. Es kann jedoch auch Benutzern der Gruppe „Benutzerdefiniert“ diese Berechtigung zugewiesen werden. Ein Benutzer mit dieser Berechtigung kann die Konfiguration beliebiger Benutzer modifizieren. Hierzu zählen das Erstellen oder Löschen beliebiger Benutzer, SSH-Schlüssel-Verwaltung für Benutzer usw. Weisen Sie diese Berechtigung daher mit Bedacht zu.

VORSICHT: Die Möglichkeit, SSH-Schlüssel hochzuladen, anzuzeigen und/oder zu löschen basiert auf der Benutzerberechtigung "Benutzer konfigurieren". Diese Berechtigung ermöglicht Benutzern, den SSH-Schlüssel eines anderen Benutzers zu konfigurieren. Erteilen Sie diese Berechtigung mit Bedacht.

Generieren öffentlicher Schlüssel für Windows

So verwenden Sie die Anwendung *PuTTY-Schlüsselgenerator* zum Erstellen des Grundschlüssels:

1. Starten Sie die Anwendung und wählen Sie RSA als den Schlüsseltyp.
2. Geben Sie die Anzahl Bits für den Schlüssel ein. Die Anzahl an Bits muss zwischen 2048 und 4096 Bits sein.
3. Klicken Sie auf **Generieren** und bewegen Sie die Maus gemäß Anleitung im Fenster.
   Die Schlüssel wurden erstellt.
4. Sie können das Schlüsselanmerkungsfeld ändern.
5. Geben Sie eine Passphrase zur Sicherung des Schlüssels ein.
6. Speichern Sie den öffentlichen und den privaten Schlüssel.

Generieren öffentlicher Schlüssel für Linux

Um die Anwendung *ssh-keygen* für die Erstellung des Basisschlüssels zu verwenden, öffnen Sie ein Terminalfenster, und geben Sie an der Shell-Eingabeaufforderung den Befehl `ssh-keygen -t rsa -b 2048 -C testing` ein,

wobei:

- `-t` ist *rsa*.

- `-b` die Bit-Verschlüsselungsgröße zwischen 2048 und 4096 angibt.
- `-C` das Ändern der Anmerkung des öffentlichen Schlüssels ermöglicht und optional ist.

ANMERKUNG: Bei den Optionen wird zwischen Groß- und Kleinschreibung unterschieden.

Folgen Sie den Anweisungen. Laden Sie die öffentliche Datei nach der Ausführung des Befehls hoch.

VORSICHT: Schlüssel, die über die Linux Management Station über den Befehl „ssh-keygen“ generiert werden, liegen im Nicht-4716-Format vor. Konvertieren Sie diese Schlüssel über den Befehl `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub` in das 4716-Format. Nehmen Sie keine Änderungen an den Berechtigungen für diese Schlüsseldatei vor. Die Konvertierung muss über Standardberechtigungen erfolgen.

ANMERKUNG: iDRAC unterstützt nicht die ssh-agent-Weiterleitung von Schlüsseln.

SSH-Schlüssel hochladen

Sie können bis zu 4 öffentliche Schlüssel *pro Benutzer* hochladen, die über eine SSH-Schnittstelle verwendet werden können. Stellen Sie sicher, dass Sie sich vor dem Hinzufügen öffentlicher Schlüssel unbedingt die Schlüssel ansehen, ob sie bereits eingerichtet sind, sodass kein Schlüssel versehentlich überschrieben wird.

Beim Hinzufügen neuer öffentlicher Schlüssel müssen Sie sicherstellen, dass bestehende Schlüssel nicht den Index belegen, zu dem der neue Schlüssel hinzugefügt werden soll. Der iDRAC prüft nicht, ob vorherige Schlüssel gelöscht wurden, bevor neue Schlüssel hinzugefügt werden. Wenn ein neuer Schlüssel hinzugefügt wird, kann dieser nicht verwendet werden, wenn die SSH-Schnittstelle aktiviert ist.

SSH-Schlüssel über die Web-Schnittstelle hochladen

So laden Sie SSH-Schlüssel hoch:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Benutzerauthentifizierung** > **Lokale Benutzer**.
   Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
   Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **SSH-Schlüsselkonfigurationen SSH-Schlüssel hochladen** aus, und klicken Sie dann auf **Weiter**.
   Daraufhin wird die Seite **SSH-Schlüssel hochladen** angezeigt.
4. Laden Sie die SSH-Schlüssel über eines der folgenden Verfahren hoch:
   - Schlüsseldatei hochladen
   - Inhalte der Schlüsseldatei in das Textfeld kopieren

   Weitere Informationen finden Sie in der iDRAC Online-Hilfe.
5. Klicken Sie auf **Anwenden**.

SSH-Schlüssel über RACADM hochladen

Um die SSH-Schlüssel hochzuladen, führen Sie den folgenden Befehl aus:

ANMERKUNG: Sie können einen Schlüssel nicht gleichzeitig hochladen und kopieren.

- Lokaler RACADM: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
- Remote-RACADM über Telnet oder SSH: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <key-text>`

Beispiel: Um einen gültigen Schlüssel für die Benutzer-ID 2 auf iDRAC für den ersten Schlüsselsektor mithilfe einer Datei hochzuladen, führen Sie den folgenden Befehl aus:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

ANMERKUNG: Die Option `-f` wird für Telnet/ssh/seriellen RACADM nicht unterstützt.

SSH-Schlüssel anzeigen

Sie können die Schlüssel anzeigen, die nach iDRAC hochgeladen wurden.

SSH-Schlüssel über die Web-Schnittstelle anzeigen

So zeigen Sie die SSH-Schlüssel an:

1. Gehen Sie in der Web-Schnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Benutzerauthentifizierung** > **Lokale Benutzer**.
   Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
   Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **SSH-Schlüsselkonfiguration** die Option **SSH-Schlüssel anzeigen/entfernen** aus, und klicken Sie dann auf **Weiter**.
   Daraufhin wird die Seite **SSH-Schlüssel anzeigen/entfernen** mit den Schlüsseldetails angezeigt.

SSH-Schlüssel über RACADM anzeigen

Führen Sie zum Anzeigen der SSH-Schlüssel den folgenden Befehl aus:

- Spezifischer Schlüssel – `racadm sshpkauth -i <2 to 16> -v -k <1 to 4>`
- Alle Schlüssel – `racadm sshpkauth -i <2 to 16> -v -k all`

SSH-Schlüssel löschen

Bevor Sie die öffentlichen Schlüssel löschen, müssen Sie sicherstellen, dass Sie die Schlüssel anzeigen, wenn sie eingerichtet sind, so dass ein Schlüssel nicht versehentlich gelöscht werden kann.

SSH-Schlüssel über die Web-Schnittstelle löschen

So löschen Sie SSH-Schlüssel:

1. Gehen Sie in der Web-Schnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Benutzerauthentifizierung** > **Lokale Benutzer**.
   Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
   Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **SSH-Schlüsselkonfiguration** die Option **SSH-Schlüssel anzeigen/entfernen** aus, und klicken Sie dann auf **Weiter**.
   Daraufhin werden auf der Seite **SSH-Schlüssel anzeigen/entfernen** die Schlüsseldetails angezeigt.
4. Wählen Sie für die zu löschenden Schlüssel die Option **Entfernen** aus, und klicken Sie dann auf „Anwenden“.
   Die ausgewählten Schlüssel werden daraufhin gelöscht.

SSH-Schlüssel über RACADM löschen

Führen Sie zum Löschen der SSH-Schlüssel die folgenden Befehle aus:

- Spezifischer Schlüssel – `racadm sshpkauth -i <2 to 16> -d -k <1 to 4>`
- Alle Schlüssel – `racadm sshpkauth -i <2 to 16> -d -k all`

7

Benutzerkonten und Berechtigungen konfigurieren

Sie können Benutzerkonten mit spezifischen Berechtigungen (*rollenbasierten Berechtigungen*) einrichten, um Ihr System über iDRAC zu verwalten und um die Systemsicherheit zu gewährleisten. Standardmäßig ist iDRAC mit einem lokalen Administratorkonto konfiguriert. Der Standardbenutzername lautet *root*, und das Kennwort lautet *calvin*. Als Administrator können Sie Benutzerkonten einrichten, damit andere Benutzer auf iDRAC zugreifen können.

Sie können lokale Benutzer oder Verzeichnisdienste einrichten, wie z. B. Microsoft Active Directory oder LDAP, um Benutzerkonten einzurichten. Durch die Verwendung eines Verzeichnisdienstes verfügen Sie über einen zentralen Standort für die Verwaltung berechtigter Benutzerkonten.

iDRAC unterstützt den rollenbasierten Zugriff auf Benutzer mit einem Satz aus zugewiesenen Berechtigungen. Die folgenden Rollen sind verfügbar: Administrator, Operator, Schreibgeschützt oder Kein/e/r. Die Rolle definiert den Umfang der zugewiesenen Berechtigungen.

Themen:

Zugehöriger Link

Lokale Benutzer konfigurieren
Konfigurieren von Active Directory-Benutzern
Generische LDAP-Benutzer konfigurieren

Empfohlene Zeichen in Benutzernamen und Kennwörtern

Dieser Abschnitt enthält Details zu den empfohlenen Zeichen beim Erstellen und Verwenden von Benutzernamen und Kennwörtern.

Verwenden Sie beim Erstellen von Benutzernamen und Kennwörtern die folgenden Zeichen:

Tabelle 18. Empfohlene Zeichen für Benutzernamen

Zeichen	Baulänge
0-9	1-16
A-Z	
a-z	
- ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >	

Tabelle 19. Empfohlene Zeichen für Kennwörter

Zeichen	Baulänge
0-9	1-20
A-Z	
a-z	
' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	

ANMERKUNG: Sie können möglicherweise Benutzernamen und Kennwörter erstellen, die andere Zeichen enthalten. Um Kompatibilität mit allen Schnittstellen zu gewährleisten, wird empfohlen, nur die hier aufgeführten Zeichen zu verwenden.

ANMERKUNG: Die zulässigen Zeichen in Benutzernamen und Kennwörtern für Netzwerkfreigaben werden durch den Typ der Netzwerkfreigabe bestimmt. iDRAC unterstützt gültige Zeichen für Netzwerkfreigabe-Anmeldeinformationen gemäß dem Freigabetyp mit Ausnahme von <, > und , (Komma).

ANMERKUNG: Um die Sicherheit zu erhöhen, wird empfohlen, komplexe Kennwörter zu verwenden, die aus mindestens acht Zeichen bestehen und Klein- und Großbuchstaben, Zahlen und Sonderzeichen enthalten. Es wird außerdem empfohlen, Kennwörter nach Möglichkeit regelmäßig zu ändern.

Lokale Benutzer konfigurieren

Sie können in iDRAC bis zu 16 lokale Benutzer mit spezifischen Zugriffsberechtigungen konfigurieren. Bevor Sie einen iDRAC-Benutzer erstellen, müssen Sie überprüfen, ob etwaige aktuelle Benutzer vorhanden sind. Sie können Benutzernamen, Kennwörter und Rollen mit den Berechtigungen für diese Benutzer definieren. Die Benutzernamen und Kennwörter können über sichere iDRAC-Schnittstellen geändert werden (z. B. über die Web-Schnittstelle, RACADM oder WS-MAN). Sie können auch die SNMPv3 Authentifizierung für jeden Benutzer aktivieren oder deaktivieren.

Lokale Benutzer über die iDRAC-Webschnittstelle konfigurieren

So fügen Sie lokale iDRAC-Benutzer hinzu und konfigurieren sie:

ANMERKUNG: Sie müssen die Berechtigung „Benutzer konfigurieren“ besitzen, um einen iDRAC-Benutzer zu erstellen.

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Benutzerauthentifizierung** > **Lokale Benutzer**.
Die Seite **Benutzer** wird angezeigt.

2 In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.

ANMERKUNG: Benutzer 1 ist für den anonymen IPMI-Benutzer reserviert; diese Konfiguration kann nicht geändert werden.

Die Seite **Benutzer-Hauptmenü** wird angezeigt.

3 Wählen Sie **Benutzer konfigurieren** aus, und klicken Sie dann auf **Weiter**.
Die Seite **Benutzerkonfiguration** wird angezeigt.

4 Aktivieren Sie die Benutzer-ID und geben Sie Benutzername, Kennwort und Zugriffsberechtigungen des Benutzers an. Sie können auch SNMPv3-Authentifizierung für den Benutzer aktivieren. Weitere Informationen finden Sie in der *iDRAC Online-Hilfe*.

5 Klicken Sie auf **Anwenden**. Der Benutzer wird mit den erforderlichen Berechtigungen erstellt.

Lokale Benutzer über RACADM konfigurieren

ANMERKUNG: Sie müssen als Benutzer root angemeldet sein, um RACADM-Befehle auf einem Remote-Linux-System ausführen zu können.

Sie können einen oder mehrere iDRAC-Benutzer über RACADM konfigurieren.

Um mehrere iDRAC-Benutzer mit identischen Konfigurationseinstellungen zu konfigurieren, führen Sie folgende Schritte durch:

- Erstellen Sie mit Hilfe der RACADM-Beispiele in diesem Abschnitt eine Stapeldatei mit RACADM-Befehlen, und führen Sie diese Stapeldatei dann auf jedem verwalteten System aus.
- Erstellen Sie die iDRAC-Konfigurationsdatei und führen Sie unter Verwendung derselben Konfigurationsdatei den Befehl **racadm set** auf den einzelnen verwalteten Systemen aus.

Wenn Sie einen neuen iDRAC konfigurieren oder den Befehl **racadm racresetcfg** verwendet haben, ist der einzige aktuelle Benutzer **root** mit dem Kennwort **calvin**. Der Befehl **racadm racresetcfg** setzt den iDRAC auf die ursprünglichen Standardwerte zurück.

ANMERKUNG: Benutzer können im Laufe der Zeit aktiviert und deaktiviert werden. Infolgedessen kann ein Benutzer auf jedem iDRAC eine unterschiedliche Indexnummer besitzen.

Um zu überprüfen, ob ein Benutzer existiert, geben Sie den folgenden Befehl einmal für jeden Index (1-16) ein:

```
racadm get iDRAC.Users.<index>.UserName
```

Mehrere Parameter und Objekt-IDs werden mit ihren aktuellen Werten angezeigt. Das Schlüsselfeld ist `iDRAC.Users.UserName=`. Wenn ein Benutzername hinter = angezeigt wird, wird diese Indexnummer verwendet.

ANMERKUNG: Sie können auch `racadm get -f <myfile.cfg>` verwenden und die Datei myfile.cfg, in der alle IDRAC-Konfigurationsparameter enthalten sind, anzeigen oder bearbeiten.

Zur Aktivierung der SNMP v3-Authentifizierung für einen Benutzer, verwenden Sie die Objekte **SNMPv3AuthenticationType**, **SNMPv3Enable**, **SNMPv3PrivacyType**. Weitere Informationen finden Sie im *RACADM Command Line Interface Guide (RACADM-Befehlszeilenschnittstelle-Handbuch)* unter **dell.com/idracmanuals**.

Wenn Sie die Konfigurations-XML-Datei verwenden, dann dann verwenden Sie die Attribute **AuthenticationProtocol, ProtocolEnable,** und **PrivacyProtocol**, um die SNMPv3-Authentifizierung zu aktivieren.

iDRAC-Benutzer über RACADM hinzufügen

1 Stellen Sie den Index und den Benutzernamen ein.

```
racadm set idrac.users.<index>.username <user_name>
```

Parameter	Beschreibung
`<index>`	Eindeutiger Index des Benutzers
`<user_name>`	Benutzername

2 Legen Sie das Kennwort fest.

```
racadm set idrac.users.<index>.password <password>
```

3 Legen Sie die Benutzerberechtigungen fest.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

4 Aktivieren Sie den Benutzer.

```
racadm set.idrac.users.<index>.enable 1
```

Für eine Überprüfung verwenden Sie den folgenden Befehl:

```
racadm get idrac.users.<index>
```

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Aktivieren des iDRAC-Benutzers mit Berechtigungen

Um einen Benutzer mit spezifischen administrativen Berechtigungen (rollenbasierte Autorität) zu aktivieren:

1 Lokalisieren Sie einen verfügbaren Benutzerindex.

```
racadm get iDRAC.Users <index>
```

2 Geben Sie die folgenden Befehle mit dem neuen Benutzernamen und dem neuen Kennwort ein.

```
racadm set iDRAC.Users.<index>.Privilege <user privilege bit mask value>
```

ANMERKUNG: Der Standard-Berechtigungswert ist „0“, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt. Eine Liste gültiger Bit-Maskenwerte für spezifische Benutzerberechtigungen ist im *iDRAC RACADM Command Line Interface Reference Guide (iDRAC-RACADM-Referenzhandbuch für die Befehlszeilenoberfläche)* enthalten, das auf der Dell Support-Website unter dell.com/idracmanuals verfügbar ist.

Konfigurieren von Active Directory-Benutzern

Wenn Ihr Unternehmen die Microsoft Active Directory-Software verwendet, kann die Software so konfiguriert werden, dass sie Zugriff auf iDRAC bietet. Sie können dann bestehenden Benutzern im Verzeichnisdienst iDRAC-Benutzerberechtigungen erteilen und diese steuern. Hierbei handelt es sich um eine lizenzierte Funktion.

ANMERKUNG: Die Verwendung der Active Directory-Software zum Erkennen von iDRAC Benutzern wird von den Betriebssystemen Microsoft Windows 2000, Windows Server 2003 und Windows Server 2008 unterstützt.

Sie können die Benutzerauthentifizierung über Active Directory konfigurieren, um sich am iDRAC anzumelden. Rollenbasierte Autorität kann bereitgestellt werden, die es einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren.

Die iDRAC-Rolle und Berechtigungsnamen haben sich seit einer früheren Generation von Servern geändert. Die Rollennamen sind:

Tabelle 20. iDRAC-Rollen

Aktuelle Generation	Vorherige Generation	Benutzerberechtigungen
Administratorkennwort	Administratorkennwort	Anmelden, Konfigurieren, Benutzer konfigurieren, Protokolle, Systemsteuerung, Auf virtuelle Konsole zugreifen, Auf virtuelle Datenträger zugreifen, Systemvorgänge, Debug
Operator	Hauptbenutzer	Anmelden, Konfigurieren, Systemsteuerung, Auf virtuelle Konsole zugreifen, Auf virtuelle Datenträger zugreifen, Systemvorgänge, Debug
Nur-Lesen	Gastbenutzer	Anmelden
Keine	Keine	Keine

Tabelle 21. DRAC/iDRAC-Benutzerberechtigungen

Aktuelle Generation	Vorherige Generation	Beschreibung
Anmelden	Am iDRAC anmelden	Ermöglicht dem Benutzer, sich am iDRAC anzumelden.
Konfigurieren	iDRAC konfigurieren	Ermöglicht dem Benutzer, den iDRAC zu konfigurieren.

Aktuelle Generation	Vorherige Generation	Beschreibung
Benutzer konfigurieren	Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern den Zugriff auf das System zu erlauben.
Protokolle	Protokolle löschen	Aktiviert den Benutzer zum Löschen des Systemereignisprotokolls (SEL).
Systemsteuerung	Serversteuerungsbefehle ausführen	Ermöglicht Aus- und Einschalten des Host-Systems.
Auf die virtuelle Konsole zugreifen	Auf die Umleitung der virtuellen Konsole zugreifen (bei Blade-Servern)	Ermöglicht dem Benutzer, die virtuelle Konsole auszuführen.
	Auf die virtuelle Konsole zugreifen (bei Rack- oder Tower-Servern)	
Auf virtuelle Datenträger zugreifen	Auf virtuelle Datenträger zugreifen	Ermöglicht dem Benutzer, virtuelle Datenträger auszuführen und zu verwenden.
Systemvorgänge	Testwarnungen	Ermöglicht vom Benutzer initiierte und erzeugte Ereignisse und die Informationen werden als asychnrone Benachrichtigung versendet und protokolliert.
Fehlersuche	Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Zugehöriger Link

Voraussetzungen für die Verwendung der Active Directory-Authentifizierung für iDRAC

Unterstützte Active Directory-Authentifizierungsmechanismen

Voraussetzungen für die Verwendung der Active Directory-Authentifizierung für iDRAC

Um die Active Directory-Authentifizierungsfunktion auf dem iDRAC verwenden zu können, stellen Sie sicher, dass Sie:

- eine Active Directory-Infrastrukur bereitgestellt haben. Weitere Informationen finden Sie auf der Microsoft-Website.
- PKI in die Active Directory-Infrastruktur integriert haben. iDRAC verwendet die standardmäßige PKI-Methode (Public Key Infrastructure - Infrastruktur des öffentlichen Schlüssels), um eine sichere Authentifizierung in das Active Directory herzustellen. Weitere Informationen finden Sie auf der Microsoft-Website.
- das Secure Socket Layer (SSL) auf allen Domänen-Controllern aktiviert haben, mit denen sich iDRAC zur Authentifizierung mit allen Domänen-Controllern verbindet.

Zugehöriger Link

SSL auf Domänen-Controller aktivieren

SSL auf Domänen-Controller aktivieren

Wenn Benutzer durch das iDRAC gegen einen Active Directory-Domänen-Controller authentifiziert werden, wird eine SSL-Sitzung mit dem Domänen-Controller gestartet. Der Domänen-Controller muss ein von der Zertifizierungsstelle (CA) signiertes Zertifikat erstellen – das Stammzertifikat, das auch in das iDRAC geladen wird. Damit also die iDRAC-Authentifizierung auf einem *beliebigen* Domänen-Controller möglich ist – egal, ob es sich um den Stamm-Domänen-Controller oder den untergeordneten Domänen-Controller handelt – muss dieser Domänen-Controller ein SSL-aktiviertes, von der CA der Domäne signiertes SSL-Zertifikat aufweisen.

Wenn Sie die Microsoft Enterprise Stamm-CA verwenden, um alle Domänen-Controller-SSL-Zertifikate *automatisch* zuzuweisen, müssen Sie:

1 SSL-Zertifikat auf jedem Domain-Controller installieren.
2 Das CA-Stammzertifikat des Domänen-Controllers zu iDRAC exportieren.
3 Das SSL-Zertifikat der iDRAC-Firmware importieren.

Zugehöriger Link

SSL-Zertifikat für jeden Domänen-Controller installieren
Exportieren des CA-Stammzertifikats des Domänen-Controllers zu iDRAC
Importieren des SSL-Zertifikats der iDRAC-Firmware

SSL-Zertifikat für jeden Domänen-Controller installieren

So installieren Sie das SSL-Zertifikat für jeden Controller:

1 Klicken Sie auf **Start** > **Verwaltung** > **Domänensicherheitsrichtlinie**.
2 Erweitern Sie den Ordner **Richtlinien öffentlicher Schlüssel,** klicken Sie mit der rechten Maustaste auf **Automatische Zertifikatanforderungs-Einstellungen** und klicken Sie auf **Automatische Zertifikatanforderung**.
Daraufhin wird der **Assistent für die Einrichtung der automatischen Zertifikatanforderung** angezeigt.
3 Klicken Sie auf **Weiter**, und wählen Sie dann **Domänen-Controller** aus.
4 Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertigstellen**. Daraufhin wird das SSL-Zertifikat installiert.

Exportieren des CA-Stammzertifikats des Domänen-Controllers zu iDRAC

ANMERKUNG: Wenn Ihr System Windows 2000 ausführt oder Sie eine eigenständige CA verwenden, können die nachfolgenden Schritte variieren.

So exportieren Sie das Stamm-Zertifizierungsstellenzertifikat des Domänen-Controllers nach iDRAC:

1 Suchen Sie den Domänen-Controller, der den Microsoft Enterprise-CA-Dienst ausführt.
2 Klicken Sie auf **Start** > **Ausführen**.
3 Geben Sie `mmc` ein und klicken Sie auf **OK**.
4 Klicken Sie im Fenster **Konsole 1** (MMC) auf **Datei** (oder auf **Konsole** auf Windows 2000-Systemen**)** und wählen Sie **Snap-in hinzufügen/entfernen**.
5 Klicken Sie im Fenster **Snap-In hinzufügen/entfernen** auf **Hinzufügen**.
6 Wählen Sie im Fenster **Eigenständiges Snap-In** die Option **Zertifikate** aus und klicken Sie auf **Hinzufügen**.
7 Wählen Sie **Computer** und klicken Sie auf **Weiter.**
8 Wählen Sie **Arbeitsplatz** aus, klicken Sie auf **Fertig stellen**, und klicken Sie schließlich auf **OK**.
9 Gehen Sie im Fenster **Konsole 1** zum Ordner **Zertifikate Persönliche Zertifikate**.
10 Suchen Sie das CA-Stammzertifikat, klicken Sie mit der rechten Maustaste darauf, wählen Sie **Alle Aufgaben** aus, und klicken Sie auf **Exportieren...**
11 Klicken Sie im **Zertifikate exportieren-Assistenten** auf **Weiter** und wählen Sie **Privaten Schlüssel nicht exportieren** aus.
12 Klicken Sie auf **Weiter** und wählen Sie **Base-64-kodiert X.509 (.cer)** als Format.
13 Klicken Sie auf **Weiter**, um das Zertifikat in einem Verzeichnis auf dem System zu speichern.
14 Laden Sie das in Schritt 13 gespeicherte Zertifikat auf das iDRAC.

Importieren des SSL-Zertifikats der iDRAC-Firmware

Das iDRAC-SSL-Zertifikat ist identisch mit dem Zertifikat, das für den iDRAC-Web Server verwendet wird. Alle iDRAC-Controller werden mit einem selbstsignierten Standard-Zertifikat versendet.

Wenn der Active Directory-Server so eingestellt ist, dass der Client während der Initialisierungsphase einer SSL-Sitzung authentifiziert wird, muss das iDRAC-Serverzertifikat auf den Active Directory-Domänen-Controller hochgeladen werden. Dieser zusätzliche Schritt ist nicht erforderlich, wenn das Active Directory während der Initialisierungsphase einer SSL-Sitzung keine Client-Authentifizierung ausführt.

ANMERKUNG: Wenn Ihr System Windows 2000 ausführt, können die folgenden Schritte abweichen.

ANMERKUNG: Wenn das SSL-Zertifikat der iDRAC-Firmware von einer Zertifizierungsstelle signiert wurde und das Zertifikat dieser Zertifizierungsstelle bereits in der Liste der vertrauenswürdigen Stammzertifizierungsstellen des Domänen-Controllers verzeichnet ist, müssen die Schritte in diesem Abschnitt nicht ausgeführt werden.

So importieren Sie das SSL-Zertifikat der iDRAC-Firmware in alle Listen vertrauenswürdiger Zertifikate der Domänen-Controller:

1. Laden Sie das iDRAC SSL-Zertifikat unter Verwendung des folgenden RACADM-Befehls herunter:
   ```
   racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
   ```
2. Öffnen Sie am Domänen-Controller ein Fenster der **MMC-Konsole** und wählen Sie **Zertifikate** > **Vertrauenswürdige Stammzertifizierungsstellen** aus.
3. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, wählen Sie **Alle Aufgaben** aus, und klicken Sie auf **Importieren**.
4. Klicken Sie auf **Weiter** und suchen Sie die SSL-Zertifikatdatei.
5. Installieren Sie das iDRAC-SSL-Zertifikat in der **vertrauenswürdigen Stammzertifizierungsstelle** der einzelnen Domänen-Controller.
   Wenn Sie Ihr eigenes Zertifikat installiert haben, stellen Sie sicher, dass die Zertifizierungsstelle, die das Zertifikat signiert hat, in der Liste **Vertrauenswürdige Stammzertifizierungsstellen** aufgeführt ist. Wenn die Zertifizierungsstelle nicht auf der Liste ist, müssen Sie sie auf allen Domänen-Controllern installieren.
6. Klicken Sie auf **Weiter** und wählen Sie aus, ob Windows den Zertifikatspeicher automatisch aufgrund des Zertifikattyps auswählen soll, oder suchen Sie selbst nach einem Speicher.
7. Klicken Sie auf **Fertig stellen**, und klicken Sie dann auf **OK**. Das SSL-Zertifikat für die iDRAC-Firmware wird in alle Listen mit vertrauenswürdigen Zertifikaten für Domänen-Controller importiert.

Unterstützte Active Directory-Authentifizierungsmechanismen

Sie können mit Active Directory den Benutzerzugriff auf iDRAC mittels zweier Methoden definieren:

- Die *Standardschemalösung*, die nur Microsoft-Standard-Active Directory-Gruppenobjekte verwendet.
- Die *Erweiterte Schemalösung*, die über benutzerdefinierte Active Directory-Objekte verfügt. Alle Zugriffssteuerungsobjekte werden im Active Directory verwahrt. Bei der Konfiguration des Benutzerzugangs auf verschiedenen iDRAC-Karten mit unterschiedlichen Ebenen der Benutzerberechtigung besteht maximale Flexibilität.

Zugehöriger Link

Übersicht des Standardschema-Active Directory
Übersicht über Active Directory mit erweitertem Schema

Übersicht des Standardschema-Active Directory

Wie in der folgenden Abbildung dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration unter Active Directory und unter iDRAC.

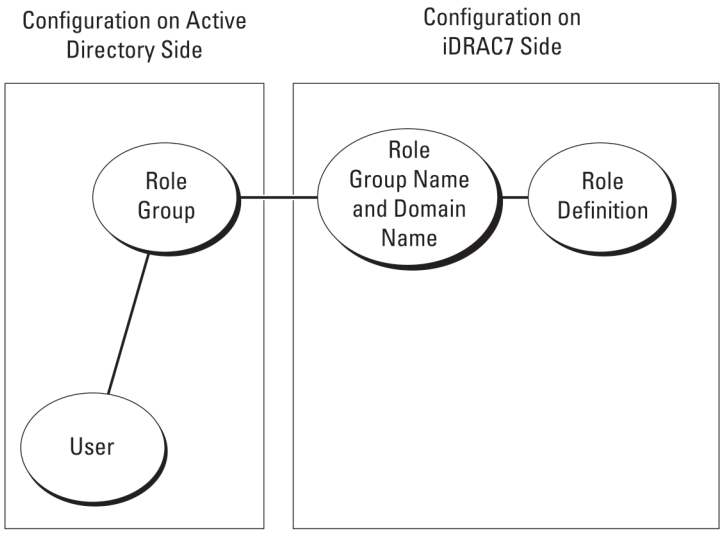


Abbildung 1. Konfiguration von iDRAC mit Active Directory-Standardschema

In Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der iDRAC-Zugriff hat, ist Mitglied der Rollengruppe. Um diesem Benutzer Zugriff auf einen bestimmten iDRAC zu gewähren, muss der Rollengruppenname und der zugehörige Domänenname auf dem bestimmten iDRAC konfiguriert werden. Die Rolle und die Berechtigungsebene wird auf jedem iDRAC definiert, nicht in Active Directory. Sie können bis zu fünf Rollengruppen für jeden iDRAC konfigurieren. Tabellenreferenznummer zeigt die Standardberechtigungen der Rollengruppen.

Tabelle 22. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppen	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
Rollengruppe 1	Keine	Am iDRAC anmelden, iDRAC konfigurieren, Benutzer konfigurieren, Protokolle löschen, Serversteuerungsbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen	0x000001ff
Rollengruppe 2	Keine	Am iDRAC anmelden, iDRAC konfigurieren, Serversteuerungsbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen	0x000000f9
Rollengruppe 3	Keine	Melden Sie sich bei iDRAC an.	0x00000001
Rollengruppe 4	Keine	Keine zugewiesenen Berechtigungen	0x00000000
Rollengruppe 5	Keine	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bitmasken-Werte werden nur verwendet, wenn das Standardschema mit RACADM eingerichtet wird.

Einfache Domänen (Single Domains) und mehrfache Domänen (Multiple Domains)

Wenn sich alle Anmeldebenutzer und Rollengruppen sowie die verschachtelten Gruppen in derselben Domäne befinden, müssen lediglich die Adressen der Domänen-Controller auf dem iDRAC konfiguriert werden. In diesem Muster einer einfachen Domäne wird jede Art von Gruppe unterstützt.

Wenn alle Anmeldebenutzer und Rollengruppen oder beliebige der verschachtelten Gruppen mehreren Domänen angehören, müssen Server-Adressen des Globalen Katalogs auf dem iDRAC konfiguriert werden. In diesem Muster mehrfacher Domänen müssen alle Rollengruppen und, falls vorhanden, alle verschachtelten Gruppen einer Universalgruppe angehören.

Active Directory-Standardschema konfigurieren

So konfigurieren Sie CMC für den Zugriff auf eine Active Directory-Anmeldung:

1 Öffnen Sie auf einem Active Directory-Server (Domänen-Controller) das Active Directory-Benutzer- und -Computer-Snap-In.
2 Erstellen Sie eine Gruppe, oder wählen Sie eine vorhandene Gruppe aus. Fügen Sie den Active Directory-Benutzer als Mitglied der Active Directory-Gruppe für den Zugriff auf iDRAC hinzu.
3 Konfigurieren Sie den Gruppennamen, den Domänennamen und die Rollenberechtigungen auf iDRAC über die iDRAC-Web-Schnittstelle oder RACADM.

Zugehöriger Link

Active Directory mit Standardschema unter Verwendung der CMC-Webschnittstelle konfigurieren
Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM

Active Directory mit Standardschema unter Verwendung der CMC-Webschnittstelle konfigurieren

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

1 Gehen Sie in der iDRAC-Webschnittstelle nach **Übersicht** > **iDRAC-Einstellungen** > **Benutzerauthentifizierung** > **Verzeichnisdienste**.
Die Seite **Verzeichnisdienste** wird angezeigt.
2 Wählen Sie die Option **Microsoft Active Directory** und klicken Sie dann auf **Anwenden**.
Die Seite **Active Directory-Konfiguration und Verwaltung** wird angezeigt.
3 Klicken Sie auf **Active Directory konfigurieren**.
Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 1 von 4 wird angezeigt.
4 Aktivieren Sie optional die Zertifikatüberprüfung, und laden Sie das durch die Zertifizierungsstelle signierte digitale Zertifikat hoch, das im Rahmen der Initiierung von SSL-Verbindungen bei der Kommunikation mit dem Active Directory (AD)-Server verwendet wird. Aus diesem Grund müssen die Domänen-Controller und die FQDN des globalen Katalogs angegeben werden. Dies folgt im nächsten Schritt. Folglich sollte die DNS in den Netzwerkeinstellungen ordnungsgemäß konfiguriert werden.
5 Klicken Sie auf **Weiter**.
Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 2 von 4 wird angezeigt.
6 Aktivieren Sie Active Directory, und geben Sie die Standortinformationen zu den Active Directory-Servern und -Benutzerkonten an. Geben Sie außerdem an, wie lange iDRAC bei der Anmeldung bei iDRAC auf Antworten von Active Directory warten muss.

ANMERKUNG: Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die Adressen des Domain Controller Servers und die FQDN des globalen Katalogs an. Stellen Sie sicher, dass DNS unterÜbersicht > iDRAC-Einstellungen > Netzwerk ordnungsgemäß konfiguriert ist.

7 Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 3 von 4** wird angezeigt.

8 Wählen Sie **Standardschema** aus, und klicken Sie auf „Weiter“.

Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 4a von 4 wird angezeigt.

9 Geben Sie den Standort der globalen Katalogservers für Active Directory an, und geben Sie außerdem die Berechtigungsgruppen an, die für die Autorisierung von Benutzern verwendet werden.

10 Klicken Sie auf eine **Rollengruppe**, um die Steuerungsauthentifizierungsrichtlinie für Benutzer unter dem Standardschemacode zu konfigurieren.

Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 4b von 4** wird angezeigt.

11 Geben Sie die Berechtigungen an, und klicken Sie auf **Anwenden**.

Die Einstellungen werden angewendet, und die Seite **Active Directory – Konfiguration und Verwaltung – Schritt 4a von 4** wird angezeigt.

12 Klicken Sie auf **Fertigstellen**. Daraufhin werden die Active Directory-Einstellungen für das Standardschema konfiguriert.

Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM

1 Verwenden Sie die folgenden Befehle:

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ADGroup.Name <common name of the role group>
racadm set iDRAC.ADGroup.Domain <fully qualified domain name>
racadm set iDRAC.ADGroup.Privilege <Bit-mask value for specific RoleGroup permissions>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog1 <fully qualified domain name or IP address
of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog2 <fully qualified domain name or IP address
of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog3 <fully qualified domain name or IP address
of the domain controller>
```

- Geben Sie unbedingt den vollständig qualifizierten Domänennamen (FQDN) des Domänencontrollers ein, nicht den FQDN der Domäne selbst. Geben Sie z. B. `servername.dell.com` ein, nicht `dell.com`.
- Informationen zu Bitmaskenwerten für spezifische Rollengruppenberechtigungen finden Sie unter Tabelle 22. Standardeinstellungsberechtigungen der Rollengruppe.
- Sie müssen mindestens eine der drei Domänencontrolleradressen angeben. iDRAC versucht solange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung erfolgreich hergestellt ist. Mit Standardschema sind dies die Adressen der Domänencontroller, auf denen sich die Benutzerkonten und Rollengruppen befinden.
- Der globale Katalogserver ist nur für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen in verschiedenen Domänen befinden. Bei mehreren Domänen kann nur die Universalgruppe verwendet werden.
- Wenn die Zertifikatsüberprüfung aktiviert ist, muss der vollständig qualifizierte Domänenname (FQDN) oder die IP-Adresse, die Sie in diesem Feld angeben, mit dem Feld „Servername“ oder „Alternativer Servername“ Ihres Domänen-Controller-Zertifikats übereinstimmen.
- Um die Zertifikatvalidierung während eines SSL-Handshake zu deaktivieren, verwenden Sie den folgenden Befehl:

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
  ```

  In diesem Fall brauchen Sie kein CA-Zertifikat zu laden.
- Um die Zertifikatvalidierung während eines SSL-Handshake (optional) durchzusetzen, verwenden Sie den folgenden Befehl:

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
  ```

  In diesem Fall müssen Sie mit dem folgenden RACADM-Befehl das CA-Zertifikat hochladen:

  ```
  racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
  ```

ANMERKUNG: Wenn die Zertifikatüberprüfung aktiviert ist, geben Sie die Adressen des Domänencontrollerservers und den FQDN des globalen Katalogs an. Stellen Sie sicher, dass DNS unter Overview (Übersicht) > iDRAC Settings (iDRAC-Einstellungen) > Network (Netzwerk) korrekt konfiguriert ist.

Die Verwendung des folgenden RACADM-Befehls kann optional sein.

```
racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
```

2 Wenn DHCP auf dem iDRAC aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgenden Befehl ein:

```
racadm set iDRAC.IPv4.DNSFromDHCP 1
```

3 Wenn DHCP auf dem iDRAC deaktiviert ist oder Sie die DNS IP-Adresse manuell eingeben möchten, geben Sie den folgenden RACADM-Befehl ein:

```
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

4 Wenn Sie eine Liste von Benutzerdomänen konfigurieren möchten, sodass für die Anmeldung an der Webschnittstelle nur der Benutzername eingegeben werden muss, verwenden Sie den folgenden Befehl:

```
racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
domain controller>
```

Sie können bis zu 40 Benutzerdomänen mit Indexzahlen zwischen 1 und 40 konfigurieren.

Übersicht über Active Directory mit erweitertem Schema

Für die Verwendung der Lösung mit dem erweiterten Schema benötigen Sie die Active Directory-Schema-Erweiterung.

Optimale Verfahren für das erweiterte Schema

Das erweiterte Schema verwendet Dell-Zuordnungsobjekte, um iDRAC und Berechtigung beizutreten. Dies ermöglicht Ihnen die Verwendung von iDRAC basierend auf den umfassend zugewiesenen Berechtigungen. Die standardmäßige Zugriffssteuerungsliste (ACL) von Dell-Zuordnungsobjekten ermöglicht Self- als auch Domänenadministratoren die Verwaltung der Berechtigungen und die Reichweite der iDRAC-Objekte.

Standardmäßig erben die Dell-Zuordnungsobjekte nicht alle Berechtigungen aus den übergeordneten Active-Directory-Objekten. Wenn Sie Vererbung für das Dell-Zuordnungsobjekt aktivieren, werden die geerbten Berechtigungen für dieses Zuordnungsobjekt für die ausgewählten Benutzer und Gruppen gewährt. Dies kann zu unabsichtlichen Berechtigungen führen, die iDRAC zur Verfügung gestellt werden.

Um das erweiterte Schema sicher zu verwenden, empfiehlt Dell, dass Sie die Vererbung von Dell-Zuordnungsobjekten innerhalb der erweiterten Schemaimplementierung nicht aktivieren.

Active Directory-Schemaerweiterungen

Bei den Active Directory-Daten handelt es sich um eine verteilte Datenbank von *Attributen* und *Klassen.* Das Active Directory-Schema enthält die Regeln, die den Typ der Daten bestimmen, die der Datenbank hinzugefügt werden können bzw. darin gespeichert werden. Die Benutzerklasse ist ein Beispiel einer *Klasse,* die in der Datenbank gespeichert wird. Beispielhafte Attribute der Benutzerklasse sind der Vorname, der Nachname bzw. die Telefonnummer des Benutzers. Sie können die Active Directory-Datenbank erweitern, indem Sie Ihre eigenen eindeutigen *Attribute* und *Klassen* für besondere Anforderungen hinzufügen. Dell hat das Schema um die erforderlichen Änderungen zur Unterstützung von Remote-Management-Authentifizierung und -Autorisierung erweitert.

Jedes *Attribut* bzw. jede *Klasse,* das/die zu einem vorhandenen Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert werden. Um branchenweit eindeutige IDs zu gewährleisten, unterhält Microsoft eine Datenbank von Active Directory-Objektbezeichnern (OIDs). Wenn also Unternehmen das Schema erweitern, sind diese Erweiterungen eindeutig und ergeben keine

Konflikte. Um das Schema im Active Directory von Microsoft zu erweitern, hat Dell eindeutige OIDs (Namenserweiterungen) und eindeutig verlinkte Attribut-IDs für die Attribute und Klassen erhalten, die dem Verzeichnisdienst hinzugefügt werden.

- Erweiterung ist: `dell`
- Basis-OID lautet: `1.2.840.113556.1.8000.1280`
- Der RAC-LinkID-Bereich ist: `12070 to 12079`

Übersicht über die iDRAC-Schemaerweiterungen

Dell hat das Schema um *Zuordnungs-*, *Geräte-* und *Berechtigungs*eigenschaften erweitert. Die *Zuordnungs*eigenschaft wird zur Verknüpfung der Benutzer oder Gruppen mit einem spezifischen Satz an Berechtigungen für ein oder mehrere iDRAC-Geräte verwendet. Dieses Modell ist unkompliziert und gibt dem Administrator höchste Flexibilität bei der Verwaltung verschiedener Benutzergruppen, iDRAC-Berechtigungen und iDRAC-Geräten im Netzwerk.

Für jedes iDRAC des Netzwerkes, das Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein iDRAC-Geräteobjekt erstellen. Sie können mehrere Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt nach Bedarf mit beliebig vielen Benutzern, Benutzergruppen, oder iDRAC-Geräteobjekten verbunden werden kann. Die Benutzer und iDRAC-Benutzergruppen können Mitglieder beliebiger Domänen im Unternehmen sein.

Jedes Zuordnungsobjekt darf jedoch nur mit einem Berechtigungsobjekt verbunden werden (bzw. jedes Zuordnungsobjekt kann Benutzer, Benutzergruppen oder iDRAC-Geräteobjekte nur mit einem Berechtigungsobjekt verbinden). Dies ermöglicht dem Administrator, die Berechtigungen jedes Benutzers über spezielle iDRAC-Geräte zu steuern.

Das iDRAC-Geräteobjekt ist die Verknüpfung zur iDRAC-Firmware für die Abfrage des Active Directory auf Authentifizierung und Autorisierung. Wenn ein iDRAC dem Netzwerk hinzugefügt wird, muss der Administrator den iDRAC und sein Geräteobjekt mit seinem Active Directory-Namen so konfigurieren, dass Benutzer Authentifizierung und Genehmigung bei Active Directory ausführen können. Der Administrator muss außerdem iDRAC mindestens einem Zuordnungsobjekt hinzufügen, damit Benutzer Authentifizierungen vornehmen können.

Die folgende Abbildung zeigt, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für die gesamte Authentifizierung und Genehmigung erforderlich ist.

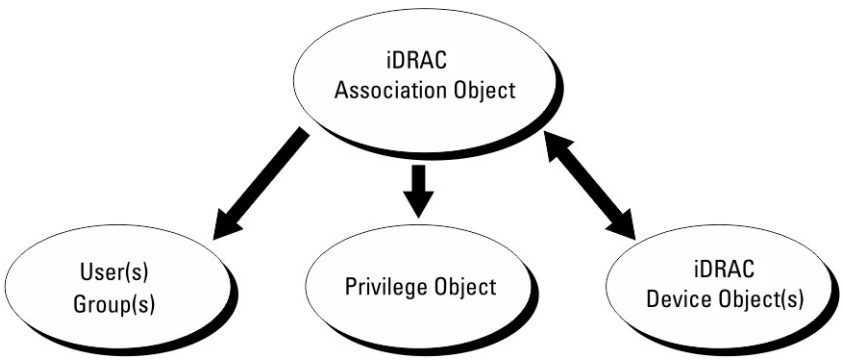


Abbildung 2. Typisches Setup für Active Directory-Objekte

Sie können eine beliebige Anzahl an Zuordnungsobjekten erstellen. Es ist jedoch erforderlich, dass Sie mindestens ein Zuordnungsobjekt erstellen, und Sie müssen ein iDRAC-Geräteobjekt für jedes iDRAC auf dem Netzwerk haben, das zum Zweck der Authentifizierung und Autorisierung mit dem iDRAC mit dem Active Directory integriert werden soll.

Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer bzw. Gruppen und auch iDRAC-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die Benutzer, die Berechtigungen auf iDRAC-Geräten haben.

Über die Dell-Erweiterung zum ADUC MMC Snap-In können nur Berechtigungsobjekte und iDRAC-Objekte derselben Domäne mit dem Verbindungsobjekt verbunden werden. Mit der Dell-Erweiterung können keine Gruppen oder iDRAC-Objekte aus anderen Domänen als Produktmitglied des Verbindungsobjektes hinzugefügt werden.

Wenn Sie Universalgruppen von unterschiedlichen Domänen hinzufügen, erstellen Sie ein Zuordnungsobjekt mit Universalreichweite. Die durch das Dell Schema Extender-Dienstprogramm erstellten Standardzuordnungsobjekte sind lokale Domänengruppen und funktionieren nicht mit Universalgruppen anderer Domänen.

Benutzer, Benutzergruppen oder verschachtelte Benutzergruppen jeglicher Domäne können dem Verbindungsobjekt hinzugefügt werden. Lösungen mit erweitertem Schema unterstützen jede Art von Benutzergruppe sowie jede Benutzergruppe, die über mehrere Domänen verschachtelt und von Microsoft Active Directory zugelassen ist.

Unter Verwendung des erweiterten Schemas Berechtigungen ansammeln

Die Methode zur Authentifizierung des erweiterten Schemas unterstützt das Ansammeln von Berechtigungen über unterschiedliche Berechtigungsobjekte, die mit demselben Benutzer über verschiedene Zuordnungsobjekte in Verbindung stehen. Mit anderen Worten sammelt die Authentifizierung des erweiterten Schemas Berechtigungen an, um dem Benutzer den Supersatz aller zugewiesener Berechtigungen zu ermöglichen, die den verschiedenen, demselben Benutzer zugeordneten Berechtigungsobjekten entsprechen.

Die folgende Abbildung enthält ein Beispiel für das Ansammeln von Berechtigungen unter Verwendung des erweiterten Schemas.

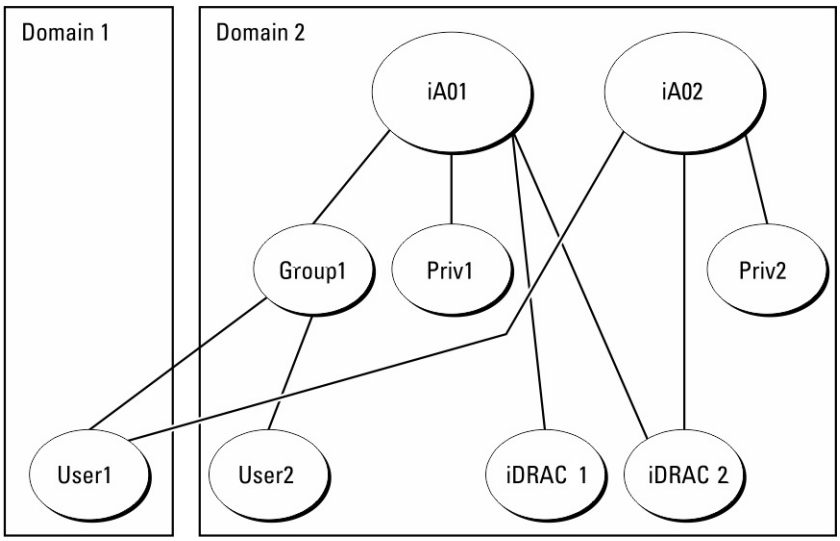


Abbildung 3. Ansammeln von Berechtigungen für einen Benutzer

Die Abbildung stellt zwei Zuordnungsobjekte dar – A01 und A02. Benutzer1 ist über beide Verbindungsobjekte mit iDRAC2 verbunden.

Die Authentifizierung des erweiterten Schemas sammelt Berechtigungen an, um dem Benutzer den maximalen Satz aller möglichen Berechtigungen zur Verfügung zu stellen, und berücksichtigt dabei die zugewiesenen Berechtigungen der verschiedenen Berechtigungsobjekte für den gleichen Benutzer.

In diesem Beispiel verfügt Benutzer1 über die Berechtigungen von Priv1 und Priv2 auf dem iDRAC2. Benutzer1 hat ausschließlich Priv1-Berechtigungen auf dem iDRAC1. Benutzer2 hat die Berechtigungen von Priv1 sowohl auf dem iDRAC1 als auch auf dem iDRAC2. Diese Darstellung zeigt auch, dass Benutzer1 einer anderen Domäne und auch einer Gruppe angehören kann.

Active Directory mit erweitertem Schema konfigurieren

So konfigurieren Sie Active Directory für den Zugriff auf iDRAC:

1 Erweitern des Active Directory-Schemas.
2 Active Directory-Benutzer und Computer-Snap-In erweitern.
3 iDRAC-Benutzer mit Berechtigungen zum Active Directory hinzufügen.
4 Konfigurieren Sie die iDRAC Active Directory-Eigenschaften über die iDRAC-Web-Schnittstelle oder RACADM.

Zugehöriger Link

Übersicht über Active Directory mit erweitertem Schema
Dell-Erweiterung zu Active Directory Benutzer- und Computer-Snap-In installieren
iDRAC-Benutzer und -Berechtigungen zu Active Directory hinzufügen
Active Directory mit erweitertem Schema unter Verwendung der iDRAC-Webschnittstelle konfigurieren
Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM

Erweitern des Active Directory-Schemas

Mit der Erweiterung des Active Directory-Schemas werden eine Dell-Organisationseinheit, Schemaklassen und -attribute sowie Beispielberechtigungen und Zuordnungsobjekte zum Active Directory-Schema hinzugefügt. Bevor Sie das Schema erweitern, müssen Sie sicherstellen, dass Sie die Schema-Admin-Berechtigungen auf dem Schema Master-FSMO-Rollenbesitzer (Flexible Single Master Operation) der Domänenstruktur besitzen.

ANMERKUNG: Stellen Sie sicher, dass die Schema-Erweiterung für dieses Produkt sich von den Vorgänger-Generationen der Dell Remote Management-Produkte unterscheidet. Das vorherige Schema kann bei diesem Produkt nicht verwendet werden.

ANMERKUNG: Eine Erweiterung des neuen Schemas ändert nichts an den Vorgängerversionen des Produktes.

Sie können das Schema mit einer der folgenden Methoden erweitern:

- Dell Schema Extender-Dienstprogramm
- LDIF-Script-Datei

Die Dell-Organisationseinheit wird dem Schema nicht hinzugefügt, wenn Sie die LDIF-Skriptdatei verwenden.

Die LDIF-Dateien und Dell Schema Extender befinden sich auf der DVD *Dell Systems Management Tools and Documentation* in den folgenden jeweiligen Verzeichnissen:

- DVD-Laufwerk **:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- <DVDdrive>: **\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender**

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Files**.

Sie können Schema Extender oder die LDIF-Dateien an einem beliebigen Standort kopieren und ausführen.

Dell Schema Extender verwenden

VORSICHT: Das Dienstprogramm „Dell Schema Extender“ verwendet die Datei SchemaExtenderOem.ini. Um sicherzustellen, dass das Dell Schema Extender-Dienstprogramm richtig funktioniert, modifizieren Sie den Namen dieser Datei nicht.

1 Klicken Sie im **Begrüßungsbildschirm** auf **Weiter**.
2 Lesen Sie die Warnung und vergewissern Sie sich, dass Sie sie verstehen und klicken Sie dann auf **Weiter**.
3 Wählen Sie **Aktuelle Anmeldeinformationen Verwenden** aus, oder geben Sie einen Benutzernamen und ein Kennwort mit Schema-Administratorrechten ein.

4 Klicken Sie auf **Weiter,** um Dell Schema Extender auszuführen.

5 Klicken Sie auf **Fertigstellen**.

Das Schema wird erweitert. Um die Schema-Erweiterung zu überprüfen, verwenden Sie die Microsoft-Verwaltungskonsole (MMC) und das Active Directory-Schema-Snap-In, um zu prüfen, ob Klassen und Attribute vorhanden sind. Näheres zur Benutzung der Verwaltungskonsole (MMC) und des Active Directory-Schema-Snap-In finden Sie in der Microsoft-Dokumentation.

Klassen und Attribute

Tabelle 23. Klassendefinitionen für Klassen, die zum Active Directory-Schema hinzugefügt wurden

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabelle 24. DelliDRACdevice-Klasse

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Beschreibung	Stellt das Dell iDRAC-Gerät dar. iDRAC muss im Active Directory als delliDRACDevice konfiguriert sein. Mit dieser Konfiguration kann iDRAC CMC Lightweight Directory Access Protocol (LDAP)-Abfragen an Active Directory senden.
Klassentyp	Strukturklasse
SuperClasses	dellProduct
Attribute	dellSchemaVersion
	dellRacType

Tabelle 25. delliDRACAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Beschreibung	Stellt das Dell Zuordnungsobjekt dar. Das Zuordnungsobjekt ist die Verbindung zwischen Benutzern und Geräten.
Klassentyp	Strukturklasse
SuperClasses	Gruppe
Attribute	dellProductMembers
	dellPrivilegeMember

Tabelle 26. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Beschreibung	Legt die Berechtigungen für iDRAC fest (Autorisierungsrechte)
Klassentyp	Erweiterungsklasse
SuperClasses	Keine
Attribute	dellIsLoginUser
	dellIsCardConfigAdmin
	dellIsUserConfigAdmin
	dellIsLogClearAdmin
	dellIsServerResetUser
	dellIsConsoleRedirectUser
	dellIsVirtualMediaUser
	dellIsTestAlertUser
	dellIsDebugCommandAdmin

Tabelle 27. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Beschreibung	Wird als Container-Klasse für die Dell-Berechtigungen (Autorisierungsrechte) verwendet.
Klassentyp	Strukturklasse
SuperClasses	Benutzer
Attribute	dellRAC4Privileges

Tabelle 28. dellProduct Class

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Beschreibung	Die Hauptklasse, von der alle Dell-Produkte abgeleitet werden.
Klassentyp	Strukturklasse
SuperClasses	Computer
Attribute	dellAssociationMembers

Tabelle 29. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden

Attributname/Beschreibung	Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
dellPrivilegeMember Die Liste von dellPrivilege-Objekten, die zu diesem Attribut gehören.	1.2.840.113556.1.8000.1280.1.1.2.1 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Die Liste von dellRacDevice- und DelliDRACDevice-Objekten, die zu dieser Rolle gehören. Dieses Attribut ist der Vorwärtslink zum dellAssociationMembers-Rückwärtslink. Link-ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE, wenn der Benutzer Anmeldungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.3 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.4 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.5 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE, wenn der Benutzer Protokolllöschungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.7 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE, wenn der Benutzer über Virtuelle-Konsole-Rechte auf dem Gerät verfügt.	1.2.840.113556.1.8000.1280.1.1.2.8 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE, wenn der Benutzer Rechte für den virtuellen Datenträger auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser	1.2.840.113556.1.8000.1280.1.1.2.10	TRUE

Attributname/Beschreibung	Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
TRUE, wenn der Benutzer Testwarnungsbenutzerrechte auf dem Gerät hat.	Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsDebugCommandAdmin TRUE, wenn der Benutzer Debug-Befehl-Admin-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion Die aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren.	1.2.840.113556.1.8000.1280.1.1.2.12 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Dieses Attribut ist der aktuelle RAC-Typ für das dellRacDevice-Objekt und der Rückwärtslink zum dellAssociationObjectMembers-Vorwärtslink.	1.2.840.113556.1.8000.1280.1.1.2.13 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Liste der dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist der Rückwärtslink zum Attribut dellProductMembers. Link-ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Dell-Erweiterung zu Active Directory Benutzer- und Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch das Active Directory-Benutzer- und -Computer-Snap-In erweitern, so dass der Administrator iDRAC-Geräte, Benutzer und Benutzergruppen, iDRAC-Zuordnungen und iDRAC-Berechtigungen verwalten kann.

Wenn Sie die Systems Management Software mit der DVD *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsverfahrens die Option **Snap-In von Active Directory-Benutzern und -Computern** auswählen. Das Schnellinstallationshandbuch zu Dell OpenManage-Software enthält zusätzliche Anleitungen zur Installation von Systemverwaltungssoftware. Die Snap-In-Installation für 64-Bit-Versionen von Windows finden Sie unter:

<DVD-Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

Weitere Informationen über Active Directory-Benutzer- und -Computer-Snap-In finden Sie in der Microsoft-Dokumentation.

iDRAC-Benutzer und -Berechtigungen zu Active Directory hinzufügen

Mit dem von Dell erweiterten Active Directory-Benutzer- und -Computer-Snap-In können Sie iDRAC-Benutzer und -Berechtigungen hinzuzufügen, indem Sie Gerät-, Zuordnungs- und Berechtigungsobjekte erstellen. Um die einzelnen Objekte hinzuzufügen, führen Sie folgende Verfahren durch:

- Erstellen eines iDRAC-Geräteobjekts
- Erstellen eines Berechtigungsobjekts
- Erstellen eines Zuordnungsobjekts
- Einem Zuordnungsobjekt Objekte hinzufügen

Zugehöriger Link

Objekte zu einem Zuordnungsobjekt hinzufügen
Erstellen von iDRAC-Geräteobjekten
Berechtigungsobjekt erstellen
Zuordnungsobjekt erstellen

Erstellen von iDRAC-Geräteobjekten

So erstellen Sie ein iDRAC-Geräteobjekt:

1 Klicken Sie im Fenster **Console Root** (MCC) mit der rechten Maustaste auf einen Container.
2 Wählen Sie **Neu** > **Dell Remote Management Object Advanced** aus.
Das Fenster **Neues Objekt** wird angezeigt.
3 Geben Sie einen Namen für das neue Objekt ein. Dieser Name muss mit dem iDRAC-Namen identisch sein, den Sie im Rahmen der Konfiguration der Active Directory-Eigenschaften über die iDRAC-Webschnittstelle eingegeben haben.
4 Wählen Sie **iDRAC-Geräteobjekt** und klicken Sie auf OK.

Berechtigungsobjekt erstellen

So erstellen Sie ein Berechtigungsobjekt:

ANMERKUNG: Sie müssen ein Berechtigungsobjekt in der gleichen Domäne erstellen, in der auch das verknüpfte Zuordnungsobjekt vorhanden ist.

1 Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2 Wählen Sie **Neu** > **Dell Remote Management Object Advanced** aus.
Das Fenster **Neues Objekt** wird angezeigt.
3 Geben Sie einen Namen für das neue Objekt ein.
4 Wählen Sie **Berechtigungsobjekt** und klicken Sie auf OK.
5 Klicken Sie mit der rechten Maustaste auf das Berechtigungsobjekt, das Sie erstellt haben, und wählen Sie **Eigenschaften** aus.
6 Klicken Sie auf die Registerkarte **Remote-Verwaltungsberechtigungen**, und weisen Sie die Berechtigungen für den Benutzer oder die Gruppe zu.

Zuordnungsobjekt erstellen

So erstellen Sie ein Zuordnungsobjekt:

ANMERKUNG: Das iDRAC-Zuordnungsobjekt wird von der Gruppe abgeleitet und hat einen Wirkungsbereich in einer lokalen Domäne.

1 Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2 Wählen Sie **Neu** > **Dell Remote Management Object Advanced** aus.
Das Fenster **Neues Objekt** wird angezeigt.
3 Geben Sie einen Namen für das neue Objekt ein, und wählen Sie **Zuordnungsobjekt** aus.
4 Wählen Sie den Bereich für das **Zuordnungsobjekt** und klicken Sie auf OK.
5 Geben Sie den authentifizierten Benutzern Zugriffsberechtigungen für den Zugriff auf die angelegten Zuordnungsobjekte.

Zugehöriger Link

Benutzerzugriffsberechtigungen für verknüpfte Objekte bereitstellen

Benutzerzugriffsberechtigungen für verknüpfte Objekte bereitstellen

Um den authentifizierten Benutzern Zugriffsberechtigungen für den Zugriff auf die angelegten Zuordnungsobjekte zu geben:

1 Gehen Sie zu **Verwaltung** > **ADSI-Editor**. Daraufhin wird das Fenster **ADSI-Editor** angezeigt.
2 Wechseln Sie im rechten Bereich zum angelegten Zuordnungsobjekt, klicken Sie auf die rechte Maustaste und wählen Sie **Eigenschaften**.
3 Klicken Sie auf Registerkarte **Sicherheit** auf **Hinzufügen**.
4 Geben Sie `Authenticated Users` ein, klicken Sie auf **Namen überprüfen**, und klicken Sie dann auf **OK**. Die authentifizierten Benutzer werden zur Liste der **Gruppen- oder Benutzernamen** hinzugefügt.
5 Klicken Sie auf **OK**.

Objekte zu einem Zuordnungsobjekt hinzufügen

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und iDRAC-Geräte oder iDRAC-Gerätegruppen zuordnen.

Sie können Benutzergruppen und iDRAC-Geräte hinzufügen.

Zugehöriger Link

Benutzer oder Benutzergruppen hinzufügen
Berechtigungen hinzufügen
Hinzufügen von iDRAC-Geräten oder iDRAC-Gerätegruppen

Benutzer oder Benutzergruppen hinzufügen

So fügen Sie Benutzer oder Benutzergruppen hinzu:

1 Klicken Sie mit der rechten Maustaste auf das **Zuordnungsobjekt** und wählen Sie **Eigenschaften** aus.
2 Wählen Sie das Register **Benutzer** und klicken Sie auf **Hinzufügen.**
3 Geben Sie den Namen des Benutzers oder der Benutzergruppe ein und klicken Sie auf **OK**.

Berechtigungen hinzufügen

So fügen Sie Berechtigungen hinzu:

Klicken Sie auf das Register **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, welche die Berechtigungen des Benutzers bzw. der Benutzergruppe bei Authentifizierung eines iDRAC-Geräts definiert. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

1 Wählen Sie das Register **Berechtigungsobjekt** und klicken Sie auf **Hinzufügen**.
2 Geben Sie den Namen des Berechtigungsobjekts ein und klicken Sie auf **OK**.
3 Klicken Sie auf das Register **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, welche die Berechtigungen des Benutzers bzw. der Benutzergruppe bei Authentifizierung eines iDRAC-Geräts definiert. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

Hinzufügen von iDRAC-Geräten oder iDRAC-Gerätegruppen

So fügen Sie iDRAC-Geräte oder iDRAC-Gerätegruppen hinzu:

1 Wählen Sie die Registerkarte **Produkte** und klicken Sie auf **Hinzufügen**.
2 Geben Sie die Namen der iDRAC-Geräte oder iDRAC-Gerätegruppen ein und klicken Sie auf **OK**.
3 Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.
4 Klicken Sie auf das Register **Produkte** und fügen Sie ein iDRAC-Gerät hinzu, das mit dem Netzwerk verbunden ist, das den definierten Benutzern oder Benutzergruppen zur Verfügung steht. Einem Zuordnungsobjekt können mehrere iDRAC-Geräte hinzugefügt werden.

Active Directory mit erweitertem Schema unter Verwendung der iDRAC-Webschnittstelle konfigurieren

So konfigurieren Sie Active Directory mit erweitertem Schema über die Web-Schnittstelle:

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Benutzerauthentifizierung** > **Verzeichnisdienste** > **Microsoft Active Directory**.

Die **Active Directory-**Zusammenfassungsseite wird angezeigt.

2 Klicken Sie auf **Active Directory konfigurieren**.

Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 1 von 4 wird angezeigt.

3 Aktivieren Sie optional die Zertifikatvalidierung, und laden Sie das durch die Zertifikatstelle signierte digitale Zertifikat hoch, das im Rahmen der Initiierung von SSL-Verbindungen während der Kommunikation mit dem Active Directory (AD)-Server verwendet wird.

4 Klicken Sie auf **Weiter**.

Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 2 von 4 wird angezeigt.

5 Geben Sie die Speicherortinformationen für die Active Directory (AD)-Server und Benutzerkonten an. Geben Sie außerdem die Dauer an, die iDRAC im Rahmen des Anmeldeprozesses auf Antworten von AD warten muss.

ANMERKUNG:

- Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die Adressen für den Domain Controller Server und FQDN an. Stellen Sie sicher, dass DNS unter **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** korrekt konfiguriert ist.
- Wenn sich die Benutzer und iDRAC-Objekte in unterschiedlichen Domänen befinden, wählen Sie nicht die Option **Benutzerdomäne von Anmeldung** aus. Wählen Sie stattdessen **Eine Domäne angeben** aus, und geben Sie den Namen der Domäne ein, in der das iDRAC-Objekt verfügbar ist.

6 Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 3 von 4** wird angezeigt.

7 Wählen Sie **Erweitertes Schema** aus, und klicken Sie auf **Weiter**.

Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 4 von 4 wird angezeigt.

8 Geben Sie den Namen und den Speicherort des iDRAC-Geräteobjekts unter Active Directory (AD) an, und klicken Sie auf **Fertigstellen**.

Die Active Directory-Einstellungen für den Modus „Erweitertes Schema“ wird konfiguriert.

Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM

So konfigurieren Sie Active Directory mit erweitertem Schema unter Verwendung von RACADM:

1 Verwenden Sie die folgenden Befehle:

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ActiveDirectory.RacName <RAC common name>
racadm set iDRAC.ActiveDirectory.RacDomain <fully qualified rac domain name>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
address of the domain controller>
```

- Geben Sie unbedingt den vollständig qualifizierten Domänennamen (FQDN) des Domänen-Controllers ein, nicht den FQDN der Domäne selbst. Geben Sie z.B. `servername.dell.com` ein und nicht `dell.com`.

- Sie müssen mindestens eine der drei Adressen bereitstellen. iDRAC versucht so lange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte. Mit erweitertem Schema sind diese der FQDN oder die IP-Adresse des Domänen-Controllers, auf dem sich das iDRAC-Gerät befindet.
- Um die Zertifikatvalidierung während eines SSL-Handshake zu deaktivieren, verwenden Sie den folgenden Befehl:

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
  ```

  In diesem Fall brauchen Sie kein CA-Zertifikat zu laden.
- So erzwingen Sie die Zertifikatvalidierung während eines SSL-Handshake (optional):

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
  ```

  In diesem Fall müssen Sie mit dem folgenden Befehl ein CA-Zertifikat laden:

  ```
  racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
  ```

  ANMERKUNG: Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die Adressen des Domain Controller Server und von FQDN an. Stellen Sie sicher, dass DNS unterÜbersicht > iDRAC-Einstellungen > Netzwerk ordnungsgemäß konfiguriert ist.

  Die Verwendung des folgenden RACADM-Befehls kann optional sein.

  ```
  racadm sslcertdownload -t 0x1 -f <RAC SSL certificate>
  ```

2 Wenn DHCP auf dem iDRAC aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgenden Befehl ein:

```
racadm set iDRAC.IPv4.DNSFromDHCP 1
```

3 Wenn DHCP auf dem iDRAC deaktiviert ist oder Sie ihre DNS IP-Adresse manuell eingeben möchten, arbeiten Sie mit den folgenden Befehlen:

```
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

4 Möchten Sie eine Liste mit Benutzerdomänen konfigurieren, sodass für die Anmeldung an der iDRAC-Webschnittstelle nur der Benutzername eingegeben werden muss, verwenden Sie dazu den folgenden Befehl:

```
racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
domain controller>
```

Sie können bis zu 40 Benutzerdomänen mit Indexzahlen zwischen 1 und 40 konfigurieren.

Active Directory-Einstellungen testen

Sie können die Active Directory-Einstellungen testen, um zu überprüfen, ob Ihre Konfiguration korrekt ist oder um Fehler bei der Active Directory-Anmeldung zu analysieren.

Active Directory-Einstellungen über die iDRAC-Webschnittstelle testen

So testen Sie die Active Directory-Einstellungen:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Benutzerauthentifizierung** > **Verzeichnisdienste** > **Microsoft Active Directory**.

Die **Active Directory-**Zusammenfassungsseite wird angezeigt.

2 Klicken Sie auf **Testeinstellungen**.

3 Geben Sie einen Test-Benutzernamen (z. B. **Benutzername@domain.com**) und ein Kennwort ein, und klicken Sie dann auf **Test starten**. Daraufhin werden detaillierte Testergebnisse und ein Testprotokoll angezeigt.

Überprüfen Sie gegebenenfalls die einzelnen Fehlermeldungen und mögliche Lösungen im Testprotokoll.

ANMERKUNG: Wenn die Active Directory-Einstellungen überprüft werden und dabei „Zertifikatsüberprüfung aktiviert“ ausgewählt ist, erfordert iDRAC, dass der Active Directory-Server über den FQDN und nicht über eine IP-Adresse identifiziert wird. Wenn der Active Directory-Server über eine IP-Adresse identifiziert wird, schlägt die Zertifikatsvalidierung fehl, da iDRAC nicht mit dem Active Directory-Server kommunizieren kann.

Active Directory-Einstellungen über RACADM testen

Um die Active-Directory-Einstellungen zu testen, verwenden Sie den Befehl **testfeature**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Generische LDAP-Benutzer konfigurieren

iDRAC bietet eine allgemeine Lösung zur Unterstützung LDAP-basierter Authentifizierung (Lightweight Directory Access Protocol). Für diese Funktion ist auf Ihren Verzeichnisdiensten keine Schemaeweiterung erforderlich.

Um die iDRAC LDAP-Implementierung generisch zu gestalten, werden die Gemeinsamkeiten der verschiedenen Verzeichnisdienste dazu genutzt, Benutzer in Gruppen zusammenzufassen und danach die Beziehung zwischen Benutzer und Gruppe festzulegen. Die Verzeichnisdienst-spezifische Maßnahme ist hierbei das Schema. Es können beispielsweise verschiedene Attributnamen für die Gruppe, Benutzer und die Verbindung zwischen dem Benutzer und der Gruppe vergeben werden. Diese Maßnahmen können im iDRAC konfiguriert werden.

ANMERKUNG: Die Smart Card-basierte Zweifaktor-Authentifizierung (TFA) und einfache Anmeldung (SSO) werden nicht für den allgemeinen LDAP-Verzeichnisdienst unterstützt.

Zugehöriger Link

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der iDRAC-Webschnittstelle
Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der iDRAC-Webschnittstelle

So konfigurieren Sie den generischen LDAP-Verzeichnisdienst über die Web-Schnittstelle:

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Benutzerauthentifizierung** > **Verzeichnisdienste** > **Generischer LDAP-Verzeichnisdienst**.

Die Seite **Generisches LDAP - Konfiguration und Verwaltung** zeigt die aktuellen Einstellungen für das generische LDAP an.

2 Klicken Sie auf **Generischen LDAP-Verzeichnisdienst konfigurieren**.

3 Aktivieren Sie optional Zertifikatsvalidierung und laden Sie das digitale Zertifikat hoch, das Sie zum Aufbau von SSL-Verbindungen bei der Kommunikation mit einem generischen LDAP-Server verwendet haben.

ANMERKUNG: Bei dieser Version wird eine LDAP-Bindung, die nicht auf einem SSL-Anschluss basiert, nicht unterstützt. Nur LDAP über SSL wird unterstützt.

4 Klicken Sie auf **Weiter**.

Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung** Schritt 2 von 3 wird angezeigt.

5 Aktivieren Sie die generische LDAP-Authentifizierung, und geben Sie die Speicherortinformationen zu den generischen LDAP-Servern und -Benutzerkonten an.

ANMERKUNG: Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die FQDN des LDAP-Servers an, und stellen Sie sicher, dass DNS unter Übersicht > iDRAC-Einstellungen > Netzwerk korrekt konfiguriert ist.

ANMERKUNG: Bei dieser Version werden verschachtelte Gruppen nicht unterstützt. Die Firmware sucht nach dem Mitglied der Gruppe, das dem Benutzer-DN entspricht. Weiterhin wird nur Einzeldomäne unterstützt. Übergreifende Domänen werden nicht unterstützt.

6 Klicken Sie auf **Weiter**.

Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung** Schritt 3a von 3 wird angezeigt.

7 Klicken Sie auf **Rollengruppe**.

Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung** Schritt 3b von 3 wird angezeigt.

8 Geben Sie den abgegrenzten Namen für die Gruppe und die mit dieser Gruppe verbundenen Berechtigungen ein, und klicken Sie dann auf **Anwenden**.

> **ANMERKUNG: Wenn Sie Novell eDirectory verwenden und die folgenden Zeichen für den Gruppen-Domänennamen verwendet haben, müssen diese Zeichen umgeschrieben werden: # (Hash-Zeichen), " (doppelte Anführungszeichen), ; (Semikolon), > (größer als), , (Komma) oder < (kleiner als).**

Die Rollengruppeneinstellungen werden gespeichert. Die Seite **Allgemeine LDAP - Konfiguration und Verwaltung – Schritt 3a von 3** zeigt die Rollengruppeneinstellungen an.

9 Wenn Sie weitere Rollengruppen konfigurieren möchten, wiederholen Sie die Schritte 7 und 8.

10 Klicken Sie auf **Fertigstellen**. Der generische LDAP-Verzeichnisdienst ist damit konfiguriert.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM

Um den LDAP-Verzeichnisdienst zu konfigurieren, verwenden Sie die Objekte in den Gruppen **iDRAC.LDAP** und **iDRAC.LDAPRole**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Einstellungen für LDAP-Verzeichnisdienst testen

Sie können die Einstellungen für LDAP-Verzeichnisdienste testen, um zu überprüfen, ob Ihre Konfiguration korrekt ist oder um Fehler bei der Active Directory-Anmeldung zu analysieren.

Testen der Einstellungen des LDAP-Verzeichnisdienstes über die iDRAC-Webschnittstelle

So testen Sie die Einstellungen für den LDAP-Verzeichnisdienst:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Benutzerauthentifizierung** > **Verzeichnisdienste** > **Allgemeiner LDAP-Verzeichnisdienst**.

Die Seite **Generisches LDAP - Konfiguration und Verwaltung** zeigt die aktuellen Einstellungen für das generische LDAP an.

2 Klicken Sie auf **Testeinstellungen**.

3 Geben Sie den Benutzernamen und das Kennwort eines Verzeichnisbenutzers ein, der zur Überprüfung der LDAP-Einstellungen ausgewählt wurde. Das Format hängt vom verwendeten *Attribut der Benutzeranmeldung* ab und der eingegebene Benutzername muss dem Wert des gewählten Attributs entsprechen.

> **ANMERKUNG: Wenn beim Testen der LDAP-Einstellungen Enable Certificate Validation (Zertifikatsüberprüfung aktivieren) ausgewählt ist, verlangt iDRAC, dass der LDAP-Server über den FQDN und nicht über eine IP-Adresse identifiziert wird. Wenn der LDAP-Server über eine IP-Adresse identifiziert wird, schlägt die Zertifikatsvalidierung fehl, da iDRAC nicht mit dem LDAP-Server kommunizieren kann.**

> **ANMERKUNG: Wenn generisches LDAP aktiviert ist, versucht iDRAC zunächst, den Benutzer als Verzeichnisbenutzer anzumelden. Schlägt dies fehl, wird die Suche nach lokalen Benutzern aktiviert.**

Die Testergebnisse und das Testprotokoll werden angezeigt.

LDAP-Verzeichnisdiensteinstellungen über RACADM testen

Um die LDAP-Verzeichnisdiensteinstellungen zu testen, verwenden Sie den Befehl `testfeature`. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* unter **dell.com/idracmanuals**.

8

iDRAC für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren

In diesem Abschnitt erhalten Sie Informationen zur Konfiguration von iDRAC für die Smart Card-Anmeldung (für lokale und Active Directory-Benutzer) und die einmalige Anmeldung (SSO, für Active Directory-Benutzer.) Die SSO- und Smart Card-Anmeldungen sind lizenzierte Funktionen.

iDRAC unterstützt die Kerberos-basierte Active Directory-Authentifizierung für die Unterstützung von Smart Card- und SSO-Anmeldungen. Weitere Informationen zu Kerberos finden Sie auf der Microsoft-Website.

Themen:

Zugehöriger Link

iDRAC-SSO-Anmeldung für Active Directory-Benutzer konfigurieren
iDRAC-Smart Card-Anmeldung für lokale Benutzer konfigurieren
iDRAC-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren

Voraussetzungen für die einmalige Active Directory-Anmeldung oder die Smart Card-Anmeldung

Die Voraussetzungen für die Active Directory-basierten SSO- oder Smart Card-Anmeldungen lauten wie folgt:

- Synchronisieren Sie die iDRAC-Zeit mit der Zeit des Active Directory-Domänen-Controllers. Wenn Sie dies nicht tun, schlägt die Kerberos-Authentifizierung auf iDRAC fehl. Sie können die Funktion für Zeitzone und NTP verwenden, um die Zeit zu synchronisieren. Weitere Informationen dazu finden Sie unter Konfigurieren von Zeitzonen und NTP.
- Registrieren Sie den iDRAC als Computer in der Active Directory-Root-Domäne.
- Generieren Sie eine Keytab-Datei über das Ktpass-Tool.
- Um die einmalige Anmeldung für das erweiterte Schema zu aktivieren, stellen Sie sicher, dass die Option **Benutzer bei Delegierungen aller Dienste vertrauen (nur Kerberos)** auf der Registerkarte **Delegierung** für den Keytab-Benutzer ausgewählt ist. Diese Registerkarte ist erst verfügbar, nachdem die Keytab-Datei über das ktpass-Dienstprogramm erstellt wurde.
- Konfigurieren Sie den Browser für die Aktivierung der SSO-Anmeldung.
- Erstellen Sie die Active Directory-Objekte, und stellen Sie die erforderlichen Berechtigungen bereit.
- Konfigurieren Sie für SSO auf den DNS-Servern die Zone für die Rückwärtssuche für das Subnetz, auf dem sich iDRAC befindet.

  ANMERKUNG: Wenn der Host-Name mit der DNS-Rückwärtssuche nicht übereinstimmt, schlägt die Kerberos-Authentifizierung fehl.
- Konfigurieren Sie den Browser für die Unterstützung der SSO-Anmeldung. Weitere Informationen finden Sie unter Konfigurieren von unterstützten Webbrowsern.

ANMERKUNG: Google Chrome und Safari unterstützen Active Directory für die SSO-Anmeldung nicht.

Zugehöriger Link

Registrieren von iDRAC als einen Computer in der Active Directory-Stammdomäne
Kerberos Keytab-Datei generieren
Active Directory-Objekte erstellen und Berechtigungen bereitstellen

Registrieren von iDRAC als einen Computer in der Active Directory-Stammdomäne

So registrieren Sie iDRAC in der Active Directory-Stammdomäne:

1 Klicken Sie auf **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Netzwerk**.
Die Seite **Netzwerk** wird angezeigt.
2 Stellen Sie eine gültige IP-Adresse für den **bevorzugten/alternativen DNS-Server** bereit. Dieser Wert steht für eine gültige IP-Adresse für den DNS-Server, der Teil der Stammdomäne ist.
3 Wählen Sie **iDRAC auf DNS registrieren** aus.
4 Geben Sie einen gültigen **DNS-Domänennamen an**.
5 Stellen Sie sicher, dass die Netzwerk-DNS-Konfiguration mit den Active Directory-DNS-Informationen übereinstimmt.
Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Kerberos Keytab-Datei generieren

Zur Unterstützung der SSO- und Smart Card-Anmeldungs-Authentifizierung unterstützt iDRAC die Konfiguration zur Selbstaktivierung als Kerberos-Dienst in einem Windows-Kerberos-Netzwerk. Die Kerberos-Konfiguration am iDRAC umfasst dieselben Schritte wie die Konfiguration eines Kerberos-Dienstes als Sicherheitsprinzipal in Windows Server Active Directory auf einem Nicht-Windows-Server.

Mit dem *ktpass*-Hilfsprogramm (wird von Microsoft als Teil der Server-Installations-CD/DVD bereitgestellt) werden die Bindungen des Dienstprinzipalnamens (SPN =Service Principal Name) zu einem Benutzerkonto erstellt und die Vertrauensinformationen in eine MIT-artige Kerberos-*Keytab*-Datei exportiert, die eine Vertrauensbeziehung zwischen einem externen Benutzer oder System und dem Schlüsselverteilungscenter (KDC = Key Distribution Centre) aktiviert. Die Keytab-Datei enthält einen kryptografischen Schlüssel, der zum Verschlüsseln der Informationen zwischen Server und KDC dient. Das Hilfsprogramm "ktpass" ermöglicht es UNIX-basierten Diensten, die Kerberos-Authentifizierung unterstützen, die von einem Kerberos-KDC-Dienst für Windows Server bereitgestellten Interoperabilitätsfunktionen zu verwenden. Weitere Informationen zum Dienstprogramm **ktpass** finden Sie auf der Microsoft-Website unter: **technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

Sie müssen vor dem Erstellen einer Keytab-Datei ein Active Directory-Benutzerkonto zur Benutzung mit der Option **-mapuser** des Befehls `ktpass` einrichten. Außerdem müssen Sie denselben Namen verwenden wie den iDRAC-DNS-Namen, zu dem Sie die erstellte Keytab-Datei hochladen.

So generieren Sie eine Keytab-Datei mithilfe des ktpass-Tools:

1 Führen Sie das Dienstprogramm *ktpass* auf dem Domänen-Controller (Active Directory-Server) aus, auf dem Sie den iDRAC einem Benutzerkonto in Active Directory zuordnen möchten.
2 Verwenden Sie den folgenden ktpass-Befehl, um die Kerberos-Keytab-Datei zu erstellen:

```
C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -mapuser DOMAINNAME
\username -mapOp set -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass [password] -out c:
\krbkeytab
```

Der Verschlüsselungstyp lautet AES256-SHA1. Der Prinzipaltyp lautet KRB5_NT_PRINCIPAL. Die Eigenschaften des Benutzerkontos, dem der Dienstprinzipalname zugeordnet ist, muss „**AES 256“-Verschlüsselungstypen für dieses Konto verwenden** ordnungsgemäß aktiviert haben.

ANMERKUNG: Verwenden Sie – gemäß dem Beispiel – Kleinbuchstaben für den iDRAC-Namen und die Service-Prinzip-Bezeichnung und Großbuchstaben für den Domänennamen.

3 Führen Sie den folgenden Befehl aus:

```
C:\>setspn -a HTTP/iDRACname.domainname.com username
```

Es wird eine Keytab-Datei generiert.

ANMERKUNG: Wenn beim iDRAC-Benutzer, für den die Keytab-Datei erstellt wird, Probleme auftreten, erstellen Sie bitte einen neuen Benutzer und eine neue Keytab-Datei. Wenn dieselbe Keytab-Datei, die ursprünglich erstellt wurde, erneut ausgeführt wird, wird sie nicht korrekt konfiguriert.

Active Directory-Objekte erstellen und Berechtigungen bereitstellen

Führen Sie die folgenden Schritte für das erweiterte Active Directory-Schema auf der Basis der SSO-Anmeldung aus:

1 Erstellen Sie das Geräteobjekt, Berechtigungsobjekt und das Zuordnungsobjekts im Active Directory-Server.
2 Einstellung von Zugangsberechtigungen für das angelegte Berechtigungsobjekt. Es wird empfohlen, keine Administratorberechtigungen zu vergeben, da hiermit einige Sicherheitsprüfungen umgangen werden könnten.
3 Ordnen Sie das Geräteobjekt und das Berechtigungsobjekt mit dem Zuordnungsobjekt zu.
4 Fügen Sie dem Geräteobjekt den vorherigen SSO-Benutzer (anmeldender Benutzer) zu.
5 Vergeben Sie die Zugangsberechtigung zum Zugriff auf das angelegte Zuordnungsobjekt an *authentifizierte Benutzer*.

Zugehöriger Link

iDRAC-Benutzer und -Berechtigungen zu Active Directory hinzufügen

iDRAC-SSO-Anmeldung für Active Directory-Benutzer konfigurieren

Stellen Sie vor der Konfiguration von iDRAC für die Active Directory-SSO-Anmeldung sicher, dass alle Voraussetzungen erfüllt sind.

Sie können iDRAC für Active Directory-SSO konfigurieren, wenn Sie ein Benutzerkonto auf der Basis von Active Directory einrichten.

Zugehöriger Link

Voraussetzungen für die einmalige Active Directory-Anmeldung oder die Smart Card-Anmeldung
Active Directory mit Standardschema unter Verwendung der CMC-Webschnittstelle konfigurieren
Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM
Active Directory mit erweitertem Schema unter Verwendung der iDRAC-Webschnittstelle konfigurieren
Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM

iDRAC-SSO-Anmeldung für Active Directory-Benutzer über die Webschnittstelle konfigurieren

So konfigurieren Sie iDRAC für die Active Directory-SSO-Anmeldung:

ANMERKUNG: Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

1 Überprüfen Sie, ob der iDRAC-DNS-Name mit dem vollständigen, qualifizierten iDRAC-Domänennamen übereinstimmt. Gehen Sie dazu in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Netzwerk**, und rufen Sie die Eigenschaft **DNS-Domänenname** ab.

2 Während Sie Active Directory für die Einrichtung eines Benutzerkontos auf der Basis eines Standardschemas oder eines erweiterten Schemas konfigurieren, führen Sie die folgenden zwei zusätzlichen Schritte für die Konfiguration von SSO aus:

- Laden Sie die Keytab-Datei auf die Seite **Active Directory-Konfiguration und Verwaltung – Schritt 1 von 4** hoch.
- Wählen Sie die Option **Einmaliges Anmelden aktivieren** auf der Seite **Active Directory-Konfiguration und Verwaltung – Schritt 2 von 4** aus.

iDRAC SSO-Anmeldung für Active Directory-Benutzer über RACADM konfigurieren

Um SSO zu aktivieren, führen Sie die Schritte zum Konfigurieren von Active Directory und den folgenden Befehl aus:

```
racadm set iDRAC.ActiveDirectory.SSOEnable 1
```

iDRAC-Smart Card-Anmeldung für lokale Benutzer konfigurieren

So konfigurieren Sie einen lokalen iDRAC-Benutzer für die Smart Card-Anmeldung:

1 Laden Sie das Smart Card-Benutzerzertifikat und das vertrauenswürdige Zertifizierungsstellenzertifikat nach iDRAC noch.

2 Smart Card-Anmeldung aktivieren

Zugehöriger Link

Zertifikate abrufen
Smart Card-Benutzerzertifikat hochladen
Smart Card-Anmeldung aktivieren oder deaktivieren

Smart Card-Benutzerzertifikat hochladen

Bevor Sie das Benutzerzertifikat hochladen, stellen Sie sicher, dass das Benutzerzertifikat des Smart Card-Anbieters im Base64-Format vorliegt. SHA-2-Zertifikate werden ebenfalls unterstützt.

Zugehöriger Link

Zertifikate abrufen

Smart Card-Benutzerzertifikat über die Web-Schnittstelle hochladen

So laden Sie ein Smart Card-Benutzerzertifikat hoch:

1 Gehen Sie in der Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Benutzerauthentifizierung** > **Lokale Benutzer**.

Die Seite **Benutzer** wird angezeigt.

2 In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.

Die Seite **Benutzer-Hauptmenü** wird angezeigt.

3 Wählen Sie unter **Smart Card-Konfigurationen** die Option **Benutzerzertifikat hochladen** aus, und klicken Sie dann auf **Weiter**.

Daraufhin wird die Seite **Benutzerzertifikat hochladen** angezeigt.

4 Führen Sie einen Suchlauf durch, wählen Sie dann das Base64-Benutzerzertifikat aus, und klicken Sie auf **Anwenden**.

Smart Card-Benutzerzertifikat über RACADM hochladen

Um ein Smart Card-Benutzerzertifikat hochzuladen, verwenden Sie das Objekt **usercertupload**. Weitere Informationen finden Sie im *iDRACRACADM Command Line Interface Reference Guide (iDRACRACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* unter **dell.com/idracmanuals**.

Vertrauenswürdiges Zertifizierungsstellenzertifikat für Smart Card hochladen

Bevor Sie das Zertifizierungsstellenzertifikat hochladen, müssen Sie sicherstellen, dass Sie über ein Zertifikat verfügen, das von der Zertifizierungsstelle signiert wurde.

Zugehöriger Link

Zertifikate abrufen

Vertrauenswürdiges Zertifizierungsstellenzertifikat für Smart Card über die Web-Schnittstelle hochladen

So laden Sie ein vertrauenswürdiges Zertifizierungsstellenzertifikat für die Smart Card-Anmeldung hoch:

1 Gehen Sie in der Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk** > **Benutzerauthentifizierung** > **Lokale Benutzer**.

Die Seite **Benutzer** wird angezeigt.

2 In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.

Die Seite **Benutzer-Hauptmenü** wird angezeigt.

3 Wählen Sie unter **Smart Card-Konfiguration** die Option **Zertifikat einer vertrauenswürdigen Zertifizierungsstelle hochladen** aus, und klicken Sie dann auf **Weiter**.

Daraufhin wird die Seite **Zertifikat einer vertrauenswürdigen Zertifizierungsstelle hochladen** angezeigt.

4 Suchen Sie das vertrauenswürdige Zertifizierungsstellenzertifikat, und klicken Sie auf **Anwenden**.

Vertrauenswürdiges Zertifizierungsstellenzertifikat für Smart Card über RACADM hochladen

Um ein vertrauenswürdiges Zertifikat einer vertrauenswürdigen Zertifizierungsstelle für die Smart Card-Anmeldung hochzuladen, verwenden Sie das Objekt **usercertupload**. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* unter **dell.com/idracmanuals**.

iDRAC-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren

Vor der Konfiguration der iDRAC-Smart-Card-Anmeldung für Active Directory-Benutzer müssen Sie sicherstellen, dass die erforderlichen Voraussetzungen erfüllt sind.

So konfigurieren Sie iDRAC für die Smart Card-Anmeldung:

1 Führen Sie über die iDRAC-Webschnittstelle, während Sie Active Directory für die Einrichtung eines Benutzerkontos auf der Basis eines Standard- oder eines erweiterten Schemas konfigurieren, auf der Seite **Active Directory-Konfiguration und Verwaltung – Schritt 1 von 4** die folgenden Aktivitäten aus:
   - Aktivieren Sie die Zertifikatüberprüfung.
   - Laden Sie ein vertrauenswürdiges, von einer Zertifikatzertifizierungsstelle signiertes Zertifikat hoch.
   - Laden Sie die Keytab-Datei hoch.
2 Aktivieren Sie die Smart Card-Anmeldung. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Zugehöriger Link

Smart Card-Anmeldung aktivieren oder deaktivieren
Zertifikate abrufen
Kerberos Keytab-Datei generieren
Active Directory mit Standardschema unter Verwendung der CMC-Webschnittstelle konfigurieren
Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM
Active Directory mit erweitertem Schema unter Verwendung der iDRAC-Webschnittstelle konfigurieren
Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM

Smart Card-Anmeldung aktivieren oder deaktivieren

Vor der Aktivierung oder Deaktivierung der Smart Card-Anmeldung für iDRAC müssen Sie Folgendes sicherstellen:

- Die iDRAC-Berechtigungen sind konfiguriert.
- Die lokale iDRAC-Benutzerkonfiguration oder die Active Directory-Benutzerkonfiguration mit den entsprechenden Zertifikaten ist abgeschlossen.

ANMERKUNG: Wenn die Smart Card-Anmeldung aktiviert ist, sind SSH, Telnet, IPMI über LAN, Serielle Verbindung über LAN und Remote-RACADM deaktiviert. Zur Erinnerung: Wenn die Smart Card-Anmeldung deaktiviert ist, werden die Schnittstellen nicht automatisch aktiviert.

Zugehöriger Link

Zertifikate abrufen
iDRAC-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren
iDRAC-Smart Card-Anmeldung für lokale Benutzer konfigurieren

Smart Card-Anmeldung über die Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Smart Card-Anmeldefunktion:

1 Gehen Sie in der iDRAC-Webschnittstelle nach **Übersicht** > **iDRAC-Einstellungen** > **Benutzerauthentifizierung** > **Smart Card**.
   Daraufhin wird die Seite **Smart Card** angezeigt.
2 Wählen Sie in der Drop-Down-Liste **Smart Card-Anmeldung konfigurieren** die Option **Aktiviert** aus, um die Smart Card-Anmeldung zu aktivieren, oder wählen Sie **Mit Remote-RACADM aktiviert** aus. Wählen Sie ansonsten die Option **Deaktiviert** aus.
   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
3 Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.
   Bei nachfolgenden Anmeldeversuchen über die iDRAC-Web-Schnittstelle werden Sie dazu aufgefordert, eine Smart Card-Anmeldung auszuführen.

Smart Card-Anmeldung über RACADM aktivieren oder deaktivieren

Um die Smart Card-Anmeldung zu aktivieren, verwenden Sie den Befehl **set** mit Objekten in der Gruppe **iDRAC.SmartCard**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Smart Card-Anmeldung über das Dienstprogramm für die iDRAC-Einstellungen aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Smart Card-Anmeldefunktion:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen nach **Smart Card**.

Daraufhin wird die Seite **iDRAC-Einstellungen – Smart Card** angezeigt

2 Wählen Sie die Option **Aktiviert** aus, um die Smart Card-Anmeldung zu aktivieren. Oder wählen Sie **Deaktiviert** aus. Weitere Informationen zu diesen Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Smart Card-Anmeldefunktion wird entsprechend Ihrer Auswahl entweder aktiviert oder deaktiviert.

9

iDRAC für das Versenden von Warnungen konfigurieren

Sie können Warnungen und Maßnahmen für bestimmte Ereignisse festlegen, die auf dem Managed System auftreten. Ein Ereignis tritt auf, wenn der Status einer Systemkomponente vom vordefinierten Zustand abweicht. Wenn ein Ereignis mit einem Ereignisfilter übereinstimmt und Sie diesen Filter für die Generierung einer Warnung konfiguriert haben (per E-Mail, SNMP-Trap, IPMI-Warnung, Remote-Systemprotokolle oder WS-Ereignisse), wird eine Warnung an ein oder mehrere konfigurierte Ziele gesendet. Wenn der gleiche Ereignisfilter auch zum Ausführen einer Maßnahme (z. B. Neustart, Aus- und Einschalten oder Ausschalten des Systems) konfiguriert wurde, wird diese Maßnahme ausgeführt. Sie können für jedes Ereignis nur eine Maßnahme festlegen.

So konfigurieren Sie iDRAC zum Versenden von Warnungen:

1 Aktivieren Sie Warnungen.
2 Optional können Sie die Warnungen auf der Basis der Kategorie oder des Schweregrads filtern.
3 Konfigurieren Sie E-Mail-Warnungen, IPMI-Warnungen, SNMP-Traps, Remote System-Protokolle, Redfish-Ereignisse, Betriebssystemprotokolle und/oder WS-Ereignis-Einstellungen.
4 Aktivieren Sie die folgenden Ereigniswarnungen und Maßnahmen:
   - Senden von E-Mail-Warnungen, IPMI-Warnungen, SNMP-Traps, Remote System-Protokollen, Redfish-Ereignissen, Betriebssystemprotokollen oder WS-Ereignissen an die konfigurierten Ziele.
   - Führen Sie einen Neustart aus, schalten Sie das Gerät aus, oder führen Sie einen Aus- und Einschaltvorgang auf dem Managed System durch.

Themen:

Zugehöriger Link

Warnungen aktivieren und deaktivieren

Zum Senden einer Warnung an konfigurierte Ziele oder zum Ausführen einer Ereignismaßnahme müssen Sie die globale Warnoption aktivieren. Diese Eigenschaft überschreibt die individuell festgelegten Warnungen oder Ereignismaßnahmen.

Zugehöriger Link

Warnungen filtern

Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren

Warnungen über die Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Generierung von Warnungen:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Warnungen**. Daraufhin wird die Seite **Warnungen** angezeigt.

2 Im Abschnitt **Warnungen**:

- Wählen Sie die Option **Aktivieren** aus, um die Generierung von Warnungen zu aktivieren oder um eine Ereignismaßnahme auszuführen.
- Wählen Sie die Option **Deaktivieren** aus, um die Generierung von Warnungen zu deaktivieren oder um eine Ereignismaßnahme zu deaktivieren.

3 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Warnungen über RACADM aktivieren oder deaktivieren

Geben Sie folgenden Befehl ein:

```
racadm set iDRAC.IPMILan.AlertEnable <n>
```

n=0 – Deaktiviert

n=1 – Aktiviert

Warnungen über das Dienstprogramm für iDRAC-Einstellungen aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Generierung von Warnungen oder Ereignismaßnahmen:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Warnungen**.

Die Seite **Warnungen für iDRAC-Einstellungen** wird angezeigt.

2 Wählen Sie unter **Plattformereignisse** die Option **Aktiviert** aus, um die Warnungsgenerierung oder die Ereignismaßnahme zu aktivieren. Wählen Sie ansonsten **Deaktiviert** aus. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen.*

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Warnungseinstellungen sind damit konfiguriert.

Warnungen filtern

Sie können Warnungen auf der Basis der Kategorie und des Schweregrads filtern.

Zugehöriger Link

Warnungen aktivieren und deaktivieren

Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren

Filtern von Warnungen über die iDRAC-Webschnittstelle

So filtern Sie Warnungen auf der Basis der Kategorie und des Schweregrads:

ANMERKUNG: Selbst wenn Sie als Benutzer nur über Leseberechtigungen verfügen, können Sie die Warnungen filtern.

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Warnungen**. Daraufhin wird die Seite **Warnungen** angezeigt.

2 Wählen Sie unter **Warnungsfilter** eine oder mehrere der folgenden Kategorien aus:

- Systemzustand
- Bei Lagerung
- Konfiguration
- Audit
- Updates
- Arbeitsanmerkungen

3 Wählen Sie eine oder mehrere der folgenden Schweregrade aus:

- Informativ
- Warnung
- Kritisch

4 Klicken Sie auf **Anwenden**.

Der Abschnitt **Warnungsergebnisse** zeigt die Ergebnisse auf der Basis der ausgewählten Kategorie und des Schweregrads an.

Warnungen über RACADM filtern

Um die Warnungen zu filtern, verwenden Sie den Befehl **eventfilters**. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Ereigniswarnungen einrichten

Sie können Ereigniswarnungen, wie z. B. E-Mail-Warnungen, IPMI-Warnungen, SNMP-Traps, Remote-System-Protokolle, Betriebssystemprotokolle und WS-Ereignisse so einstellen, dass sie an die konfigurierten Ziele gesendet werden.

Zugehöriger Link

Warnungen aktivieren und deaktivieren

Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren

Warnungen filtern

Remote-Systemprotokollierung konfigurieren

Konfigurieren von WS-Ereignisauslösung

Konfigurieren von Redfish-Ereignissen

Ereigniswarnungen über die Web-Schnittstelle einrichten

So legen Sie eine Ereigniswarnung über die Web-Schnittstelle fest:

1 Stellen Sie sicher, dass Sie E-Mail-Warnung, IPMI-Warnung, SNMP-Trap-Einstellungen und/oder Einstellungen des Remote System-Protokolls konfiguriert haben.

2 Gehen Sie zu **Übersicht** > **Server** > **Warnungen**.

Die Seite **Warnungen** wird angezeigt.

3 Wählen Sie unter **Warnergebnisse** eine oder alle der folgenden Warnungen für die benötigten Ereignisse aus:

- E-Mail-Warnung
- SNMP-Trap
- IPMI-Warnung
- Remote System-Protokoll
- BS-Protokoll
- WS-Ereignisauslösung

4 Klicken Sie auf **Anwenden**.

Die Einstellung wird gespeichert.

5 Wählen Sie im Abschnitt **Warnungen** die Option **Aktivieren** aus, um Warnungen an konfigurierte Ziele zu senden.

6 Optional können Sie ein Testereignis versenden. Geben Sie in das Feld **Meldungs-ID für Testereignis** die Meldungs-ID ein, um zu testen, ob die Warnung erzeugt wird, und klicken Sie auf **Test**. Eine Liste der Meldungs-IDs finden Sie im *Event Messages Guide* (Handbuch für Ereignismeldungen) unter **dell.com/support/manuals**.

Ereigniswarnungen über RACADM einrichten

Zur Einrichtung einer Ereigniswarnung verwenden Sie den Befehl **eventfilters**. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Alarmwiederholungsereignis einrichten

Sie können iDRAC so konfigurieren, dass in bestimmten Intervallen weitere Ereignisse erzeugt werden, wenn das System weiterhin überhalb des Schwellenwertes für die Einlasstemperatur betrieben wird. Das standardmäßige Intervall beträgt 30 Tage. Der gültige Bereich liegt zwischen 0 und 366 Tagen. Ein Wert von 0 zeigt an, dass Ereignisse nicht wiederholt werden.

ANMERKUNG: Sie müssen die Berechtigung zum Konfiguirieren des iDRAC („Configure iDRAC“) besitzen, um den Wert für die Alarmwiederholung einzustellen.

Einrichten eines Alarmwiederholungsereignisses über die iDRAC-Webschnittstelle

So legen Sie einen Wert für die Alarmwiederholung fest:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Warnungen** > **Alarmwiederholung**.

Die Seite **Alarmwiederholung** wird angezeigt.

2 Geben Sie in der Spalte **Wiederholung** einen Wert für die Alarmhäufigkeit für die gewünschte Kategorie, den Alarm und die Schweregrade ein.

Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

3 Klicken Sie auf **Anwenden**.

Die Einstellungen für die Alarmwiederholung werden gespeichert.

Alarmwiederholungsereignis über RACADM einrichten

Verwenden Sie den Befehl **eventfilters**, um über den RACADM Alarm-Wiederholungsereignisse einzurichten. Weitere Informationen hierzu finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)*, das unter **dell.com/idracmanuals** verfügbar ist.

Ereignismaßnahmen festlegen

Sie können Ereignismaßnahmen festlegen, z. B. das Ausführen eines Neustarts, Aus- und Einschalten und Ausschalten. Es ist auch möglich, keine Maßnahme auf dem System auszuführen.

Zugehöriger Link

Warnungen filtern

Warnungen aktivieren und deaktivieren

Ereignismaßnahmen über die Web-Schnittstelle einrichten

So richten Sie eine Ereignismaßnahme ein:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Warnungen**. Daraufhin wird die Seite **Warnungen** angezeigt.

2 Wählen Sie unter **Warnergebnisse** im Drop-Down-Menü **Maßnahmen** für jedes Ereignis eine Maßnahme aus:
- Neustarten
- Aus- und Einschalten
- Ausschalten
- Keine Maßnahme

3 Klicken Sie auf **Anwenden**.

Die Einstellung wird gespeichert.

Ereignismaßnahmen über RACADM einrichten

Zur Konfiguration einer Ereignisaktion verwenden Sie den Befehl **eventfilters**. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren

Die Management Station verwendet Traps der Art „Simple Network Management Protocol“ (SNMP) und „Intelligent Platform Management Interface“ (IPMI), um Daten vom iDRAC zu empfangen. Bei Systemen mit einer größeren Anzahl an Knoten ist es für eine Management Station möglicherweise nicht effizient, jeden einzelnen iDRAC in Bezug auf einen potenziell möglichen Zustand abzufragen. Ereignis-Traps können eine Management Station beispielsweise mit einem Lastenausgleich zwischen Knoten oder durch das Generieren einer Warnung unterstützen, wenn ein Authentifizierungsfehler auftritt.

Sie können die IPv4- und IPv6-Warnungsziele, die E-Mail-Einstellungen und die SMTP-Server-Einstellungen konfigurieren und diese Einstellungen testen. Sie können auch angeben, welche SNMP-v3-Benutzer die SNMP-Traps erhalten sollen.

Vor der Konfigurierung der Einstellungen für E-Mails, SNMPs oder IPMI-Traps müssen Sie Folgendes sicherstellen:

- Sie verfügen über Berechtigungen zum Konfigurieren von RAC.
- Sie haben die Ereignisfilter konfiguriert.

Zugehöriger Link

IP-basierte Warnziele konfigurieren
Konfigurieren von E-Mail-Benachrichtigungen

IP-basierte Warnziele konfigurieren

Sie können die IPv6- oder IPv4-Adressen für den Empfang von IPMI-Warnungen oder SNMP-Traps konfigurieren.

Weitere Informationen zu den erforderlichen iDRAC-MIBs zur Überwachung der Server unter Verwendung von SNMP finden Sie im *SNMP Reference Guide (SNMP-Referenzhandbuch)* unter **dell.com/support/manuals**.

IP-basierte Warnziele über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Warnungszieleinstellungen unter Verwendung der Web-Schnittstelle:

1 Gehen Sie zu **Übersicht** > **Server** > **Warnungen** > **SNMP- und E-Mail-Einstellungen**.

2 Wählen Sie die Option **Zustand** aus, um ein Warnungsziel (IPv4-Adresse, IPv6-Adresse oder vollständig qualifizierter Domänenname (FQDN)) zum Empfang der Traps zu aktivieren.

Sie können bis zu acht Zieladressen angeben. Weitere Informationen zu den Optionen finden Sie in der *iDRAC-Online-Hilfe*.

3 Wählen Sie die SNMP-v3-Benutzer aus, an die Sie den SNMP-Trap senden möchten.

4 Geben Sie die iDRAC-SNMP-Community-Zeichenfolge (nur für SNMPv1- und v2) und die SNMP-Warnungsschnittstellennummer ein.

Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

> **ANMERKUNG: Der Wert für die Community-Zeichenkette zeigt die Community-Zeichenkette an, die für einen Warnungs-Trap der Art „Simple Network Management Protocol“ (SNMP) verwendet wird, der von iDRAC aus versendet wird. Stellen Sie sicher, dass die Ziel-Community-Zeichenkette mit der iDRAC-Community-Zeichenkette übereinstimmt. Der Standardwert lautet „Öffentlich“.**

5 Um zu testen, ob die IP-Adresse die IPMI- oder SNMP-Traps empfängt, klicken Sie auf die Option **Senden**, die sich entweder unter **IPMI-Trap testen** oder unter **SNMP-Trap testen** befindet.

6 Klicken Sie auf **Anwenden**.

Die Warnungsziele sind damit konfiguriert.

7 Wählen Sie im Abschnitt **SNMP-Trap-Format** die Protokollversion aus, die zum Senden der Traps an die Trap-Ziele – **SNMP v1**, **SNMP v2** oder **SNMP v3** verwendet werden soll, und klicken Sie auf **Anwenden**.

> **ANMERKUNG: Die Option SNMP Trap Format gilt nur für SNMP-Traps und nicht für IPMI-Traps. IPMI-Traps werden immer im Format SNMP v1 gesendet und basieren nicht auf der konfigurierten Option SNMP Trap Format.**

Das SNMP-Trap-Format ist konfiguriert.

IP-Warnungsziele über RACADM konfigurieren

So konfigurieren Sie Trap-Warnungseinstellungen:

1 So aktivieren Sie Traps:

```
racadm set idrac.SNMP.Alert.<index>.Enable <n>
```

Parameter	Beschreibung
`<index>`	Zielindex. Zulässige Werte sind 1 bis 8.

Parameter	Beschreibung
<n>=0	Trap deaktivieren
<n>=1	Trap aktivieren

2 So konfigurieren Sie die Adresse für das Trap-Ziel:

```
racadm set idrac.SNMP.Alert.<index>.DestAddr <Address>
```

Parameter	Beschreibung
<index>	Zielindex. Zulässige Werte sind 1 bis 8.
<Address>	Eine gültige IPv4-, IPv6- oder FQDN-Adresse

3 Konfigurieren Sie die SNMP-Community-Namen-Zeichenkette.

```
racadm set idrac.ipmilan.communityname <community_name>
```

Parameter	Beschreibung
<community_name>	Der SNMP-Community-Name.

4 So konfigurieren Sie das SNMP-Ziel:

- Stellen Sie das SNMP-Trap-Ziel für SNMPv3 ein:

  ```
  racadm set idrac.SNMP.Alert.<index>.DestAddr <IP address>
  ```

- Stellen Sie SNMPv3-Benutzer für die Trap-Ziele ein:

  ```
  racadm set idrac.SNMP.Alert.<index>.SNMPv3Username <user_name>
  ```

- Aktivieren Sie SNMPv3 für einen Benutzer:

  ```
  racadm set idrac.users.<index>.SNMPv3Enable Enabled
  ```

5 So testen bei Bedarf Sie den Trap:

```
racadm testtrap -i <index>
```

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

IP-basierte Warnziele über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

Sie können Warnungsziele (IPv4, IPv6 oder FQDN)unter Verwendung des Dienstprogramms für die iDRAC-Einstellungen konfigurieren. Gehen Sie wie folgt vor:

1 Gehen Sie im **Dienstprogramm für die iDRAC-Einstellungen** zu **Warnungen**.

Die Seite **Warnungen für iDRAC-Einstellungen** wird angezeigt.

2 Aktivieren Sie unter **Trap-Einstellungen** die IP-Adresse(n) für den Empfang der Traps und geben Sie die IPv4, IPv6- oder FQDN-Zieladresse(n) ein. Sie können bis zu acht Adressen angeben.

3 Geben Sie die Community-Namen-Zeichenkette ein.

Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

4 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Warnungsziele sind damit konfiguriert.

Konfigurieren von E-Mail-Benachrichtigungen

Sie können die E-Mail-Adresse für den Empfang der E-Mail-Warnungen konfigurieren. Außerdem können Sie die Einstellungen für die SMTP-Server-Adresse konfigurieren.

ANMERKUNG: Wenn Ihr Mail-Server Microsoft Exchange Server 2007 ist, ist sicherzustellen, dass der iDRAC-Domänenname so konfiguriert ist, dass der Mail-Server die E-Mail-Warnungen des iDRAC empfängt.

ANMERKUNG: E-Mail-Warnungen unterstützen sowohl IPv4- als auch IPv6-Adressen. Der DRAC DNS-Domänenname muss beim Nutzen von IPv6 festgelegt werden.

Zugehöriger Link

Konfigurieren der Adresseneinstellungen des SMTP-E-Mail-Servers

E-Mail-Warnungseinstellungen über Web-Schnittstelle konfigurieren

So konfigurieren Sie die E-Mail-Warnungseinstellungen über die Web-Schnittstelle:

1. Gehen Sie zu **Übersicht** > **Server** > **Warnungen** > **SNMP- und E-Mail-Einstellungen**.
2. Wählen Sie die Option **Status** aus, um die E-Mail-Adresse für den Empfang der Warnungen zu aktivieren; geben Sie außerdem eine gültige E-Mail-Adresse ein. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
3. Klicken Sie auf **Senden** bei **E-Mail testen**, um die konfigurierten E-Mail-Warnungseinstellungen zu testen.
4. Klicken Sie auf **Anwenden**.

E-Mail-Warnungseinstellungen mit RACADM konfigurieren

1. E-Mail-Warnung aktivieren:

```
racadm set iDRAC.EmailAlert.Enable.[index] [n]
```

Parameter	Beschreibung
`index`	E-Mail-Zielindex. Zulässige Werte sind 1 bis 4.
`n=0`	Deaktiviert E-Mail-Warnungen.
`n=1`	Aktiviert E-Mail-Warnungen.

2. Konfigurieren der E-Mail-Einstellungen:

```
racadm set iDRAC.EmailAlert.Address.[index] [email-address]
```

Parameter	Beschreibung
`index`	E-Mail-Zielindex. Zulässige Werte sind 1 bis 4.
`email-address`	Ziel-E-Mail-Adresse, die die Plattformereigniswarnungen empfängt.

3. So konfigurieren Sie eine benutzerdefinierte Meldung:

```
racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
```

Parameter	Beschreibung
`index`	E-Mail-Zielindex. Zulässige Werte sind 1 bis 4.
`custom-message`	Benutzerdefinierte Meldung

4. So testen Sie bei Bedarf die konfigurierte E-Mail-Warnung:

```
racadm testemail -i [index]
```

Parameter	Beschreibung
`index`	Zu testender E-Mail-Zielindex. Zulässige Werte sind 1 bis 4.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Konfigurieren der Adresseneinstellungen des SMTP-E-Mail-Servers

Sie müssen die SMTP-Server-Adresse für E-Mail-Warnungen konfigurieren, damit diese an bestimmte Ziele versendet werden können.

Konfigurieren von Adresseinstellungen für den SMTP-E-Mail-Server über die iDRAC-Webschnittstelle

So konfigurieren Sie die SMTP-Server-Adresse:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Warnungen** > **SNMP- und E-Mail-Einstellungen**.
2. Geben Sie eine gültige IP-Adresse oder den voll qualifizierten Domänennamen (FQDN) des in der Konfiguration zu verwendenden SMTP-Servers ein.
3. Wählen Sie die Option **Authentifizierung aktivieren** aus, und geben Sie den Benutzernamen und das Kennwort (eines Benutzers mit Zugriff auf den SMTP-Server) ein.
4. Geben Sie die SMTP-Portnummer ein.

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
5. Klicken Sie auf **Anwenden**.

   Die SMTP-Einstellungen sind damit konfiguriert.

Adresseinstellungen für den SMTP-E-Mail-Server über RACADM konfigurieren

So konfigurieren Sie den SMTP-E-Mail-Server:

```
racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP E-mail Server IP Address>
```

Konfigurieren von WS-Ereignisauslösung

Das WS-Ereignisauslösungsprotokoll wird verwendet, damit ein Client-Dienst (Abonnent) bei einem Server (Ereignisquelle) Interesse (Abonnement) daran registrieren kann, Meldungen mit den Serverereignissen (Benachrichtigungen oder Ereignismeldungen) zu empfangen. Clients, die am Empfang von WS-Ereignisauslösungsmeldungen interessiert sind, können iDRAC abonnieren und Ereignisse in Zusammenhang mit Jobs des Lifecycle-Controllers erhalten.

Die Schritte, die zur Konfiguration der WS-Ereignisauslösungsfunktion für den Empfang von WS-Ereignisauslösungsnachrichten zu Änderungen im Zusammenhang mit Lifecycle Controller-Jobs erforderlich sind, werden im Spezifikationsdokument der Web-Dienst-Ereignisunterstützung für iDRAC 1.30.30 beschrieben. Neben dieser Spezifikation finden Sie die vollständigen Informationen zum WS-Ereignisauslösungsprotokoll im Dokument DSP0226 (DMTF WS-Verwaltungsspezifikationen), Abschnitt 10 Benachrichtigungen (Ereignisauslösung). Die Jobs im Zusammenhang mit Lifecycle Controller sind im Dokument DCIM-Job-Kontrollprofil beschrieben.

Konfigurieren von Redfish-Ereignissen

Das Redfish-Ereignisauslösungsprotokoll wird verwendet, damit ein Client-Dienst (Abonnent) bei einem Server (Ereignisquelle) Interesse (Abonnement) daran registrieren kann, Meldungen mit den Redfish-Ereignissen (Benachrichtigungen oder Ereignismeldungen) zu empfangen. Clients, die am Empfang von Redfish-Ereignisauslösungsmeldungen interessiert sind, können iDRAC abonnieren und Ereignisse im Zusammenhang mit Lifecycle Controller-Jobs erhalten.

Überwachung von Gehäuseereignissen

Auf dem PowerEdge FX2-/FX2s-Gehäuse können Sie die Einstellung **Chassis Management and Monitoring (Gehäuseverwaltung und -überwachung)** in iDRAC aktivieren, um Gehäuseverwaltungs- und -überwachungsaufgaben durchzuführen, wie z. B. die Überwachung der Gehäusekomponenten, die Konfiguration von Warnungen, die Verwendung von iDRAC-RACADM zur Weiterleitung von CMC-RACADM-Befehlen und die Aktualisierung der Gehäuseverwaltungs-Firmware. Mit dieser Einstellung können Sie sogar dann die Server im Gehäuse

verwalten, wenn sich der CMC nicht im Netzwerk befindet. Sie können für diesen Wert **Disabled (Deaktiviert)** einstellen, um die Gehäuseereignisse weiterzuleiten. Standardmäßig ist diese Einstellung auf **Enabled (Aktiviert)** festgelegt.

ANMERKUNG: Damit sich diese Einstellung auswirkt, müssen Sie sicherstellen, dass in CMC die Gehäuseverwaltung im Server - Einstellung auf Überwachen oder Verwalten und Überwachen eingestellt ist.

Wenn die Option **Chassis Management and Monitoring (Gehäuseverwaltung und -überwachung)** auf **Enabled (Aktiviert)** eingestellt ist, generiert und protokolliert iDRAC Gehäuseereignisse. Die generierten Ereignisse werden in das iDRAC-Ereignissubsystem integriert und Warnungen werden ähnlich wie die übrigen Ereignisse erzeugt.

Der CMC leitet auch die für iDRAC generierten Ereignisse weiter. Falls der iDRAC auf dem Server nicht funktionsfähig ist, stellt der CMC die ersten 16 Ereignisse in die Warteschlange und protokolliert die übrigen im CMC-Protokoll. Diese 16 Ereignisse werden an den iDRAC gesendet, sobald **Chassis monitoring (Gehäuseüberwachung)** auf „Enabled“ (Aktiviert) gesetzt wird.

In Fällen, in denen der iDRAC ermittelt, dass eine erforderliche CMC-Funktion nicht vorhanden ist, wird eine Warnmeldung angezeigt, die Sie darüber informiert, dass bestimmte Funktionen ohne eine CMC-Firmware-Aktualisierung möglicherweise nicht funktionsfähig sind.

Überwachung von Gehäuseereignissen unter Verwendung der iDRAC-Webschnittstelle

Zur Überwachung von Gehäuseereignissen unter Verwendung der iDRAC-Webschnittstelle führen Sie die folgenden Schritte aus:

ANMERKUNG: Dieser Abschnitt wird nur für PowerEdge FX2-/FX2s-Gehäuse und bei Einstellung des Gehäuseverwaltung im Servermodus in CMC auf Überwachen oder Verwalten und Überwachen angezeigt.

1. Klicken Sie in der CMC-Schnittstelle auf **Gehäuseübersicht** > **Setup** > **Allgemein**.
2. Wählen Sie aus dem Dropdown-Menü **Gehäuseverwaltung in Servermodus** den Eintrag **Verwalten und Überwachen** aus und klicken Sie auf **Anwenden**.
3. Starten Sie die iDRAC-Webschnittstelle und klicken Sie auf **Übersicht** > **iDRAC-Einstellungen** > **CMC**.
4. Stellen Sie im Abschnitt **Gehäuseverwaltung in Servermodus** sicher, dass im Drop-Down-Feld **Fähigkeit von iDRAC Aktiviert** eingestellt wurde.

Überwachung von Gehäuseereignissen unter Verwendung von RACADM

Diese Einstellung kann nur auf PowerEdge FX2-/FX2s-Servern angewendet werden und wenn der **Gehäuseverwaltung im Server-**Modus auf **Überwachung** oder **Verwalten und Überwachen** eingestellt wurde.

Zur Überwachung von Gehäuseereignissen unter Verwendung von iDRAC-RACADM:

```
racadm get system.chassiscontrol.chassismanagementmonitoring
```

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

IDs für Warnungsmeldung

Die folgende Tabelle enthält eine Liste mit Meldungs-IDs, die bei Warnungen angezeigt werden.

Tabelle 30. IDs für Warnungsmeldungen

Meldungs-ID	Beschreibung
AMP	Stromstärke
ASR	Automatische Systemrücksetzung
BAR	Sichern/Wiederherstellen
BAT	Akkuereignis
BIOS	BIOS Management
Boot (Startvorgang)	Boot-Steuerung
CBL	Kabel
CPU	Prozessor
CPUA	Verfahren nicht vorhanden
CTL	Speicher-Controller
DH	Zertifikatverwaltung
DIS	Automatische Ermittlung
ENC	Speichergehäuse
Lüfter (FAN)	Lüfterereignis
FSD	Fehlersuche
HWC	Hardware-Konfiguration
IPA	DRAC-IP-Änderung
ITR	Eingriff
JCP	Auftragssteuerung
LC	Lifecycle-Controller
LIC	Lizenzierung
Verbindung	Link-Status
Protokoll	Protokollereignis
MEM	Speicher
NDR	NIC-Betriebssystemtreiber
Netzwerkadapter	NIC-Konfiguration

Meldungs-ID	Beschreibung
OSD	BS-Bereitstellung
OSE	BS-Ereignis
PCI	PCI-Gerät
PDR	Physische Festplatte
PR	Teileaustausch
PST	BIOS POST
Netzteil	Stromversorgung
PSUA	PSU nicht vorhanden
PWR	Stromverbrauch
RAC	RAC-Ereignis
RDU	Redundanz
Rot	FW-Download
RFL	IDSDM-Datenträger
RFLA	IDSDM nicht vorhanden
RFM	FlexAddress-SD
RRDU	IDSDM-Redundanz
RSI	Remote-Dienst
SEC	Sicherheitsereignis
Systemereignisprotokoll	System-Ereignisprotokoll
SRD	Software-RAID
SSD	PCIe-SSD-Laufwerke
STOR	Speicher
SUP	FW-Aktualisierungsaufgabe
SWC	Software-Konfiguration
SWU	Software-Änderung
[SYS]	System Info
tmp	Temperatur
TST	Test-Warnung

Meldungs-ID	Beschreibung
UEFI (UEFI-Modus)	UEFI-Ereignis
usr	Benutzerverfolgung
VDR	Virtuelle Festplatte
VF	vFlash-SD-Karte
VFL	vFlash-Ereignis
VFLA	vFlash nicht vorhanden
VLT	Spannung
VME	Virtueller Datenträger
VRM	Virtuelle Konsole
WRK	Arbeitsanmerkung

10

Protokolle verwalten

iDRAC bietet ein Lifecycle-Protokoll, das Ereignisse zum System, zu Speichergeräten, zu Netzwerkgeräten, zu Firmware-Aktualisierungen, zu Konfigurationsänderungen, zu Lizenzmeldungen, usw. enthält. Die Systemereignisse sind jedoch auch als separates Protokoll mit der Bezeichnung „Systemereignisprotokoll“ (SEL) verfügbar. Das Lifecycle-Protokoll ist über die iDRAC-Web-Schnittstelle, über RACADM und die WS-MAN-Schnittstelle verfügbar.

Wenn das Lifecycle-Protokoll eine Größe von 800 KB erreicht, werden die Protokolle komprimiert und archiviert. Sie können nur die nicht archivierten Protokolleinträge anzeigen und Filter und Kommentare auf nicht archivierte Protokolle anwenden. Zum Anzeigen von archivierten Protokollen müssen Sie das gesamte Lifecycle-Protokoll auf einen Speicherort auf Ihrem System exportieren.

Themen:

Zugehöriger Link

Systemereignisprotokoll anzeigen

Wenn ein Systemereignis auf einem Managed System auftritt, wird es im Systemereignisprotokoll (SEL) erfasst. Der gleiche SEL-Eintrag ist auch im LC-Protokoll verfügbar.

Systemereignisprotokoll über die Web-Schnittstelle anzeigen

Um das Systemereignisprotokoll (SEL) anzuzeigen, gehen Sie in der iDRAC-Webschnittstelle auf **Übersicht** > **Server** > **Protokolle**.
Auf der Seite **System Event Log (Systemereignisprotokoll)** werden eine Systemzustandsanzeige, ein Zeitstempel und eine Beschreibung für jedes protokollierte Ereignis angezeigt. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Klicken Sie auf **Speichern unter**, um das **SEL** in einem Speicherort Ihrer Wahl zu speichern.

ANMERKUNG: Wenn Sie Internet Explorer verwenden und ein Problems beim Speichern auftritt, laden Sie die kumulative Sicherheitsaktualisierung für Internet Explorer herunter. Sie können diese von der Microsoft-Support-Website unter support.microsoft.com herunterladen.

Klicken Sie zum Löschen aller Protokolle auf **Protokoll löschen**.

ANMERKUNG: Die Schaltfläche Protokoll löschen wird nur angezeigt, wenn Sie über die Berechtigung Protokolle löschen verfügen.

Nachdem das SEL gelöscht wurde, wird ein Eintrag im Lifecycle Controller-Protokoll erstellt. Der Protokolleintrag enthält den Benutzernamen und die IP-Adresse, von der aus das SEL gelöscht wurde.

Systemereignisprotokoll über RACADM anzeigen

So zeigen Sie das Systemereignisprotokoll (SEL) an:

```
racadm getsel <options>
```

Wenn keine Argumente vorgegeben werden, wird das gesamte Protokoll angezeigt.

So zeigen Sie die Anzahl der SEL-Einträge an: `racadm getsel -i`

So löschen Sie die SEL-Einträge: `racadm clrsel`

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* unter **dell.com/idracmanuals**.

Anzeigen des Systemereignisprotokolls unter Verwendung des Dienstprogramms für die iDRAC-Einstellungen

Sie können die Gesamtzahl der Einträge im Systemereignisprotokoll (SEL) unter Verwendung des Dienstprogramms für die iDRAC-Einstellungen anzeigen und die Protokolle löschen. Dies geschieht so:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Systemereignisprotokoll**.
   Das **iDRAC- Settings.System Event Log** zeigt die **Gesamtzahl der Einträge** an.
2. Um die Einträge zu löschen, wählen Sie **Ja**. Ansonsten wählen Sie **Nein**.
3. Klicken Sie zum Anzeigen der Systemereignisse auf **Systemereignisprotokoll anzeigen**.
4. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Lifecycle-Protokoll anzeigen

Die Lifecycle Controller-Protokolle enthalten die Änderungsverlaufsdaten in Bezug auf die Komponenten, die auf einem verwalteten System installiert sind. Sie können auch Arbeitsanmerkungen zu jedem Protokolleintrag hinzufügen.

Die folgenden Ereignisse und Aktivitäten werden protokolliert:

- Systemereignisse
- Speichergeräte
- Netzwerkgeräte
- Konfiguration
- Audit
- Updates

Wenn Sie sich über eine der folgenden Schnittstellen bei iDRAC anmelden oder von iDRAC abmelden, werden die Anmelde- und Abmeldeereignisse bzw. Anmeldefehler in den Lifecycle-Protokollen aufgezeichnet:

- Telnet
- SSH

- Webschnittstelle
- RACADM
- SM-CLP
- IPMI über LAN
- Seriell
- Virtuelle Konsole
- Virtueller Datenträger

Sie können Protokolle auf Basis der Kategorie und des Schweregrads anzeigen und filtern. Sie können außerdem Arbeitsanmerkungen zu einem Protokollereignis hinzufügen und exportieren.

ANMERKUNG: Lifecycle-Protokolle für Änderungen am Persönlichkeitsmodus werden nur während des Warmstarts des Hosts generiert.

Wenn Sie Konfigurationsaufträge mittels RACADM-CLI oder iDRAC-Webschnittstelle initiieren, enthält das Lifecycle-Protokoll Informationen über den Benutzer, verwendete Schnittstelle und die IP-Adresse des Systems, von dem aus Sie den Job initiieren.

Zugehöriger Link

Filtern der Lifecycle-Protokolle
Exportieren von Lifecycle Controller-Protokollen mithilfe der Webschnittstelle
Anmerkungen zu Lifecycle-Protokollen hinzufügen

Lifecycle-Protokoll über die Web-Schnittstelle anzeigen

Klicken Sie zum Anzeigen der Lifecycle-Protokolle auf **Übersicht** > **Server** > **Protokolle** > **Lifecycle-Protokoll**. Daraufhin wird die Seite **Lifecycle-Protokoll** angezeigt. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Filtern der Lifecycle-Protokolle

Sie können Protokolle auf der Basis der Kategorie, des Schweregrads, des Schlüsselworts oder des Datumsbereichs filtern.
So filtern Sie die Lifecycle-Protokolle:

1 Führen Sie auf der Seite **Lifecycle-Protokoll** im Abschnitt **Protokollfilter** einen oder alle der folgenden Schritte aus:
   - Wählen Sie den **Protokolltyp** aus dem Dropdown-Menü.
   - Wählen Sie den Schweregrad aus der Drop-Down-Liste **Schweregrad** aus.
   - Geben Sie ein Schlüsselwort ein.
   - Legen Sie den Datumsbereich fest.
2 Klicken Sie auf **Anwenden**.
   Die gefilterten Protokolleinträge werden daraufhin unter **Protokollergebnisse** angezeigt.

Anmerkungen zu Lifecycle-Protokollen hinzufügen

So fügen Sie Anmerkungen zu den Lifecycle-Protokollen hinzu:

1 Klicken Sie auf der Seite **Lifecycle-Protokoll** auf das Plus-Symbol (+) für den gewünschten Protokolleintrag.
   Daraufhin werden die Nachrichten-ID-Details angezeigt.
2 Geben Sie die gewünschten Anmerkungen für den Protokolleintrag in das Feld **Anmerkung** ein.
   Die Anmerkungen werden daraufhin im Feld **Anmerkung** angezeigt.

Lifecycle-Protokoll über RACADM anzeigen

Verwenden Sie zum Anzeigen von Lifecycle-Protokollen den Befehl `lclog`.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Exportieren der Lifecycle Controller-Protokolle

Sie können das gesamte Lifecycle Controller-Protokoll (aktive und archivierte Einträge) in einer einzigen Zip-XML-Datei auf eine Netzwerkfreigabe oder auf das lokale System exportieren. Die Erweiterung der komprimierten XML-Datei lautet **.xml.gz**. Die Dateieinträge sind auf Grundlage ihrer Sequenznummern von der niedrigsten bis zur höchsten Sequenznummer sortiert.

Exportieren von Lifecycle Controller-Protokollen mithilfe der Webschnittstelle

So exportieren Sie Lifecycle Controller-Protokolle mithilfe der Webschnittstelle:

1 Klicken Sie auf der Seite **Lifecycle-Protokoll** auf **Exportieren**.

2 Wählen Sie aus den folgenden Optionen aus:

- **Netzwerk** – Exportiert die Lifecycle-Controller-Protokolle an einen freigegebenen Speicherort im Netzwerk.
- **Lokal** – Exportiert die Lifecycle-Controller-Protokolle an einen Speicherort auf dem lokalen System.

ANMERKUNG: Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen.

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

3 Klicken Sie auf **Exportieren**, um das Protokoll an den gewünschten Speicherort zu exportieren.

ANMERKUNG: iDRAC kann nicht auf eine CIFS-Freigabe zugreifen, wenn alle folgenden Bedingungen zutreffen:

- Die Windows CIFS-Freigabe befindet sich in einer Domäne.
- Das SMB2-Protokoll ist aktiviert und die LAN-Manager-Authentifizierung ist auf „Nur NTLMv2-Antworten senden. *LM NTLM verweigern* eingestellt“.

Exportieren von Lifecycle Controller-Protokollen mit RACADM

Verwenden Sie zum Exportieren von Lifecycle-Controller-Protokollen den Befehl `lclog export`.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* unter **dell.com/support/manuals**.

Arbeitsanmerkungen hinzufügen

Jeder Benutzer, der sich bei iDRAC anmeldet, kann Arbeitsanmerkungen hinzufügen. Diese werden im Lifecycle-Protokoll als ein Ereignis gespeichert. Sie müssen über iDRAC-Protokollberechtigungen verfügen, um Arbeitsanmerkungen hinzufügen zu können. Pro neuer Arbeitsanmerkung sind bis zu 255 Zeichen zulässig.

ANMERKUNG: Sie können keine Arbeitsanmerkungen löschen.

So fügen Sie eine Arbeitsanmerkung hinzu:

1 Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **Server** > **Eigenschaften** > **Zusammenfassung**.
Die Seite **Systemzusammenfassung** wird angezeigt.

2 Geben Sie unter **Arbeitsanmerkungen** den gewünschten Test in das leere Textfeld ein.

ANMERKUNG: Es wird empfohlen, nicht zu viele Sonderzeichen zu verwenden.

3 Klicken Sie auf **Hinzufügen**.
Die Arbeitsanmerkung wird zum Protokoll hinzugefügt. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Remote-Systemprotokollierung konfigurieren

Sie können Lifecycle-Protokolle an ein Remote-System senden. Vor diesem Schritt müssen Sie Folgendes sicherstellen:

- iDRAC und das Remote-System sind über eine Netzwerkkonnektivität verbunden.
- Das Remote-System und iDRAC befinden sich auf dem gleichen Netzwerk.

Remote-System-Protokollierung über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Remote-Syslog-Server-Einstellungen:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Protokolle** > **Einstellungen**.
Die Seite **Remote-Syslog-Einstellungen** wird angezeigt.

2 Aktivieren Sie die Remote-Syslog, und geben Sie die Server-Adresse und die Schnittstellennummer an. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

3 Klicken Sie auf **Anwenden**.
Die Einstellungen werden gespeichert. Alle in das Lifecycle-Protokoll geschriebenen Protokolle werden gleichzeitig auf die konfigurierten Remote-Server geschrieben.

Remote-Systemanmeldung über RACADM konfigurieren

Um die Remote-System-Protokollierungseinstellungen zu konfigurieren, verwenden Sie den Befehl **set** mit den Objekten in der Gruppe **iDRAC.SysLog**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

11

Stromversorgung überwachen und verwalten

Sie können iDRAC zum Überwachen und Verwalten der Stromversorgungsanforderungen auf dem Managed System verwenden. Diese Funktion unterstützt Sie dabei, das System vor Stromausfällen zu schützen, da der Stromzufluss auf dem System entsprechend verteilt und der Stromverbrauch reguliert wird.

Zentrale Funktionen:

- **Stromverbrauchsüberwachung** – Zeigen Sie den Stromverbrauchsstatus, den Verlauf der Strommessungen, die aktuellen Durchschnittswerte, die Höchstwerte, usw. für das Managed System an.
- **Strombegrenzung** – Zeigen Sie die Strombegrenzung für das Managed System an und legen Sie sie fest, einschließlich der Anzeige des geringsten und maximalen potenziellen Stromverbrauchs. Dies ist eine Lizenzfunktion.
- **Stromsteuerung** – Über diese Funktion können Sie Stromsteuerungsvorgänge (z. B. Einschalten, Ausschalten, Systemrücksetzung, Aus- und einschalten und ordnungsgemäßes Herunterfahren) auf dem Managed System ausführen.
- **Netzteiloptionen** – Konfigurieren Sie die Netzteiloptionen, z. B. die Redundanzrichtlinie, das Austauschen von Laufwerken im laufenden Betrieb und die Korrektur des Leistungsfaktors.

Themen:

Zugehöriger Link

Stromversorgung überwachen
Stromsteuerungsvorgänge ausführen
Strombegrenzung
Netzteiloptionen konfigurieren
Netzschalter aktivieren oder deaktivieren
Festlegen des Warnungsschwellenwerts für den Stromverbrauch

Stromversorgung überwachen

iDRAC führt eine Dauerüberwachung des Stromverbrauchs im System durch und zeigt die folgenden Stromwerte an:

- Stromverbrauchswarnung und kritische Schwellenwerte.
- Kumulativer Stromverbrauch, Stromverbrauchshöchstwert und Ampere-Höchstwert.
- Stromverbrauch in der letzten Stunden, am vorherigen Tag oder in der abgelaufenen Woche.
- Durchschnittliche, Mindest- und Höchstleistungsaufnahme
- Verlaufshöchstwerte und Zeitstempel für Höchstwerte.
- Höchst-Aussteuerungsreserve und ummittelbare Aussteuerungsreserve-Werte (für Rack- und Tower-Server).

ANMERKUNG: Das Histogramm für den Leistungsaufnahmentrend des Systems (stündlich, täglich, wöchentlich) wird nur so lange beibehalten, wie iDRAC ausgeführt wird. Falls iDRAC neu gestartet wird, gehen die vorhandenen Daten zum Stromverbrauch verloren, und das Histogramm wird neu gestartet.

Stromversorgung über die Web-Schnittstelle überwachen

Um die Stromüberwachungsinformationen anzuzeigen, gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Strom/Thermisch** > **Stromüberwachung**. Daraufhin wird die Seite **Stromüberwachung** angezeigt. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Stromversorgung über RACADM überwachen

Um die Stromüberwachungsinformationen anzuzeigen, verwenden Sie den Befehl **get** mit den Objekten in der Gruppe **System.Power**. Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Festlegen des Warnungsschwellenwerts für den Stromverbrauch

Sie können den Warnungsschwellenwert für den Stromverbrauchssensor in Rack- und Tower-Systemen festlegen. Der Schwellenwert für Warnungen/kritischen Stromverbrauch für Rack- und Tower-Systeme kann sich ändern, nachdem das System aus- und wieder eingeschaltet wurde, und zwar auf Basis der PSU-Kapazität und der Redundanzrichtlinie. Der Warnungsschwellenwert darf jedoch den Schwellenwert für kritischen Stromverbrauch nicht übersteigen, auch wenn die Kapazität der PSU für die Redundanzrichtlinie geändert wird.

Der strombezogene Warnungsschwellenwert für Blade-Systeme ist auf „CMC-Stromzuweisung“ gesetzt.

Wenn ein Vorgang zum Zurücksetzen auf die Standardmaßnahme durchgeführt wird, werden die Stromversorgungsschwellenwerte auf den Standard festgelegt.

Sie müssen über Benutzerberechtigungen zum Konfigurieren verfügen, um den Warnungsschwellenwert für den Stromverbrauchssensor festzulegen.

ANMERKUNG: Der Warnungsschwellenwert wird nach Durchführung einer Aktualisierung von racreset oder iDRAC auf den Standardwert zurückgesetzt.

Einrichten der Warnschwelle für den Stromverbrauch über die Webschnittstelle

1. Gehen Sie in der iDRAC-Webschnittstelle auf **Übersicht** > **Server** > **Leistung/Thermisch** > **Stromüberwachung**.
   Die Seite **Stromüberwachung** wird angezeigt.
2. Geben Sie im Abschnitt **Aktueller Strommesswert und Schwellenwerte** in der Spalte **Warnungsschwellenwert** den Wert in **Watt** oder **BTU/h** ein.
   Die Werte müssen niedriger sein als die Werte für den **Fehlerschwellenwert**. Die Werte werden auf den nächsten Wert abgerundet, der durch 14 teilbar ist. Wenn Sie **Watt** eingeben, berechnet das System automatisch den Wert für **BTU/h**. Wenn Sie in ähnlicher Weise den BTU/h-Wert eingeben, wird der Wert für **Watt** angezeigt.
3. Klicken Sie auf **Anwenden**. Die Werte werden daraufhin konfiguriert.

Stromsteuerungsvorgänge ausführen

iDRAC ermöglicht, im Remote-Zugriff die Maßnahmen Einschalten, Ausschalten, Reset, ordentliches Herunterfahren, nicht maskierbarer Interrupt (NMI) oder Aus- und Einschalten mithilfe der Webschnittstelle oder RACADM auszuführen.

Sie können diese Vorgänge auch mithilfe der Remote-Dienste des Lifecycle-Controllers oder der WS-Verwaltung durchführen. Weitere Informationen finden Sie im *Lifecycle Controller Remote Services Quick Start Guide (Lifecycle-Controller Remote-Dienste – Schnellstarthandbuch)* unter **dell.com/idracmanuals** und im Profildokument *Dell Power State Management (Dell Verwaltung des Energiezustands)* unter **delltechcenter.com**.

Server-Stromsteuervorgänge, die vom iDRAC initiiert werden, sind unabhängig vom Verhalten des Betriebsschalters, das im BIOS konfiguriert ist. Sie können die Funktion „PushPowerButton“ zum ordnungsgemäßen Herunterfahren oder Einschalten des Systems auch dann verwenden, wenn das BIOS so konfiguriert ist, dass keine Aktion ausgeführt werden soll, wenn der physische Betriebsschalter gedrückt wird.

Stromsteuerungsvorgänge über die Web-Schnittstelle ausführen

So führen Sie Stromsteuerungsvorgänge aus:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Leistung/Thermisch** > **Stromkonfiguration** > **Stromsteuerung**. Daraufhin wird die Seite **Stromsteuerung** angezeigt.
2. Wählen Sie die erforderliche Stromsteuerungsmaßnahme aus:
   - System einschalten
   - System ausschalten
   - NMI (Non-Masking Interrupt, nicht-maskierbare Unterbrechung)
   - Ordentliches Herunterfahren
   - System zurücksetzen (Softwareneustart)
   - System aus- und wieder einschalten (Hardwareneustart)
3. Klicken Sie auf **Anwenden**. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Stromsteuerungsvorgänge über RACADM ausführen

Verwenden Sie zum Ausführen von Strommaßnahmen den Befehl **serveraction**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Strombegrenzung

Sie können die Stromverbrauchs-Schwellenwerte anzeigen, die den Bereich des Gleich- und Drehstrom-Stromverbrauchs abdecken, den ein System unter schwerer Belastung gegenüber dem Rechenzentrum meldet. Hierbei handelt es sich um eine Lizenzfunktion.

Strombegrenzung bei Blade-Servern

Bevor ein Blade-Server eines PowerEdge M1000e oder PowerEdge VRTX-Gehäuses hochfährt, versorgt iDRAC den CMC mit dessen Stromanforderungen. Sie liegen höher als der eigentliche Strom, den der Blade-Server verbrauchen kann und werden auf der Basis von eingeschränkten Hardware-Bestandsinformationen berechnet. Es kann ein kleinerer Strombereich angefordert werden, nachdem der Server

basierend auf der vom Server tatsächlich verbrauchten Energie hochgefahren wird. Wenn der Stromverbrauch mit der Zeit zunimmt und der Server Strom im Bereich der maximal ihm zugewiesenen Strommenge verbraucht, kann iDRAC eine Erhöhung der maximalen potenziellen Stromverbrauchs anfordern und erhöht auf diese Weise den Power-Envelope. iDRAC erhöht lediglich seine Anforderung in Bezug auf den maximalen potenziellen Stromverbrauch für den CMC. Es wird keine geringere potenzielle Mindestenergie angefordert, wenn der Verbrauch sinkt. iDRAC fordert mehr Strom an, wenn der Stromverbrauch über den vom CMC zugewiesenen Stromwert hinausgeht.

Nach dem Einschalten und Initialisieren des Systems berechnet iDRAC eine neue Stromanforderung, die auf der tatsächlichen Blade-Konfiguration basiert. Das Blade wird auch dann mit Strom versorgt, wenn der CMC keine neue Stromanforderung erfüllen kann.

CMC fordert sämtliche ungenutzte Energie von Servern niedrigerer Priorität zurück und ordnet die zurückgeforderte Energie einem Infrastrukturmodul höherer Priorität oder einem Server zu.

Wenn nicht genügend Energie zugewiesen ist, startet der Blade-Server nicht. Wenn dem Blade ausreichend Energie zugewiesen wurde, schaltet das iDRAC die Systemversorgung ein.

Strombegrenzungsrichtlinie anzeigen und konfigurieren

Wenn die Strombegrenzungsrichtlinie aktiviert ist, werden benutzerdefinierte Strombegrenzungen für das System durchgesetzt. Falls nicht, wird die Hardware-Stromschutzrichtlinie verwendet, die standardmäßig implementiert ist. Diese Stromschutzrichtlinie ist unabhängig von der benutzerdefinierten Richtlinie. Die Systemleistung wird dynamisch angepasst, um die Leistungsaufnahme nahe am festgelegten Schwellenwert zu halten.

Der tatsächliche Stromverbrauch kann bei niedriger Auslastung geringer sein und den Schwellenwert für einen Augenblick überschreiten, bis Leistungsanpassungen abgeschlossen sind. Beispiel: Eine gegebene Systemkonfiguration sieht 700 W für den höchsten potenziellen Stromverbrauch und 500 W für den geringsten potenziellen Stromverbrauch vor. Sie können einen Strombudgetschwellenwert festlegen und aktivieren, um den Verbrauch von derzeit 650 W auf 525 W zu senken. Ab diesem Punkt wird die Leistung des Systems dynamisch angepasst, um den Stromverbrauch unter dem benutzerspezifizierten Schwellenwert von 525 W zu halten.

Wenn der Wert für die Strombegrenzung auf einen Wert unterhalb des empfohlenen Schwellenwerts gesetzt ist, ist iDRAC möglicherweise nicht in der Lage, die angeforderte Strombegrenzung aufrecht zu erhalten.

Sie können den Wert in Watt, BTU/h oder als Prozentsatz (%) der empfohlenen maximalen Strombegrenzung angeben.

Bei einer Stromobergrenze in BTU/h wird bei der Umrechnung in Watt auf die nächste Ganzzahl aufgerundet. Bei der Rückumwandlung der Stromobergrenze von Watt in BTU/h erfolgt die Aufrundung in gleicher Weise. Folglich kann sich der geschriebene Wert nominal vom angezeigten Wert unterscheiden. Beispiel: Ein auf 600 BTU/h eingestellter Schwellenwert wird als 601 BTU/h angezeigt.

Strombegrenzungsrichtlinie über die Web-Schnittstelle konfigurieren

So zeigen Sie die Stromrichtlinien an:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Leistung/Thermisch** > **Stromkonfiguration** > **Stromkonfiguration**. Daraufhin wird die Seite **Stromkonfiguration** angezeigt.

   Die Seite **Stromkonfiguration** wird angezeigt. Die aktuelle Strombegrenzungsrichtlinie wird im Abschnitt **Aktive Strombegrenzungsrichtlinie** angezeigt.

2 Wählen Sie die Option **Aktivieren** unter **iDRAC-Strombegrenzungsrichtlinie** aus.

3 Geben Sie im Abschnitt **Benutzerdefinierte Begrenzungen** die maximale Stromgrenze in Watt und BTU/h oder den maximalen Prozentsatz der empfohlenen Systembegrenzung an.

4 Klicken Sie auf **Anwenden**, um die Werte zu übernehmen.

Strombegrenzungsrichtlinie über RACADM konfigurieren

Um die Werte für die aktuelle Strombegrenzung anzuzeigen und zu konfigurieren, verwenden Sie die folgenden Objekte mit dem Befehl `set`:

- System.Power.Cap.Enable
- System.Power.Cap.Watts
- System.Power.Cap.Btuhr
- System.Power.Cap.Percent

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Strombegrenzungsrichtlinie über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

So zeigen Sie die Stromrichtlinien an und konfigurieren sie:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Stromkonfiguration**.

> **ANMERKUNG: Der Link Stromkonfiguration ist nur verfügbar, wenn die Netzteileinheit des Servers die Stromüberwachung unterstützt.**

Daraufhin wird die Seite **iDRAC-Einstellungen – Stromkonfiguration** angezeigt.

2 Wählen Sie **Aktiviert** aus, um die **Stromobergrenzenrichtlinie** zu aktivieren. Wählen Sie ansonsten **Deaktiviert** aus.

3 Verwenden Sie die empfohlenen Einstellungen, oder geben Sie unter **Benutzerdefinierte Richtlinie für Stromobergrenze** die gewünschten Grenzwerte ein.

Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

4 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Damit sind die Strombegrenzungswerte konfiguriert.

Netzteiloptionen konfigurieren

Sie können die Netzteiloptionen konfigurieren, so z. B. die Redundanzrichtlinie, das Austauschen von Laufwerken im laufenden Betrieb und die Korrektur des Leistungsfaktors.

Das Hotspare ist eine Netzteilfunktion, über die die redundanten Netzteilgeräte (PSUs) je nach Server-Belastung ausgeschaltet werden können. Auf diese Weise können die übrigen PSUs mit einer höheren Auslastung und Effizienz laufen. Die PSUs müssen diese Funktion jedoch unterstützen, damit gewährleistet ist, dass sie bei Bedarf schnell eingeschaltet werden können.

In einem System mit zwei Netzteilen kann entweder PSU 1 oder PSU 2 als primäres Netzteil konfiguriert werden. In einem System mit vier Netzteilen muss ein Netzteilpaar (1+1 oder 2+2) als primäres Netzteil festgelegt werden.

Nachdem Hot Spare aktiviert wurde, werden die Netzteileinheiten aktiv oder gehen je nach Auslastung in den Energiesparmodus über. Wenn Hot Spare aktiviert ist, wird die asymmetrische elektrische Leistungsfreigabe zwischen zwei Netzteilen aktiviert ist. Dabei ist ein Netzteil *aktiv* und erbringt den Großteil der Leistung, während sich das andere Netzteil im Ruhemodus befindet und eine geringe Leistungsmenge erbringt. Dies wird oft als 1+0 mit zwei Netzteilen und aktiviertem Hot Spare bezeichnet. Wenn sich alle PSU-1 in Stromkreis A und alle PSU-2 in Stromkreis B befinden, so ist bei aktiviertem Hot Spare (werkseitige Standardeinstellung) Stromkreis C weniger stark ausgelastet und löst die Warnmeldungen aus. Ist Hot Spare deaktiviert, so wird die Last gleichmäßig im Verhältnis 50:50 zwischen den beiden Netzteilen aufgeteilt, und die Stromkreise A und B weisen in der Regel die gleiche Last auf.

Der Leistungsfaktor ist das Verhältnis aus verbrauchter Wirkleistung und der Scheinleistung. Wenn die Korrektur des Leistungsfaktors aktiviert ist, verbraucht der Server eine geringe Menge Strom, wenn der Host ausgeschalten ist. Per Standardeinstellung ab Werk ist die Korrektur des Leistungsfaktors bereits aktiviert.

Netzteiloptionen über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Netzteiloptionen:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Leistung/Thermisch** > **Stromversorgungskonfiguration** > **Stromversorgungskonfiguration**. Daraufhin wird die Seite **Stromversorgungskonfiguration** angezeigt.

2 Wählen Sie unter **Netzteiloptionen** die erforderlichen Optionen aus. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

3 Klicken Sie auf **Anwenden**. Die Netzteiloptionen sind damit konfiguriert.

Netzteiloptionen über RACADM konfigurieren

Verwenden Sie zum Konfigurieren der Netzteiloptionen die folgenden Objekte mit dem Befehl `set`:

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Netzteiloptionen über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

So konfigurieren Sie die Netzteiloptionen:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Stromkonfiguration**.

> **ANMERKUNG: Der Link Stromkonfiguration ist nur verfügbar, wenn die Netzteileinheit des Servers die Stromüberwachung unterstützt.**

Daraufhin wird die Seite **iDRAC-Einstellungen – Stromkonfiguration** angezeigt.

2 Führen Sie unter **Netzteiloptionen** die folgenden Schritte aus:
- Aktivieren oder deaktivieren Sie die Netzteilredundanz.
- Aktivieren oder deaktivieren Sie das Hotspare.
- Legen Sie das primäre Netzteilgerät fest.
- Aktivieren oder deaktivieren Sie die Leistungsfaktorkorrektur. Weitere Informationen zu diesen Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Netzteiloptionen sind damit konfiguriert.

Netzschalter aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie den Netzschalter auf dem Managed System:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Frontblendensicherheit**.

Die Seite **iDRAC-Einstellungen Frontblendensicherheit** wird angezeigt.

2 Wählen Sie **Aktiviert** zum Aktivieren des Betriebsschalters oder **Deaktiviert**, um ihn zu deaktivieren.

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Einstellungen werden gespeichert.

12

Durchführen einer Bestandsaufnahme, Überwachung und Konfiguration von Netzwerkgeräten

Sie können den Bestand für die folgenden Netzwerkgeräte erfassen und diese überwachen und konfigurieren:

- Netzwerkadapter (NICs)
- Konvergente Netzwerkadapter (CNAs)
- LAN auf Hauptplatinen (LOMs)
- Netzwerktochterkarten (NDCs)
- Mezzanine-Karten (nur für Blade-Server)

Bevor Sie NPAR oder eine einzelne Partition auf CNA-Geräten deaktivieren, stellen Sie sicher, dass Sie alle E/A-Identitätsattribute (Beispiele: IP-Adresse, virtuelle Adressen, Initiatoren und Speicherziele) und Attribute auf Partitionsebene (Beispiel: Bandbreitenzuweisung) löschen. Sie können eine Partition entweder durch Änderung der Attributeinstellung „VirtualizationMode“ zu „NPAR“ oder durch Deaktivierung aller Merkmale auf einer Partition deaktivieren.

Je nach Typ des installierten CNA-Geräts können die Einstellungen der Partitionsattribute eventuell nicht vom letzten Zeitpunkt übernommen werden, an dem die Partition aktiv war. Legen Sie alle E/A-Identitätsattribute und partitionsbezogenen Attribute beim Aktivieren einer Partition fest. Sie können eine Partition entweder durch Änderung der Attributeinstellung „VirtualizationMode“ zu „NPAR“ oder durch Aktivierung eines Merkmals (Beispiel: NicMode) auf der Partition aktivieren.

Themen:

Zugehöriger Link

Bestandsaufnahme und Überwachung von FC-HBA-Geräten
Dynamische Konfiguration von virtuellen Adressen, Initiator- und Speicherziel-Einstellungen

Bestandsaufnahme für Netzwerkgeräte erstellen und Netzwerkgeräte überwachen

Sie können den Zustand remote überwachen und die Bestandsaufnahme für die Netzwerkgeräte im Managed System anzuzeigen:

Für jedes Gerät können Sie folgende Informationen zu den Schnittstellen und aktivierten Partitionen abrufen:

- Link-Status
- Eigenschaften
- Einstellungen und Funktionen
- Empfangs- und Übertragungsstatistiken

- iSCSI-, FCoE-Initiator- und Zielinformationen

Zugehöriger Link

Durchführen einer Bestandsaufnahme, Überwachung und Konfiguration von Netzwerkgeräten

Dynamische Konfiguration von virtuellen Adressen, Initiator- und Speicherziel-Einstellungen

Netzwerkgeräte über die Web-Schnittstelle überwachen

Um die Netzwerkgeräteinformationen über die Webschnittstelle anzuzeigen, gehen Sie zu **Übersicht** > **Hardware** > **Netzwerkgeräte**. Daraufhin wird die Seite **Netzwerkgeräte** angezeigt. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

ANMERKUNG: Wenn der BS-Treiberzustand den Status als „Betriebsbereit“ darstellt, werden der Betriebssystem-Treiberstatus oder der UEFI-Treiberstatus angezeigt.

Netzwerkgeräte über RACADM überwachen

Um Informationen über Netzwerkgeräte anzuzeigen, verwenden Sie die Befehle **hwinventory** und **nicstatistics**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Zusätzliche Eigenschaften werden möglicherweise angezeigt, wenn Sie RACADM oder WS-MAN neben den auf der iDRAC-Web-Schnittstelle angezeigten Eigenschaften verwenden.

Bestandsaufnahme und Überwachung von FC-HBA-Geräten

Sie können den Funktionszustand und die Bestandsaufnahme der Fibre Channel Host Bus Adapter- (FC HBA) Geräte im Managed System anzeigen. Die FC HBAs von Emulex und QLogic werden unterstützt. Für jedes FC-HBA-Gerät können Sie die folgenden Informationen zu den Ports anzeigen lassen:

- Linkstatus und Information
- Schnittstellen-Eigenschaften
- Empfangs- und Übertragungsstatistiken

Zugehöriger Link

Durchführen einer Bestandsaufnahme, Überwachung und Konfiguration von Netzwerkgeräten

FC-HBA-Geräte mit der Webschnittstelle überwachen

Um die FC-HBA-Geräteinformationen mit der Webschnittstelle überwachen zu können, wechseln Sie zu **Übersicht** > **Hardware** > **Fibre Channel**. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC Online-Hilfe*.

Im Seitennamen werden auch die Steckplatznummer, die angibt, wo das FC-HBA-Gerät verfügbar ist, und der Typ des FC-HBA-Geräts angezeigt.

Überwachung von FC-HBA-Geräten unter Verwendung von RACADM

Um die FC-HBA-Geräteinformationen unter Verwendung von RACADM anzuzeigen, verwenden Sie den Befehl **hwinventory**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Dynamische Konfiguration von virtuellen Adressen, Initiator- und Speicherziel-Einstellungen

Sie können die virtuelle Adresse, die Initiator- und Speicherzieleinstellungen dynamisch anzeigen und konfigurieren und eine Beständigkeitsrichtlinie anwenden. Die Anwendung kann damit die Einstellungen auf Basis von Betriebszustandsänderungen (Neustart des Betriebssystems, Warm-Reset, Kalt-Reset oder Aus- und Einschalten) und auf Basis der Beständigkeitsrichtlinieneinstellung für diesen Betriebszustand anwenden. Dies bietet mehr Flexibilität bei Bereitstellungen, die eine schnelle Neukonfiguration der Systemrechenlasten auf einem anderen System erfordern.

Die virtuellen Adressen sind:

- Virtuelle MAC-Adresse
- Virtuelle iSCSI MAC-Adresse
- Virtuelle FIP-MAC-Adresse
- Virtuelle WWN
- Virtuelle WWPN

ANMERKUNG: Wenn Sie die Richtlinie für die Persistenz löschen, werden alle virtuellen Adressen auf die werkseitig eingestellte permanente Adresse zurückgesetzt.

ANMERKUNG: Bei einigen Karten mit virtuellen FIP-, virtuellen WWN- und virtuellen WWPN-MAC-Attributen werden die virtuellen WWN- und virtuellen WWPN-MAC-Attribute beim Konfigurieren der virtuellen FIP automatisch konfiguriert.

Durch die Verwendung der E/A-Identitätsfunktion können Sie:

- die virtuellen Adressen für Netzwerk- und Fibre Channel-Geräte (zum Beispiel NIC, CNA, FC HBA) anzeigen und konfigurieren.
- den Initiator (für iSCSI und FCoE) und die Speicher-Zieleinstellungen (für iSCSI, FCoE und FC) konfigurieren.
- die Beständigkeit oder das Löschen der konfigurierten Werte zu einem Stromausfall oder zu warmen oder kalten Systemrücksetzungen festlegen.

Die Werte für die virtuellen Adressen sowie die Initiator- und Speicherziele ändern sich möglicherweise je nach der Art und Weise, wie die Hauptstromversorgung beim System-Reset durchgeführt wird und ob das NIC-, CNA- oder FC-HBA-Gerät über die Notstromversorgung mit Strom versorgt wird. Die Beständigkeit von E/A-Identitätseinstellungen kann auf Basis der Richtlinieneinstellung erreicht werden, die Sie unter Verwendung des iDRAC vorgenommen haben.

Nur wenn die E/A-Identitätsfunktion aktiviert ist, werden die Beständigkeitsrichtlinien wirksam. Jedes Mal, wenn das System zurückgesetzt oder eingeschaltet wird, werden die Werte auf Grundlage der Einstellungen für die Richtlinie gelöscht oder beibehalten.

ANMERKUNG: Nachdem die Werte gelöscht wurden, können sie erst wieder angewendet werden, nachdem der Konfigurationsjob ausgeführt wurde.

Zugehöriger Link

Durchführen einer Bestandsaufnahme, Überwachung und Konfiguration von Netzwerkgeräten
Unterstützte Karten für die E/A-Identitätsoptimierung
Unterstützte NIC-Firmware-Versionen für die E/A-Identitätsoptimierung
Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung
Konfigurieren der Einstellungen für die Beständigkeitsrichtlinie

Unterstützte Karten für die E/A-Identitätsoptimierung

Die folgende Tabelle zeigt die Karten, die die E/A-Identitätsoptimierungsfunktion unterstützen.

Tabelle 31. Unterstützte Karten für die E/A-Identitätsoptimierung

Hersteller	Typ
Broadcom	• 5720 PCIe 1 GB • 5719 PCIe 1 GB • 57810 PCIe 10 GB • 57810 bNDC 10 GB • 57800 rNDC 10 GB + 1 GB • 57840 rNDC 10 GB • 57840 bNDC 10 GB • 5720 rNDC 1 GB • 5719 Mezz 1 GB • 57810 Mezz 10 GB • 5720 bNDC 1 GB
Intel	• i350 Mezz 1 GB • x520+i350 rNDC 10 GB + 1 GB • I350 bNDC 1 GB • x540 PCIe 10 GB • x520 PCIe 10 GB • i350 PCIe 1 GB • x540+i350 rNDC 10 GB + 1 GB • i350 rNDC 1 GB • x520 bNDC 10 GB • 40G 2P XL710 QSFP+ rNDC
Mellanox	• ConnectX-3 10G • ConnectX-3 40G • ConnectX-3 10G • ConnectX-3 Pro 10G • ConnectX-3 Pro 40G • ConnectX-3 Pro 10G
QLogic	• QME2662 Mezz FC16 • QLE2660 PCIe FC16 • QLE2662 PCIe FC16
Emulex	• LPM16002 Mezz FC16 • LPe16000 PCIe FC16 • LPe16002 PCIe FC16 • LPM16002 Mezz FC16 • LPM15002 • LPe15000 • LPe15002 • OCm14104B-UX-D • OCm14102B-U4-D • OCm14102B-U5-D • OCe14102B-UX-D • OCm14104B-UX-D • OCm14102B-U4-D

Hersteller	Typ
	• OCm14102B-U5-D • OCe14102B-UX-D • OCm14104-UX-T rNDC 10 GB • OCm14102-U2-D bNDC 10 GB • OCm14102-U3-D Mezz 10 GB • OCe14102-UX-D PCIe 10 GB

Unterstützte NIC-Firmware-Versionen für die E/A-Identitätsoptimierung

In der 13. Generation der Dell PowerEdge-Server ist die erforderliche NIC-Firmware standardmäßig verfügbar.

Die folgende Tabelle zeigt die NIC-Firmware-Versionen, die die E/A-Identitätsoptimierungsfunktion unterstützen.

Virtuelle oder Flex-Adresse und Beständigkeitsrichtlinien-Verhalten, wenn iDRAC auf FlexAddress-Modus oder Konsolenmodus eingestellt ist

Die folgende Tabelle beschreibt die Konfiguration der virtuellen Adressverwaltung (VAM) und das Beständigkeitsrichtlinien-Verhalten in Abhängigkeit vom Status der Flex Address-Funktion im CMC, dem in iDRAC eingestellten Modus, des E/A-Identitätsfunktionsstatus in iDRAC und der XML-Konfiguration.

Tabelle 32. Virtuelle/Flex-Adresse und Verhalten der Beständigkeitsregel

FlexAddress-Funktionsstatus im CMC	In iDRAC festgelegter Modus	Funktionsstatus der E/A-Identität in iDRAC	XML-Konfiguration	Beständigkeitsrichtlinie	Beständigkeitsrichtlinie löschen – Virtuelle Adresse
FlexAddress aktiviert	FlexAddress-Modus	Enabled (Aktiviert)	Virtuelle Adressverwaltung (VAM) ist konfiguriert.	Konfigurierte VAM besteht weiterhin	Auf Flex-Adresse eingestellt
FlexAddress aktiviert	FlexAddress-Modus	Enabled (Aktiviert)	VAM nicht konfiguriert	Auf Flex-Adresse eingestellt	Keine Beständigkeit – Hat Flex-Adresse
FlexAddress aktiviert	FlexAdress-Modus	Disabled (Deaktiviert)	Mit dem in Lifecycle Controller angegebenen Pfad konfiguriert	Einstellung auf Flex-Adresse für diesen Zyklus	Keine Beständigkeit – Hat Flex-Adresse
FlexAddress aktiviert	FlexAdress-Modus	Disabled (Deaktiviert)	VAM nicht konfiguriert	Auf Flex-Adresse eingestellt	Auf Flex-Adresse eingestellt
Flex-Adresse deaktiviert	FlexAdress-Modus	Enabled (Aktiviert)	VAM konfiguriert	Konfigurierte VAM besteht weiterhin	Nur Beständigkeit – Löschen ist nicht möglich.
Flex-Adresse deaktiviert	FlexAdress-Modus	Enabled (Aktiviert)	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Beständigkeit wird nicht unterstützt.

FlexAddress-Funktionsstatus im CMC	In iDRAC festgelegter Modus	Funktionsstatus der E/A-Identität in iDRAC	XML-Konfiguration	Beständigkeitsrichtlinie	Beständigkeitsrichtlinie löschen – Virtuelle Adresse
					Abhängig von Kartenfunktionsweise
Flex-Adresse deaktiviert	FlexAdress-Modus	Disabled (Deaktiviert)	Mit dem in Lifecycle Controller angegebenen Pfad konfiguriert	Lifecycle Controller-Konfiguration besteht für diesen Zyklus weiterhin	Beständigkeit wird nicht unterstützt. Abhängig von Kartenfunktionsweise
Flex-Adresse deaktiviert	FlexAdress-Modus	Disabled (Deaktiviert)	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Auf Hardware-MAC-Adresse eingestellt
FlexAddress aktiviert	Konsolenmodus	Enabled (Aktiviert)	VAM konfiguriert	Konfigurierte VAM besteht weiterhin	Beständigkeit und Löschen muss funktionieren
FlexAddress aktiviert	Konsolenmodus	Enabled (Aktiviert)	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Auf Hardware-MAC-Adresse eingestellt
FlexAddress aktiviert	Konsolenmodus	Disabled (Deaktiviert)	Mit dem in Lifecycle Controller angegebenen Pfad konfiguriert	Lifecycle Controller-Konfiguration besteht für diesen Zyklus weiterhin	Beständigkeit wird nicht unterstützt. Abhängig von Kartenfunktionsweise
Flex-Adresse deaktiviert	Konsolenmodus	Enabled (Aktiviert)	VAM konfiguriert	Konfigurierte VAM besteht weiterhin	Beständigkeit und Löschen muss funktionieren
Flex-Adresse deaktiviert	Konsolenmodus	Enabled (Aktiviert)	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Auf Hardware-MAC-Adresse eingestellt
Flex-Adresse deaktiviert	Konsolenmodus	Disabled (Deaktiviert)	Mit dem in Lifecycle Controller angegebenen Pfad konfiguriert	Lifecycle Controller-Konfiguration besteht für diesen Zyklus weiterhin	Beständigkeit wird nicht unterstützt. Abhängig von Kartenfunktionsweise
FlexAddress aktiviert	Konsolenmodus	Disabled (Deaktiviert)	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Auf Hardware-MAC-Adresse eingestellt

Systemverhalten für FlexAddress und E/A-Identität

Tabelle 33. Systemverhalten für FlexAddress und E/A-Identität

	FlexAddress-Funktionsstatus im CMC	Funktionsstatus der E/A-Identität in iDRAC	Verfügbarkeit von Remote-Agent-VA für den Neustart-Zyklus	VA-Programmierungsquelle	Neustartzyklus-VA-Persistenzverhalten
Server mit FA-äquivalenter Persistenz	Aktiviert	Deaktiviert		FlexAddress von CMC	Gemäß FlexAddress-Spezifikation
	-, Aktiviert oder Deaktiviert	Aktiviert	Ja – Neu oder Beständig	Virtuelle Adresse des Remote-Agenten	Gemäß FlexAddress-Spezifikation
			Nein	Virtuelle Adresse gelöscht	
	Deaktiviert	Deaktiviert			

	FlexAddress-Funktionsstatus im CMC	Funktionsstatus der E/A-Identität in iDRAC	Verfügbarkeit von Remote-Agent-VA für den Neustart-Zyklus	VA-Programmierungsquelle	Neustartzyklus-VA-Persistenzverhalten
Server mit Richtlinienfunktion für VAM-Persistenz	Aktiviert	Deaktiviert		FlexAddress von CMC	Gemäß FlexAddress-Spezifikation
	Aktiviert	Aktiviert	Ja – Neu oder Beständig	Virtuelle Adresse des Remote-Agenten	Gemäß Remote-Agenten-Richtlinieneinstellung
			Nein	FlexAddress von CMC	Gemäß FlexAddress-Spezifikation
	Deaktiviert	Aktiviert	Ja – Neu oder Beständig	Virtuelle Adresse des Remote-Agenten	Gemäß Remote-Agenten-Richtlinieneinstellung
			Nein	Virtuelle Adresse gelöscht	
	Deaktiviert	Deaktiviert			

Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung

Normalerweise werden die Geräte nach dem Systemstart konfiguriert und nach einem Neustart initialisiert. Sie können die Funktion zur E/A-Identitätsoptimierung für einen optimierten Start aktivieren. Wenn sie aktiviert ist, werden zwischen dem Zurücksetzen und dem Initialisieren des Geräts die virtuelle Adresse, der Initiator und die Speicherzielattribute eingestellt. Auf diese Weise wird ein zweiter BIOS-Neustart umgangen. Die Gerätekonfiguration und der Startvorgang finden im Rahmen eines einzigen Systemstarts statt, wodurch die Startzeitleistung optimiert wird.

Stellen Sie vor dem Aktivieren der E/A-Identitätsoptimierung Folgendes sicher:

- Sie verfügen über Anmelde-, Konfigurations- und Systemsteuerungsberechtigungen.
- BIOS, iDRAC und Netzwerkkarten werden auf die neueste Firmware aktualisiert. Weitere Informationen zu den unterstützten Versionen finden Sie unter Unterstützte Karten für die E/A-Identitätsoptimierung und unter Unterstützte NIC-Firmwareversion für die E/A-Identitätsoptimierung.

Nach dem Aktivieren der E/A-Identitätsoptimierungsfunktion exportieren Sie die XML-Konfigurationsatei von iDRAC, ändern Sie die erforderlichen E/A-Identitätsattribute in der XML-Konfigurationsdatei, und importieren Sie die Datei zurück nach iDRAC.

Eine Liste der E/A-Identitätttsptimierungsattribute, die Sie in der XML-Datei ändern können, finden Sie im Dokument *NIC Profile* (NIC-Profile) unter **delltechcenter.com/idrac**.

ANMERKUNG: Ändern Sie keine Attribute außerhalb der E/A-Identitätsoptimierung.

Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung mithilfe der Webschnittstelle

So aktivieren oder deaktivieren Sie die E/A-Identitätsoptimierung:

1 Gehen Sie in der iDRAC-Webschnittstelle auf **Übersicht** > **Hardware** > **Netzwerkgeräte**.
Die Seite **Netzwerkgeräte** wird angezeigt.

2 Klicken Sie auf die Registerkarte **I/O Identity Optimization (Optimierung der E/A-Identität)** und wählen Sie die Option **I/O Identity Optimization (Optimierung der E/A-Identität)** aus, um diese Funktion zu aktivieren. Löschen Sie diese Option zum Deaktivieren.

3 Klicken Sie auf **Anwenden,** um die Einstellung zu übernehmen.

Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung mithilfe von RACADM

Verwenden Sie zum Aktivieren der E/A-Identitätsoptimierung den folgenden Befehl:

```
racadm set idrac.ioidopt.IOIDOptEnable Enabled
```

Nach Aktivierung dieser Funktion müssen Sie das System neu starten, damit die Einstellungen wirksam werden.

Verwenden Sie zum Deaktivieren der E/A-Identitätsoptimierung den folgenden Befehl:

```
racadm set idrac.ioidopt.IOIDOptEnable Disabled
```

Verwenden Sie zum Anzeigen der Einstellungen für die E/A-Identitätsoptimierung den folgenden Befehl:

```
racadm get iDRAC.IOIDOpt
```

Konfigurieren der Einstellungen für die Beständigkeitsrichtlinie

Mit der E/A-Identität können Sie Richtlinien zum Festlegen der Verhaltensweisen bei der Systemzurücksetzung und beim Aus- und Einschalten des Systems konfigurieren, die die Beständigkeit oder das Löschen der Einstellungen für virtuelle Adresse, Initiator und Speicherziel bestimmen. Jedes einzelne Beständigkeitsrichtlinienattribut gilt für alle Anschlüsse und Partitionen aller entsprechenden Geräte im System. Das Geräteverhalten von mit Hilfsstrom betriebenen Geräten unterscheidet sich von demjenigen von Geräten ohne Hilfsstromversorgung.

ANMERKUNG: Die Funktion Persistence Policy (Beständigkeitsrichtlinie) funktioniert bei Standardeinstellung eventuell nicht, wenn das Attribut VirtualAddressManagement in iDRAC auf den Modus FlexAddress eingestellt ist und die FlexAddress-Funktion in CMC deaktiviert ist. Stellen Sie sicher, dass Sie das Attribut VirtualAddressManagement in iDRAC auf den Modus Console (Konsole)einstellen oder die FlexAddress-Funktion in CMC aktivieren.

Sie können die folgenden Beständigkeitsrichtlinien konfigurieren:

- Virtuelle Adresse: Auxiliär-betriebene Geräte
- Virtuelle Adresse: Nicht-auxiliär-betriebene Geräte
- Initiator
- Speicherziel

Stellen Sie vor dem Anwenden der Beständigkeitsrichtlinie sicher, dass:

- Sie mindestens einmal eine Bestandsaufnahme der Netzwerk-Hardware erstellen, also die Option für die System-Bestandsaufnahme beim Neustart (CSIOR) aktiviert ist.
- Sie die E/A-Identitätsoptimierung aktivieren.

Ereignisse im Lifecycle Controller-Protokoll protokolliert werden, wenn Folgendes zutrifft:

- Die E/A-Identitätsoptimierung ist aktiviert oder deaktiviert.
- Die Beständigkeitsrichtlinie wurde geändert.
- Virtuelle Adresse, Initiator- und Ziel-Werte werden basierend auf der Richtlinie eingestellt. Ein einzelner Protokolleintrag wird für die konfigurierten Geräte und die Werte protokolliert, die für diese Geräte eingestellt werden, wenn die Richtlinie angewendet wird.

Ereignismaßnahmen werden für SNMP-, E-Mail- oder WS-Ereignisbenachrichtigungen aktiviert. Protokolle sind ebenfalls in den Remote-Syslogs enthalten.

Tabelle 34. Standardwerte für die Beständigkeitsrichtlinie

Beständigkeitsrichtlinie	Stromausfall	Hardwarestart	Softwareneustart
Virtuelle Adresse: Auxiliär-betriebene Geräte	Nicht ausgewählt	Ausgewählt	Ausgewählt
Virtuelle Adresse: Nicht-auxiliär-betriebene Geräte	Nicht ausgewählt	Nicht ausgewählt	Ausgewählt
Initiator	Ausgewählt	Ausgewählt	Ausgewählt
Speicherziel	Ausgewählt	Ausgewählt	Ausgewählt

ANMERKUNG: Wenn eine persistente Richtlinie deaktiviert ist und Sie die Maßnahme zum Löschen der virtuellen Adresse durchführen, kann die virtuelle Adresse durch erneutes Aktivieren der persistenten Richtlinie nicht abgerufen werden. Sie müssen die virtuelle Adresse nach Aktivierung der persistenten Richtlinie erneut einrichten.

ANMERKUNG: Wenn eine Beständigkeitsrichtlinie aktiv ist und die virtuellen Adressen, Initiator- oder Speicherziele auf einer CNA-Gerätepartition eingerichtet sind, setzen Sie die für die virtuellen Adressen, Initiator- und Speicherziele konfigurierten Werte nicht zurück und löschen Sie sie nicht, bevor Sie den „VirtualizationMode“ oder die Merkmale der Partition geändert haben. Die Aktion erfolgt automatisch beim Deaktivieren der Beständigkeitsrichtlinie. Sie können auch eine Konfigurationsaufgabe verwenden, um die Attribute der virtuellen Adresse explizit auf 0s und die Werte der Initiator- und Speicherziele wie in Standardwerte für iSCSI-Initiator und Speicherziel definiert einzustellen.

Zugehöriger Link

Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung

Konfigurieren der Richtlinieneinstellungen für die Persistenz über die iDRAC-Webschnittstelle

So konfigurieren Sie die Richtlinie für die Persistenz:

1. Gehen Sie in der iDRAC-Webschnittstelle auf **Übersicht** > **Hardware** > **Netzwerkgeräte**.
   Die Seite **Netzwerkgeräte** wird angezeigt.
2. Klicken Sie auf die Registerkarte **E/A-Identitätsoptimierung**.
3. Wählen Sie im Abschnitt **Richtlinie für die Persistenz** eine oder mehrere der folgenden Elemente für jede Persistenz-Richtlinie aus:
   - **Wechselstromverlust** – Die virtuelle Adresse oder die Zieleinstellungen bleiben erhalten, wenn ein Stromausfall eintritt.
   - **Hardwareneustart** – Die virtuelle Adresse oder die Zieleinstellungen bleiben erhalten, wenn ein Hardwareneustart erforderlich ist.
   - **Softwareneustart** – Die virtuelle Adresse oder die Zieleinstellungen bleiben erhalten, wenn ein Softwareneustart erforderlich ist.
4. Klicken Sie auf **Anwenden**.
   Die Persistenz-Richtlinien werden konfiguriert.

Konfigurieren der Persistenz-Richtlinieneinstellungen über RACADM

Um eine Richtlinie für die Persistenz festzulegen, verwenden Sie das folgende racadm-Objekt mit dem Unterbefehl **set**:

- Verwenden Sie für virtuelle Festplatten die Objekte **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyAuxPwrd** und **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyNonAuxPwrd**.
- Verwenden Sie für Initiatoren das Objekt **iDRAC.IOIDOPT.InitiatorPersistencePolicy**.
- Verwenden Sie für Speicherziele das Objekt **iDRAC.IOIDOpt.StorageTargetPersistencePolicy**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Standardwerte für iSCSI-Initiator und Speicherziel

Die folgenden Tabellen enthalten die Liste der Standardwerte für die iSCSI-Initiator- und Speicherziele, wenn die Persistenzrichtlinien gelöscht werden.

Tabelle 35. iSCSI-Initiator – Standardwerte

iSCSI-Initiator	Standardeinstellungen im IPv4-Modus	Standardeinstellungen im IPv6-Modus
IscsiInitiatorIpAddr	0.0.0.0	::
IscsiInitiatorIpv4Addr	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Addr	::	::
IscsiInitiatorSubnet	0.0.0.0	0.0.0.0
IscsiInitiatorSubnetPrefix	0	0
IscsiInitiatorGateway	0.0.0.0	::
IscsiInitiatorIpv4Gateway	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Gateway	::	::
IscsiInitiatorPrimDns	0.0.0.0	::
IscsiInitiatorIpv4PrimDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6PrimDns	::	::
IscsiInitiatorSecDns	0.0.0.0	::
IscsiInitiatorIpv4SecDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6SecDns	::	::
iscsiInitiatorName	Wert wurde gelöscht	Wert wurde gelöscht
IscsiInitiatorChapId	Wert wurde gelöscht	Wert wurde gelöscht
IscsiInitiatorChapPwd	Wert wurde gelöscht	Wert wurde gelöscht
IPVer	Ipv4	

Tabelle 36. Attribut für iSCSI-Speicherziel – Standardwerte

Attribute für iSCSI-Speicherziel	Standardeinstellungen im IPv4-Modus	Standardeinstellungen im IPv6-Modus
ConnectFirstTgt	Deaktiviert	Deaktiviert
FirstTgtIpAddress	0.0.0.0	::
FirstTgtTcpPort	3260	3260

Attribute für iSCSI-Speicherziel	Standardeinstellungen im IPv4-Modus	Standardeinstellungen im IPv6-Modus
FirstTgtBootLun	0	0
FirstTgtIscsiName	Wert wurde gelöscht	Wert wurde gelöscht
FirstTgtChapId	Wert wurde gelöscht	Wert wurde gelöscht
FirstTgtChapPwd	Wert wurde gelöscht	Wert wurde gelöscht
FirstTgtIpVer	Ipv4	
ConnectSecondTgt	Deaktiviert	Deaktiviert
SecondTgtIpAddress	0.0.0.0	::
SecondTgtTcpPort	3260	3260
SecondTgtBootLun	0	0
SecondTgtIscsiName	Wert wurde gelöscht	Wert wurde gelöscht
SecondTgtChapId	Wert wurde gelöscht	Wert wurde gelöscht
SecondTgtChapPwd	Wert wurde gelöscht	Wert wurde gelöscht
SecondTgtIpVer	Ipv4	

13

Verwalten von Speichergeräten

Beginnend mit iDRAC-Version 2.00.00.00 wird die agentenlose iDRAC-Verwaltung um die Funktionen zur direkten Konfiguration der neuen PERC9-Controller erweitert. Sie können damit die an Ihr System angeschlossenen Speicherkomponenten während der Ausführung remote konfigurieren. Zu diesen Komponenten gehören RAID- und Nicht-RAID-Controller und die angeschlossenen Kanäle, Ports, Gehäuse und Festplatten.

Die vollständige Speichersubsystemerkennung, -topologie, -systemüberwachung und -konfiguration erfolgen über das Comprehensive Embedded Management (CEM)-Framework durch die Verknüpfung mit den internen und externen PERC-Controllern über das MCTP-Protokoll über die I2C-Schnittstelle. Für eine Echtzeitkonfiguration unterstützt das CEM PERC9-Controller. Die Firmware-Version für PERC9-Controller muss 9.1 oder höher sein.

Unter Verwendung von iDRAC können Sie die meisten der in OpenManage Storage Management verfügbaren Funktionen ausführen, einschließlich der Echtzeitkonfigurationsbefehle (ohne Neustart) (beispielsweise die Befehle zum Erstellen virtueller Festplatten). Sie können RAID vollständig konfigurieren, bevor Sie das Betriebssystem installieren.

Sie können die Controller-Funktionen ohne Zugriff auf das BIOS konfigurieren und verwalten. Diese Funktionen umfassen das Konfigurieren von virtuellen Festplatten und das Anwenden von RAID-Leveln und Ersatzgeräten für den Schutz von Daten. Sie können zahlreiche weitere Controller-Funktionen initiieren, wie z. B. Neuerstellung und Fehlerbehebung. Sie können Ihre Daten schützen, indem Sie Datenredundanz konfigurieren oder Ersatzgeräte zuweisen.

Zu den Speichergeräten gehören:

- Controller: Die meisten Betriebssysteme lesen und schreiben Daten nicht direkt über die Festplatten, sondern senden stattdessen Lese- und Schreibanweisungen an einen Controller. Der Controller ist die Hardware in Ihrem System, die direkt mit den Festplatten kommuniziert, um Daten zu lesen und zu schreiben. Ein Controller besitzt Konnektoren (Kanäle oder Ports), die mit einer oder mehreren Festplatten oder mit einem Gehäuse verbunden sind, das physische Festplatten enthält. RAID-Controller können sich über die Grenzen von Festplatten hinaus erstrecken, sodass mithilfe der Kapazität von mehr als einer Festplatte erweiterter Speicherplatz – oder eine virtuelle Festplatte – erstellt werden kann. Controller führen auch andere Aufgaben durch, wie z. B. das Starten von Neuerstellungen, Initialisieren von Festplatten usw. Um diese Aufgaben durchzuführen, erfordert der Controller spezielle Software wie Firmware und Treiber. Um ordnungsgemäß zu funktionieren, muss die erforderliche Mindestversion von Firmware und Treiber auf dem Controller installiert sein. Unterschiedliche Controller besitzen verschiedene Eigenschaften im Hinblick auf das Lesen und Schreiben von Daten und Ausführen von Aufgaben. Wenn Sie diese Merkmale richtig verstehen, können Sie den Speicher am effizientesten verwalten.
- Physische Festplatten oder physische Geräte befinden sich in einem Gehäuse oder sind mit dem Controller verbunden. Bei einem RAID-Controller werden die physischen Festplatten oder Geräte für die Erstellung von virtuellen Festplatten verwendet.
- Bei virtuellen Festplatten handelt es sich um Speicher, der unter Verwendung einer oder mehrerer Festplatten von einem RAID-Controller erstellt wird. Obwohl eine virtuelle Festplatte aus mehreren physischen Festplatten erstellt werden kann, wird sie vom Betriebssystem als eine einzelne Festplatte betrachtet. Je nach verwendetem RAID-Level kann die virtuelle Festplatte für den Fall eines Festplattenausfalls eventuell redundante Daten beibehalten oder bestimmte Leistungsattribute besitzen. Virtuelle Festplatten können nur auf einem RAID-Controller erstellt werden.
- Gehäuse – Es wird extern mit dem System verbunden, während die Rückwandplatine und deren physische Festplatten integriert sind.
- Die Rückwandplatine ähnelt einem Gehäuse. Bei einer Rückwandplatine sind der Controller-Konnektor und die physischen Festplatten mit dem Gehäuse verbunden, sie verfügt jedoch nicht über die Verwaltungsfunktionen (Temperatursonden, Alarme usw.) eines externen Gehäuses. Physische Festplatten können sich in einem Gehäuse befinden oder an die Rückwandplatine eines Systems angeschlossen sein.

Es können nicht nur die im Gehäuse enthaltenen physischen Festplatten verwaltet werden, sondern auch der Status der Lüfter, Netzteile und Temperatursonden des Gehäuses überwacht werden. Gehäuse sind Hot-Plug-fähig. Hot-Plugging ist das Hinzufügen einer Komponente zu einem System, während das Betriebssystem ausgeführt wird.

Die physischen Geräte, die am Controller angeschlossen sind, müssen über die neueste Firmware verfügen. Die neueste unterstützte Firmware erhalten Sie von Ihrem Dienstanbieter.

Speicherereignisse vom PERC werden den entsprechenden SNMP-Traps und WSMAN-Ereignissen zugeordnet. Alle Änderungen an den Speicherkonfigurationen werden im Lifecycle-Protokoll protokolliert.

Tabelle 37. PERC-Fähigkeit

PERC-Fähigkeit	CEM-konfigurationsfähiger Controller (PERC 9.1 oder höher)	Nicht-CEM-konfigurationsfähiger Controller (PERC 9.0 und darunter)
Echtzeit	Wenn keine vorhandenen ausstehenden oder geplanten Jobs für den Controller vorhanden sein, wird die Konfiguration angewendet. Bei ausstehenden oder geplanten Aufgaben für diesen Controller müssen die Aufgaben gelöscht werden, oder Sie müssen warten, bis die Aufgaben abgeschlossen sind, bevor Sie die Konfiguration während der Ausführung anwenden. „Während der Ausführung“ bedeutet, dass kein Neustart erforderlich ist.	Die Konfiguration wird angewendet. Es wird eine Fehlermeldung angezeigt. Die Aufgabenerstellung schlägt fehl und Sie können keine Echtzeitaufgaben unter Verwendung der Webschnittstelle erstellen.
Bereitgestellt	Wenn alle Vorgänge den Status „Bereitgestellt“ haben, wird die Konfiguration bereitgestellt und nach dem Neustart oder in Echtzeit angewendet.	Die Konfiguration wird nach dem Neustart angewendet.

Themen:

Zugehöriger Link

Zum Verständnis von RAID-Konzepten
Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen
Anzeigen der Speichergerätetopologie
Verwalten von Controllern
Verwalten von physischen Festplatten
Verwalten von Gehäusen oder Rückwandplatinen
Verwalten von PCIe-SSDs
Verwalten von virtuellen Festplatten
Blinken oder Beenden des Blinkens der Komponenten-LEDs
Unterstützte Controller
Unterstützte Gehäuse
Übersicht über die unterstützten Funktionen für Speichergeräte

Zum Verständnis von RAID-Konzepten

Storage Management verwendet RAID-Technologie (Redundantes Array unabhängiger Festplatten), um Speicherverwaltungsfunktionalität bereitzustellen. Kenntnisse von Storage Management setzen ein Verständnis von RAID-Konzepten voraus, sowie eine gewisse Vertrautheit mit der Art und Weise, wie die RAID-Controller Ihres Systems und das Betriebssystem mit Festplattenspeicherplatz umgehen.

RAID

RAID ist eine Technologie zum Verwalten der Datenspeicherung auf physischen Festplatten, die sich im System befinden oder damit verbunden sind. Ein Hauptaspekt von RAID ist die Fähigkeit, mehrere physische Festplatten einzubeziehen, sodass die kombinierte Speicherkapazität mehrerer physischer Festplatten als ein einziger, erweiterter Festplattenspeicherplatz betrachtet werden kann. Ein anderer wichtiger Punkt bei RAID ist die Möglichkeit, redundante Daten zu erhalten, die dazu verwendet werden können, Daten im Falle eines Festplattenausfalls wiederherzustellen. RAID verwendet verschiedene Methoden, um Daten zu speichern und zu rekonstruieren, wie z. B. Striping, Datenspiegelung und Parität. Es gibt verschiedene RAID-Level, die verschiedene Methoden zur Speicherung und zum Rekonstruieren von Daten verwenden. Die RAID-Level besitzen verschiedene Eigenschaften in Bezug auf Lese/Schreib-Leistung, Datensicherung und Speicherkapazität. Da nicht alle RAID-Level redundante Daten erhalten, können einige RAID-Level verlorene Daten nicht wiederherstellen. Das von Ihnen ausgewählte RAID-Level hängt davon ab, ob Ihre Priorität bei Leistung, Sicherung oder Speicherkapazität liegt.

ANMERKUNG: Die zur Implementierung von RAID verwendeten Angaben werden vom RAID Advisory Board (RAB) definiert. Obwohl das RAB die RAID-Level definiert, kann die kommerzielle Implementierung von RAID-Leveln von unterschiedlichen Herstellern von den tatsächlichen RAID-Spezifikationen abweichen. Die von einem bestimmten Hersteller verwendete Implementierung kann eventuell die Lese- bzw. Schreibleistung und den Grad der Datenredundanz beeinflussen.

Hardware- und Software-RAID

RAID kann entweder mit Hardware oder Software implementiert werden. Ein System, das Hardware-RAID verwendet, besitzt einen RAID-Controller, der die RAID-Stufen implementiert und Lese- bzw. Schreibvorgänge von Daten von/auf physische(n) Festplatten verarbeitet. Wenn über das Betriebssystem zur Verfügung gestellte Software-RAID verwendet wird, setzt das Betriebssystem die RAID-Stufen um. Aus diesem Grund kann die ausschließliche Verwendung von Software-RAID die Systemleistung herabsetzen. Es kann jedoch Software-RAID zusätzlich zu Hardware-RAID-Datenträgern verwendet werden, um eine bessere Leistung und Vielseitigkeit der RAID-Datenträger-Konfiguration bereit zu stellen. Zum Beispiel kann ein Paar von Hardware-RAID-5-Datenträgern über zwei RAID-Controller gespiegelt werden, um RAID-Controller-Redundanz bereitzustellen.

RAID-Konzepte

RAID verwendet bestimmte Methoden, um Daten auf Festplatten zu schreiben. Mit diesen Methoden kann RAID eine Datenredundanz oder verbesserte Leistung bereit stellen. Diese Methoden umfassen:

- Datenspiegelung – Duplizieren von Daten von einer physischen Festplatte auf eine andere physische Festplatte. Datenspiegelung bietet Datenredundanz, indem zwei Kopien derselben Daten auf verschiedenen physischen Festplatten aufrechterhalten werden. Wenn einer der Datenspiegelungsfestplatten ausfällt, kann das System weiterhin mit der unbeeinflussten Festplatte betrieben werden. Beide Seiten des Spiegels enthalten zu jeder Zeit die gleichen Daten. Beide Seiten des Spiegels können als die betriebsbereite Seite fungieren. Die Lesevorgänge einer gespiegelten RAID-Festplattengruppe sind leistungsmäßig mit einer RAID 5-Festplattengruppe vergleichbar, jedoch sind die Schreibvorgänge schneller.
- Striping – Mit Festplatten-Striping werden Daten über alle physischen Festplatten in einer virtuellen Festplatte geschrieben. Jedes Stripe besteht aus aufeinander folgenden Datenadressen der virtuellen Festplatte, die in Einheiten fester Größe jeder physischen Festplatte in einem sequentiellen Muster zugeordnet werden. Zum Beispiel: Wenn die virtuelle Festplatte fünf physische Festplatten enthält, schreibt das Stripe Daten zu den physischen Festplatten eins bis fünf, ohne eine der physischen Festplatte zu wiederholen. Die Größe des von einem Stripe beanspruchten Speicherplatzes ist auf jeder physischen Festplatte gleich. Der Teil eines Stripes, der sich auf einer physischen Festplatte befindet, ist ein Stripe-Element. Das Striping an sich bietet keine Datenredundanz. Striping zusammen mit Parität bietet Datenredundanz.
- Stripe Grösse – Der gesamte Festplattenspeicherplatz, der von einem Stripe belegt wird, ohne eine Paritätsfestplatte einzuschließen. Beispiel: Ein Stripe hat 64 KB Festplattenspeicherplatz und 16 KB Daten auf jeder Festplatte im Stripe. In diesem Fall ist die Stripe-Größe 64 KB und die Stripe-Elementgröße ist 16 KB.
- Stripe-Element – Ein Stripe-Element ist ein Teil eines Stripes, welcher sich auf einer einzigen physischen Festplatte befindet.
- Stripe-Elementgröße – Die Menge des Festplattenspeicherplatzes, die von einem Stripe-Element benutzt wird. Beispiel: Ein Stripe hat 64 KB Festplattenspeicherplatz und 16 KB Daten auf jeder Festplatte im Stripe. In diesem Fall ist die Stripe-Elementgröße 16 KB und die Stripe-Größe ist 64 KB.
- Parität – Parität bezieht sich auf redundante Daten, die unter Verwendung eines Algorithmus in Verbindung mit Striping erhalten werden. Wenn einer der gestripten Festplatten ausfällt, können die Daten von den Paritätsinformationen mit dem Algorithmus rekonstruiert werden.
- Bereich – Ein Bereich ist eine RAID-Technik, mit der Speicherplatz von Gruppen physischer Festplatten in einer virtuellen RAID 10, 50, oder 60 Festplatte kombiniert wird.

RAID-Level

Jede RAID-Stufe verwendet eine Kombination von Datenspiegelung, Striping und Parität, um Datenredundanz oder eine verbesserte Lese- und Schreibleistung bereitzustellen. Details zu den einzelnen RAID-Stufen finden Sie unter RAID-Stufen auswählen.

Datenspeicher-Organisation zur erhöhten Verfügbarkeit und Leistung

RAID stellt verschiedene Methoden oder RAID-Stufen zur Organisation des Festplattenspeichers bereit. Einige RAID-Stufen erhalten redundante Daten, so dass Daten nach einem Festplattenversagen wiederhergestellt werden können. Verschiedene RAID-Stufen verbessern oder vermindern eventuell die E/A-Leistung (Lesen und Schreiben) des Systems.

Die Aufrechterhaltung redundanter Daten erfordert die Verwendung zusätzlicher physischer Festplatten. Die Einschließung von zusätzlichen Festplatten erhöht die Wahrscheinlichkeit eines Festplattenversagens. Durch die Unterschiede in E/A-Leistung und Redundanz ist eine RAID-Stufe eventuell geeigneter als eine andere, je nach den Anwendungen in der Betriebsumgebung und den gespeicherten Datentypen.

Wenn eine RAID-Stufe ausgewählt wird, treffen die folgenden Leistungs- und Kostenerwägungen zu:

- Verfügbarkeit oder Fehlertoleranz – Verfügbarkeit oder Fehlertoleranz bezieht sich auf die Fähigkeit eines Systems, Vorgänge zu erhalten und Zugriff auf Daten anzugeben, selbst wenn eine seiner Komponente fehlerhaft ist. Auf RAID-Datenträgern wird Verfügbarkeit oder Fehlertoleranz durch die Erhaltung von redundanten Daten bereitgestellt. Redundante Daten umfassen Spiegel (vervielfältigte Daten) und Paritätsinformationen (Daten werden mit einem Algorithmus rekonstruiert).

- Leistung – Lese- und Schreibleistung kann erhöht oder verringert werden, abhänging von der von Ihnen ausgewählten RAID-Stufe. Einige RAID-Stufen eignen sich eventuell besser für bestimmte Anwendungen.
- Kosteneffizienz – Das Erhalten der redundanten Daten oder Paritätsinformationen, die dem RAID-Volumen zugeordnet sind, erfordert zusätzlichen Festplattenspeicherplatz. Wenn die Daten temporär, leicht reproduzierbar oder nicht unbedingt notwendig sind, können die erhöhten Kosten der Datenredundanz eventuell nicht gerechtfertigt werden.
- Zwischenzeitlicher Fehler (MTBF) – Das zusätzliche Verwenden von Festplatten, um Datenredundanz zu erhalten, erhöht außerdem die Möglichkeit, dass jederzeit ein Festplattenfehler eintreten kann. Obwohl dies in Fällen, in denen redundante Daten erforderlich sind, nicht verhindert werden kann, hat es Auswirkungen auf das Arbeitspensum des System-Support-Personals Ihres Unternehmens.
- Volume – Volume bezieht sich auf eine einzige, nicht-RAID virtuelle Festplatte. Sie können Volumen unter Verwendung von Dienstprogrammen wie O-ROM erstellen <Ctrl> <r>. Storage Management unterstützt die Erstellung von Datenträgern nicht. Sie können jedoch Datenträger anzeigen und Laufwerke dieser Datenträger verwenden, um neue virtuelle Festplatten zu erstellen oder Online-Kapazitätserweiterung (Online Capacity Expansion OCE) vorhandener virtueller Festplatten, vorausgesetzt, es ist genügend freier Speicherplatz vorhanden.

Auswählen der RAID-Stufen

RAID kann zur Steuerung des Datenspeichers auf mehreren Festplatten verwendet werden. Jede RAID-Stufe oder -Verkettung besitzt unterschiedliche Leistungs- und Datenschutz-Eigenschaften.

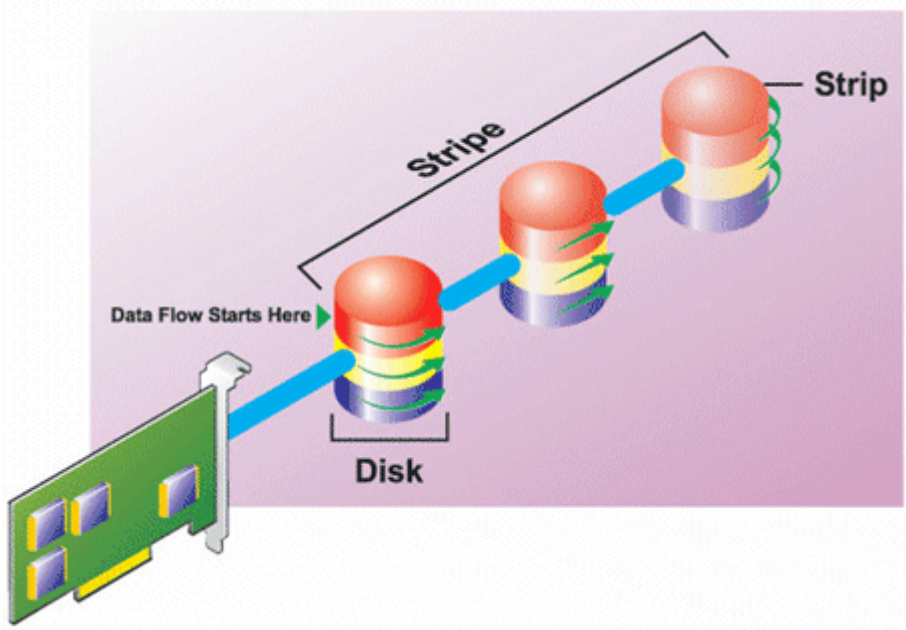
ANMERKUNG: Die H3xx-PERC-Controller bieten keine Unterstützung für die RAID-Stufen 6 und 60.

Die folgenden Themen enthalten spezifische Informationen zur Art und Weise wie jede RAID-Stufe Daten speichert, sowie als auch deren spezifische Leistungs- und Schutzeigenschaften:

- RAID-Stufe 0 (Striping)
- RAID-Stufe 1 (Datenspiegelung)
- RAID-Stufe 5 (Striping mit verteilter Parität)
- RAID-Stufe 6 (Striping mit zusätzlicher verteilter Parität)
- RAID-Stufe 50 (Striping über RAID 5-Sets)
- RAID-Stufe 60 (Striping über RAID 6-Sets)
- RAID-Stufe 10 (Striping über gespiegelte Sets)

RAID-Level 0 – Striping

RAID 0 verwendet Daten-Striping, wobei Daten in gleich großen Segmenten auf alle physischen Festplatten geschrieben werden. RAID 0 bietet keine Datenredundanz.

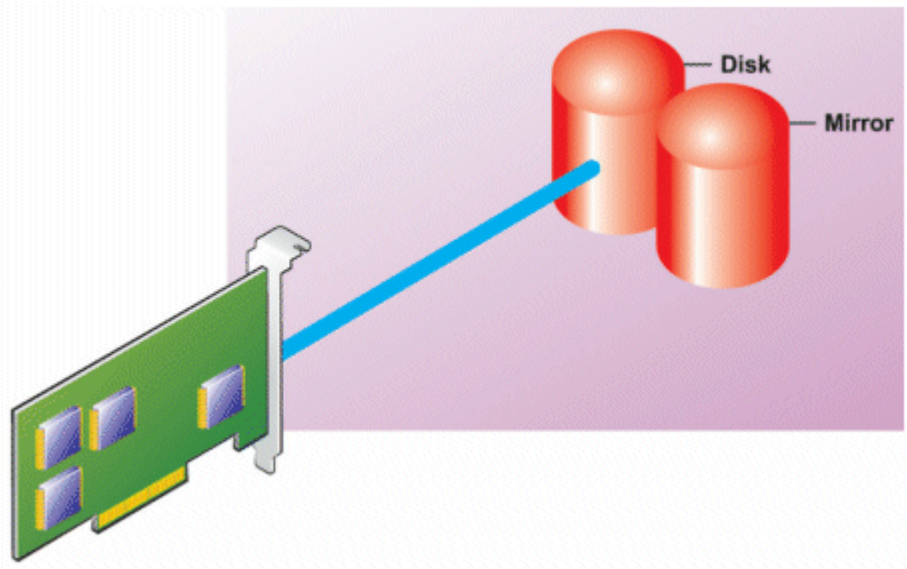


RAID 0-Eigenschaften:

- Gruppiert *n* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von (kleinste Festplattengröße) **n* Festplatten.
- Daten werden auf den Festplatten abwechselnd gespeichert.
- Es werden keine redundanten Daten gespeichert. Wenn eine Festplatte fehlerhaft wird, fällt die große virtuelle Festplatte aus – ohne eine Möglichkeit zur Neuerstellung der Daten
- Bessere Lese- und Schreibleistung.

RAID-Level 1 – Datenspiegelung

RAID 1 stellt die einfachste Art und Weise dar, redundante Daten zu erhalten. Mit RAID 1 werden Daten auf eine oder mehrere physische Festplatten gespiegelt oder dupliziert. Wenn eine physische Festplatte ausfällt, können die Daten unter Verwendung der Daten der anderen Seite der Spiegelung neu erstellt werden.

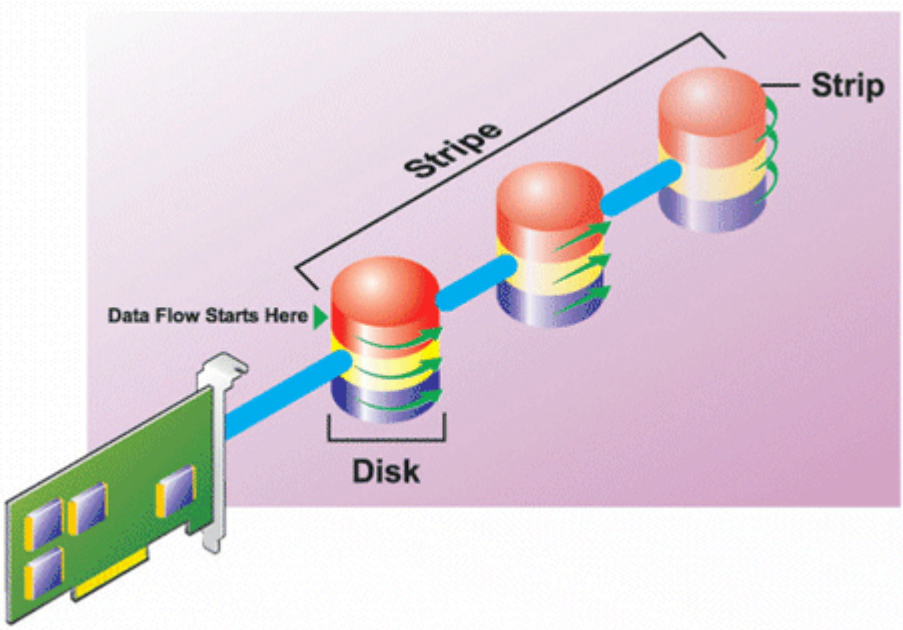


RAID 1-Eigenschaften:

- Gruppiert *n* + *n* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von *n* Festplatten. Controller, die derzeit von der Speicherverwaltung unterstützt werden, erlauben die Auswahl von zwei Festplatten während der Erstellung einer RAID 1-Konfiguration. Da diese Festplatten gespiegelt werden, ist die Gesamtspeicherkapazität gleich der einer Festplatte.
- Die Daten werden auf den beiden Festplatten repliziert.
- Wenn eine Festplatte ausfällt, kann die virtuelle Festplatte weiterhin betrieben werden. Die Daten werden von der Spiegelung der ausgefallenen Festplatte gelesen.
- Bessere Leseleistung, aber etwas langsamere Schreibleistung.
- Redundanz zum Schutz der Daten.
- RAID 1 ist in Bezug auf Festplattenspeicherplatz teurer, da die doppelte Anzahl von Festplatten verwendet wird, die zum Speichern der Daten ohne Redundanz erforderlich wären.

RAID-Level 5 – Striping mit verteilter Parität

RAID 5 bietet Datenredundanz, indem Daten-Striping zusammen mit Paritätsinformationen verwendet wird. Anstatt eine physische Festplatte für Parität zu bestimmen, werden die Paritätsinformationen über alle physischen Festplatten in der Festplattengruppe gestriped.

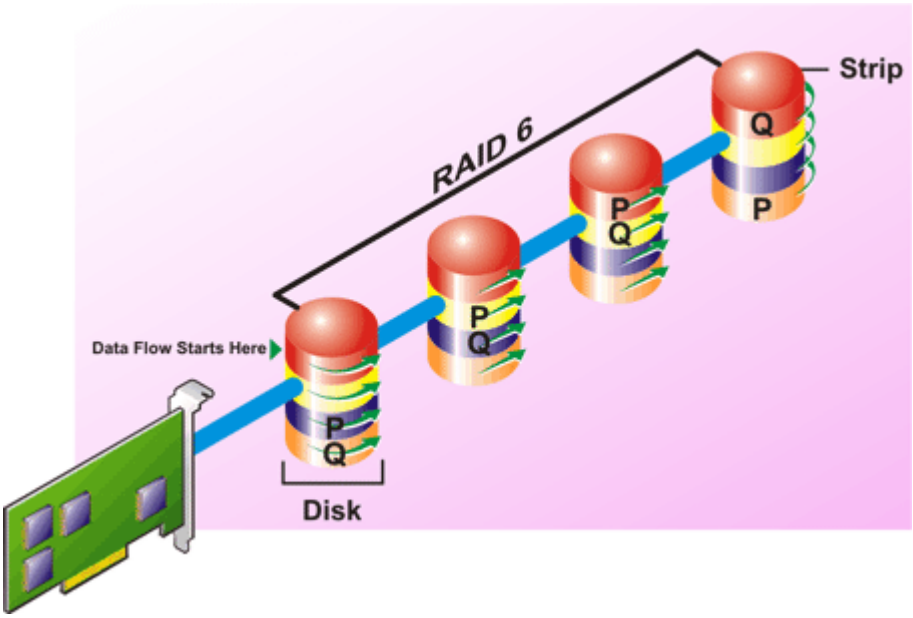


RAID 5-Eigenschaften:

- Gruppiert *n* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von (*n*-1) Festplatten.
- Redundante Informationen (Parität) werden abwechselnd auf allen Festplatten gespeichert.
- Wenn eine Festplatte fehlerhaft wird, funktioniert die virtuelle Festplatte weiterhin, wird aber mit geringerer Leistung ausgeführt. Die Daten werden von den verbleibenden Festplatten rekonstruiert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Redundanz zum Schutz der Daten.

RAID-Level 6 – Striping mit zusätzlicher verteilter Parität

RAID 6 bietet Datenredundanz, indem Daten-Striping zusammen mit Paritätsinformationen verwendet wird. Wie bei RAID 5 wird auch hier die Parität innerhalb jedes Stripes verteilt. Aber RAID 6 verwendet eine zusätzliche physische Festplatte zur Speicherung der Paritätsdaten, sodass jeder Stripe in der Festplattengruppe zwei Festplattenblöcke mit Paritätsdaten vorhält. Durch diese zusätzliche Parität sind die Daten auch dann geschützt, wenn zwei Festplatten ausfallen. In der folgenden Abbildung werden die beiden Sätze von Paritätsinformationen als **P** und **Q** gekennzeichnet.



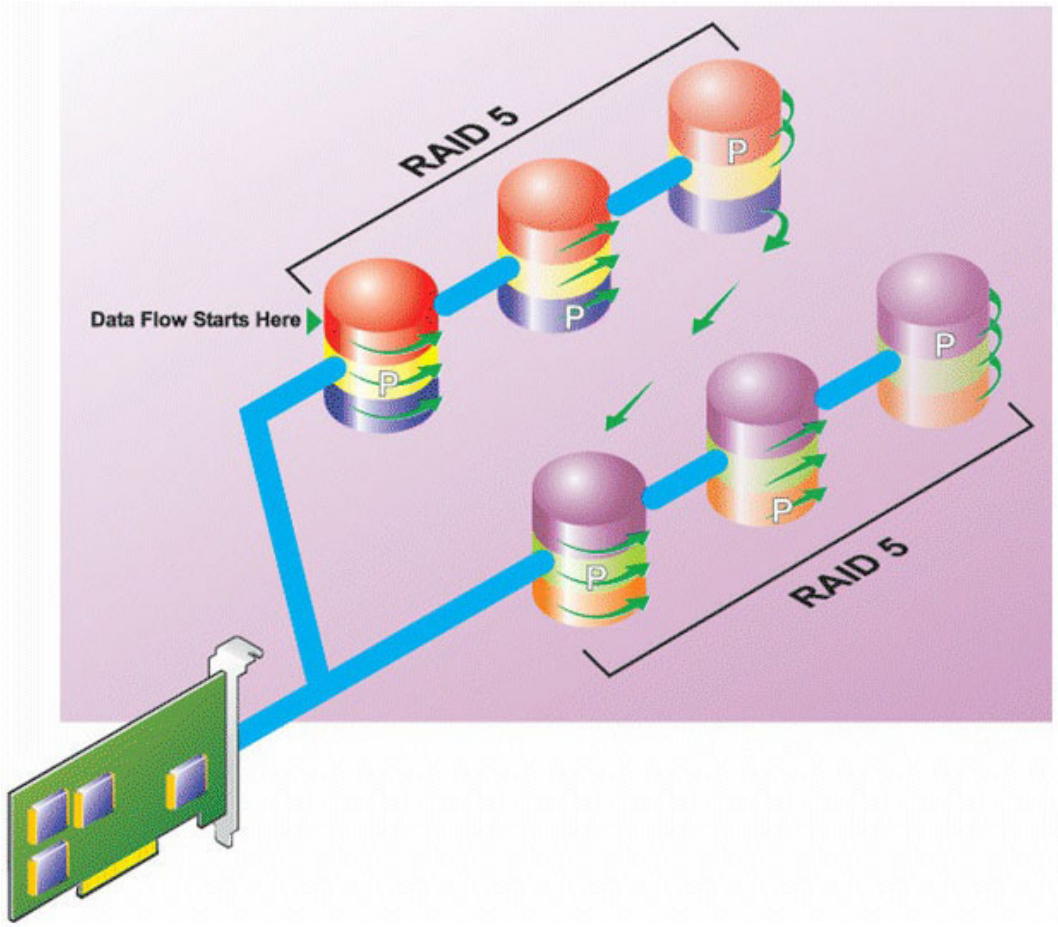
RAID 6-Eigenschaften:

- Gruppiert *n* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von (*n*-2) Festplatten.
- Redundante Informationen (Parität) werden abwechselnd auf allen Festplatten gespeichert.
- Die virtuelle Festplatte bleibt auch bei zwei Festplattenausfällen noch betriebsfähig. Die Daten werden von den verbleibenden Festplatten rekonstruiert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Erhöhte Redundanz zum Schutz der Daten.
- Für Parität sind zwei Festplatten pro Bereich erforderlich. RAID 6 ist in Bezug auf Festplattenspeicherplatz teurer.

RAID-Level 50 – Striping über RAID 5-Sets

Bei RAID 50 erfolgt das Striping über mehr als einen Bereich physischer Festplatten. Eine RAID 5-Festplattengruppe, die mit drei physischen Festplatten implementiert ist und dann mit einer Festplattengruppe von drei weiteren physischen Festplatten fortfährt, wäre beispielsweise RAID 50.

Es ist möglich, RAID 50 zu implementieren, auch wenn die Hardware dies nicht direkt unterstützt. In diesem Fall würden Sie mehr als eine virtuelle RAID 5-Festplatte implementieren und die RAID 5-Festplatten dann in dynamische Festplatten umwandeln. Sie können dann ein dynamisches Volume erstellen, das sich über alle virtuellen RAID 5-Festplatten erstreckt.

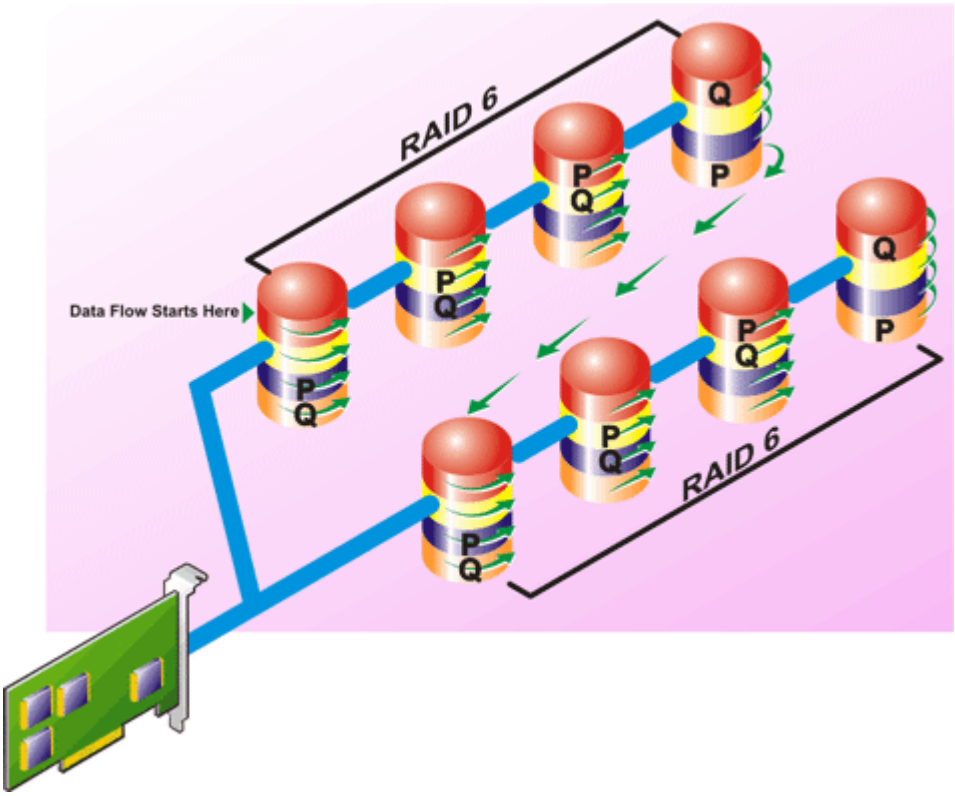


RAID 50-Eigenschaften:

- Gruppiert *n***s* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von *s**(*n*-1) Festplatten, wobei *s* die Anzahl von Bereichen und *n* die Anzahl von Festplatten innerhalb jeden Bereiches darstellt.
- Redundante Informationen (Parität) werden abwechselnd auf allen Festplatten jedes RAID 5-Bereiches gespeichert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Erfordert die gleiche Menge an Paritätsinformationen wie RAID 5.
- Daten werden über alle Bereiche gestriped. RAID 50 ist in Bezug auf Festplattenspeicherplatz teurer.

RAID-Level 60 – Striping über RAID 6-Sets

Bei RAID 60 erfolgt das Striping über mehrere Gruppen physischer Festplatten, die als RAID 6 konfiguriert sind. Eine RAID 6-Festplattengruppe, die mit vier physischen Festplatten implementiert ist und dann mit einer Festplattengruppe von vier weiteren physischen Festplatten fortfährt, wäre beispielsweise RAID 60.

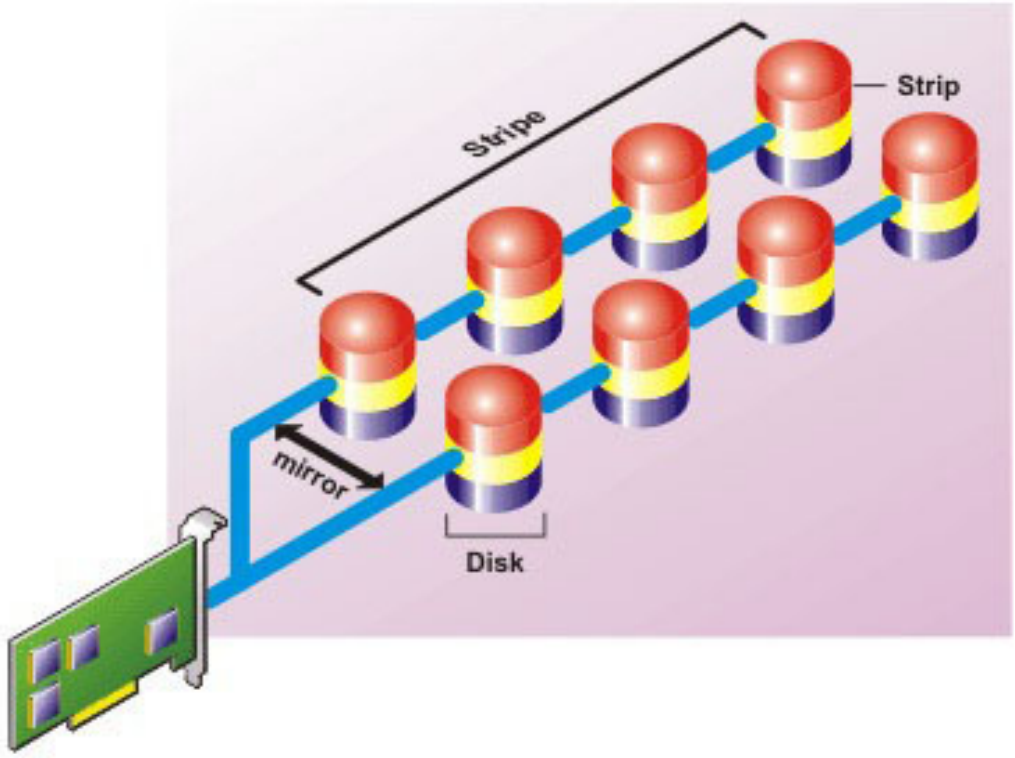


RAID 60-Eigenschaften:

- Gruppiert *n***s* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von *s**(*n*-2) Festplatten, wobei *s* die Anzahl von Bereichen und *n* die Anzahl von Festplatten innerhalb jeden Bereiches darstellt.
- Redundante Informationen (Parität) werden abwechselnd auf allen Festplatten jedes RAID 6-Bereiches gespeichert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Erhöhte Redundanz bietet höhere Datensicherung als ein RAID 50.
- Erfordert verhältnismäßig die gleiche Menge an Paritätsinformationen wie RAID 6.
- Für Parität sind zwei Festplatten pro Bereich erforderlich. RAID 60 ist in Bezug auf Festplattenspeicherplatz teurer.

RAID-Level 10 – Striped-Mirrors

Für RAB ist RAID-Level 10 eine Implementierung von RAID-Level 1. RAID 10 kombiniert gespiegelte physische Festplatten (RAID 1) und Daten-Striping (RAID 0). Mit RAID 10 werden Daten über mehrere physische Festplatten gestriped. Die gestripte Festplattengruppe wird dann auf einen anderen Satz physischer Festplatten gespiegelt. RAID 10 kann als ein *Spiegel von Stripes* betrachtet werden.



RAID 10-Eigenschaften:

- Gruppiert *n* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von (*n*/2) Festplatten, wobei *n* für eine gerade Ganzzahl steht.
- Gespiegelte Daten werden über Sätze physischer Festplatten gestriped. Dieses Level bietet Redundanz durch Datenspiegelung.
- Wenn eine Festplatte ausfällt, kann die virtuelle Festplatte weiterhin betrieben werden. Die Daten werden von der verbleibenden gespiegelten Festplatte gelesen.
- Verbesserte Lese- und Schreibleistung.
- Redundanz zum Schutz der Daten.

RAID-Level-Leistung vergleichen

In der folgenden Tabelle werden die Leistungseigenschaften der am häufigsten verwendeten RAID-Level verglichen. Diese Tabelle bietet allgemeine Richtlinien zur Auswahl eines RAID-Levels. Schätzen Sie Ihre spezifischen Umgebungsanforderungen ab, bevor Sie ein RAID-Level wählen.

Tabelle 38. RAID-Level-Leistungsvergleich

RAID-Stufe	Datenverfügbarkeit	Leseleistung	Schreibleistung	Neuerstellungsleistung	Mindestanzahl von erforderlichen Festplatten	Vorschläge zur Verwendung
RAID 0	Keine	Sehr gut	Sehr gut	k. A.	N	Nicht-kritische Daten
RAID 1	Ausgezeichnet	Sehr gut	Gut	Gut	(N = 1)	Kleine Datenbanken, Datenbank-Protokolle und

RAID-Stufe	Datenverfügbarkeit	Leseleistung	Schreibleistung	Neuerstellungsleistung	Mindestanzahl von erforderlichen Festplatten	Vorschläge zur Verwendung
						kritische Informationen
RAID 5	Gut	Sequenzielles Lesen: Gut. Direktes Lesen: Sehr gut	Mittelmäßig, es sei denn Rückschreiben in Cache wird verwendet	Mittelmäßig	N + 1 (N = wenigstens zwei Festplatten)	Datenbanken und andere lese-intensive direkte Verwendungen
RAID 10	Ausgezeichnet	Sehr gut	Mittelmäßig	Gut	2N x X	Daten-intensive Umgebungen (große Datensätze)
RAID 50	Gut	Sehr gut	Mittelmäßig	Mittelmäßig	N + 2 (N = wenigstens 4)	Mittelgroße direkte oder Daten-intensive Verwendungen
RAID 6	Ausgezeichnet	Sequenzielles Lesen: Gut. Direktes Lesen: Sehr gut	Mittelmäßig, es sei denn Rückschreiben in Cache wird verwendet	Schlecht	N + 2 (N = wenigstens zwei Festplatten)	Kritische Informationen. Datenbanken und andere lese-intensive direkte Verwendungen
RAID 60	Ausgezeichnet	Sehr gut	Mittelmäßig	Schlecht	N + 2 (N = wenigstens 2)	Kritische Informationen. Mittelgroße direkte oder Daten-intensive Verwendungen
N = Anzahl physischer Festplatten X = Anzahl von RAID-Sets						

Unterstützte Controller

Unterstützte RAID-Controller

Die iDRAC-Schnittstellen unterstützen die folgenden PERC9-Controller:

- PERC H830
- PERC H730P
- PERC H730
- PERC H330

Die iDRAC-Schnittstellen unterstützen die folgenden PERC8-Controller:

- PERC H810

- PERC H710P
- PERC H710
- PERC H310

Die iDRAC-Schnittstellen unterstützen die folgenden modularen PERC8-Controller:

- PERC FD33xS
- PERC FD33xD

ANMERKUNG: Weitere Informationen zum Konfigurieren und Ändern des Controller-Modus auf dem PERC FD33xS und PERC FD33xD-Controller finden Sie im *Dell Chassis Management Controller Version 1.2 für PowerEdge FX2-/FX2s-Benutzerhandbuch*, das unter dell.com/support/manuals verfügbar ist.

Unterstützte Nicht-RAID-Controller

Die iDRAC-Schnittstelle unterstützt externe SAS-HBA-Controller mir 12 GBit/s, interne HBA330-Controller und SATA-Laufwerke, diese jedoch nur auf internen HBA330-Controllern.

Unterstützte Gehäuse

iDRAC unterstützt MD1200-, MD1220-, MD1400- und MD1420-Gehäuse.

ANMERKUNG: Redundant Array of Inexpensive Disks (RBODs), die mit HBA-Controllern verbunden sind, werden nicht unterstützt.

Übersicht über die unterstützten Funktionen für Speichergeräte

Die folgende Tabelle enthält die Funktionen, die über iDRAC durch die Speichergeräte unterstützt werden.

ANMERKUNG: Funktionen wie das Vorbereiten auf das Entfernen und das Aufleuchten oder Erlöschen der Komponenten-LED gelten nicht für HHHL PCIe SSD-Karten.

Tabelle 39. Unterstützte Funktionen für Speichergeräte

Funktion	PERC 9-Controller						PERC 8-Controller				PCIe-SSD-Laufwerke
	H830	H730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
Physische Festplatte als einen globalen Hotspare zuweisen oder die Zuweisung rückgängig machen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Virtuelle Festplatte erstellen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Cache-Richtlinien für virtuelle Festplatten bearbeiten	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar

Funktion	PERC 9-Controller						PERC 8-Controller				PCIe-SSD-Laufwerke
	H830	H730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
Übereinstimmung der virtuellen Festplatte überprüfen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Übereinstimmungsüberprüfung abbrechen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
Virtuelle Festplatten initialisieren	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Initialisierung abbrechen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
Virtuelle Festplatten verschlüsseln	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Dedizierten Hotspare zuweisen und Zuweisung rückgängig machen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Löschen virtueller Festplatten	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Patrol Read-Modus einstellen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Patrol Read – Nicht konfigurierte Bereiche	Echtzeit (nur in Web-Schnittstelle)	Echtzeit (nur in Web-Schnittstelle)	Echtzeit (nur in Web-Schnittstelle)	Echtzeit (nur in Web-Schnittstelle)	Echtzeit (nur in Web-Schnittstelle)	Echtzeit (nur in Web-Schnittstelle)	Bereitgestellt (nur in Web-Schnittstelle)	Bereitgestellt (nur in Web-Schnittstelle)	Bereitgestellt (nur in Web-Schnittstelle)	Bereitgestellt (nur in Web-Schnittstelle)	Nicht anwendbar
Übereinstimmungsüberprüfungsmodus	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Copyback-Betriebsart	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Lastausgleichsmodus	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Übereinstimmungsüberprüfungsrate	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar

Funktion	PERC 9-Controller						PERC 8-Controller				PCIe-SSD-Laufwerke
	H830	H730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
Neuerstellungsrate	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Hintergrundinitialisierungsrate	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Rekonstruktionsrate	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Fremdkonfiguration importieren	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Fremdkonfiguration automatisch importieren	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Fremdkonfiguration löschen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Controller-Konfiguration zurücksetzen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Sicherheitsschlüssel erstellen oder ändern	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar
Bestandsaufnahme und die Remote-Überwachung des Status von PCIe SSD-Geräte	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Echtzeit
Entfernen der PCIe SSD vorbereiten	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Echtzeit
Daten sicher löschen	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Bereitgestellt
Backplane-Modus konfigurieren	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
Komponenten-LEDs blinken oder Blinken beenden	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit

Funktion	PERC 9-Controller						PERC 8-Controller				PCIe-SSD-Laufwerke
	H830	H730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
Controller-Modus ändern	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar

Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen

Sie können den Zustand remote überwachen und die Bestandsliste für die folgenden Comprehensive Embedded Management (CEM)-aktivierten Speichergeräte im Managed System über die iDRAC-Webschnittstelle anzeigen:

- RAID-Controller, Nicht-RAID-Controller und PCIe-Extender
- Gehäuse mit Gehäuseverwaltungsmodulen (EMMs), Netzteile, Lüftersonde und Temperatursonde
- Physische Laufwerke
- Virtuelle Laufwerke
- Batterien

WS-MAN, RACADM und WS-MAN zeigen die Informationen für die meisten Speichergeräte jedoch im System an.

Es werden auch Informationen zu kürzlich aufgetretenen Speicherereignissen und zur Topologie der Speichergeräte angezeigt.

Für Speicherereignisse werden Warnungen und SNMP-Traps angezeigt. Diese Ereignisse werden im Lifecycle-Protokoll erfasst.

ANMERKUNG: Wenn Sie den WSMAN-Befehl der Gehäuseansicht auf einem System aufzählen, während ein Netzteilkabel entfernt wird, wird der primäre Status des Gehäuses als Funktionsfähig und nicht als Warnung angezeigt.

Netzwerkgeräte über die Web-Schnittstelle überwachen

So zeigen Sie die Speichergeräteinformationen über die Web-Schnittstelle an:

- Gehen Sie zu **Übersicht** > **Speicher** > **Zusammenfassung**, um eine Zusammenfassung zu den Speicherkomponenten und den kürzlich protokollierten Ereignissen anzuzeigen. Diese Seite wird automatisch alle 30 Sekunden aktualisiert.
- Gehen Sie zu **Übersicht** > **Speicher** > **Topologie**, um die hierarchisch-physische Ansicht der Aggregation mit den wichtigsten Speicherkomponenten anzuzeigen.
- Gehen Sie zu **Übersicht** > **Speicher** > **Physische Festplatten** > **Eigenschaften**, um die Informationen zur physischen Festplatte anzuzeigen. Daraufhin wird die Seite **Eigenschaften der physischen Festplatten** angezeigt.
- Gehen Sie zu **Übersicht** > **Speicher** > **Virtuelle Festplatten** > **Eigenschaften**, um die Informationen zu virtuellen Festplatten anzuzeigen. Daraufhin wird die Seite **Eigenschaften der physischen Festplatten** angezeigt.
- Gehen Sie zu **Übersicht** > **Speicher** > **Controller** > **Eigenschaften**, um die RAID-Controller-Informationen anzuzeigen. Daraufhin wird die Seite **Controller-Eigenschaften** angezeigt.
- Gehen Sie zu **Übersicht** > **Speicher** > **Gehäuse** > **Eigenschaften**, um die Gehäuseinformationen anzuzeigen. Daraufhin wird die Seite **Gehäuseeigenschaften** angezeigt.

Sie können Filter verwenden, um spezifische Geräteinformationen anzuzeigen.

Weitere Informationen zu den angezeigten Eigenschaften und zur Verwendung der Filteroptionen finden Sie in der *iDRAC-Online-Hilfe*.

Speichergerät über RACADM überwachen

Um die Speichergeräteinformationen anzuzeigen, verwenden Sie den Befehl **storage**.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Überwachen der Verwendung der Rückwandplatine über das Dienstprogramm für iDRAC-Einstellungen

Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Systemzusammenfassung**. Daraufhin wird die Seite **iDRAC-Einstellungen - Systemzusammenfassung** angezeigt. Der Abschnitt **Bestandsaufnahme für die Rückwandplatine** zeigt die Rückwandplatineninformationen an. Weitere Informationen den Feldern finden Sie in der *Online-Hilfe zum Dienstprogramm für die iDRAC-Einstellungen*.

Anzeigen der Speichergerätetopologie

Diese Seite dient der Ansicht der hierarchischen physischen Aufbewahrung der wichtigsten Speicherkomponenten. Auf dieser Seite werden die Controller, die an diesen angeschlossenen Gehäuse sowie ein Link zu der physischen Festplatte in jedem Gehäuse aufgelistet. Zudem werden die physischen Festplatten angezeigt, welche direkt mit dem Controller verbunden sind.

Um die Speichergerätetopologie anzuzeigen, gehen Sie zu **Übersicht** > **Speicher** > **Topologie**. Die Seite **Topologie** zeigt die hierarchische Darstellung der Speicherkomponenten im System an.

Klicken Sie für die Ansicht der jeweiligen Komponentendetails auf die zugehörigen Links.

Verwalten von physischen Festplatten

Sie können die folgenden Aktionen für die physischen Festplatten ausführen:

- Eigenschaften physischer Laufwerke anzeigen.
- Physische Festplatte als einen globalen Hotspare zuweisen oder die Zuweisung rückgängig machen.
- In RAID-fähige Festplatte konvertieren.
- In nicht-RAID-fähige Festplatte konvertieren.
- Blinken der LED oder Beenden des Blinkens.

Zugehöriger Link

Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen
Zuweisen oder Aufheben der Zuweisung der physischen Festplatte als globales Hotspare

Zuweisen oder Aufheben der Zuweisung der physischen Festplatte als globales Hotspare

Ein globaler Hotspare ist eine nicht verwendete Backup-Festplatte, die Teil der Festplattengruppe ist. Hotspares verbleiben im Standby-Modus. Wenn eine in einer virtuellen Festplatte verwendete physische Festplatte fehlerhaft ist, wird der zugewiesene Hotspare aktiviert, um die fehlerhafte physische Festplatte ohne Unterbrechung des Systems und ohne Benutzereingriff zu ersetzen. Wenn ein Hotspare aktiviert wird, werden die Daten aller redundanten virtuellen Festplatten neu erstellt, die die fehlerhafte physische Festplatte verwendet haben.

ANMERKUNG: Ab der iDRAC-Version 2.30.30.30 können Sie globale Hotspares hinzufügen, wenn keine virtuellen Festplatten erstellt werden.

Sie können die Hotspare-Zuweisung ändern, indem Sie die Zuweisung einer Festplatte rückgängig machen und eine andere Festplatte auswählen. Sie können auch mehr als eine physische Festplatte als globalen Hotspare zuweisen.

Globale Hotspares müssen manuell zugewiesen, bzw. die Zuweisung muss manuell rückgängig gemacht werden. Sie sind keinen spezifischen virtuellen Festplatten zugewiesen. Wenn Sie ein Hotspare einer virtuellen Festplatte zuweisen möchten (es ersetzt jede

physische Festplatte, die in der virtuellen Festplatte fehlerhaft ist), dann verwenden Sie Zuweisen und Aufheben der Zuweisung von dedizierten Hotspares.

Wenn virtuelle Festplatten gelöscht werden, ist es möglich, dass die Zuweisung für alle zugewiesenen globalen Hotspares rückgängig gemacht wird, wenn die letzte virtuelle Festplatte, die mit dem Controller verknüpft ist, gelöscht wird.

Wenn Sie die Konfiguration zurücksetzen, wird die Zuweisung für alle virtuellen Festplatten gelöscht, und die Zuweisung für alle Hotspares wird aufgehoben.

Sie sollten sich mit den Größenanforderungen und anderen Überlegungen, die bei Hotspares zu beachten sind, vertraut machen.

Führen Sie vor dem Zuweisen einer physischen Festplatte als globaler Hotspare die folgenden Schritte aus:

- Stellen Sie sicher, dass der Lifecycle Controller aktiviert ist.
- Wenn sich keine Laufwerke im Zustand „Bereit“ befinden, dann fügen Sie zusätzliche Festplatten hinzu, und stellen Sie sicher, dass sich die Festplatten im betriebsbereiten Status befinden.
- Wenn keine virtuellen Festplatten vorhanden sind, erstellen Sie mindestens eine virtuelle Festplatte.
- Wenn sich physische Laufwerke im Nicht-RAID-Modus befinden, dann konvertieren Sie sie unter Verwendung von iDRAC-Schnittstellen wie z. B. die iDRAC-Webschnittstelle, RACADM, WS-MAN oder <STRG+R> verwenden in den RAID-Modus.

Wenn Sie eine physische Festplatte als globales Hotspare im Modus „Zu ausstehenden Vorgängen hinzufügen“ zugewiesen haben, wird der ausstehende Vorgang, jedoch kein Job erstellt. Wenn Sie dann versuchen, die Zuweisung der gleichen Festplatte als globales Hotspare aufzuheben, wird der Vorgang „Zuweisung für globales Hotspare anstehend“ deaktiviert.

Wenn Sie die Zuweisung einer physischen Festplatte als globales Hotspare im Modus „Zu ausstehenden Vorgängen hinzufügen“ aufgehoben haben, wird der ausstehende Vorgang, jedoch kein Job erstellt. Wenn Sie dann versuchen, die gleiche Festplatte als globales Hotspare zuzuweisen, wird der Vorgang „Aufhebung der Zuweisung für globales Hotspare anstehend“ deaktiviert.

Zuweisen oder Aufheben der Zuweisung von globalen Hotspares über die Webschnittstelle

So weisen Sie ein globalen Hotspares einer physischen Festplatte zu oder heben die Zuweisung auf:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Physische Festplatten** > **Setup**.
Daraufhin wird die Seite **Setup von physischen Festplatten** angezeigt.
2 Wählen Sie im Drop-Down-Menü **Controller** den Controller aus, um die zugehörigen physikalischen Laufwerke anzuzeigen.
3 Um die Zuweisung als globales Hotspare zu erreichen, wählen Sie aus dem Drop-Down-Menü in der Spalte **Allen zuweisen** die Option **Globales Hotspare** für eine oder mehrere physische Festplatten aus.
4 Um die Zuweisung als globales Hotspare zurückzunehmen, wählen Sie aus dem Drop-Down-Menü in der Spalte **Allen zuweisen** die Option **Zuweisung für globales Hotspare zurücknehmen** für eine oder mehrere physische Festplatten aus.
5 Wählen Sie im Dropdown-Menü die Option **Betriebsmodus anwenden**, wenn Sie die Einstellungen übernehmen möchten.
6 Klicken Sie auf **Anwenden**.
Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

Zugehöriger Link

Auswählen des Betriebsmodus über die Webschnittstelle

Zuweisen oder Aufheben der Zuweisung für globale Hotspares über RACADM

Verwenden Sie den Befehl **storage** und legen Sie den Typ als globalen Hotspare fest.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Zugehöriger Link

Auswählen des Betriebsmodus über RACADM

Konvertieren einer physischen Festplatte in den RAID- und Nicht-RAID-Modus

Durch die Konvertierung einer physischen Festplatte in den RAID-Modus können Sie die Festplatte für alle RAID-Vorgänge verwenden. Wenn sich eine Festplatte im Nicht-RAID-Modus befindet, wird die Festplatte im Gegensatz zu nicht konfigurierten Festplatten im Status „Good“ (Gut) für das Betriebssystem freigegeben und in einem direkten Passthrough-Modus verwendet.

Sie können die physischen Festplatten folgendermaßen in den RAID- und Nicht-RAID-Modus konvertieren:

- Beginnen Sie mit der Verwendung der iDRAC-Netzwerkschnittstellen, wie z.B. der Webschnittstelle, RACADM oder WS-Man.
- Durch Drücken von Strg+R während des Server-Neustarts und Auswahl des erforderlichen Controllers.

ANMERKUNG: Dieser Task wird auf PERC-Hardware-Controllern, die im HBA-Modus ausgeführt werden, nicht unterstützt.

ANMERKUNG: Konvertierung in den Nicht-RAID-Modus für PERC 8-Controller wird nur für PERC H310- und H330-Controller unterstützt.

ANMERKUNG: Wenn sich die mit einem PERC-Controller verbundenen physischen Laufwerke im Nicht-RAID-Modus befinden, wird die in den iDRAC-Schnittstellen (z. B. iDRAC-GUI, RACADM und WS-MAN) angezeigte Datenträgergröße möglicherweise als ein wenig kleiner als die tatsächliche Laufwerksgröße angezeigt. Sie können Betriebssysteme jedoch mit der vollen Kapazität des Datenträgers bereitstellen.

Konvertierung von physikalischen Festplatten in den RAID-fähigen oder nicht-RAID-Modus mithilfe der iDRAC-Web-Schnittstelle

Führen Sie zum Konvertieren der physikalischen Festplatten in den RAID-Modus oder den Nicht-RAID-Modus die folgenden Schritte aus:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Physische Festplatten** > **Setup**.
   Die Seite **Setup** wird angezeigt.
2. Wählen Sie im Drop-Down-Menü **Controller** einen Controller aus.
   Alle physischen Festplatten, die dem ausgewählten RAID-Controller zugeordnet sind, werden angezeigt.
3. Wählen Sie aus dem Drop-Down-Menü **Maßnahme – Allen zuweisen** die gewünschte Option (**Zu RAID konvertieren** oder **Zu NonRAID konvertieren)** für alle Festplatten aus, oder wählen Sie die Option für bestimmte Festplatten im **Aktions**-Dropdown-Menü aus.
4. Wählen Sie im Dropdown-Menü die Option **Betriebsmodus anwenden**, wenn Sie die Einstellungen übernehmen möchten.
5. Klicken Sie auf **Anwenden**.
   Die Einstellungen werden basierend auf der im Betriebsmodus ausgewählten Option angewendet.

Konvertierung von physikalischen Festplatten in den RAID-fähigen oder nicht-RAID-Modus mithilfe von RACADM

Verwenden Sie je nachdem, ob Sie in den RAID- oder Nicht-RAID-Modus konvertieren möchten die folgenden RACADM-Befehle

- Verwenden Sie den Befehl `racadm storage converttoraid`, um in den RAID-Modus zu konvertieren.
- Verwenden Sie den Befehl `racadm storage converttononraid`, um in den Nicht-RAID-Modus zu konvertieren.

Weitere Informationen zu den Befehlen finden Sie im RACADM-Befehlszeilen-Referenzhandbuch für iDRAC unter **dell.com/idracmanuals**.

Verwalten von virtuellen Festplatten

Sie können die folgenden Vorgänge für die virtuellen Festplatten ausführen:

- Erstellen
- Löschen
- Richtlinien bearbeiten
- Initialisieren
- Übereinstimmungsüberprüfung
- Übereinstimmungsüberprüfung abbrechen
- Virtuelle Festplatten verschlüsseln
- Dedizierte Ersatzlaufwerke zuweisen oder die Zuweisung rückgängig machen
- Blinken von virtuellen Festplatten und Blinken beenden

ANMERKUNG: Sie können 192 virtuelle Datenträger verwalten und überwachen, wenn die automatische Konfiguration über PERC-Controller-BIOS Human Interface Infrastructure (HII) und Dell OpenManage Server Administrator (OMSA) aktiviert ist.

Zugehöriger Link

Erstellen von virtuellen Festplatten
Bearbeiten von Cache-Richtlinien für virtuelle Laufwerke
Löschen von virtuellen Festplatten
Überprüfen der Übereinstimmung der virtuellen Festplatte
Initialisieren von virtuellen Festplatten
Verschlüsseln der virtuellen Laufwerke
Zuweisen oder Aufheben der Zuweisung von dezidierten Hotspares
Verwalten von virtuellen Festplatten über die Webschnittstelle
Verwalten von virtuellen Festplatten über RACADM

Erstellen von virtuellen Festplatten

Um RAID-Funktionen zu implementieren, muss eine virtuelle Festplatte erstellt werden. Eine virtuelle Festplatte bezieht sich auf Speicher, der von einem RAID-Controller aus einer oder mehreren physischen Festplatte(n) erstellt wurde. Obwohl eine virtuelle Festplatte aus mehreren physischen Festplatten erstellt werden kann, wird sie vom Betriebssystem als eine einzelne Festplatte betrachtet.

Bevor Sie eine virtuelle Festplatte erstellen, sollten Sie sich mit den Informationen unter Erwägungen vor der Erstellung von virtuellen Festplatten vertraut machen.

Sie können eine virtuelle Festplatte über die physischen Festplatten erstellen, die mit dem PERC-Controller verbunden sind. Für die Erstellung einer virtuellen Festplatte müssen Sie über die Benutzerberechtigung für die Serversteuerung verfügen. Sie können maximal 64 virtuelle Festplatten und maximal 16 virtuellen Festplatten in derselben Laufwerksgruppe erstellen.

In den folgenden Fällen können Sie keine virtuelle Festplatte erstellen:

- Physische Laufwerke sind für die Erstellung virtueller Laufwerke nicht verfügbar. Fügen Sie zusätzliche physische Laufwerke hinzu.
- Die maximale Anzahl von virtuellen Festplatten, die auf dem Controller erstellt werden können, wurde erreicht. Sie müssen mindestens ein virtuelles Laufwerk löschen, um ein neues virtuelles Laufwerk erstellen zu können.
- Die von einer Laufwerksgruppe unterstützte maximale Anzahl virtueller Festplatten wurde erreicht. Sie müssen erst eine virtuelle Festplatte aus der ausgewählten Gruppe löschen, um eine neue virtuelle Festplatte erstellen zu können.
- Auf dem ausgewählten Controller wird derzeit ein Job ausgeführt oder ist geplant. Sie müssen warten, bis der Job abgeschlossen ist, oder Sie können den Job löschen, bevor Sie einen neuen Arbeitsvorgang beginnen. Sie können den Status des geplanten Jobs auf der Seite Job-Warteschlange anzeigen und verwalten.

- Physische Festplatte befindet sich im Nicht-RAID-Modus. Sie muss unter Verwendung der iDRAC-Schnittstellen wie beispielsweise der iDRAC-Web-Schnittstelle, RACADM, WS-MAN, oder <STRG+R> in den RAID-Modus konvertiert werden.

ANMERKUNG: Wenn Sie eine virtuelle Festplatte im Modus „Zu ausstehenden Vorgängen hinzufügen“ erstellen und ein Job nicht erstellt wird und Sie dann die virtuelle Festplatte löschen, wird der ausstehende Erstellungsvorgang für die virtuelle Festplatte gelöscht.

Erwägungen vor der Erstellung von virtuellen Festplatten

Vor dem Erstellen von virtuellen Festplatten sollten Sie Folgendes beachten:

- Nicht auf dem Controller gespeicherte virtuelle Festplattennamen – Die Namen der von Ihnen erstellten virtuellen Festplatten werden nicht auf dem Controller gespeichert. Falls Sie einen Neustart mit einem anderen Betriebssystem ausführen, könnte das neue Betriebssystem die virtuelle Festplatte eventuell mit seiner eigenen Namenkonvention umbenennen.
- Die Festplattengruppierung ist eine logische Gruppierung von Festplatten, die mit einem RAID-Controller verbunden sind, auf dem mehr als eine virtuelle Festplatte erstellt wurde, so dass alle virtuellen Festplatten in der Festplattengruppe alle physische Festplatten in der Festplattengruppe verwenden. Die aktuelle Implementierung unterstützt das Blocken von gemischten Festplattengruppen während dem Erstellen von logischen Geräten.
- Physische Festplatten sind an Festplattengruppen gebunden, daher gibt es keine Vermischung von RAID-Stufen auf einer Festplattengruppe.
- Die Anzahl von physischen Festplatten, die in einer virtuellen Festplatte enthalten sein können, unterliegt Einschränkungen. Diese Einschränkungen hängen vom Controller ab. Wenn eine virtuelle Festplatte erstellt wird, unterstützen Controller eine bestimmte Anzahl von Stripes und Bereichen (Methoden zur Speicherkombination auf physischen Festplatten). Da die Gesamtanzahl von Stripes und Bereichen eingeschränkt ist, wird die Anzahl physischer Festplatten, die verwendet werden können, ebenso eingeschränkt. Die Einschränkungen von Stripes und Bereichen wirken sich wie folgt auf die möglichen Verkettungen und RAID-Stufen aus:
  - Die maximale Anzahl von Bereichen wirkt sich auf Verkettung, RAID 10, RAID 50 und RAID 60 aus.
  - Die maximale Anzahl von Stripes wirkt sich auf RAID 0, RAID 5, RAID 50, RAID 6 und RAID 60 aus.
  - Die Anzahl physischer Festplatten in einem Spiegel ist immer 2. Dies wirkt sich auf RAID 1 und RAID 10 aus.
- Virtuelle Festplatten können auf PCIe-SSDs nicht erstellt werden.

Erstellen von virtuellen Festplatten über die Webschnittstelle

So erstellen Sie eine virtuelle Festplatte:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Virtuelle Festplatten** > **Erstellen**.

Die Seite **Virtuelle Festplatte erstellen** wird angezeigt.

2 Führen Sie im Abschnitt **Einstellungen** die folgenden Schritte aus:

a Geben Sie den Namen des virtuellen Laufwerks ein.

b Wählen Sie aus dem Drop-Down-Menü **Controller** den Controller aus, für den Sie die virtuelle Festplatte erstellen möchten.

c Wählen Sie die RAID-Stufe für die virtuelle Festplatte aus dem Drop-Down-Menü **Layout** aus.

Nur jene RAID-Stufen, die vom Controller unterstützt werden, werden im Drop-Down-Menü angezeigt, und zwar auf Basis der Gesamtzahl der verfügbaren physikalischen Festplatten.

d Wählen Sie den **Medientyp**, die **Blockgröße**, die **Leserichtlinie**, die **Schreibrichtlinie**, die **Festplatten-Cache-Regeln** und die **T10-PI-Fähigkeit** aus.

Es werden nur die Werte, die vom Controller unterstützt werden, in den Drop-Down-Menüs für diese Eigenschaften angezeigt.

e Geben Sie im Feld **Kapazität** die Größe des virtuellen Laufwerks ein.

Es wird die maximale Größe angezeigt, die dann auf Basis der ausgewählten Festplatten aktualisiert wird.

f Das Feld **Bereichsanzahl** wird auf Basis der ausgewählten physischen Festplatten (Schritt 3) angezeigt. Sie können diesen Wert nicht festlegen. Er wird automatisch berechnet, nachdem Sie Festplatten für mehrere RAID-Stufen ausgewählt haben. Wenn Sie RAID 10 ausgewählt haben und der Controller die unregelmäßige RAID 10-Stufe unterstützt, wird der Wert für die Bereichsanzahl nicht angezeigt. Der Controller legt automatisch den entsprechenden Wert fest.

3 Wählen Sie im Abschnitt **Physische Festplatten auswählen** die Anzahl der physischen Festplatten aus.

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

4 Wählen Sie im Dropdown-Menü die Option **Betriebsmodus anwenden**, wenn Sie die Einstellungen übernehmen möchten.

5 Klicken **Sie auf**.

Basierend auf der Option **Betriebsmodus wählen** werden die Einstellungen angewendet.

Erstellen von virtuellen Festplatten über RACADM

Verwenden Sie den Befehl `racadm storage createvd`.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Bearbeiten von Cache-Richtlinien für virtuelle Laufwerke

Sie können die Lese-, Schreib- oder Festplatten-Cache-Regeln einer virtuellen Festplatte ändern.

ANMERKUNG: Bei einigen der Controller werden nicht alle Lese- oder Schreibrichtlinien unterstützt. Aus diesem Grund wird, wenn eine Richtlinie angewendet wird, eine Fehlermeldung angezeigt.

Die Leseregeln bestimmen, ob der Controller beim Suchen von Daten sequenzielle Sektoren auf der virtuellen Festplatte lesen soll.

- **Adaptives Vorauslesen**: Der Controller leitet das Vorauslesen nur dann ein, wenn durch die letzten zwei Leseanforderungen ein Zugriff auf sequenzielle Sektoren der Festplatte erfolgte. Wenn durch nachfolgende Leseanforderungen ein Zugriff auf wahlfreie Sektoren der Festplatte erfolgt, verwendet der Controller keine Richtlinie für Vorauslesen mehr. Der Controller prüft weiterhin, ob Leseanforderungen auf sequenzielle Sektoren der Festplatte zugreifen und startet, falls erforderlich, das Vorauslesen.

ANMERKUNG: Frühere Generationen von PERC-Controllern unterstützen die Leserichtlinieneinstellungen No Read Ahead (Kein Vorauslesen) , Read Ahead (Vorauslesen) und Adaptive Read Ahead (Adaptives Vorauslesen). Bei PERC 8 und PERC 9 sind die Einstellungen Read Ahead (Vorauslesen) und Adaptive Read Ahead (Adaptives Vorauslesen) auf Controler-Ebene funktional identisch. Zum Zwecke der Abwärtskompatibilität ermöglichen einige Systemverwaltungsschnittstellen und PERC 8- und 9-Controller weiterhin die Einstellung der Leserichtlinie auf Adaptive Read Ahead (Adaptives Vorauslesen). Obwohl es möglich ist, Read Ahead (Vorauslesen) oder Adaptive Read Ahead (Adaptives Vorauslesen) auf PERC 8 oder PERC 9 einzustellen, gibt es keinen funktionalen Unterschied.

- **Vorauslesen**: Beim Suchen von Daten liest der Controller sequenzielle Sektoren auf dem virtuellen Laufwerk. Mithilfe der Richtlinie für das Vorauslesen kann eventuell die Systemleistung verbessert werden, wenn die Daten auf sequenzielle Sektoren der virtuellen Festplatte geschrieben werden.
- **Kein Vorauslesen** – Das Auswählen der Regel „Kein Vorauslesen“ gibt an, dass der Controller die Regel „Vorauslesen“ nicht verwenden sollte.

Die Schreibregeln bestimmen, ob der Controller ein Schreibanfrage-Beendungssignal sendet, wenn sich die Daten im Cache befinden oder nachdem sie auf die Festplatte geschrieben wurden.

- **Durchschreiben**: Der Controller sendet erst dann ein Signal für den Abschluss der Schreibanforderung, nachdem die Daten auf das Laufwerk geschrieben wurden. Das Durchschreibe-Caching bietet bessere Datensicherheit als das Rückschreibe-Caching, da das System annimmt, dass die Daten erst verfügbar sind, nachdem sie sicher auf die Festplatte geschrieben wurden.
- **Rückschreiben**: Der Controller sendet ein Signal zum Abschluss der Schreibanforderung, sobald sich die Daten im Controller-Cache befinden, jedoch noch nicht auf die Festplatte geschrieben wurden. Rückschreibe-Caching kann die Systemleistung verbessern, da nachfolgende Leseanforderungen die Daten schneller aus dem Cache als von der Festplatte abrufen können. Es kann jedoch im Falle eines Festplattenausfalls zu Datenverlust kommen, da ein Systemausfall das Schreiben der Daten auf die Festplatte verhindert. Bei anderen Anwendungen können ebenfalls Probleme auftreten, wenn bei bestimmten Aktionen die Verfügbarkeit der Daten auf der Festplatte vorausgesetzt wird.
- **Rückschreiben erzwingen**: Der Schreib-Cache wird unabhängig davon aktiviert, ob sich im Controller ein Akku befindet. Wenn der Controller keine Batterie hat und Rückschreiben in Cache erzwingen verwendet wird, kann bei einem Stromausfall ein Datenverlust auftreten.

Die Festplatten-Cache-Richtlinie gilt für Lesevorgänge auf bestimmten virtuellen Festplatten. Diese Einstellungen wirken sich nicht auf die Richtlinie für das Vorauslesen aus.

ANMERKUNG:

- Der nicht flüchtige Controller-Cache und die Akkusicherung des Controller-Caches wirken sich auf die Leserichtlinie oder die Schreibrichtlinie aus, die ein Controller unterstützen kann. Nicht alle PERCs sind mit Akkus oder Cache ausgerüstet.
- Für das Vorauslesen und das Zurückschreiben ist Cache erforderlich. Wenn der Controller also nicht über Cache verfügt, können Sie den Richtlinienwert nicht festlegen.

  Wenn der PERC mit Cache ausgerüstet ist, aber nicht mit einem Akku, und die Richtlinie so festgelegt wurde, dass der Zugriff auf den Cache erforderlich ist, kann es bei einem Stromausfall zu Datenverlusten kommen. Daher wird diese Richtlinie bei einigen PERCs nicht unterstützt.

  Daher wird je nach PERC der Richtlinienwert festgelegt.

Löschen von virtuellen Festplatten

Das Löschen einer virtuellen Festplatte zerstört alle Informationen, einschließlich der Dateisysteme und Datenträger, die sich auf der virtuellen Festplatte befinden, und entfernt die virtuelle Festplatte aus der Konfiguration des Controllers. Wenn virtuelle Festplatten gelöscht werden, kann bei allen zugewiesenen globalen Hotspares die Zuweisung rückgängig gemacht werden, wenn die letzte virtuelle Festplatte gelöscht wird, die mit dem Controller verknüpft ist. Wenn die letzte virtuelle Festplatte einer Festplattengruppe gelöscht wird, werden alle zugewiesenen dedizierten Hotspares automatisch globale Hotspares.

Sie müssen über die Berechtigung zur Anmeldung und zur Server-Steuerung verfügen, um die virtuellen Festplatten zu löschen.

Wenn dieser Vorgang zulässig ist, können Sie eine startfähige virtuelle Festplatte löschen. Dieser Vorgang erfolgt über das Seitenband und ist unabhängig vom Betriebssystem. Somit wird eine Warnmeldung angezeigt, die Sie vor dem Löschen der virtuellen Festplatte warnt.

Wenn eine virtuelle Festplatte gelöscht wird und eine neue virtuelle Festplatte, mit den gleichen Eigenschaften wie die gelöschte virtuelle Festplatte, sofort neu erstellt wird, erkennt der Controller die Daten, als ob die erste virtuelle Festplatte nie gelöscht worden wäre. In diesem Fall, wenn Sie die alten Daten nach der Neuerstellung der neuen virtuellen Festplatte nicht behalten möchten, initialisieren Sie die virtuelle Festplatte erneut.

Überprüfen der Übereinstimmung der virtuellen Festplatte

Dieser Vorgang dient der Überprüfung der Übereinstimmung der redundanten (Paritäts-) Informationen. Dieser Task gilt nur für redundante virtuelle Festplatten. Falls erforderlich erstellt die Übereinstimmungsüberprüfung die redundanten Daten neu. Falls die virtuelle Festplatte einen herabgesetzten Status aufweist, kann eine Übereinstimmungsprüfung möglicherweise die virtuelle Festplatte in den betriebsbereiten Status zurückversetzen. Sie können eine Übereinstimmungsprüfung unter Verwendung des Internets oder RACADM vornehmen.

Sie können die Übereinstimmungsprüfung auch abbrechen. Das Abbrechen der Übereinstimmungsüberprüfung ist ein Echtzeit-Vorgang.

Sie müssen über die Berechtigung zur Anmeldung und zur Server-Steuerung verfügen, um die Übereinstimmung von virtuellen Festplatten zu prüfen.

ANMERKUNG: Konsistenzprüfung wird nicht unterstützt, wenn die Laufwerke im RAID0-Modus eingerichtet sind.

Initialisieren von virtuellen Festplatten

Das Initialisieren virtueller Festplatten löscht alle Daten auf der Festplatte, es ändert jedoch nicht die Konfiguration der virtuellen Festplatte. Sie müssen eine konfigurierte virtuelle Festplatte vor der Verwendung initialisieren.

ANMERKUNG: Initialisieren Sie keine virtuellen Laufwerke, wenn Sie versuchen, eine vorhandene Konfiguration neu zu erstellen.

Sie können eine Schnellinitialisierung oder eine vollständige Initialisierung durchführen oder die Initialisierung abbrechen.

ANMERKUNG: Das Abbrechen der Initialisierung ist ein Echtzeitvorgang. Sie können die Initialisierung nur über die iDRAC-Webschnittstelle, nicht aber über RACADM abbrechen.

Schnellinitialisierung

Die Schnellinitialisierung initialisiert alle auf dem virtuellen Laufwerk enthaltenen physischen Festplatten. Mit der Schnellinitialisierung werden die Metadaten auf den physischen Festplatten aktualisiert, sodass der gesamte Festplattenspeicherplatz für künftige Schreibvorgänge verfügbar ist. Die Initialisierung kann schnell abgeschlossen werden, da vorhandene Informationen auf den physischen Festplatten nicht gelöscht werden, obwohl die auf den physischen Festplatten verbleibenden Informationen bei künftigen Schreibvorgängen überschreiben werden.

Die Schnellinitialisierung löscht nur die Startsektor- und Stripe-Informationen. Führen Sie nur dann eine Schnellinitialisierung durch, wenn Sie zeitlich eingeschränkt sind oder die Festplatten neu sind oder noch nicht verwendet wurden. Die Schnellinitialisierung nimmt in der Regel weniger Zeit in Anspruch (etwa 30 bis 60 Sekunden).

VORSICHT: Das Ausführen einer schnellen Initialisierung bewirkt, dass auf vorhandene Daten nicht mehr zugegriffen werden kann.

Bei einer Schnellinitialisierung werden keine Nullen in die Festplattenblöcke auf den physischen Festplatten geschrieben. Da kein Schreibvorgang ausgeführt wird, verursacht sie eine geringere Leistungsverschlechterung der Festplatte.

Eine Schnellinitialisierung auf einer virtuellen Festplatte überschreibt die ersten und letzten 8 MB der virtuellen Festplatte und löscht alle Startdaten oder Partitionsinformationen. Dieser Vorgang dauert nur 2–3 Sekunden und wird beim Neuerstellen von virtuellen Festplatten empfohlen.

Eine Hintergrundinitialisierung beginnt fünf Minuten nach Abschluss der Schnellinitialisierung.

Vollständige oder langsame Initialisierung

Die vollständige Initialisierung (auch als langsame Initialisierung bezeichnet) initialisiert alle auf dem virtuellen Laufwerk enthaltenen physischen Festplatten. Die Metadaten auf den physischen Festplatten werden aktualisiert und alle vorhandenen Daten und Dateisysteme werden gelöscht. Sie können eine vollständige Initialisierung nach der Erstellung der virtuellen Festplatte durchführen. Im Vergleich zur Schnellinitialisierung ist die vollständige Initialisierung unter Umständen besser geeignet, wenn Sie Probleme mit einer physischen Festplatte haben oder vermuten, dass sie beschädigte Festplattenblöcke aufweist. Die vollständige Initialisierung weist beschädigte Blöcke neu zu und schreibt Nullen in alle Festplattenblöcke.

Bei der vollständigen Initialisierung einer virtuellen Festplatte ist keine Hintergrundinitialisierung erforderlich. Außerdem kann der Host nicht auf die virtuelle Festplatte zugreifen. Wenn das System während der vollständigen Initialisierung neu gestartet wird, wird der Vorgang abgebrochen und eine Hintergrundinitialisierung beginnt auf dem virtuellen Laufwerk.

Es wird empfohlen, stets eine vollständige Initialisierung auf Festplatten durchzuführen, die zuvor Daten enthalten haben. Eine vollständige Initialisierung kann zwischen 1 bis 2 Minuten pro GB dauern. Die Geschwindigkeit richtet sich nach dem Controller-Modell, der Geschwindigkeit der Festplatten und der Firmware-Version.

Die vollständige Initialisierung initialisiert eine physische Festplatte nach der anderen.

ANMERKUNG: Die vollständige Initialisierung wird nur in Echtzeit unterstützt. Nur wenige Controller unterstützen eine vollständige Initialisierung.

Verschlüsseln der virtuellen Laufwerke

Wenn die Verschlüsselung auf einem Controller deaktiviert ist (d. h., der Sicherheitsschlüssel auf einem Controller wurde gelöscht), können Sie die Verschlüsselung für virtuelle Festplatten, die aus SED-Laufwerken erstellt wurden, manuell aktivieren. Falls die virtuelle Festplatte nach der Aktivierung der Verschlüsselung auf einem Controller erstellt wird, wird die virtuelle Festplatte automatisch verschlüsselt. Sie wird automatisch als verschlüsselte, virtuelle Festplatte konfiguriert, es sei denn, die aktivierte Verschlüsselungsoption wird während der Erstellung der virtuellen Festplatte deaktiviert.

Sie müssen über die Berechtigung zur Anmeldung und zur Server-Steuerung zur Verwaltung der Schlüssel für die Verschlüsselung verfügen.

Zuweisen oder Aufheben der Zuweisung von dezidierten Hotspares

Ein dedizierter Hotspare ist eine nicht verwendete Backup-Festplatte, die einer 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.

Sie müssen über Berechtigungen zum Anmelden und für die Server-Steuerung verfügen, um diesen Vorgang auszuführen.

Nur T10-PI-fähige physischen Festplatten (DIF) können als Hotspare den T10-PI-fähigen virtuellen Festplatten (DIF) zugewiesen werden. Alle nicht-T10-PI-(DIF)-fähigen -Laufwerke, die als dedizierter Hotspare zugewiesen sind, werden nicht zu einem Hotspare, wenn T10-PI-(DIF) zu einem späteren Zeitpunkt auf einem virtuellen Laufwerk aktiviert wird.

Sie können nur Festplatten mit 4 KB als Hotspare zu virtuellen 4-KB-Festplatten zuweisen.

Wenn Sie eine physische Festplatte als dediziertes Hotspare im Modus „Zu ausstehenden Vorgängen hinzufügen“ zugewiesen haben, wird der ausstehende Vorgang erstellt, jedoch kein Job. Wenn Sie versuchen, die Zuordnung des dedizierten Hotspares aufzuheben, wird der ausstehende Vorgang für das Zuweisen eines dedizierten Hotspares gelöscht.

Wenn Sie die Zuweisung einer physischen Festplatte als dediziertes Hotspare im Modus „Zu ausstehenden Vorgängen hinzufügen“ aufgehoben haben, wird der ausstehende Vorgang erstellt, jedoch kein Job. Wenn Sie versuchen, das dedizierte Hotspare zuzuweisen, wird der ausstehende Vorgang für das Aufheben der Zuweisung eines dedizierten Hotspares gelöscht.

ANMERKUNG: Solange der Protokollexport andauert, können Sie auf der Seite Virtuelle Festplatten verwalten keine Informationen zu dedizierten Hotspares anzeigen. Wenn der Protokollexport abgeschlossen ist, laden Sie die Seite Virtuelle Festplatten verwalten neu oder aktualisieren Sie sie, um die Informationen anzuzeigen.

Verwalten von virtuellen Festplatten über die Webschnittstelle

1 Gehen Sie auf der iDRAC-Webschnittstelle zu**Übersicht** > **Speicher** > **Virtuelle Festplatten** > **Verwalten** .
Die Seite **Virtuelle Festplatten verwalten** wird angezeigt.
2 Wählen Sie aus dem Drop-Down-Menü **Controller** den Controller aus, für den Sie die virtuellen Festplatten verwalten möchten.
3 Wählen Sie bei einem oder mehreren virtuellen Festplatten aus den einzelnen Dropdown-Menüs die Option **Aktion** aus.
Sie können mehrere Maßnahmen für ein virtuelles Laufwerk festlegen. Wenn Sie eine Maßnahme auswählen, wird ein zusätzliches Drop-Down-Menü **Maßnahme** angezeigt. Wählen Sie eine weitere Maßnahme aus dem Drop-Down-Menü aus. Die bereits ausgewählte Maßnahme wird im zusätzlichen Drop-Down-Menü **Maßnahme** nicht angezeigt. Außerdem wird der Link **Entfernen** neben der ausgewählten Maßnahme angezeigt. Klicken Sie auf diesen Link, um die ausgewählte Maßnahme zu entfernen.
   - **„Löschen“**

- **Bearbeiten der Regel: Lese-Cache** – Ändern Sie die Lese-Cache-Regel auf eine der folgenden Optionen:
  - **Kein Vorauslesen**
  - **Vorauslesen**
  - **Adaptives Vorauslesen**

    ANMERKUNG: Frühere Generationen von PERC-Controller unterstützen die Leserichtlinieneinstellungen Kein Vorauslesen, Vorauslesen, und Adaptives Vorauslesen. Bei PERC 8 und PERC 9 entsprechend sich die Einstellungen Vorauslesen und Adaptives Vorauslesen auf Controllerebene funktional. Zu Zwecken der Abwärtskompatibilität ermöglichen einige Systemverwaltungsschnittstellen und PERC 8 und 9-Controller weiterhin die Einstellung der Leseregel auf Adaptives Vorauslesen. Auch wenn es möglich ist, Vorauslesen oder Adaptives Vorauslesen auf PERC 8 oder PERC 9 einzustellen, hat dies keine funktionale Bedeutung.
- **Bearbeiten der Regel: Schreib-Cache** – Ändern Sie die Schreib-Cache-Regel auf eine der folgenden Optionen:
  - **Durchschreiben**
  - **Rückschreiben**
  - **Rückschreiben erzwingen**
- **Bearbeiten der Regel: Disk-Cache** – Ändern Sie die Laufwerk-Cache-Regel auf eine der folgenden Optionen:
  - **Standardeinstellung**
  - **Enabled (Aktiviert)**
  - **Disabled (Deaktiviert)**
- **Initialisieren: Schnell** – Aktualisiert die Metadaten auf den physischen Festplatten, so dass der gesamte Festplattenspeicherplatz für künftige Schreibvorgänge verfügbar ist. Die Initialisierungsoption kann schnell abgeschlossen werden, da vorhandene Informationen auf den physischen Festplatten nicht gelöscht werden, obwohl künftige Schreibvorgänge die auf den physischen Festplatten verbleibenden Informationen überschreiben werden.
- **Initialisieren: Vollständig**: Alle vorhandenen Daten und Dateisysteme werden gelöscht.

  ANMERKUNG: Die Option Initialisieren: Vollständig gilt nicht für PERC H330-Controller.
- **Übereinstimmungsüberprüfung** - Zum Überprüfen der Übereinstimmung eines virtuellen Laufwerks wählen Sie **Übereinstimmungsüberprüfung** im entsprechenden Dropdown-Menü.

  ANMERKUNG: Übereinstimmungsprüfung wird nicht unterstützt auf Laufwerken, die im RAID0-Modus eingerichtet sind.
- **Virtuelle Festplatte verschlüsseln** – Verschlüsselt die virtuelle Festplatte. Wenn der Controller verschlüsselungsfähig ist, können Sie die Sicherheitsschlüssel erstellen, ändern oder löschen.

  ANMERKUNG: Die Option Virtuelles Laufwerk verschlüsseln ist nur dann verfügbar, wenn das virtuelle Laufwerk unter Verwendung der Laufwerke mit einem selbstverschlüsselnden Laufwerk (SED, Self-Encrypting Drive) erstellt wird.
- **Verwalten von dedizierten Hotspares** – Zuweisung oder Aufhebung einer Zuweisung einer physischen Festplatte als dediziertes Hotspare. Nur die gültigen dedizierten Hotspares werden angezeigt. Wenn es keine gültigen dedizierten Hotspares gibt, wird dieser Abschnitt im Drop-Down-Menü nicht angezeigt.

Weitere Informationen zu diesen Optionen finden Sie in der *CMC-Online-Hilfe*.

4 Wählen Sie im Dropdown-Menü die Option **Betriebsmodus anwenden**, wenn Sie die Einstellungen übernehmen möchten.

5 Klicken Sie auf **Apply (Anwenden)**.

Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

Verwalten von virtuellen Festplatten über RACADM

Verwenden Sie die folgenden RACADM-Befehle, um virtuelle Festplatten zu verwalten:

- So löschen Sie eine virtuelle Festplatte:
  ```
  racadm storage deletevd:<VD FQDD>
  ```
- So initialisieren Sie eine virtuelle Festplatte:
  ```
  racadm storage init:<VD FQDD> -speed {fast|full}
  ```
- So überprüfen Sie die Übereinstimmung von virtuellen Festplatten (nicht unterstützt auf RAID0):
  ```
  racadm storage ccheck:<vdisk fqdd>
  ```

So brechen Sie die Konsistenzprüfung ab:

```
racadm storage cancelcheck: <vdisks fqdd>
```

- So verschlüsseln Sie virtuelle Festplatten:

```
racadm storage encryptvd:<VD FQDD>
```

- So weisen Sie dedizierte Hotspares zu oder machen die Zuweisung rückgängig:

```
racadm storage hotspare:<Physical Disk FQDD> -assign <option> -type dhs -vdkey: <FQDD of VD>
```

<option>=yes	Hotspare zuweisen
<Option>=no	Zuweisung von Hotspare aufheben

Verwalten von Controllern

Sie können die folgenden Schritte für Controller ausführen:

- Controller-Eigenschaften konfigurieren
- Fremdkonfigurationen importieren oder automatisch importieren
- Fremdkonfiguration löschen
- Controller-Konfiguration zurücksetzen
- Sicherheitsschlüsseln erstellen, ändern oder löschen

Zugehöriger Link

Konfigurieren der Controller-Eigenschaften
Importieren oder automatisches Importieren von Fremdkonfigurationen
Fremdkonfiguration löschen
Zurücksetzen der Controller-Konfiguration
Unterstützte Controller
Übersicht über die unterstützten Funktionen für Speichergeräte
Konvertieren einer physischen Festplatte in den RAID- und Nicht-RAID-Modus

Konfigurieren der Controller-Eigenschaften

Sie können die folgenden Eigenschaften für den Controller konfigurieren:

- Patrol Read-Modus (automatisch oder manuell)
- Patrol Read starten oder stoppen, wenn der Patrol Read-Modus manuell bedient wird
- Patrol Read – Nicht konfigurierte Bereiche
- Übereinstimmungsüberprüfungsmodus
- Copyback-Modus
- Lastausgleichsmodus
- Übereinstimmungsüberprüfungsrate
- Neuerstellungsrate
- Hintergrund-Initialisierungsrate
- Rekonstruktionsrate
- Erweiterter automatischer Fremdkonfigurationsimport
- Sicherheitsschlüssel erstellen oder ändern

Sie müssen über die Berechtigung zur Anmeldung und Server-Steuerung verfügen, um die Controller-Eigenschaften konfigurieren zu können.

Überlegungen zum Patrol Read-Modus

Patrol Read identifiziert Festplattenfehler, um Festplattenausfälle und Datenverlust oder -beschädigung zu vermeiden.

Patrol Read wird unter den folgenden Umständen nicht auf einer physischen Festplatte ausgeführt:

- Die physikalische Festplatte ist nicht in einer virtuellen Festplatte eingeschlossen oder als Hotspare zugewiesen.
- Die physikalische Festplatte ist in einer virtuellen Festplatte enthalten, die zurzeit in eines der folgenden Verfahren eingebunden ist:
  - Eine Neuerstellung
  - Eine Neukonfiguration oder ein Neuaufbau
  - Eine Hintergrundinitialisierung
  - Eine Übereinstimmungsüberprüfung

Zusätzlich wird der Patrol Read-Vorgang bei hoher E/A-Aktivität unterbrochen und wieder aufgenommen, wenn die E/A-Aktivitäten abgeschlossen sind.

ANMERKUNG: Weitere Informationen dazu, wie oft der Patrol Read-Vorgang ausgeführt wird, wenn er sich im automatischen Modus befindet, stehen in der entsprechenden Controller-Dokumentation zur Verfügung.

ANMERKUNG: Patrol Read-Modusvorgänge wie Start (Starten) und Stop (Beenden) werden nicht unterstützt, wenn keine virtuellen Festplatten auf dem Controller vorhanden sind. Sie können die Vorgänge zwar erfolgreich unter Verwendung der iDRAC-Schnittstellen aufrufen, die Vorgänge schlagen jedoch fehl, wenn die zugehörige Aufgabe gestartet wird.

Load-Balance

Die Eigenschaft für den Lastausgleich ermöglicht die automatische Nutzung beider Controller-Schnittstellen oder -Anschlüsse, die mit demselben Gehäuse verbunden sind, um E/A-Aufforderungen weiterzuleiten. Diese Eigenschaft ist nur bei SAS-Controllern verfügbar.

Hintergrund-Initialisierungsrate

Auf PERC-Controllern startet die Hintergrundinitialisierung einer redundanten, virtuellen Festplatte automatisch innerhalb von 0 bis 5 Sekunden, nachdem die virtuelle Festplatte erstellt wurde. Die Hintergrundinitialisierung einer redundanten, virtuellen Festplatte bereitet die virtuelle Festplatte darauf vor, redundante Daten beizubehalten, und verbessert die Schreibleistung. Nachdem z. B. die Hintergrundinitialisierung einer virtuellen RAID 5-Festplatte abgeschlossen ist, werden die Paritätsinformationen initialisiert. Nachdem die Hintergrundinitialisierung einer virtuellen RAID 1-Festplatte abgeschlossen ist, werden die physischen Festplatten gespiegelt.

Der Hintergrundinitialisierungsvorgang hilft dem Controller, Probleme zu identifizieren und zu korrigieren, die später mit den redundanten Daten auftreten können. In dieser Hinsicht ähnelt der Hintergrundinitialisierungsvorgang einer Übereinstimmungsüberprüfung. Die Hintergrundinitialisierung sollte ausgeführt werden können, bis sie abgeschlossen ist. Im Falle einer Unterbrechung startet die Hintergrundinitialisierung automatisch innerhalb von 0 bis 5 Minuten erneut. Einige andere Vorgänge, wie z. B. Lese- und Schreibvorgänge, sind möglich, während die Hintergrundinitialisierung ausgeführt wird. Andere Vorgänge, wie z. B. das Erstellen einer virtuellen Festplatte, können nicht gleichzeitig mit der Hintergrundinitialisierung ausgeführt werden. Diese Vorgänge verursachen das Abbrechen der Hintergrundinitialisierung.

Die Hintergrundinitialisierungsrate, konfigurierbar zwischen 0 % und 100 %, repräsentiert den Prozentsatz der Systemressourcen, die zum Ausführen der Hintergrundinitialisierung bestimmt wurden. Im Falle von 0 % hat die Hintergrundinitialisierung die niedrigste Priorität für den Controller, nimmt die meiste Zeit zur Durchführung in Anspruch und stellt die Einstellung mit dem geringsten Einfluss auf die Systemleistung dar. Eine Hintergrundinitialisierung von 0 % bedeutet nicht, dass der Ablauf angehalten oder unterbrochen wird. Bei 100 % hat die Hintergrundinitialisierung die höchste Priorität für den Controller. Die Zeit für die Hintergrundinitialisierung wird minimiert und stellt die Einstellung mit dem größten Einfluss auf die Systemleistung dar.

Übereinstimmungsüberprüfung

Bei der Übereinstimmungsüberprüfung wird die Richtigkeit der redundanten (Paritäts-)Informationen geprüft. Diese Aufgabe bezieht sich nur auf redundante, virtuelle Festplatten. Bei Bedarf können über die Übereinstimmungsüberprüfung redundante Daten neu erstellt werden. Falls die virtuelle Festplatte keine Redundanz aufweist, kann sie möglicherweise durch das Durchführen einer Übereinstimmungsüberprüfung in den betriebsbereiten Status überführt werden.

Die Übereinstimmungsüberprüfungsrate, konfigurierbar zwischen 0 % und 100 %, repräsentiert den Prozentsatz der Systemressourcen, die zum Ausführen der Übereinstimmungsüberprüfung bestimmt wurden. Im Falle von 0 % hat die Übereinstimmungsüberprüfung die niedrigste Priorität für den Controller, nimmt die meiste Zeit zur Durchführung in Anspruch und stellt die Einstellung mit dem geringsten Einfluss auf die Systemleistung dar. Eine Übereinstimmungsüberprüfungsrate von 0 % bedeutet nicht, dass die Übereinstimmungsüberprüfung angehalten oder unterbrochen wird. Bei 100 % hat die Übereinstimmungsüberprüfung die höchste Priorität für den Controller. Die Zeit für die Übereinstimmungsüberprüfung wird minimiert und stellt die Einstellung mit dem größten Einfluss auf die Systemleistung dar.

Sicherheitsschlüssel erstellen oder ändern

Bei der Konfiguration der Controller-Eigenschaften können Sie die Sicherheitsschlüssel erstellen oder ändern. Der Controller verwendet den Verschlüsselungsschlüssel, um den Zugriff auf SED-Laufwerke freizugeben oder zu sperren. Sie können nur jeweils einen Verschlüsselungsschlüssel für jeden verschlüsselungsfähigen Controller erstellen. Der Sicherheitsschlüssel wird mithilfe der Funktion „Local Key Management“ (LKM) verwaltet. LKM wird zur Generierung der Schlüssel-ID sowie des Kennworts oder Schlüssels verwendet. Diese Daten sind erforderlich, um das virtuelle Laufwerk zu sichern. Wenn Sie LKM verwenden, müssen Sie den Verschlüsselungsschlüssel erstellen, indem Sie die Verschlüsselungsschlüsselkennung und die Passphrase angeben.

Dieser Task wird auf den PERC-Hardware-Controllern, die im HBA-Modus ausgeführt werden, nicht unterstützt.

Wenn Sie den Sicherheitsschlüssel im Betriebsmodus „Zu ausstehenden Vorgängen hinzufügen“ erstellen und kein Job erstellt wurde und Sie dann den Sicherheitsschlüssel löschen, wird der Job „Ausstehende Sicherheitsschlüsselerstellung“ gelöscht.

Konfigurieren der Controller-Eigenschaften über die Webschnittstelle

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Controller** > **Setup**.
   Daraufhin wird die Seite **Controller-Setup** angezeigt.
2. Wählen Sie im Abschnitt **Controller-Eigenschaften konfigurieren** im Drop-Down-Feld **Controller** den Controller aus, den Sie konfigurieren möchten.
3. Geben Sie die erforderlichen Informationen für die verschiedenen Eigenschaften an.
   Die Spalte **Aktueller Wert** zeigt die vorhandenen Werte für jede Eigenschaft. Sie können diesen Wert ändern, indem Sie die entsprechende Option aus dem Dropdown-Menü **Aktion** für jede Eigenschaft auswählen.
   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
4. Wählen Sie im Dropdown-Menü die Option **Betriebsmodus anwenden**, wenn Sie die Einstellungen übernehmen möchten.
5. Klicken Sie auf **Anwenden**.
   Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

Konfigurieren von VR-Controller-Eigenschaften über RACADM

- So legen Sie den Patrol Read-Modus fest:

```
racadm set storage.controller.<index>.PatrolReadMode  {Automatic | Manual | Disabled}
```

- Wenn der Patrol Read-Modus auf „Manuell“ eingestellt ist, verwenden Sie die folgenden Befehle zum Starten und Beenden des Patrol Read-Modus:

```
racadm storage patrolread:<Controller FQDD> -state {start|stop}
```

> **ANMERKUNG: Patrol Read-Modusvorgänge wie „Start“ (Starten) und „Stop“ (Beenden) werden nicht unterstützt, wenn keine virtuellen Festplatten auf dem Controller vorhanden sind. Sie können die Vorgänge zwar erfolgreich unter Verwendung der iDRAC-Schnittstellen aufrufen, die Vorgänge schlagen jedoch fehl, wenn die zugehörige Aufgabe gestartet wird.**

- Um den Übereinstimmungsüberprüfungsmodus festzulegen, verwenden Sie das Objekt **Storage.Controller.CheckConsistencyMode**.
- Um den Copyback-Modus zu aktivieren oder zu deaktivieren, verwenden Sie das Objekt **Storage.Controller.CopybackMode**.
- Um den Lastausgleichsmodus zu aktivieren oder zu deaktivieren, verwenden Sie das Objekt **Storage.Controller.PossibleloadBalancedMode**.
- Um den Prozentsatz der Systemressourcen festzulegen, der für die Ausführung der Übereinstimmungsüberprüfung auf einer redundanten virtuellen Festplatte abgestellt sind, verwenden das Objekt **Storage.Controller.CheckConsistencyRate**.
- Um den Prozentsatz der Controller-Ressourcen festzulegen, der für die Neuerstellung einer fehlerhaften Festplatte abgestellt wurden, verwenden Sie das Objekt **Storage.Controller.RebuildRate**.
- Um den Prozentsatz der Controller-Ressourcen festzulegen, der für die Hintergrundinitialisierung einer virtuellen Festplatte nach deren Erstellung abgestellt wurden, verwenden Sie das Objekt **Storage.Controller.BackgroundInitializationRate**
- Um den Prozentsatz der Controller-Ressourcen festzulegen, der für die Neuerstellung einer Festplattengruppe nach dem Hinzufügen einer physischen Festplatte oder der Änderungen der RAID-Ebene einer virtuellen Festplatte in einer Festplattengruppe abgestellt wurde, verwenden Sie das Objekt **Storage.Controller.ReconstructRate**.
- Um den erweiterten automatischen Import einer Fremdkonfigurationen für den Controller zu (de-)aktivieren, verwenden Sie das Objekt **Storage.Controller.EnhancedAutoImportForeignConfig**.
- Verwenden Sie zum Erstellen, Ändern oder Löschen des Sicherheitsschlüssels zum Verschlüsseln von virtuellen Festplatten die folgenden Befehle:

```
racadm storage createsecuritykey:<Controller FQDD> -key <Key id> -passwd <passphrase>
racadm storage modifysecuritykey:<Controller FQDD> -key <key id> -oldpasswd <old passphrase> -
newpasswd <new passphrase>
racadm storage deletesecuritykey:<Controller FQDD>
```

Importieren oder automatisches Importieren von Fremdkonfigurationen

Eine Fremdkonfiguration sind Daten, die sich auf physischen Festplatten befinden, die von einem Controller zu einem anderen verschoben worden sind. Virtuelle Festplatten, die sich auf physischen Festplatten befinden, die verschoben wurden, werden als Fremdkonfiguration betrachtet.

Sie können Fremdkonfigurationen importieren, sodass virtuelle Festplatten nach dem Verschieben von physischen Festplatten nicht verloren gehen. Eine Fremdkonfiguration kann nur importiert werden, wenn sie eine virtuelle Festplatte enthält, die entweder den Zustand „Ready“ (Bereit) oder „Degraded“ (Herabgesetzt) hat, oder ein Ersatzgerät, das für eine virtuelle Festplatte bestimmt ist, die importiert werden kann oder bereits vorhanden ist.

Alle Daten der virtuellen Festplatten müssen vorhanden sein, doch wenn die virtuelle Festplatte eine redundante RAID-Stufe verwendet, dann sind die zusätzlichen redundanten Daten nicht erforderlich.

Wenn zum Beispiel die Fremdkonfiguration nur eine Seite einer Spiegelung auf einer virtuellen RAID 1-Festplatte enthält, befindet sich die virtuelle Festplatte im Zustand „Degraded“ (Herabgesetzt) und kann importiert werden. Wenn die Fremdkonfiguration nur eine physische Festplatte enthält, die ursprünglich als RAID 5 mit drei physischen Festplatten konfiguriert wurde, gilt für die virtuelle RAID 5-Festplatte der Status „Failed“ (Fehlerhaft) und sie kann nicht importiert werden.

Eine Fremdkonfiguration kann neben virtuellen Festplatten auch eine physische Festplatte enthalten, die auf einem Controller als Ersatzgerät zugewiesen wurde und dann auf einen anderen Controller verschoben wurde. Die Aufgabe zum Import einer

Fremdkonfiguration importiert die neue physische Festplatte als Ersatzgerät. Wenn die physische Festplatte auf dem vorhergehenden Controller ein dediziertes Ersatzgerät war, aber die virtuelle Festplatte, der das Ersatzgerät zugewiesen war, nicht mehr in der Fremdkonfiguration enthalten ist, wird die physische Festplatte als globales Ersatzgerät importiert.

Wenn über einen Schlüsselmanager (Local Key Manager, LKM) gesperrte Fremdkonfigurationen erkannt wurden, ist der Import von Fremdkonfigurationen in iDRAC in dieser Version nicht möglich. Sie müssen die Festplatten über die Tastenkombination STRG+R freigeben und dann den Import der Fremdkonfiguration von iDRAC fortsetzen.

Die Aufgabe zum Import einer Fremdkonfiguration wird nur angezeigt, wenn der Controller eine Fremdkonfiguration erkannt hat. Durch Überprüfung des Zustands der physischen Festplatte können Sie auch feststellen, ob eine physische Festplatte eine Fremdkonfiguration (virtuelle Festplatte oder Ersatzgerät) enthält. Wenn der Zustand der physischen Festplatte „Foreign“ (Fremd) ist, enthält die physische Festplatte sämtliche oder einige Teile einer virtuellen Festplatte oder verfügt über eine Ersatzgerätezuweisung.

ANMERKUNG: Mit der Aufgabe zum Import einer Fremdkonfiguration werden alle virtuellen Festplatten auf physischen Festplatten importiert, die dem Controller hinzugefügt wurden. Wenn mehr als eine fremde virtuelle Festplatte vorhanden ist, werden alle Konfigurationen importiert.

Der PERC9-Controller bietet Unterstützung für den automatischen Import der Fremdkonfiguration ohne weitere Benutzerinteraktion. Der automatische Import kann aktiviert oder deaktiviert werden. Wenn diese Option aktiviert ist, kann der PERC-Controller automatisch die ermittelten Fremdkonfigurationen ohne manuellen Eingriff importieren. Wenn diese Option deaktiviert ist, wird der Import einer Fremdkonfiguration von PERC nicht automatisch ausgeführt.

Sie müssen über die Berechtigung zur Anmeldung und Serversteuerung für den Import von Fremdkonfigurationen verfügen.

Dieser Task wird auf den PERC-Hardware-Controllern, die im HBA-Modus ausgeführt werden, nicht unterstützt.

ANMERKUNG: Es wird nicht empfohlen, ein externes Gehäusekabel zu entfernen, während das Betriebssystem auf dem System ausgeführt wird. Das Entfernen eines Kabels könnte zu einer Fremdkonfiguration führen, wenn die Verbindung wiederhergestellt wird.

Sie können Fremdkonfigurationen in den folgenden Fällen verwalten:

- Alle physischen Laufwerke in einer Konfiguration werden entfernt und wieder eingesetzt.
- Einige der physischen Laufwerke in einer Konfiguration werden entfernt und wieder eingesetzt.
- Alle physischen Laufwerke eines virtuellen Laufwerks werden entfernt, aber zu unterschiedlichen Zeitpunkten, und dann wieder eingesetzt.
- Die physischen Laufwerke eines nicht redundanten virtuellen Laufwerks werden entfernt.

Die folgenden Beschränkungen gelten für die physischen Laufwerke, die für den Import in Frage kommen:

- Der Laufwerksstatus einer physischen Festplatte kann sich zwischen dem Zeitpunkt des Scannens der Fremdkonfiguration und dem Zeitpunkt des tatsächlichen Imports ändern. Der Import einer Fremdkonfiguration erfolgt nur für Laufwerke, die den Status Unconfigured Good (Unkonfiguriert, Gut) aufweisen.
- Festplatten, die fehlerhaft oder offline sind, können nicht importiert werden.
- Die Firmware unterbindet den Import von mehr als acht Fremdkonfigurationen.

Importieren von Fremdkonfigurationen über die Webschnittstelle

So importieren Sie die Fremdkonfiguration:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Controller** > **Setup**.
   Daraufhin wird die Seite **Controller-Setup** angezeigt.
2. Wählen Sie im Abschnitt **Fremdkonfiguration** im Drop-Down-Menü **Controller** den Controller aus, den Sie konfigurieren möchten.
3. Wählen Sie aus dem Drop-Down-Menü **Betriebsmodus anwenden** den Zeitpunkt für den Import aus.
4. Klicken Sie auf **Fremdkonfiguration importieren**.

Basierend auf dem ausgewählten Betriebsmodus wird die Konfiguration importiert.

Um Fremdkonfigurationen automatisch zu importieren, aktivieren Sie im Abschnitt **Controller-Eigenschaften konfigurieren** die Option **Erweiterter automatischer Fremdkonfigurationsimport**, wählen Sie dann die Option **Betriebsmodus anwenden** aus, und klicken Sie auf **Anwenden**.

ANMERKUNG: Sie müssen das System neu starten, nachdem Sie die Option Erweiterter automatischer Fremdkonfigurationsimport aktiviert haben, damit die Fremdkonfigurationen importiert werden.

Importieren von Fremdkonfigurationen über RACADM

So importieren Sie die Fremdkonfiguration:

```
racadm storage importconfig:<Controller FQDD>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Fremdkonfiguration löschen

Nach dem Umsetzen einer physischen Festplatte von einem Controller zu einem anderen ist es möglich, dass die physische Festplatte eine gesamte virtuelle Festplatte oder einen Teil einer virtuellen Festplatte enthält (Fremdkonfiguration). Durch Überprüfung es Zustands der physischen Festplatte können Sie feststellen, ob eine vorher verwendete physische Festplatte eine Fremdkonfiguration (virtuelle Festplatte) enthält. Wenn der Zustand der physischen Festplatte „Fremd“ ist, enthält die physische Festplatte eine gesamte virtuelle Festplatte oder einen Teil einer virtuellen Festplatte. Sie können die Informationen zur virtuellen Festplatte von den neu verbundenen physischen Festplatten löschen.

Der Vorgang „Fremdkonfiguration löschen“ löscht dauerhaft alle Daten auf den physischen Festplatten, die dem Controller hinzugefügt wurden. Wenn mehr als eine fremde virtuelle Festplatte vorhanden ist, werden all Konfigurationen gelöscht. Es ist daher vielleicht besser, die virtuelle Festplatte zu importieren, als die Daten zu zerstören. Ein Initialisierung muss ausgeführt werden, um fremde Daten zu entfernen. Wenn Sie über eine unvollständige Fremdkonfiguration verfügen, die nicht importiert werden kann, können Sie die Option „Fremde Konfiguration löschen“ verwenden, um die Fremddaten auf den physischen Festplatten zu löschen.

Löschen von Fremdkonfigurationen über die Webschnittstelle

So löschen Sie eine Fremdkonfiguration:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Controller** > **Setup**.
   Daraufhin wird die Seite **Controller-Setup** angezeigt.
2. Wählen Sie im Abschnitt **Fremdkonfiguration** im Drop-Down-Menü **Controller** den Controller aus, für den Sie die Fremdkonfiguration löschen möchten.
3. Wählen Sie im Drop-Down-Menü die Option **Betriebsmodus anwenden** aus, wenn Sie die Daten löschen möchten.
4. Klicken Sie auf **Löschen**.
   Basierend auf dem ausgewählten Betriebsmodus werden die virtuellen Festplatten, die sich auf der physischen Festplatte befinden, gelöscht.

Löschen von Fremdkonfigurationen über RACADM

So löschen Sie eine Fremdkonfiguration:

```
racadm storage clearconfig:<Controller FQDD>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Zurücksetzen der Controller-Konfiguration

Sie können die Konfiguration für einen Controller zurücksetzen. Dieser Vorgang löscht virtuelle Festplatten auf dem Controller und macht die Zuweisung aller Ersatzgeräte rückgängig. Es werden keine Daten gelöscht, sondern es werden nur die Festplatten aus der Konfiguration entfernt. Beim Zurücksetzen der Konfiguration werden auch keine Fremdkonfigurationen entfernt. Die Echtzeit-Unterstützung dieser Funktion steht nur auf der PERC-Firmwareversion 9.1 zur Verfügung. Beim Zurücksetzen der Konfiguration werden keine Daten gelöscht. Sie können die exakt gleiche Konfiguration neu erstellen, ohne einen Initialisierungsvorgang, der dazu führen kann, dass die Daten wiederhergestellt werden. Sie müssen Berechtigungen zur Serversteuerung haben.

ANMERKUNG: Beim Zurücksetzen der Controller-Konfiguration werden keine Fremdkonfigurationen entfernt. Zum Entfernen einer Fremdkonfiguration führen Sie den Vorgang zum Entfernen einer Konfiguration aus.

Zurücksetzen der Controller-Konfiguration über die Webschnittstelle

Um einen Konfigurations-Reset durchzuführen:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Controller** > **Fehlerbehebung**.
   Daraufhin wird die Seite **Controller-Fehlerbehebung** angezeigt.
2. Wählen Sie im Drop-Down-Menü **Aktionen** die Option **Konfigurations-Reset** für einen oder mehrere Controller aus.
3. Wählen Sie für jeden Controller aus dem Drop-Down-Menü **Betriebsmodus anwenden** den Zeitpunkt für die Anwendung der Einstellungen aus.
4. Klicken Sie auf **Anwenden**.
   Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

Zurücksetzen der Controller-Konfiguration über RACADM

Um einen Konfigurations-Reset durchzuführen:

```
racadm storage resetconfig:<Controller FQDD>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Wechseln des Controller-Modus

Auf PERC 9.1-Controllern und höher können Sie die Merkmale des Controllers durch Umschalten des Modus von RAID auf HBA ändern. Der Controller funktioniert ähnlich wie ein HBA-Controller, bei dem die Treiber durch das Betriebssystem übergeben werden. Der Wechsel des Controller-Modus ist ein mehrstufiger Vorgang und erfolgt nicht in Echtzeit. Stellen Sie vor dem Ändern des Controller-Modus von RAID auf HBA Folgendes sicher:

- Der RAID-Controller unterstützt die Änderung des Controller-Modus. Die Option zum Ändern des Controller-Modus ist nicht auf Controllern verfügbar, auf denen das RAID-Merkmal eine Lizenz erfordert.
- Alle virtuellen Laufwerke müssen gelöscht oder entfernt werden.
- Hot Spares (Ersatzlaufwerke) müssen gelöscht oder entfernt werden.
- Fremde Konfigurationen müssen gelöscht oder deaktiviert werden.
- Alle physischen Festplatten in einem fehlerhaften Zustand müssen entfernt werden.
- Alle lokalen Sicherheitsschlüssel für SEDs müssen gelöscht werden.
- Auf dem Controller darf kein Cache beibehalten werden.
- Sie haben Berechtigungen zur Serversteuerung, um den Controller-Modus zu ändern.

ANMERKUNG: Stellen Sie sicher, dass Sie vor dem Ändern des Modus die Fremdkonfiguration, den Sicherheitsschlüssel, die virtuellen Festplatten und Hot Spares sichern, da die Daten gelöscht werden.

ANMERKUNG: Stellen Sie sicher, dass eine CMC-Lizenz für PERC FD33xS- und FD33xD-Speicherschlitten vorhanden ist, bevor Sie den Controller-Modus ändern. Weitere Informationen zur CMC-Lizenz für die Speicherschlitten finden Sie im *Benutzerhandbuch für Dell Chassis Management Controller Version 1.2 für PowerEdge FX2/FX2s* unter dell.com/support/manuals.

Ausnahmen beim Wechseln des Controller-Modus

Die folgende Liste enthält die Ausnahmen beim Festlegen des Controller-Modus mithilfe der iDRAC-Schnittstellen, wie z.B. Web-Schnittstelle, RACADM oder WS-MAN:

- Wenn sich der PERC-Controller im RAID-Modus befindet, müssen Sie alle virtuellen Festplatten, Ersatzgeräte, fremde Konfigurationen, Schlüssel oder beibehaltenen Cache löschen, bevor Sie ihn in den HBA-Modus umschalten.
- Während Sie den Controller-Modus einstellen, können Sie keine anderen RAID-Vorgänge konfigurieren. Beispiel: Wenn sich der PERC im RAID-Modus befindet und Sie den ausstehenden Wert des PERCs auf den HBA-Modus einstellen und Sie versuchen, das BGI-Attribut zu setzen, wird der ausstehende Wert nicht initialisiert.
- Wenn Sie den PERC-Controller vom RAID- auf den HBA-Modus umschalten, bleiben die Festplatten im Nicht-RAID-Zustand und werden nicht automatisch in den Status „Ready“ (Bereit) gesetzt. Darüber hinaus wird das **RAIDEnhancedAutoImportForeignConfig** Attribut automatisch auf „Enabled“ (**Aktiviert)** gesetzt.

Die folgende Liste enthält die Ausnahmen beim Festlegen des Controller-Modus mithilfe der Server-Konfigurationsprofil-Funktion bei Verwendung der WS-MAN- oder RACADM-Schnittstelle:

- Die Server-Profil-Funktion ermöglicht Ihnen neben der Einstellung des Controller-Modus die Konfiguration mehrerer RAID-Vorgänge. Befindet sich der PERC-Controller beispielsweise im HBA-Modus, dann können Sie die Export-.xml bearbeiten, um den Controller-Modus auf RAID zu ändern, Laufwerke in den „Ready“-Zustand zu konvertieren und virtuelle Festplatten zu erstellen.
- Beim Ändern des Modus von RAID auf HBA, wird das **RAIDaction Pseudo-**Attribut auf „update“ gesetzt ist (das Standardverhalten). Das Attribut wird ausgeführt und erstellt eine virtuelle Festplatte, die ausfällt. Der Controller-Modus wird geändert, der Auftrag wird jedoch mit Fehlern abgeschlossen. Um dieses Problem zu vermeiden, müssen Sie das RAIDaction-Attribut in der XML-Datei auskommentieren
- Wenn sich der PERC-Controller im HBA-Modus befindet, schlägt die Erstellung der virtuellen Festplatte fehl, wenn Sie die Import-Vorschau auf die zur Änderung des Controller-Modus auf RAID bearbeitete Export-XML-Datei anwenden, und versuchen eine virtuelle Festplatte zu erstellen. Die Import-Vorschau unterstützt bei einer Änderung des Controller-Modus keine Prüfung von RAID-Stacking-Vorgängen.

Umschalten des Controller-Modus unter Verwendung der iDRAC-Web-Schnittstelle

Führen Sie zum Umschalten des Controller-Modus die folgenden Schritte aus:

1. Klicken Sie in der iDRAC-Webschnittstelle auf **Übersicht** > **Speicher** > **Controller**.
2. Klicken Sie auf der Seite **Controller** auf **Controller-Modus** > **Setup**.
   Die **aktuelle Spalte Wert** zeigt die aktuelle Einstellung des Controllers an.
3. Wählen Sie im Drop-Down Menü den Controller-Modus aus, in den Sie wechseln möchten, und klicken Sie auf **Anwenden**.
   Starten Sie das System neu, um die Änderung in Kraft zu setzen.

Wechseln des Controller-Modus unter Verwendung von RACADM

Führen Sie die folgenden Befehle aus, um den Controller-Modus unter Verwendung von RACADM zu wechseln:

- So zeigen Sie den aktuellen Modus des Controllers an:

```
$ racadm get Storage.Controller.1.RequestedControllerMode[key=<Controller_FQDD>]
```

Die folgende Ausgabe wird angezeigt:

```
RequestedControllerMode = NONE
```

- So legen Sie den Controller-Modus als HBA fest:

```
$ racadm set Storage.Controller.1.RequestedControllerMode  HBA [Key=<Controller_FQDD>]
```

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

12-GB/s-SAS-HBA-Adapter-Vorgänge

Die Nicht-RAID-Controller sind die HBAs, die nicht alle RAID-Funktionen aufweisen. Diese unterstützen keine virtuellen Festplatten.

Die iDRAC-Schnittstelle unterstützt in dieser Version nur SAS-HBA-Controller mit 12 GBit/s und interne HBA-330-Controller.

Sie können die folgenden Schritte für Nicht-RAID-Controller ausführen:

- Anzeigen von Eigenschaften für Controller, physische Festplatten und Gehäuse, falls für den Nicht-RAID-Controller zutreffend, außerdem Anzeigen von Eigenschaften für EMMs, Lüfter, Netzteile und Temperatursensoren, die mit dem Gehäuse verknüpft sind. Die Eigenschaften werden basierend auf dem Controller-Typ angezeigt.
- Anzeigen von Informationen zum Bestand von Software und Hardware.
- Aktualisieren der Firmware für Gehäuse hinter dem 12 GB/s-SAS-HBA-Controller (in mehreren Stufen)
- Überwachen der Abfrage bzw. der Abfragehäufigkeit für den SMART-Trip-Status für physische Festplatten, wenn eine Änderung erkannt wurde
- Überwachen der Hotplugs für physische Festplatten oder des Entfernungsstatus für den Hotplug
- Blinken der LEDs oder Beenden des Blinkens

ANMERKUNG:

- Sie müssen den Vorgang „System-Bestandsaufnahme beim Neustart erstellen“ (CSIOR) durchführen, bevor die Inventarisierung oder Überwachung der Nicht-RAID-Controller erfolgt.
- Starten Sie das System neu, nachdem Sie die Firmware-Aktualisierung durchgeführt haben.
- Die Echtzeit-Überwachung auf SMART-fähigen Festplatten und SES-Gehäusesensoren erfolgt nur für SAS-HBA-Controller mit 12 GBit/s und interne HBA-330-Controller.

Zugehöriger Link

Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen
System-Bestandsaufnahme anzeigen
Aktualisieren der Gerätefirmware
Überwachen der voraussagenden Fehleranalyse auf Festplatten
Blinken oder Beenden des Blinkens der Komponenten-LEDs

Überwachen der voraussagenden Fehleranalyse auf Festplatten

Storage Management unterstützt die Selbstüberwachungsanalyse- und Berichttechnologie (SMART) auf physischen Festplatten, die SMART-aktiviert sind.

SMART führt eine voraussagende Fehleranalyse auf jeder Festplatte durch und sendet Warnungen, wenn ein Festplattenversagen vorhergesehen wird. Die Controller überprüfen physische Festplatten auf Fehlervoraussagen und leiten, falls Fehlervoraussagen gefunden wurden, entsprechende Informationen an iDRAC weiter. iDRAC gibt sofort eine Warnung aus.

Controller-Vorgänge im Nicht-RAID-Modus (HBA-Modus)

Wenn sich der Controller im Nicht-RAID-Modus (HBA-Modus) befindet, gilt Folgendes:

- Virtuelle Festplatten oder Hotspares sind nicht verfügbar.
- Der Sicherheitsstatus des Controllers ist deaktiviert.
- Alle physikalischen Festplatten befinden sich im Nicht-RAID-Modus.

Sie können die folgenden Vorgänge ausführen, wenn sich der Controller im Nicht-RAID-Modus befindet:

- Physische Festplatte blinken/Blinken deaktivieren.
- Konfigurieren Sie alle Eigenschaften einschließlich der folgenden:
  - Lastausgleichsmodus
  - Übereinstimmungsüberprüfungsmodus
  - Patrol Read-Modus
  - Copyback-Modus
  - Controller-Startmodus
  - Erweiterter automatischer Fremdkonfigurationsimport
  - Neuerstellungsrate
  - Übereinstimmungsüberprüfungsrate
  - Rekonstruktionsrate
  - Hintergrund-Initialisierungsrate
  - Gehäuse- oder Rückwandplatinen-Modus
  - Patrol Read – Nicht konfigurierte Bereiche
- Zeigen Sie alle Eigenschaften an, die auf einen RAID-Controller zutreffen, mit Ausnahme von virtuellen Festplatten.
- Fremdkonfiguration löschen

ANMERKUNG: Wenn ein Vorgang im Nicht-RAID-Modus nicht unterstützt wird, wird eine Fehlermeldung angezeigt.

Sie können die Gehäusetemperatursonden, Lüfter und Netzteile nicht überwachen, wenn sich der Controller im Nicht-RAID-Modus befindet.

Ausführen der RAID-Konfigurations-Jobs auf mehreren Speicher-Controllern

Während der Ausführung von Vorgängen auf mehr als zwei Speicher-Controllern über eine beliebige unterstützte Schnittstelle müssen Sie Folgendes sicherstellen:

- Führen Sie die Jobs auf jedem Controller einzeln aus. Warten Sie jedoch, bis jeder Job abgeschlossen wurde, bevor Sie mit der Konfiguration und der Erstellung des nächsten Controllers beginnen.
- Planen Sie mithilfe der Zeitplanoptionen mehrere Jobs zur Ausführung zu einem späteren Zeitpunkt.

Verwalten von PCIe-SSDs

Ein Peripheral Component Interconnect Express (PCIe)-SSD-Gerät ist ein Hochleistungs-Speichergerät, das für Lösungen konzipiert wurde, die eine niedrige Latenzzeit, hohe Eingabe-/Ausgabevorgänge pro Sekunde (IOPS) und Speicherzuverlässigkeit und Wartungsfunktionen der Unternehmensklasse erfordern. Die PCIe-SSD wurde basierend auf der Single Level Cell (SLC)- und Multi-Level-Cell (MLC)-NAND-Flash-Technologie mit einer PCIe 2.0- oder -PCIe-3.0-konformen Schnittstelle für Hochgeschwindigkeit entwickelt. iDRAC 2.20.20.20 und höhere Versionen unterstützen PCIe-SSD-Karten mit halber Baulänge und halber Baulänge (HHHL) auf Dell

PowerEdge-Rack- und -Tower-Servern der 13. Generation und Dell PowerEdge R920-Servern. Die HHHL-SSD-Karte lässt sich direkt in den PCI-Steckplatz auf den Servern einstecken, die nicht über Rückwandplatinen mit PCIe-SSD-Unterstützung verfügen. Sie können diese Karten auch auf Servern mit unterstützten Rückwandplatinen verwenden.

Über die iDRAC-Schnittstellen können Sie NVMe-PCIe-SSDs anzeigen und konfigurieren.

Es folgen die Hauptfunktionen des PCIe SSD:

- Hotplug-Fähigkeit
- Hochleistungsgerät

Das PCIe-SSD-Subsystem besteht aus der Rückwandplatine und einer PCIe Extender-Karte, die an die Rückwandplatine des Systems angefügt und PCIe-Konnektivität für bis zu vier oder acht PCIe-SSDs an der Vorderseite des Gehäuses und die PCIe-SSDs bereitstellt.

Sie können die folgenden Vorgänge für PCIe-SSDs ausführen:

- Bestandsaufnahme und die Remote-Überwachung des Status von PCIe-SSDs im Server
- Auf das Entfernen von PCIe SSD vorbereiten
- Daten sicher löschen
- Blinken oder Beenden des Blinkens für das LED-Gerät

Sie können die folgenden Vorgänge für HHHL SSDs ausführen:

- Bestandsaufnahme und Echtzeitüberwachung des HHHL SSD auf dem Server
- Laufwerkstatusbericht, wie z. B. Online, Fehlgeschlagen und Offline
- Fehlgeschlagener Kartenbericht und fehlgeschlagene Anmeldung bei iDRAC und OMSS
- Sicheres Löschen der Daten und Entfernen der Karte
- TTY Protokollberichte

ANMERKUNG: Funktionen wie Hotplug, das Vorbereiten auf das Entfernen und das Aufleuchten oder Erlöschen der Geräte-LED gelten nicht für HHHL PCIe SSD-Geräte.

Zugehöriger Link

Erstellen einer Bestandsaufnahme für und Überwachen von PCIe-SSDs
Vorbereiten auf das Entfernen von PCIe-SSDs
Löschen von Daten auf PCIe-SSD-Geräten

Erstellen einer Bestandsaufnahme für und Überwachen von PCIe-SSDs

Die folgenden Bestandsaufnahme- und Überwachungsinformationen sind für PCIe-SSDs verfügbar:

- Hardware-Informationen:
  - PCIe-SSD-Extender-Karte
  - PCIe-SSD-Rückwandplatine

    Wenn das System über eine dedizierte PC-Rückwandplatine verfügt, werden zwei FQDDs angezeigt. Ein FQDD ist für reguläre Laufwerke und das andere für SSDs. Wenn die Rückwandplatine freigegeben ist (universal), wird nur ein FQDD angezeigt.
- Die Software umfasst nur die Firmware-Version für die PCIe-SSD.

Erstellen einer Bestandsaufnahme für und Überwachen von PCIe-SSDs über die Webschnittstelle

Wenn Sie den Bestand für PCIe-SSD-Geräte erfassen und diese überwachen, gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Physische Festplatten**. Daraufhin wird die Seite **Eigenschaften** angezeigt. Bei PCIe-SSDs zeigt die Spalte **Name** die **PCIe-SSD** an. Erweitern Sie die Spalte, um die Eigenschaften anzuzeigen.

Bestandsaufnahme und Überwachung von PCIe-SSDs mithilfe von RACADM

Verwenden Sie den Befehl `racadm storage get controllers:<PcieSSD controller FQDD>` für die Bestandsaufnahme und die Überwachung von PCIe-SSDs.

Anzeigen aller PCIe-SSD-Festplatten:

```
racadm storage get pdisks
```

Anzeigen von PCIe-Extender-Karten:

```
racadm storage get controllers
```

Anzeigen von Informationen zur PCIe-SSD

```
racadm storage get enclosures
```

ANMERKUNG: Für alle genannten Befehle werden auch die PERC-Geräte angezeigt.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Vorbereiten auf das Entfernen von PCIe-SSDs

PCIe SSDs unterstützt den ordnungsgemäßen Hot Swap, was Ihnen das Hinzufügen oder Entfernen eines Geräts ermöglicht, ohne das System, auf dem die Geräte installiert sind, anzuhalten oder neu zu starten. Um Datenverlust zu vermeiden, müssen Sie die Aufgabe „Prepare to Remove“ (Zum Entfernen vorbereiten) verwenden, bevor Sie ein Gerät physisch entfernen.

Ein kontrollierter Hot-Swap-Vorgang wird nur unterstützt, wenn PCIe-SSDs auf einem unterstützten System installiert sind, auf dem ein unterstütztes Betriebssystem ausgeführt wird. Um sicherzustellen, dass Sie über die richtige Konfiguration für Ihre PCIe-SSD verfügen, lesen Sie das systemspezifische Benutzerhandbuch.

Der Vorgang „Zum Entfernen vorbereiten“ wird für PCIe SSDs auf den VMware vSphere (ESXi)-Systemen und HHHL PCIe SSD-Geräten nicht unterstützt.

ANMERKUNG: Der Vorgang „Zum Entfernen vorbereiten“ wird auf Systemen mit ESXi 6.0 mit iDRAC-Service-Modul-Version 2.1 oder höher unterstützt.

Der Vorgang „Zum Entfernen vorbereiten“ kann unter Verwendung des iDRAC-Service-Moduls in Echtzeit durchgeführt werden.

Bei der Vorbereitung auf die Entfernung werden alle im Hintergrund laufenden Aktivitäten und alle laufenden E/A-Aktivitäten angehalten, sodass das Gerät sicher entfernt werden kann. Dies führt dazu, dass die Status-LEDs am Gerät blinken. Sie können nach Initiierung der Aufgabe „Prepare to Remove“ (Zum Entfernen vorbereiten) das Gerät sicher aus dem System entfernen, wenn Folgendes zutrifft:

- Das PCIe SSD blinkt im LED-Muster sicher zu entfernen.
- Das System kann nicht mehr auf das PCIe SSD zugreifen.

Bevor Sie das PCIe-SSD auf die Entfernung vorbereiten, müssen folgende Voraussetzungen erfüllt sein:

- iDRAC-Servicemodul ist installiert.
- Lifecycle Controller ist aktiviert.
- Sie haben die Berechtigungen zur Serversteuerung sowie zur Anmeldung.

Vorbereiten zum Entfernen von PCIe-SSDs über die Webschnittstelle

So bereiten Sie die PCIe-SSD auf das Entfernen vor:

1 Wechseln Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Physische Festplatten** > **Setup**.

Daraufhin wird die Seite **Setup von physischen Festplatten** angezeigt.

2 Wählen Sie aus dem Drop-Down-Menü **Controller** den Extender aus, um die zugehörigen PCIe-SSDs anzuzeigen.

3 Wählen Sie in den Drop-Down-Menüs die Option **Zum Entfernen vorbereiten** für eine oder mehrere PCIe-SSDs aus.

Wenn Sie die Option **Zum Entfernen vorbereiten** ausgewählt haben und Sie die anderen Optionen in dem Drop-Down-Menü anzeigen möchten, wählen Sie **Maßnahme** aus, und klicken Sie dann auf das Drop-Down-Menü, um die anderen Optionen anzuzeigen.

ANMERKUNG: Stellen Sie sicher, dass iSM installiert ist und ausgeführt wird, und führen Sie den Vorgang `preparetoremove` aus.

4 Wählen Sie aus dem Drop-Down-Menü **Betriebsmodus anwenden** die Option **Jetzt anwenden** aus, um die Maßnahmen sofort anzuwenden.

Wenn Jobs zum Fertigstellen bereitstehen, ist diese Option grau unterlegt.

ANMERKUNG: Bei PCIe SSD-Geräten ist nur die Option Jetzt anwenden verfügbar. Dieser Vorgang wird im Modus „Bereitgestellt“ nicht unterstützt.

5 Klicken Sie auf **Anwenden**.

Wenn der Job nicht erstellt wird, wird eine Meldung angezeigt, die darauf hinweist, dass der Job nicht erfolgreich erstellt wurde. Die Meldungs-ID und die empfohlene Antwortmaßnahme werden ebenfalls angezeigt.

Wenn der Auftrag erfolgreich erstellt wurde, wird eine Meldung angezeigt, die angibt, dass die Job-ID für den ausgewählten Controller erstellt wurde. Klicken Sie auf **Job-Warteschlange**, um den Fortschritt des Jobs auf der Seite **Job-Warteschlange** anzuzeigen.

Wenn der ausstehende Vorgang nicht erstellt werden, wird eine Fehlermeldung angezeigt. Wenn der Vorgang erfolgreich war, die Auftragserstellung jedoch nicht, wird eine Fehlermeldung angezeigt.

Vorbereiten auf das Entfernen einer PCIe-SSD über RACADM

So bereiten Sie das PCIeSSD-Laufwerk auf das Entfernen vor:

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

So erstellen Sie den Zielauftrag nach der Ausführung des Befehls preparetoremove:

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

So fragen Sie die ausgegebene Job-ID ab:

```
racadm jobqueue view -i <job ID>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Löschen von Daten auf PCIe-SSD-Geräten

Die Option zum sicheren Löschen löscht dauerhaft alle Daten auf der Festplatte. Durch das Ausführen einer kryptografischen Löschung auf einer PCIe-SSD werden alle Blöcke überschrieben, dies führt zu einem permanentem Datenverlust auf der PCIe-SSD. Während der

kryptografischen Löschung kann der Host nicht auf die PCIe-SSD zugreifen. Die Änderungen werden nach dem Neustart des Systems angewendet.

Falls das System neu gestartet wird oder wenn während einer kryptografischen Löschung der Strom ausfällt, wird der Vorgang abgebrochen. Sie müssen das System neu starten und den Vorgang neu beginnen.

Stellen Sie vor dem Löschen von Daten auf PCIe-SSD-Geräten Folgendes sicher:

- Lifecycle Controller ist aktiviert.
- Sie haben die Berechtigungen zur Serversteuerung sowie zur Anmeldung.

ANMERKUNG:

- Das Löschen von PCIe-SSDs kann nur als ein gestufter Vorgang ausgeführt werden.
- Nachdem der Datenträger gelöscht wurde, zeigt er das Betriebssystem als online an, es ist jedoch nicht initialisiert. Sie müssen die Festplatte vor der erneuten Verwendung formatieren und initialisieren.
- Nachdem Sie eine PCIe-SSD per Hot-Plug verbunden haben, kann es einige Sekunden dauern, bis sie auf der Web-Schnittstelle angezeigt wird.
- Die Funktion für sicheres Löschen wird für per Hotplug verbundene PCIe SSD-Laufwerke nicht unterstützt.

Löschen von PCIe-SSD-Gerätedaten über die Webschnittstelle

So löschen Sie die Daten auf dem PCIe-SSD-Gerät:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Physische Festplatten** > **Setup**.

Daraufhin wird die Seite **Setup von physischen Festplatten** angezeigt.

2 Wählen Sie im Drop-Down-Menü **Controller** den Controller aus, für den Sie die zugehörigen PCIe-SSDs auswählen möchten.

3 Wählen Sie in den Drop-Down-Menüs die Option **Sicheres Löschen** für eine oder mehrere PCIe-SSDs aus.

Wenn Sie **Sicheres Löschen** ausgewählt haben und Sie die anderen Optionen im Dropdown-Menü anzeigen möchten, wählen Sie **Maßnahme** aus, und klicken Sie dann auf das Drop-Down-Menü, um die anderen Optionen anzuzeigen.

4 Wählen Sie im Dropdown-Menü **Betriebsmodus wählen** eine der folgenden Optionen aus:

- **Beim nächsten Neustart** – Wählen Sie diese Option aus, um die Maßnahmen während des nächsten Systemneustarts anzuwenden. Dies ist die Standardoption für PERC 8-Controller.
- **Zu einer geplanten Zeit** – Wählen Sie diese Option aus, um die Maßnahmen zu einem geplanten Datum und Uhrzeit anzuwenden:
  - **Startzeit** und **Endzeit** – Klicken Sie auf das Kalender-Symbol und wählen Sie die Tage aus. Wählen Sie aus dem Drop-Down-Menü das Zeitintervall. Die Maßnahme wird zwischen der Startzeit und Endzeit angewandt.
  - Wählen Sie aus dem Drop-Down-Menü den Typ des Neustarts aus:
    - Kein Neustart (manueller System-Neustart)
    - Ordentliches Herunterfahren
    - Erzwungenes Herunterfahren
    - System aus- und wieder einschalten (Hardwareneustart)

ANMERKUNG: Für PERC 8-Controller oder früher ist Ordentliches Herunterfahren die Standardoption. Für PERC-9-Controller ist Kein Neustart (manueller System-Neustart) die Standardoption.

5 Klicken Sie auf **Anwenden**.

Wenn der Job nicht erstellt wird, wird eine Meldung angezeigt, die darauf hinweist, dass der Job nicht erfolgreich erstellt wurde. Die Meldungs-ID und die empfohlene Antwortmaßnahme werden ebenfalls angezeigt.

Wenn der Auftrag erfolgreich erstellt wurde, wird eine Meldung angezeigt, die angibt, dass die Job-ID für den ausgewählten Controller erstellt wurde. Klicken Sie auf **Job-Warteschlange**, um den Fortschritt des Jobs auf der Seite Job-Warteschlange anzuzeigen.

Wenn der ausstehende Vorgang nicht erstellt werden, wird eine Fehlermeldung angezeigt. Wenn der Vorgang erfolgreich war, die Auftragserstellung jedoch nicht, wird eine Fehlermeldung angezeigt.

Löschen eines PCIe-SSD-Geräts unter Verwendung von RACADM

Zum sicheren Löschen eines PCIe-SSD-Geräts:

```
racadm storage secureerase:<PCIeSSD FQDD>
```

So erstellen Sie den Ziel-Job nach dem Ausführen des Befehls **secureerase**:

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW -e <start_time>
```

So fragen Sie die ausgegebene Job-ID ab:

```
racadm jobqueue view -i <job ID>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Verwalten von Gehäusen oder Rückwandplatinen

Sie können die folgenden Schritte für Gehäuse oder Rückwandplatinen ausführen:

- Eigenschaften anzeigen
- Universellen oder Split-Modus konfigurieren
- Steckplatzinformationen anzeigen (universell oder freigegeben)
- SGPIO-Modus festlegen

Zugehöriger Link

Übersicht über die unterstützten Funktionen für Speichergeräte
Unterstützte Gehäuse
Konfigurieren des Rückwandplatinen-Modus
Anzeigen von Universalsteckplätzen
Einrichten des SGPIO-Modus

Konfigurieren des Rückwandplatinen-Modus

Die Dell PowerEdge-Server der 13. Generation unterstützten eine neue interne Speichertopologie, in der zwei Speicher-Controller (PERCs) an eine Gruppe von internen Festplatten über eine einzige Erweiterung angeschlossen werden können. Diese Konfiguration wird für hohe Leistung verwendet und bietet Ausfallsicherheit oder Hochverfügbarkeit. Die Erweiterung teilt den internen Festplatten-Array auf die zwei Speicher-Controller auf. In diesem Modus zeigt die Erstellung der virtuellen Festplatte nur die Festplatten, an die an einen bestimmten Controller angeschlossenen sind. Es gibt keine Lizenzanforderungen für diese Funktion. Diese Funktion wird nur auf einigen Systemen unterstützt.

Die Rückwandplatine unterstützt die folgenden Modi:

- Unified-Modus – Dies ist der Standardmodus. Der primäre PERC-Controller hat Zugriff auf alle Laufwerke, die an die Rückwandplatine angeschlossen sind, selbst wenn ein zweiter PERC-Controller installiert ist.
- Split-Modus – Ein Controller hat Zugriff auf die ersten 12 Laufwerke, und der zweite Controller hat Zugriff auf die letzten 12 Laufwerke. Die Laufwerke, die an den ersten Controller angeschlossen sind, sind mit 0-11 nummeriert, während die Laufwerke, die an den zweiten Controller angeschlossen sind, mit 12-23 nummeriert sind.
- Split-Modus 4:20 – Ein Controller hat Zugriff auf die ersten 4 Laufwerke, und der zweite Controller hat Zugriff auf die letzten 20 Laufwerke. Die Laufwerke, die an den ersten Controller angeschlossen sind, sind mit 0-3 nummeriert, während die Laufwerke, die an den zweiten Controller angeschlossen sind, mit 4-23 nummeriert sind.
- Split-Modus 08:16 – Ein Controller hat Zugriff auf die ersten 8 Laufwerke, und der zweite Controller hat Zugriff auf die letzten 16 Laufwerke. Die Laufwerke, die an den ersten Controller angeschlossen sind, sind mit 0-7 nummeriert, während die Laufwerke, die an den zweiten Controller angeschlossen sind, mit 8-23 nummeriert sind.

- Split-Modus 16:8 – Ein Controller hat Zugriff auf die ersten 16 Laufwerke, und der zweite Controller hat Zugriff auf die letzten 8 Laufwerke. Die Laufwerke, die an den ersten Controller angeschlossen sind, sind mit 0-15 nummeriert, während die Laufwerke, die an den zweiten Controller angeschlossen sind, mit 16-23 nummeriert sind.
- Split-Modus 20:4 – Ein Controller hat Zugriff auf die ersten 20 Laufwerke, und der zweite Controller hat Zugriff auf die letzten 4 Laufwerke. Die Laufwerke, die an den ersten Controller angeschlossen sind, sind mit 0-19 nummeriert, während die Laufwerke, die an den zweiten Controller angeschlossen sind, mit 20-23 nummeriert sind.
- Informationen nicht verfügbar – Es sind keine Informationen zum Controller verfügbar.

Mit iDRAC kann der Split-Modus definiert werden, wenn der Expander in der Lage ist, diese Konfiguration zu unterstützen. Aktivieren Sie diesen Modus, bevor Sie den zweiten Controller installieren. iDRAC überprüft die Expander-Fähigkeit, bevor er die Konfiguration des Modus erlaubt. Es wird nicht überprüft, ob der zweite PERC-Controller vorhanden ist.

Um die Einstellung zu ändern, müssen Sie über eine Berechtigung zur Serversteuerung verfügen.

Wenn sich andere RAID-Vorgänge im Status „Ausstehend“ befinden oder ein RAID-Job geplant ist, können Sie keine Änderungen mehr am Rückwandplatinen-Modus vornehmen. Wenn diese Einstellung ausstehend ist, können Sie keine anderen RAID-Jobs planen.

ANMERKUNG:

- Warnungen werden angezeigt, wenn die Einstellung geändert wird, da die Wahrscheinlichkeit von Datenverlusten besteht.
- LC-Lösch- oder iDRAC-Reset-Vorgänge wirken sich nicht auf die Expander-Einstellung für diesen Modus aus.
- Dieser Vorgang wird nur in Echtzeit unterstützt und wird nicht bereitgestellt.
- Sie können die Konfiguration der Rückwandplatine mehrmals ändern.
- Der Splitting-Vorgang der Rückwandplatine kann zu Datenverlust oder Fremdkonfiguration führen, wenn sich die Zugehörigkeit eines Laufwerks zwischen den Controllern ändert.
- Je nach Laufwerkzugehörigkeit kann sich der Splitting-Vorgang der Rückwandplatine auf die RAID-Konfiguration auswirken.

Eine Änderung dieser Einstellung wirkt sich erst nach einem System-Reset aus. Wenn Sie vom Unified- zum Split-Modus wechseln, wird beim nächsten Systemstart eine Fehlermeldung angezeigt, da der zweite Controller keine Festplatten erkennen kann. Außerdem sieht der erste Controller eine Fremdkonfiguration. Wenn Sie den Fehler ignorieren, gehen die vorhandenen virtuellen Festplatten verloren.

Konfigurieren des Rückwandplatinen-Modus über die Webschnittstelle

So konfigurieren Sie den Rückwandplatinen-Modus über die iDRAC-Webschnittstelle:

1 Wechseln Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Speicher** > **Gehäuse** > **Setup**

Daraufhin wird die Seite **Gehäuse-Setup** angezeigt.

2 Wählen Sie aus dem Drop-Down-Menü **Controller** den Controller aus, um die zugehörigen Gehäuse zu konfigurieren.

3 Wählen Sie in der Spalte **Wert** den erforderlichen Modus für die erforderliche Rückwandplatine oder das erforderliche Gehäuse aus:

- Unified-Betrieb
- Split-Betrieb
- Split-Betrieb 4:20
- Split-Betrieb 8:16
- Split-Betrieb 16:8
- Split-Betrieb 20:4
- Informationen nicht verfügbar

4 Wählen Sie im Drop-Down-Menü **Betriebsmodus anwenden** die Option **Jetzt anwenden** aus, um die Maßnahmen umgehend anzuwenden. Klicken Sie anschließend auf **Anwenden**.

Eine Auftragskennung wird erstellt.

5 Wechseln Sie zur Seite **Job-Warteschlange**, und stellen Sie sicher, dass der Job-Status als „Abgeschlossen“ angezeigt wird.

6 Schalten Sie das System aus und wieder ein, damit die Einstellung wirksam wird.

Gehäuse über RACADM konfigurieren

Um das Gehäuse oder die Rückwandplatine zu konfigurieren, verwenden Sie den Befehl `set` bei den Objekten im **BackplaneMode**.

Gehen Sie wie folgt vor, um beispielsweise das Attribut „BackplaneMode“ in den Split-Betrieb zu setzen:

1 Führen Sie den folgenden Befehl zur Anzeige des aktuellen Rückwandplatinenmodus aus:

```
racadm get storage.enclosure.1.backplanecurrentmode
```

Das Ergebnis ist Folgendes:

```
BackplaneCurrentMode=UnifiedMode
```

2 Führen Sie den folgenden Befehl zur Anzeige des angeforderten Modus aus:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

Das Ergebnis ist Folgendes:

```
BackplaneRequestedMode=None
```

3 Geben Sie den folgenden Befehl ein, um den angeforderten Rückwandplatinen-Betrieb in den Split-Betrieb umzustellen:

```
racadm set storage.enclosure.1.backplanerequestedmode "splitmode"
```

Die Meldung wird angezeigt und besagt, dass der Befehl erfolgreich ist.

4 Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das Attribut **backplanerequestedmode** in den Split-Modus gesetzt wurde:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

Das Ergebnis ist Folgendes:

```
BackplaneRequestedMode=None (Pending=SplitMode)
```

5 Führen Sie den Befehl `storage get controllers` aus, und notieren Sie die Controller-Instanz-ID.

6 Führen Sie den folgenden Befehl aus, um einen Job zu erstellen:

```
racadm jobqueue create <controller instance ID> -s TIME_NOW --realtime
```

Daraufhin wird eine Job-ID ausgegeben.

7 Führen Sie den folgenden Befehl aus, um den Job-Status abzufragen:

```
racadm jobqueue view -i JID_xxxxxxxx
```

wobei `JID_xxxxxxxx` für die in Schritt 6 erstellte Job-ID steht.

Der Status wird als „Ausstehend“ angezeigt.

Setzen Sie die Abfrage der Job-ID fort, bis der Status „Fertig“ angezeigt wird (dieser Vorgang kann bis zu drei Minuten dauern).

8 Führen Sie den folgenden Befehl zur Anzeige des Attributwerts `backplanerequestedmode` aus:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

Das Ergebnis ist Folgendes:

```
BackplaneRequestedMode=SplitMode
```

9 Führen Sie den folgenden Befehl aus, um einen Kaltstart des Servers auszuführen:

```
racadm serveraction powercycle
```

10 Nachdem das System die Vorgänge für den Einschalt-Selbsttest (POST) und CSIOR abgeschlossen hat, geben Sie den folgenden Befehl ein, um `backplanerequestedmode` zu überprüfen:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

Das Ergebnis ist Folgendes:

```
BackplaneRequestedMode=None
```

11 Führen Sie die folgenden Schritte aus, um zu überprüfen, ob der Rückwandplatinenmodus auf Split-Modus gesetzt ist:

```
racadm get storage.enclosure.1.backplanecurrentmode
```

Das Ergebnis ist Folgendes:

```
BackplaneCurrentMode=SplitMode
```

12 Führen Sie den folgenden Befehl aus, und überprüfen Sie, dass nur 0–11-Laufwerke angezeigt werden:

```
racadm storage get pdisks
```

Weitere Informationen zu den RACADM-Befehlen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide* (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC), das unter **dell.com/idracmanuals** verfügbar ist.

Anzeigen von Universalsteckplätzen

Einige Power-Edge-Server-Rückwandplatinen der 13. Generation unterstützen sowohl SAS/SATA- als auch PCIe-SSD-Laufwerke im selben Steckplatz. Diese Steckplätze werden als Universalsteckplätze bezeichnet und sind zum primären Speicher-Controller (PERC) und einer PCIe-Extender-Karte verdrahtet. Die Rückwandplatinen-Firmware enthält Informationen zu den Steckplätzen, die diese Funktion unterstützen. Die Rückwandplatine unterstützt SAS/SATA-Laufwerke oder PCIe-SSD-Laufwerke. Normalerweise sind die vier höheren Steckplätze universell. Zum Beispiel unterstützen bei einer universellen Rückwandplatine, die 24 Steckplätze unterstützt, die Steckplätzen 0 - 19 nur SAS/SATA-Festplatten, während die Steckplätze 20 - 23 entweder SAS/SATA oder PCIe-SSD unterstützen.

Der Rollup-Funktionszustand für das Gehäuse stellt den kombinierten Status für alle Festplatten im Gehäuse bereit. Der Gehäuse-Link auf der Seite **Topologie** zeigt die gesamten Gehäuseinformationen an, und zwar unabhängig vom zugewiesenen Controller. Da die beiden Speicher-Controller (PERC und PCIe-Extender) an die gleiche Rückwandplatine angeschlossen werden können, wird nur die Rückwandplatine, die dem PERC-Controller zugewiesen ist, auf der Seite **Systembestand** angezeigt.

Auf der Seite **Speicher** > **Gehäuse** > **Eigenschaften** zeigt der Abschnitt **Übersicht über die physischen Festplatten** Folgendes:

- **Slot unbelegt** – Wenn ein Steckplatz leer ist.
- **PCIe-fähig** – Wenn keine PCIe-fähigen Steckplätzen vorhanden sind, wird diese Spalte nicht angezeigt.
- **Bus-Protokoll** – handelt es sich um eine universelle Rückwandplatine mit PCIe-SSD in einem der Steckplätze installiert, zeigt diese Spalte **PCIe** an.
- **Hotspare** – Diese Spalte ist bei PCIe-SSDs nicht verfügbar.

ANMERKUNG: Bei Universalsteckplätzen wird das so genannte Hot Swapping unterstützt. Wenn Sie eine PCIe-SSD-Festplatte entfernen möchten und sie durch eine SAS/SATA-Festplatte austauschen, stellen Sie sicher, dass Sie zuerst den Schritt „Zum Entfernen vorbereiten“ für die PCIe-SSD-Festplatte ausführen. Wenn Sie diesen Schritt nicht ausführen, treten auf dem Host-Betriebssystems möglicherweise Probleme auf, z. B. ein blauer Bildschirm, Kernel-Panic-Fehler usw.

Einrichten des SGPIO-Modus

Der Speicher-Controller kann eine Verbindung mit der Rückwandplatine im I2C-Modus (Standardeinstellung für Dell-Rückwandplatinen) oder im Serial General Purpose Input/Output (SGPIO)-Modus herstellen. Diese Verbindung wird für blinkende LEDs auf den Festplatten benötigt. Die Dell PERC-Controller und Rückwandplatinen unterstützen diese beiden Modi. Um bestimmte Channel-Adapter zu unterstützen, muss der Rückwandplatinen-Modus in den SGPIO-Modus geändert werden.

Der SGPIO-Modus wird nur für passive Rückwandplatinen unterstützt. Er wird nicht für Expander-Rückwandplatinen oder passive Rückwandplatinen im Downstream-Modus unterstützt. Die Rückwandplatinen-Firmware enthält Informationen über die Fähigkeiten, den aktuellen Status und den angeforderten Status.

Nach dem LC-Wipe-Vorgang oder dem iDRAC-Reset auf die Standardeinstellungen wird der SGPIO-Modus in den Status „Deaktiviert“ zurückgesetzt. Er vergleicht die iDRAC-Einstellung mit der Rückwandplatineneinstellung. Wenn die Rückwandplatine in den SGPIO-Modus gesetzt wurde, passt iDRAC seine Einstellung an die Einstellung der Rückwandplatine an.

Das Aus- und Einschalten des Servers ist erforderlich, damit die Änderungen der Einstellung wirksam werden.

Sie müssen über Berechtigungen zur Server-Steuerung verfügen, um diese Einstellung ändern zu können.

ANMERKUNG: Sie können den SGPIO-Modus nicht über die iDRAC-Web-Schnittstelle festlegen.

Festlegen des SGPIO-Modus über RACADM

Um den SGPIO-Modus zu konfigurieren, verwenden Sie den Befehl **set** mit den Objekten in der Gruppe **SGPIOMode**.

Wenn diese Option auf „Deaktiviert“ gesetzt ist, lautet der Modus „I2C“. Wenn diese Option aktiviert ist, wird der SGPIO-Modus verwendet.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Auswählen des Betriebsmodus zum Anwenden von Einstellungen

Beim Erstellen und Verwalten von virtuellen Festplatten, beim Einrichten von physischen Festplatten, Controllern und Gehäusen oder beim Zurücksetzen von Controllern und bevor Sie die verschiedenen Einstellungen anwenden, müssen Sie den Betriebsmodus auswählen. Das heißt, geben Sie an, wann Sie die Einstellungen anwenden möchten:

- Sofort
- Während des nächsten Systemneustarts
- Zu einem festgelegten Zeitpunkt
- Als eine ausstehende Operation, die als Stapel im Rahmen eines einzelnen Jobs angewendet werden sollen.

Auswählen des Betriebsmodus über die Webschnittstelle

So wählen Sie den Betriebsmodus aus, um die Einstellungen zu übernehmen:

1 Sie können den Betriebsmodus auswählen, wenn Sie sich auf einer der folgenden Seiten befinden:
   - **Übersicht** > **Speicher** > **Physische Festplatten** > **Setup**.
   - **Übersicht** > **Speicher** > **Virtuelle Festplatten** > **Erstellen**
   - **Übersicht** > **Speicher** > **Virtuelle Festplatten** > **Verwalten**
   - **Übersicht** > **Speicher** > **Controller** > **Setup**
   - **Übersicht** > **Speicher** > **Controller** > **Fehlerbehebung**
   - **Übersicht** > **Speicher** > **Gehäuse** > **Setup**
   - **Übersicht** > **Storage** > **Ausstehende Vorgänge**
2 Wählen Sie eine der folgenden Optionen aus dem Drop-Down-Menü **Betriebsmodus anwenden** aus:
   - **Jetzt anwenden** – Wählen Sie diese Option aus, um die Einstellungen umgehend anzuwenden. Diese Option ist nur für PERC 9-Controller verfügbar. Wenn Jobs fertig gestellt werden, wird diese Option ausgegraut dargestellt. Dieser Job dauert mindestens zwei Minuten.
   - **Beim nächsten Neustart** – Wählen Sie diese Option aus, um die Einstellungen während des nächsten Systemneustarts anzuwenden. Dies ist die Standardoption für PERC 8-Controller.
   - **Zu einer geplanten Zeit** – Wählen Sie diese Option aus, um die Einstellungen zu einem geplanten Datum und Uhrzeit anzuwenden:
     - **Startzeit** und **Endzeit** – Klicken Sie auf das Kalender-Symbol und wählen Sie die Tage aus. Wählen Sie aus dem Drop-Down-Menü das Zeitintervall. Die Einstellungen werden zwischen der Startzeit und Endzeit angewandt.
     - Wählen Sie aus dem Drop-Down-Menü den Typ des Neustarts aus:
       - Kein Neustart (manueller System-Neustart)
       - Ordentliches Herunterfahren

- Erzwungenes Herunterfahren
- System aus- und wieder einschalten (Hardwareneustart)

ANMERKUNG: Für PERC 8-Controller oder früher ist Ordentliches Herunterfahren die Standardoption. Für PERC-9-Controller ist Kein Neustart (manueller System-Neustart) die Standardoption.

- **Zu ausstehenden Vorgängen hinzufügen** – Wählen Sie diese Option aus, um einen ausstehenden Vorgang für die Anwendung der Einstellungen zu erstellen. Sie können alle offenen Vorgänge für einen Controller auf der Seite **Übersicht** > **Speicher** > **Ausstehende Vorgänge** anzeigen.

ANMERKUNG:

- Die Option **Zu ausstehenden Vorgängen hinzufügen** ist für die Seite **Ausstehende Vorgänge** und für PCIe-SSDs auf der Seite **Physische Festplatten** > **Setup** nicht verfügbar.
- Nur die Option **Jetzt anwenden** ist auf der Seite **Gehäuse-Setup** verfügbar.

3 Klicken Sie auf **Anwenden**.

Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

Auswählen des Betriebsmodus über RACADM

Um den Betriebsmodus auszuwählen, verwenden Sie den Befehl `jobqueue`.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Anzeigen und Anwenden von ausstehenden Vorgängen

Auf dieser Seite können Sie alle ausstehenden Vorgänge für den Speicher-Controller anzeigen und bestätigen. Alle Einstellungen werden gleichzeitig, mit dem nächsten Neustart oder zu einem geplanten Zeitpunkt, basierend auf den ausgewählten Optionen, angewendet. Sie können alle ausstehenden Vorgänge für einen Controller löschen. Einzelne ausstehende Vorgänge können nicht gelöscht werden.

Ausstehende Vorgänge werden auf die ausgewählten Komponenten (Controller, Gehäuse, physische Laufwerke und virtuelle Laufwerke) erstellt.

Konfigurationsaufträge werden nur auf einem Controller erstellt. Bei PCIe-SSDs wird der Job auf der PCIe-SSD-Festplatte und nicht auf dem PCIe-Extender erstellt.

Anzeigen, Anwenden oder Löschen von ausstehenden Vorgängen über die Webschnittstelle

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Storage** > **Ausstehende Vorgänge**.

Die Seite **Ausstehende Vorgänge** wird angezeigt.

2 Wählen Sie in der Dropdown-Liste **Komponente** den Controller aus, für den Sie die ausstehenden Vorgänge anzeigen, festschreiben oder löschen möchten.

Die Liste der ausstehenden Vorgänge wird für den ausgewählten Controller angezeigt.

ANMERKUNG:

- Ausstehende Vorgänge werden für das Importieren von Fremdkonfigurationen, Löschen von Fremdkonfigurationen, Vorgänge von Sicherheitsschlüsseln und das Verschlüsseln virtueller Laufwerke erzeugt. Sie werden jedoch nicht auf der Seite **Ausstehende Vorgänge** und in der Popup-Nachricht angezeigt .
- Aufträge für PCIe SSDs können nicht über die Seite **Ausstehende Vorgänge** erstellt werden.

3 Klicken Sie zum Löschen der ausstehenden Vorgänge für den ausgewählten Controller auf **Alle ausstehenden Vorgänge löschen**.

4 Wählen Sie aus dem Drop-Down-Menü eine der folgenden Optionen und klicken Sie auf **Anwenden**, um die ausstehenden Vorgänge anzuwenden:

- **Jetzt anwenden** – Wählen Sie diese Option, um die Vorgänge sofort anzuwenden. Diese Option ist nur für PERC 9-Controller mit der neusten Firmware-Version verfügbar.
- **Beim nächsten Neustart** – Wählen Sie diese Option aus, um die Vorgänge während des nächsten Systemneustarts anzuwenden. Dies ist die Standardoption für PERC 8-Controller. Diese Option ist auf PERC 8-Controllern und späteren Versionen verfügbar.
- **Zu einer geplanten Zeit** – Wählen Sie diese Option aus, um die Vorgänge zu einem geplanten Datum und Uhrzeit anzuwenden. Diese Option ist auf PERC 8-Controllern und späteren Versionen verfügbar.
  - **Startzeit** und **Endzeit** – Klicken Sie auf das Kalender-Symbol und wählen Sie die Tage aus. Wählen Sie aus dem Drop-Down-Menü das Zeitintervall. Die Maßnahme wird zwischen der Startzeit und Endzeit angewandt.
  - Wählen Sie aus dem Drop-Down-Menü den Typ des Neustarts aus:
    - Kein Neustart (manueller System-Neustart)
    - Ordentliches Herunterfahren
    - Erzwungenes Herunterfahren
    - System aus- und wieder einschalten (Hardwareneustart)

ANMERKUNG: Für PERC 8-Controller oder früher ist Ordentliches Herunterfahren die Standardoption. Für PERC-9-Controller ist Kein Neustart (manueller System-Neustart) die Standardoption.

5 Wenn der übermittelte Job nicht erstellt wird, wird eine Meldung angezeigt, die darauf hinweist, dass der Auftrag nicht erfolgreich erstellt wurde. Die Meldungs-ID und die empfohlene Antwortmaßnahme werden ebenfalls angezeigt.

6 Wenn der übermittelte Auftrag erfolgreich erstellt wurde, wird eine Meldung angezeigt, die angibt, dass die Auftragskennung für den ausgewählten Controller erstellt wurde. Klicken Sie auf **Job-Warteschlange**, um den Fortschritt des Auftrags auf der Seite **Job-Warteschlange** anzuzeigen.

Wenn sich das Löschen oder Importieren von Fremdkonfigurationen, Vorgänge für Sicherheitsschlüssel oder das Verschlüsseln von virtuellen Festplatten im Status „Ausstehend“ befindet und diese die einzigen noch ausstehenden Vorgänge sind, können Sie keinen Auftrag auf der Seite **Ausstehende Vorgänge** erstellen. Sie müssen einen beliebigen anderen Speicherkonfigurationsvorgang ausführen oder RACADM bzw. WSMAN verwenden, um den erforderlichen Konfigurationsauftrag auf dem entsprechenden Controller zu erstellen.

Sie können keine offenen Vorgänge für PCIe SSDs auf der Seite **Ausstehende Vorgänge** anzeigen oder löschen. Verwenden Sie den racadm-Befehl, um die ausstehenden Vorgänge für PCIe-SSD-Laufwerke zu löschen.

Anzeigen und Anwenden von ausstehenden Vorgänge über RACADM

Um ausstehende Vorgänge anzuwenden, verwenden Sie den Befehl **jobqueue**.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Speicher-Geräte – Szenarien des Anwenden-Vorgangs

Fall 1: Der Anwenden-Vorgang (Jetzt anwenden, Bei nächstem Neustart oder Zu geplantem Zeitpunkt) wurde ausgewählt und es sind keine ausstehenden Vorgänge vorhanden.

Wenn Sie die Option **Jetzt anwenden**, **Bei nächstem Neustart** oder **Zu geplantem Zeitpunkt** ausgewählt und dann auf **Anwenden** geklickt haben, wird zunächst der ausstehende Vorgang für den ausgewählten Speicher-Konfigurationsvorgang erstellt.

- Wenn der ausstehende Vorgang erfolgreich abgeschlossen wurde und keine vorherigen, ausstehenden Vorgänge vorhanden sind, wird die Aufgabe erstellt. Wenn die Aufgabe erfolgreich erstellt wurde, wird eine Meldung angezeigt, die besagt, dass die für das ausgewählte Gerät erstellte Aufgaben-ID angezeigt wird. Klicken Sie auf **Job Queue (Aufgabenwarteschlange)**, um den Fortschritt der Aufgabe auf der Seite **Job Queue (Aufgabenwarteschlange)** anzuzeigen. Wenn die Aufgabe nicht erstellt wird, wird eine Meldung angezeigt, die darauf hinweist, dass die Aufgabe nicht erfolgreich erstellt wurde. Die Meldungs-ID und die empfohlene Reaktionsmaßnahme werden ebenfalls angezeigt.

- Wenn der ausstehende Vorgang nicht erfolgreich erstellt wird und keine früheren ausstehenden Vorgänge vorhanden sind, wird eine Fehlermeldung mit einer ID und der empfohlenen Maßnahme als Antwort angezeigt.

Fall 2: Das Anwenden eines Vorgangs (Jetzt anwenden, Bei nächstem Neustart oder Zu geplantem Zeitpunkt) wurde ausgewählt und es sind ausstehende Vorgänge vorhanden.

Wenn Sie die Option **Jetzt anwenden**, **Bei nächstem Neustart** oder **Zu geplantem Zeitpunkt** ausgewählt und dann auf **Anwenden** geklickt haben, wird zunächst der ausstehende Vorgang für den ausgewählten Speicher-Konfigurationsvorgang erstellt.

- Wenn der ausstehende Vorgang erfolgreich erstellt wurde und ausstehende Vorgänge vorhanden sind, wird eine Meldung angezeigt.
  - Klicken Sie auf den Link **Ausstehende Vorgänge anzeigen**, um die ausstehenden Vorgänge für das Gerät anzuzeigen.
  - Klicken Sie auf **Create Job (Aufgabe erstellen)**, um eine Aufgabe für das ausgewählte Gerät zu erstellen. Wenn die Aufgabe erfolgreich erstellt wurde, wird eine Meldung angezeigt, die besagt, dass die für das ausgewählte Gerät erstellte Aufgaben-ID angezeigt wird. Klicken Sie auf **Job Queue (Aufgabenwarteschlange)**, um den Fortschritt der Aufgabe auf der Seite **Job Queue (Aufgabenwarteschlange)** anzuzeigen. Wenn die Aufgabe nicht erstellt wird, wird eine Meldung angezeigt, die darauf hinweist, dass die Aufgabe nicht erfolgreich erstellt wurde. Die Meldungs-ID und die empfohlene Reaktionsmaßnahme werden ebenfalls angezeigt.
  - Klicken Sie auf **Abbrechen**, um den Job nicht zu erstellen und auf der Seite zu bleiben und weitere Speicher-Konfigurationsvorgänge auszuführen.
- Wenn der ausstehende Vorgang nicht erfolgreich erstellt wurde und ausstehende Vorgänge vorhanden sind, wird eine Fehlermeldung angezeigt.
  - Klicken Sie auf **Ausstehende Vorgänge**, um die ausstehenden Vorgänge für das Gerät anzuzeigen.
  - Klicken Sie auf **Create Job For Successful Operations (Aufgabe für erfolgreiche Vorgänge erstellen)**, um eine Aufgabe für die vorhandenen ausstehenden Vorgänge zu erstellen. Wenn die Aufgabe erfolgreich erstellt wurde, wird eine Meldung angezeigt, die besagt, dass die für das ausgewählte Gerät erstellte Aufgaben-ID angezeigt wird. Klicken Sie auf **Job Queue (Aufgabenwarteschlange)**, um den Fortschritt der Aufgabe auf der Seite **Job Queue (Aufgabenwarteschlange)** anzuzeigen. Wenn die Aufgabe nicht erstellt wird, wird eine Meldung angezeigt, die darauf hinweist, dass die Aufgabe nicht erfolgreich erstellt wurde. Die Meldungs-ID und die empfohlene Reaktionsmaßnahme werden ebenfalls angezeigt.
  - Klicken Sie auf **Abbrechen**, um den Job nicht zu erstellen und auf der Seite zu bleiben und weitere Speicher-Konfigurationsvorgänge auszuführen.

Fall 3: „Zu ausstehenden Vorgängen hinzufügen“ wurde ausgewählt und es sind keine ausstehenden Vorgänge vorhanden.

Wenn Sie **Zu ausstehenden Vorgängen hinzufügen** ausgewählt und dann auf die Schaltfläche **Anwenden** geklickt haben, wird zuerst der ausstehende Vorgang für den ausgewählten Speicher-Konfigurationsvorgang erstellt.

- Wenn der ausstehende Vorgang erfolgreich erstellt wurde und keine ausstehende Vorgänge vorhanden sind, wird eine Informationsmeldung angezeigt:
  - Klicken Sie auf **OK**, um auf der Seite zu verbleiben und weitere Speicher-Konfigurationsvorgänge auszuführen.
  - Klicken Sie auf **Ausstehende Vorgänge**, um die ausstehenden Vorgänge für das Gerät anzuzeigen. Bis die Aufgabe auf dem ausgewählten Controller erstellt wurde, werden die ausstehenden Vorgänge nicht angewendet.
- Wenn der ausstehende Vorgang nicht erfolgreich erstellt wurde und keine ausstehende Vorgänge vorhanden sind, wird eine Fehlermeldung angezeigt.

Fall 4: „Zu ausstehenden Vorgängen hinzufügen“ wurde ausgewählt und es sind frühere ausstehende Vorgänge vorhanden.

Wenn Sie **Zu ausstehenden Vorgängen hinzufügen** ausgewählt und dann auf die Schaltfläche **Anwenden** geklickt haben, wird zuerst der ausstehende Vorgang für den ausgewählten Speicher-Konfigurationsvorgang erstellt.

- Wenn der ausstehende Vorgang erfolgreich erstellt wurde und ausstehende Vorgänge vorhanden sind, wird eine Informationsmeldung angezeigt:
  - Klicken Sie auf **OK**, um auf der Seite zu verbleiben und weitere Speicher-Konfigurationsvorgänge auszuführen.
  - Klicken Sie auf **Ausstehende Vorgänge**, um die ausstehenden Vorgänge für das Gerät anzuzeigen.
- Wenn der ausstehende Vorgang nicht erfolgreich erstellt wurde und ausstehende Vorgänge vorhanden sind, wird eine Fehlermeldung angezeigt.
  - Klicken Sie auf **OK**, um auf der Seite zu verbleiben und weitere Speicher-Konfigurationsvorgänge auszuführen.
  - Klicken Sie auf **Ausstehende Vorgänge**, um die ausstehenden Vorgänge für das Gerät anzuzeigen.

ANMERKUNG:

- Wird die Option zum Erstellen eines Jobs auf der Speicher-Konfigurationsseite zu irgendeinem Zeitpunkt nicht angezeigt, gehen Sie zu der Seite **Speicher-Überblick** > **Ausstehende Vorgänge**, um die vorhandenen ausstehenden Vorgänge anzuzeigen und erstellen Sie den Job auf dem entsprechenden Controller.
- Nur die Fälle 1 und 2 gelten für PCIe-SSD-Laufwerke. Sie können die ausstehenden Vorgänge für PCIe-SSD-Laufwerke nicht anzeigen und die Option **Add to Pending Operations (Zu ausstehenden Vorgängen hinzufügen)** ist daher nicht verfügbar. Verwenden Sie den racadm-Befehl, um die ausstehenden Vorgänge für PCIe-SSD-Laufwerke zu löschen.

Blinken oder Beenden des Blinkens der Komponenten-LEDs

Sie können eine physische Festplatte, eine virtuelle Festplatte und PCIe-SSDs innerhalb eines Gehäuses durch das Blinken einer der Leuchtdioden (LEDs) auf der Festplatte finden.

Sie müssen Anmeldeberechtigungen haben, um eine LED zu blinken oder das Blinken zu beenden.

Der Controller muss in der Lage sein, die Konfiguration in Echtzeit auszuführen. Die Echtzeit-Unterstützung dieser Funktion steht nur auf der PERC-Firmware ab Version 9.1 zur Verfügung.

ANMERKUNG: Blinken oder das Beenden des Blinkens wird für Server ohne Rückwandplatine nicht unterstützt.

Blinken oder Beenden des Blinkens der Komponenten-LEDs über die Webschnittstelle

So blinken Sie eine Komponenten-LED oder beenden Sie das Blinken:

1 Gehen Sie in der iDRAC-Webschnittstelle gemäß Ihren Anforderungen zu einer der folgenden Seiten:
   - **Übersicht** > **Speicher** > **Identifizieren** - Zeigt die Seite **Komponenten-LEDs identifizieren** an, auf der Sie die physischen Festplatten, virtuellen Festplatten oder PCIe-SSDs blinken oder das Blinken beenden können.
   - **Übersicht** > **Speicher** > **Physische Festplatten** > **Identifizieren**– Zeigt die Seite **Physische Festplatten identifizieren** an, auf der Sie die physischen Festplatten und PCIe-SSDs blinken und das Blinken beenden können.
   - **Übersicht** > **Speicher** > **Virtuelle Festplatten** > **Identifizieren**– Zeigt die Seite **Virtuelle Festplatten identifizieren** an, auf der Sie die virtuellen Festplatten blinken oder das Blinken beenden können.
2 Wenn Sie sich auf der Seite **Komponenten-LED identifizieren** befinden:
   - Aktivieren oder deaktivieren Sie alle Komponenten-LEDs – Wählen Sie die Option **Alle auswählen/abwählen** aus und klicken Sie auf **Blinken**, um das Blinken der Komponente-LEDs zu beginnen. Ebenso, klicken Sie auf **Blinken stoppen**, um das Blinken der Komponente-LEDs zu stoppen.
   - Aktivieren oder deaktivieren Sie einzelne Komponenten-LEDs – Wählen Sie eine oder mehrere Komponente(n) aus und klicken Sie auf **Blinken**, um das Blinken der Komponenten-LED(s) zu beginnen. Ebenso, klicken Sie auf **Blinken stoppen**, um das Blinken der Komponente-LEDs zu stoppen.
3 Wenn Sie sich auf der Seite **Physische Festplatten identifizieren** befinden:
   - Alle physischen Festplattenlaufwerke oder PCI-SSDs aktivieren oder deaktivieren – Wählen Sie die Option **Alle auswählen/abwählen** aus, und klicken Sie auf **Blinken**, um das Blinken der LEDs für die physischen Festplattenlaufwerke und PCIe-SSDs zu beginnen. Klicken Sie in gleicher Weise auf **Blinken stoppen**, um das Blinken der Komponente-LEDs zu stoppen.
   - Aktivieren oder deaktivieren Sie einzelne physischen Festplattenlaufwerke und PCIe-SSDs – Wählen Sie eine oder mehrere physischen Festplattenlaufwerke und PCIe-SSDs aus und klicken Sie auf **Blinken**, um das Blinken der LEDs für die physischen Festplattenlaufwerke und PCIe-SSDs zu beginnen. Ebenso, klicken Sie auf **Blinken stoppen**, um das Blinken der Komponente-LEDs zu stoppen.
4 Wenn Sie sich auf der Seite **Virtuelle Festplatte identifizieren** befinden:
   - Aktivieren oder deaktivieren Sie alle virtuellen Festplatten – Wählen Sie die Option **Alle auswählen/abwählen** aus und klicken Sie auf **Blinken**, um das Blinken der LEDs für die virtuellen Festplatten zu beginnen. Ebenso, klicken Sie auf **Blinken stoppen**, um das Blinken der Komponente-LEDs zu stoppen.

- Aktivieren oder deaktivieren Sie einzelne virtuelle Festplatten – Wählen Sie eine oder mehrere virtuelle Festplatten aus und klicken Sie auf **Blinken**, um das Blinken der LEDs für die virtuellen Festplatten zu beginnen. Ebenso, klicken Sie auf **Blinken stoppen**, um das Blinken der Komponente-LEDs zu stoppen.

Wenn die Vorgänge „Blinken“ oder „Blinken beenden“ nicht erfolgreich sind, wird eine Fehlermeldung angezeigt.

Aktivieren oder Deaktivieren der Komponenten-LEDs über RACADM

Verwenden Sie zum Aktivieren und Deaktivieren der LED-Komponenten die folgenden Befehle:

```
racadm storage blink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

```
racadm storage unblink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

14

Virtuelle Konsole konfigurieren und verwenden

Sie können die virtuelle Konsole dazu verwenden, das Remote-System zu verwalten, indem Sie Tastatur, Video und Maus auf der Management-Station verwenden, um die entsprechenden Geräte auf einem verwalteten Remote-Server zu steuern. Hierbei handelt es sich um eine Lizenzfunktion für Rack- und Tower-Server. Sie ist auf Blade-Servern standardmäßig verfügbar.

Zentrale Funktionen:

- Es können maximal sechs gleichzeitige Sitzungen einer virtuellen Konsole unterstützt werden. Alle Sitzungen zeigen dieselbe verwaltete Serverkonsole gleichzeitig an.
- Sie können die virtuelle Konsole in einem unterstützten Web-Browser starten, indem Sie Java, ActiveX oder das HTML5-Plugin verwenden.
- Wenn Sie die Sitzung einer virtuellen Konsole öffnen, zeigt der verwaltete Server nicht an, dass die Konsole umgeleitet wurde.
- Sie können mehrere Sitzungen für virtuelle Konsolen von einer einzelnen Management Station aus auf einem oder mehreren Managed Systems gleichzeitig öffnen.
- Es ist nicht möglich, zwei Sitzungen für virtuelle Konsolen von der Management Station aus über das gleiche Plugin auf dem verwalteten Server zu öffnen.
- Wenn ein zweiter Benutzer eine Virtuelle Konsole-Sitzung anfordert, wird der erste Benutzer benachrichtigt und erhält die Option, den Zugriff abzulehnen, den schreibgeschützten Zugriff zu erlauben oder vollständig freigegebenen Zugriff zu erlauben. Der zweite Benutzer wird benachrichtigt, dass ein anderer Benutzer die Steuerung übernommen hat. Wenn der erste Benutzer nicht innerhalb von 30 Sekunden antwortet, wird dem zweiten Benutzer je nach Standardeinstellung ein Zugriff gewährt. Wenn zwei Sitzungen gleichzeitig aktiv sind, sieht der erste Benutzer eine Meldung in der rechten oberen Ecke des Bildschirms, dass der zweite Benutzer eine aktive Sitzung hat. Wenn weder der erste noch der zweite Benutzer über Administratorberechtigungen verfügt, wird die Sitzung des zweiten Benutzers automatisch beendet, wenn der erste Benutzer seine aktive Sitzung beendet.

ANMERKUNG: Informationen zum Konfigurieren Ihres Browsers für den Zugriff auf die virtuelle Konsole finden Sie unter Web-Browser für die Verwendung der virtuellen Konsole konfigurieren.

Themen:

Zugehöriger Link

Web-Browser für die Verwendung der virtuellen Konsole konfigurieren
Virtuelle Konsole konfigurieren
Virtuelle Konsole starten

Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

Die folgende Tabelle listet die unterstützten Bildschirmauflösungen und entsprechenden Bildwiederholfrequenzen für die Sitzung einer virtuellen Konsole auf, die auf dem verwalteten Server ausgeführt wird.

Tabelle 40. Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

Bildschirmauflösung	Bildwiederholfrequenz (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60

Es wird empfohlen, die Bildschirmauflösung auf 1280x1024 Pixel oder höher einzustellen.

ANMERKUNG: Wenn eine virtuelle Konsolensitzung aktiv ist und ein Monitor mit niedrigerer Auflösung an die virtuelle Konsole angeschlossen wird, wird die Serverkonsolenauflösung bei Auswahl des Servers auf der lokalen Konsole eventuell zurückgesetzt. Wenn das System ein Linux-Betriebssystem ausführt, kann eine X11-Konsole auf dem lokalen Monitor u. U. nicht angezeigt werden. Drücken Sie die Tastenkombination Strg<Alt><F1> auf der virtuellen iDRAC-Konsole, um Linux auf eine Textkonsole umzustellen.

Virtuelle Konsole konfigurieren

Vor der Konfigurierung der virtuellen Konsole müssen Sie sicherstellen, dass die Management Station konfiguriert ist.

Sie können die virtuelle Konsole über die iDRAC-Webschnittstelle oder die RACADM-Befehlszeilenschnittstelle konfigurieren.

Zugehöriger Link

Web-Browser für die Verwendung der virtuellen Konsole konfigurieren
Virtuelle Konsole starten

Virtuelle Konsole über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die virtuelle Konsole über die iDRAC-Webschnittstelle:

1 Gehen Sie zu **Übersicht** > **Server** > **Virtuelle Konsole**. Daraufhin wird die Seite **Virtuelle Konsole** aufgerufen.
2 Aktivieren Sie die virtuelle Konsole, und geben Sie die erforderlichen Werte ein. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

   ANMERKUNG: Wenn Sie ein Nano-Betriebssystem verwenden, deaktivieren Sie die Funktion Automatische Systemsperrung auf der Seite Virtuelle Konsole.
3 Klicken Sie auf **Anwenden**. Die virtuelle Konsole ist damit konfiguriert.

Virtuelle Konsole über RACADM konfigurieren

Verwenden Sie zum Konfigurieren der virtuellen Konsole den Befehl **set** mit den Objekten in der Gruppe **iDRAC.VirtualConsole**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Vorschau der virtuellen Konsole

Bevor Sie die virtuelle Konsole starten, können Sie eine Vorschau des Zustands der virtuellen Konsole auf der Seite **System** > **Eigenschaften** > **Systemzusammenfassung** anzeigen. Der Abschnitt **Vorschau der virtuellen Konsole** zeigt ein Image an, das über den Zustand der virtuellen Konsole Aufschluss gibt. Das Image wird automatisch alle 30 Sekunden aktualisiert. Dies ist eine lizenzierte Funktion.

ANMERKUNG: Das Virtuelle Konsole-Bild ist nur verfügbar, wenn Sie Virtuelle Konsole aktiviert haben.

Virtuelle Konsole starten

Sie können die virtuelle Konsole über die iDRAC-Webschnittstelle oder eine URL starten.

ANMERKUNG: Starten Sie die Sitzung für eine virtuelle Konsole nicht über einen Web-Browser auf dem Managed System.

Stellen Sie vor dem Starten der virtuellen Konsole Folgendes sicher:

- Sie verfügen über Administratorrechte.
- Der Web-Browser ist für die Verwendung der Plugins HTML5, Java oder ActiveX konfiguriert.
- Die Mindestnetzwerkbandbreite von 1 MB/s ist verfügbar.

ANMERKUNG: Wenn der integrierte Video-Controller im BIOS deakiviert ist und Sie die virtuelle Konsole starten, ist der Viewer der virtuellen Konsole leer.

Während des Starts der virtuellen Konsole über einen 32-Bit- oder 64-Bit-IE-Browser verwenden Sie HTML5, oder das erforderliche Plugin (Java oder ActiveX), das im entsprechenden Browser zur Verfügung steht. Die Einstellungen in den Internetoptionen sind für alle Browser gleich.

Beim Starten der virtuellen Konsole über das Java-Plugin wird gelegentlich ein Java-Kompilierungsfehler angezeigt. Um dieses Problem zu lösen, wechseln Sie zu **Java-Systemsteuerung** > **Allgemein** > **Netzwerkeinstellungen**, und wählen Sie **Direkte Verbindung** aus.

Wenn die virtuelle Konsole für die Verwendung des ActiveX-Plugins konfiguriert wurde, scheitert möglicherweise der erste Startversuch. Der Grund dafür liegt in einer langsamen Netzwerkverbindung und einer Zeitüberschreitung nach zwei Minuten bei den temporären Anmeldeinformationen (die von der virtuellen Konsole für den Verbindungsaufbau verwendet werden). Beim Herunterladen des ActiveX-Client-Plugin wird diese Zeit möglicherweise überschritten. Nachdem Sie das Plugin erfolgreich heruntergeladen haben, können Sie die virtuelle Konsole wie gewohnt starten.

Um die virtuelle Konsole unter Verwendung des HTML5-Plugin zu starten, müssen Sie den Popupblocker deaktivieren.

Zugehöriger Link

Virtuelle Konsole über URL starten
Internet Explorer zur Verwendung des HTML-5-basierten Plug-In konfigurieren
Web-Browser für die Verwendung des Java-Plugin konfigurieren
IE für die Verwendung des ActiveX-Plugin konfigurieren
Virtuelle Konsole über die Webschnittstelle starten
Deaktivieren von Warnmeldungen beim Starten der Virtuellen Konsole oder Virtueller Datenträger mit dem Java- oder ActiveX-Plug-In
Mauszeiger synchronisieren

Virtuelle Konsole über die Webschnittstelle starten

Sie können die virtuelle Konsole wie folgt starten:

- Wechseln Sie zu **Übersicht** > **Server** > **Virtuelle Konsole**. Daraufhin wird die Seite **Virtuelle Konsole** angezeigt. Klicken Sie auf **Virtuelle Konsole starten**. Daraufhin wird der **Viewer für die virtuelle Konsole** gestartet.
- Wechseln Sie zu **Übersicht** > **Server** > **Eigenschaften**. Daraufhin wird die Seite **Systemzusammenfassung** angezeigt. Klicken Sie im Abschnitt **Vorschau auf virtuelle Konsole** auf **Starten**. Daraufhin wird der **Viewer für die virtuelle Konsole** gestartet.

Im **Viewer für die virtuelle Konsole** wird der Desktop des Remote-Systems angezeigt. Über diesen Viewer können Sie die Maus- und Tastaturfunktionen des Remote-Systems über Ihre Management Station steuern.

Es ist möglich, dass nach dem Starten der Anwendung mehrere Dialogfelder eingeblendet werden können. Um den unberechtigten Zugriff auf die Anwendung zu verhindern, müssen Sie diese Dialogfelder innerhalb von drei Minuten durchlaufen. Ansonsten werden Sie aufgefordert, die Anwendung erneut zu starten.

Wenn während des Starts des Viewers ein oder mehrere Fenster mit Sicherheitswarnungen angezeigt werden, klicken Sie zum Fortsetzen des Vorgangs auf „Ja“.

Im Viewer-Fenster werden eventuell zwei Mauszeiger angezeigt: einer für den verwalteten Server und ein anderer für Ihre Management Station. Zur Sychronisierung der Zeiger siehe Mauszeiger synchronisieren.

Virtuelle Konsole über URL starten

So starten Sie die virtuelle Konsole über die URL:

1 Öffnen Sie einen unterstützten Web-Browser, und geben Sie in das Adressfeld die folgende URL in Kleinbuchstaben ein: **https://iDRAC_ip/console**

2 Je nach Anmeldekonfiguration wird die entsprechende **Anmeldeseite** angezeigt:
- Wenn die Einmalanmeldung deaktiviert und die lokale, Active Directory-, LDAP- oder Smart-Anmeldung aktiviert ist, wird die entsprechende **Anmeldeseite** angezeigt.
- Wenn die Einmalanmeldung aktiviert ist, wird der **Viewer für die virtuelle Konsole** gestartet, und die **virtuelle Konsole** wird im Hintergrund angezeigt.

> ANMERKUNG: **Internet Explorer unterstützt die lokale, Active Directory-, LDAP-, Smart Card- und Einmalanmeldung. Firefox unterstützt die lokale, AD- und die Einmalanmeldung auf Windows-basierten Betriebssystemen und die lokale, Active Directory- und LDAP-Anmeldung auf Linux-basierten Betriebssystemen.**

> ANMERKUNG: **Wenn Sie keine Zugriffsberechtigung auf die virtuelle Konsole haben, aber berechtigt sind, auf den virtuellen Datenträger zuzugreifen, wird durch die Verwendung dieser URL anstatt der virtuellen Konsole der virtuelle Datenträger verwendet.**

Deaktivieren von Warnmeldungen beim Starten der Virtuellen Konsole oder Virtueller Datenträger mit dem Java- oder ActiveX-Plug-In

Sie können die Warnmeldungen, die beim Starten der Virtuellen Konsole oder des Virtuellen Datenträgers mit dem Java-Plug-In generiert werden, deaktivieren.

1 Anfänglich wird beim Start der Virtuellen Konsole oder des Virtuellen Datenträgers mit dem Java-Plug-In die Eingabeaufforderung zur Prüfung des Herausgebers angezeigt. Klicken Sie auf **Ja**.

Eine Zertifikat-Warnmeldung weist darauf hin, dass kein vertrauenswürdiges Zertifikat gefunden wurde.

> ANMERKUNG: **Wenn das Zertifikat im Zertifikatspeicher des Betriebssystem oder an einem zuvor vom Benutzer festgelegten Speicherort gefunden wird, wird diese Warnmeldung nicht angezeigt.**

2 Klicken Sie auf **Weiter**.

Der Viewer der Virtuellen Konsole oder des Virtuellen Datenträgers wird gestartet.

> ANMERKUNG: **Der Viewer des Virtuellen Datenträgers wird gestartet, wenn die Virtuelle Konsole deaktiviert ist.**

3 Klicken Sie im Menü **Extras** auf **Sitzungsoptionen** und anschließend auf die Registerkarte **Zertifikat**.

4 Klicken Sie auf **Pfad durchsuchen** und geben Sie einen Speicherort für das Benutzerzertifikat an, klicken Sie dann auf **Anwenden** und auf **OK**, und schließen Sie den Viewer.

5 Starten Sie die Virtuelle Konsole erneut.
6 Wählen Sie in der Zertifikat-Warnmeldung die Option **Diesem Zertifikat immer vertrauen** aus, und klicken Sie dann auf **Weiter**.
7 Beenden Sie den Viewer.
8 Wenn Sie die Virtuelle Konsole neu starten, wird die Warnmeldung nicht mehr angezeigt.

Viewer für virtuelle Konsole verwenden

Der Viewer für die virtuelle Konsole verfügt über verschiedene Steuerungen wie Maussynchronisierung, virtuelle Konsolenskalierung, Chatoptionen, Tastaturmakros, Stromversorgungsmaßnahmen, weitere Bootgeräte und Zugriff auf virtuelle Datenträger. Weitere Informationen zu diesen Funktionen finden Sie in der *iDRAC Online-Hilfe*.

ANMERKUNG: Wenn der Remote-Server ausgeschaltet wird, wird die Meldung „Kein Signal“ angezeigt.

Die Titelleiste des Virtuelle Konsole-Viewers zeigt den DNS-Namen oder die IP-Adresse des iDRAC an, mit dem Sie über die Management Station verbunden sind. Wenn der iDRAC keinen DNS-Namen hat, wird die IP-Adresse in diesem Format angezeigt:

- Für Rack- und Tower-Server:
  `<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>`
- Für Blade-Server:
  `<DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <fps>`

Gelegentlich zeigt der Viewer für die virtuelle Konsole möglicherweise Videos in geringer Qualität an. Der Grund dafür kann eine langsame Netzwerkverbindung sein, die dazu führt, dass ein oder zwei Video-Frames verloren gehen, wenn Sie die Sitzung für die virtuelle Konsole starten. Für die Übertragung aller Video-Frames und zur Verbesserung der nachfolgenden Video-Qualität müssen Sie eine der folgenden Maßnahmen ausführen:

- Klicken Sie auf der Seite **Systemzusammenfassung** unter **Vorschau für virtuelle Konsole** auf **Aktualisieren**.
- Schieben Sie im **Viewer für die virtuelle Konsole** auf der Registerkarte **Leistung** den Regler auf **Maximale Video-Qualität**.

HTML5-basierte virtuelle Konsole

ANMERKUNG: HTML-basierte virtuelle Konsole wird nur unter Windows 10 unterstützt. Sie müssen entweder Internet Explorer 11 oder Google Chrome verwenden, um diese Funktion verwenden zu können.

ANMERKUNG: Beim Verwenden von HTML5 für den Zugriff auf die virtuelle Konsole muss die Sprache für den Client mit den Spracheinstellungen des Tastaturlayouts, Betriebssystems und des Browsers übereinstimmen. Sie müssen beispielsweise überall auf US-Englisch oder eine andere unterstützte Sprache festgelegt werden.

Um die virtuelle HTML5-Konsole zu starten, müssen Sie die Funktion für die virtuelle Konsole in iDRAC auf der Seite „Virtuelle Konsole“ aktivieren und die Option **Virtueller Konsolentyp** auf HTML5 setzen.

Sie können die virtuelle Konsole mithilfe von einer der folgenden Methoden als Popup-Fenster starten:

- Klicken Sie auf der iDRAC-Startseite auf den Link **Starten**, der in der Konsolenvorschau verfügbar ist.
- Klicken Sie in iDRAC auf der Seite „Virtuelle Konsole“ auf **Virtuelle Konsole starten**.
- Geben Sie auf der iDRAC-Anmeldeseite **https//<iDRAC IP>/console** ein. Diese Methode wird als direktes Starten aufgerufen.

In der virtuellen HTML5-Konsole sind die folgenden Menüoptionen verfügbar:

- Chat
- Tastatur
- Bildschirmerfassung
- Aktualisieren
- Vollbildschirm

- Verbindung des Anzeigeprogramms abbrechen
- Konsolensteuerung
- Virtueller Datenträger

Die Option **Pass all keystrokes to server Alle Tastenanschläge an den Server** (Alle Tastaturbefehle an Server übergeben) wird in der virtuellen HTML5-Konsole nicht unterstützt. Verwenden Sie Tastatur und Tastaturmakros für alle Funktionstasten.

- Konsolensteuerung – Dieses Element bietet die folgenden Konfigurationsoptionen:
  - Tastatur
  - Tastaturmakros
  - Aspekt-Verhältnis
  - Berührungsmodus
  - Mausbeschleunigung
- Tastatur – Diese Tastatur verwendet Open-Source-Code. Der Unterschied zu einer physischen Tastatur besteht darin, dass die Nummerntasten auf Sonderzeichen umgeschaltet werden, wenn die **Feststelltaste** aktiviert ist. Die Funktionalität bleibt beim Drücken der Tasten für Sonderzeichen dieselbe und die Zahl wird entsprechend eingegeben, wenn die **Feststelltaste** aktiviert ist.
- Tastaturmakros – Diese werden in der virtuellen HTML5-Konsole unterstützt und als folgende Drop-Down-Optionen aufgeführt. Klicken Sie auf **Apply** (Anwenden), um die ausgewählte Tastenkombination auf dem Server anzuwenden.
  - Strg+Alt+Entf
  - Alt+Tab
  - Alt+Esc
  - Strg+Esc
  - Alt+Leertaste
  - Alt+Eingabe
  - Alt+Bindestrich
  - Alt+F4
  - Druck
  - Alt+Druck
  - <F1>
  - Pause
  - Tab
  - Strg+Eingabe
  - SysRq
  - Alt+SysRq
- Seitenverhältnis – In der virtuellen HTML-5 Konsole wird die Größe des Videobilds automatisch angepasst, damit das Bild angezeigt werden kann. Es werden folgende Konfigurationsoptionen in der Drop-Down-Liste angezeigt:
  - Wartung
  - Keine Wartung

  Klicken Sie auf **Anwenden**, um die ausgewählten Einstellungen auf den Server anzuwenden.
- Touch-Modus – Die virtuelle HTML5-Konsole unterstützt die Touchfunktion. Es werden folgende Konfigurationsoptionen in der Drop-Down-Liste angezeigt:
  - Direkt
  - Relativ

  Klicken Sie auf **Anwenden**, um die ausgewählten Einstellungen auf den Server anzuwenden.
- Mausbeschleunigung – Wählen Sie die Mausbeschleunigung je nach Betriebssystem. Es werden folgende Konfigurationsoptionen in der Drop-Down-Liste angezeigt:
  - Absolut (Windows, neueste Versionen von Linux, Mac OS-X)
  - Relativ, keine Beschleunigung

- Relativ (RHEL, frühere Versionen von Linux)
- Linux RHEL 6.x und SUSE Linux Enterprise Server 11 oder höher

Klicken Sie auf **Anwenden**, um die ausgewählten Einstellungen auf den Server anzuwenden.

- Virtueller Datenträger – Klicken Sie auf die Option **Connect Virtual Media** (Virtuellen Datenträger verbinden), um die virtuelle Datenträgersitzung zu starten. Im Menü für virtuellen Datenträger wird die Option **Browse** (Durchsuchen) zum Durchsuchen und Zuweisen der ISO- und IMG-Dateien angezeigt.

ANMERKUNG: Sie können keine physischen Datenträger, wie USB-basierte Laufwerke, CDs oder DVSs, unter Verwendung der virtuellen HTML5-Konsole zuordnen.

Unterstützte Browser

Die virtuelle HTML5-Konsole wird auf folgenden Browsern unterstützt:

- Internet Explorer 11
- Chrome 36

Weitere Informationen zu den unterstützten Browsern und Versionen finden Sie in den *iDRAC Release Notes* (iDRAC -Versionshinweisen) unter **dell.com/idracmanuals**.

Mauszeiger synchronisieren

Wenn Sie über die virtuelle Konsole eine Verbindung zu einem Managed System herstellen, wird die Mausbeschleunigungsgeschwindigkeit auf dem Managed System möglicherweise nicht mit dem Mauszeiger auf der Management Station synchronisiert, so dass möglicherweise zwei Mauszeiger im Fenster „Viewer“ angezeigt werden.

Stellen Sie bei der Verwendung von Red Hat Enterprise Linux oder Novell SUSE Linux sicher, dass der Mausmodus für Linux konfiguriert ist, bevor Sie den Viewer der virtuellen Konsole starten. Die Standardmauseinstellungen des Betriebssystems werden zum Steuern des Mauspfeils auf dem Viewer der virtuellen Konsole verwendet.

Wenn auf dem Viewer für die virtuelle Konsole des Clients zwei Mauszeiger sichtbar sind, weist dies darauf hin, dass das Betriebssystem des Servers die relative Positionierung unterstützt. Dies ist typisch für Linux-Betriebssysteme oder den Lifecycle Controller und verursacht zwei Mauszeiger, wenn sich die Einstellungen für die Mausbeschleunigung von denen des virtuellen Konsolen-Clients unterscheiden. Um dieses Problem zu beheben, wechseln Sie auf einen einzelnen Cursor oder passen Sie die Mausbeschleunigung des verwalteten Systems an die Beschleunigung der Management Station an:

- Um auf einen einzigen Cursor zu wechseln, wählen Sie im Menü **Hilfsprogramme Ein Cursor** aus.
- Um die Mausbeschleunigung einzustellen, gehen Sie zu **Hilfsprogramme** > **Sitzungsoptionen** > **Maus**. Wählen Sie in der Registerkarte **Mausbeschleunigung** je nach Betriebssystem **Windows** oder **Linux** aus.

Um den Modus mit nur einem Cursor zu beenden, drücken Sie <F9> oder die konfigurierte Beendigungstaste.

ANMERKUNG: Dies gilt nicht für verwaltete Systeme, die auf Windows-Betriebssystemen ausgeführt werden, da diese die Absolutposition unterstützen.

Wenn Sie die virtuelle Konsole verwenden, um eine Verbindung zu einem verwalteten System mit einem kürzlich installierten Linux-Betriebssystem herzustellen, können Probleme bei der Maussynchronisierung auftreten. Grund dafür kann die Funktion der vorhersehbaren Zeigerbeschleunigung des GNOME-Desktops sein. Zur korrekten Maussynchronisierung in der virtuellen Konsole von iDRAC muss diese Funktion deaktiviert sein. Um die vorhersehbare Zeigerbeschleunigung zu deaktivieren, fügen Sie im Abschnitt „Maus“ der Datei **/etc/X11/xorg.conf** Folgendes hinzu:

```
Option "AccelerationScheme" "lightweight".
```

Treten die Synchronisierungsprobleme weiterhin auf, nehmen Sie zusätzlich in der Datei **<user_home>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml** folgende Änderung vor:

Ändern Sie die Werte für `motion_threshold` und `motion_acceleration` in `-1`.

Wenn Sie die Mausbeschleunigung auf dem GNOME-Desktop ausschalten, gehen Sie im Viewer für die virtuelle Konsole zu **Extras** > **Sitzungsvorgänge** > **Maus**. Wählen Sie auf der Registerkarte **Mausbeschleunigung** die Option **Keine** aus.

Für den exklusiven Zugriff auf die Konsole des verwalteten Servers müssen Sie die lokale Konsole deaktivieren und die Anzahl für **Max. Sitzungen** auf der Seite **Virtuelle Konsole** auf `1` setzen.

Weitergeben aller Tastenanschläge über die virtuelle Konsole für Java- oder ActiveX-Plugin

Sie können die Option **Alle Tastenanschläge an den Server senden** aktivieren und alle Tastenanschläge und Tastenkombinationen von der Management Station an das Managed System durch den Virtual Console Viewer senden. Wenn dieser nicht aktiviert ist, werden alle Tastenkombinationen an die Management Station gesendet, wo die Sitzung der virtuellen Konsole ausgeführt wird. Um alle Tastenanschläge an den Server zu senden, wechseln Sie im Viewer für die virtuelle Konsole zur Registerkarte **Extras** > **Sitzungsoptionen** > **Allgemein**, und wählen Sie die Option **Alle Tastenanschläge an den Server senden** aus, um die Tastenanschläge der Management Station an das Managed System zu leiten.

Das Verhalten der Funktion „Alle Tastenanschläge an den Server senden“ hängt von den folgenden Aspekten ab:

- Plugin-Typ (Java oder ActiveX), auf Basis dessen die Sitzung für die virtuelle Konsole gestartet wird.
  Für den Java Client muss die systemeigene Bibliotheken geladen sein, damit die Modi „Alle Tastenanschläge an den Server senden“ und „Single Cursor“ funktionieren. Wenn die systemeigenen Bibliotheken nicht geladen sind, dann sind die Optionen **Alle Tastenanschläge an den Server senden** und **Single Cursor** nicht ausgewählt. Wenn Sie eine dieser Optionen dennoch auswählen, wird eine Fehlermeldung angezeigt, die darauf hinweist, dass die ausgewählten Optionen nicht unterstützt werden.

  Für den ActiveX Client muss die systemeigene Bibliothek geladen sein, damit die Option „Alle Tastenanschläge an den Server senden“ funktioniert. Wenn die systemeigenen Bibliotheken nicht geladen sind, wird die Auswahl für die Option **Alle Tastenanschläge an den Server senden** aufgehoben. Wenn Sie die Option dennoch auswählen, wird eine Fehlermeldung angezeigt, die darauf hinweist, dass die ausgewählte Funktion nicht unterstützt wird.

  Aktivieren Sie für Mac OS die Option **Zugriff für Hilfsgeräte aktivieren** im Fenster **Universeller Zugriff**, damit die Funktion „Alle Tastenanschläge an den Server senden“ aktiviert ist.
- Betriebssystem, das auf der Management Station und dem Managed System ausgeführt wird. Die Tastenkombinationen, die für das Betriebssystem auf der Management Station von Bedeutung sind, werden nicht an das Managed System weitergeleitet.
- Modus für den Viewer für die virtuelle Konsole – Fensteransicht oder Vollbildschirm.
  Im Vollbildschirmmodus ist die Funktion **Alle Tastenanschläge an den Server senden** standardmäßig aktiviert.

  Im Fenstermodus werden die Tastenanschläge nur weitergeleitet, wenn der Viewer für die virtuelle Konsole sichtbar und aktiv ist.

  Wenn Sie vom Fenster- in den Vollbildschirmmodus wechseln, wird der vorherige Status der Funktion „Alle Tastenanschläge an den Server senden“ wieder aufgenommen.

Zugehöriger Link

Java-basierte Sitzung für die virtuelle Konsole, die auf dem Windows-Betriebssystem ausgeführt wird
Java-basierte Sitzung für virtuelle Konsole, die auf dem Linux-Betriebssystem ausgeführt wird
ActiveX-basierte Sitzung für virtuelle Konsole, die auf dem Windows-Betriebssystem ausgeführt wird

Java-basierte Sitzung für die virtuelle Konsole, die auf dem Windows-Betriebssystem ausgeführt wird

- Die Tastenkombination „Strg+Alt+Entf“ wird nicht an das Managed System gesendet, sie wird jedoch immer durch Management Station interpretiert.

- Wenn die Option „Alle Tastenanschläge an den Server senden“ aktiviert ist, werden die folgenden Tastenkombinationen nicht an das verwaltete System gesendet:
  - Zurück (Browser) - Taste
  - Vor (Browser) – Taste
  - Aktualisierung (Browser) – Taste
  - Stopp (Browser) – Taste
  - Suchen (Browser) – (Taste)
  - Favoriten (Browser) – Taste
  - Start- und Startseite (Browser) – Taste
  - Stumm – Taste
  - Leiser – Taste
  - Lauter – Taste
  - Nächster Titel – Taste
  - Vorheriger Titel – Taste
  - Datenträger anhalten – Taste
  - Datenträger abspielen/anhalten – Taste
  - E-Mail starten – Taste
  - Datenträger starten – Taste
  - Anwendung 1 starten – Taste
  - Anwendung 2 starten – Taste
- Es werden alle einzelnen Tastenanschläge (keine Kombination aus verschiedenen Tasten, sondern einzelne Tastenanschläge) an das Managed System gesendet. Dazu gehören auch alle Funktionstasten sowie die Umschalt-, Alt-, Strg- und Menütasten. Einige dieser Tasten wirken sich sowohl auf der Management Station als auch auf dem Managed System aus.

  Wenn die Management Station und das Managed System beispielsweise unter einem Windows-Betriebssystem laufen und die Option „Alle Tastenanschläge weiterreichen“ deaktiviert ist, und wenn Sie die Windows-Taste zum Öffnen des **Startmenüs** drücken, wird das **Startmenü** auf der Management Station und auf dem Managed System geöffnet. Wenn die Option „Alle Tastenanschläge weiterreichen“ allerdings aktiviert ist, wird das **Startmenü** nur auf dem Managed System geöffnet, nicht aber auf der Management Station.
- Wenn die Option „Alle Tastenanschläge weiterreichen“ deaktiviert ist, hängt das Verhalten von den gedrückten Tastenkombinationen und den speziellen Tastenkombinationen ab, die durch das Betriebssystem auf der Management Station interpretiert werden.

Java-basierte Sitzung für virtuelle Konsole, die auf dem Linux-Betriebssystem ausgeführt wird

Das für das Windows-Betriebssystem dargestellte Verhalten gilt auch für das Linux-Betriebssystem, jedoch mit den folgenden Ausnahmen:

- Wenn die Option „Alle Tastenanschläge an den Server senden“ aktiviert ist, wird die Tastenkombination „<Strg+Alt+Entf>“ an das Betriebssystem auf dem Managed System weitergeleitet.
- Die magischen S-Abf-Tasten sind Tastenkombinationen, die durch den Linux-Kernel interpretiert werden. Diese sind nützlich, wenn das Betriebssystem auf der Management Station oder dem Managed System nicht mehr reagiert und Sie das System daher wiederherstellen müssen. Sie können die magischen S-Abf-Tasten auf dem Linux-Betriebssystem über eines der folgenden Verfahren aktivieren:
  - Fügen Sie einen Eintrag zu „**/etc/sysctl.conf**“ hinzu.
  - echo "1" > /proc/sys/kernel/sysrq
- Wenn die Option „Alle Tastenanschläge an den Server senden“ aktiviert ist, werden die magischen S-Abf-Tasten an das Betriebssystem auf dem Managed System weitergeleitet. Das Tastensequenzverhalten in Bezug auf das Zurücksetzen des Betriebssystems, also ein Neustart ohne Un-Mounten oder Synchronisieren, hängt davon ab, ob die magische S-Abf-Taste auf der Management Station aktiviert sind:
  - Ist die magische S-Abf-Taste auf der Management Station aktiviert, wird die Management Station über die Tastenkombinationen „<Strg+Alt+S-Abf+b>“ oder „<Alt+S-Abf+b>“, ungeachtet vom Status des Systems, zurückgesetzt.

- Ist die magische S-Abf-Taste auf der Management Station deaktiviert, wird das Betriebssystem auf dem Managed System über die Tastenkombinationen „<Strg+Alt+S-Abf+b>“ oder „<Alt+S-Abf+b>“ zurückgesetzt.
- Weitere S-Abf-Tastenkombinationen (z. B. „<Alt+S-Abf+k>“, „<Strg+Alt+S-Abf+m>“, usw.) werden unabhängig davon, ob die S-Abf-Tasten auf der Management Station aktiviert sind, an das Managed System weitergeleitet.

Verwenden der magischen S-Abf-Tasten über die Remote-Konsole

Sie können die magischen S-Abf-Tasten über die Remote-Konsole über eine der folgenden Optionen aktivieren:

- Opensoure-IPMI-Tool
- Verwenden von SSH/Telnet oder External Serial Connector

Verwenden des Opensource-IPMI-Hilfsprogramms

Stellen Sie sicher, dass die BIOS/iDRAC-Einstellungen die Konsolenumleitung über SOL unterstützen.

1 Führen Sie an der Eingabeaufforderung den folgenden Befehl zum Aktivieren von SOL aus:

```
Ipmitool –I lanplus –H <ipaddr> -U <username> -P <passwd> sol activate
```

Die SOL-Sitzung wird aktiviert.

2 Nachdem der Server auf das Betriebssystem gestartet wurde, wird die Anmeldeaufforderung `localhost.localdomain` angezeigt. Melden Sie sich unter Verwendung des Benutzernamens und des Kennworts an.

3 Wenn die S-Abf-Funktion nicht aktiviert ist, aktivieren Sie sie über den Befehl `echo 1 >/proc/sys/kernel/sysrq`.

4 Führen Sie eine Break-Sequenz mit dem Befehl `~B` aus.

5 Verwenden Sie die magische S-Abf-Taste, um die Abf-Funktion zu aktivieren. Beispiel: Der folgende Befehl zeigt die Arbeitspeicherinformationen auf der Konsole an:

```
echo m > /proc/sysrq-trigger displays
```

Verwenden von SSH oder Telnet oder externen seriellen Anschlüssen – direkte Verbindung über serielles Kabel

1 Führen Sie bei Telnet/SSH-Sitzungen nach dem Anmelden über den iDRAC-Benutzernamen und das Kennwort bei der `/admin>`-Eingabeaufforderung den Befehl `console com2` aus. Die `localhost.localdomain`-Eingabeaufforderung wird angezeigt.

2 Bei der Konsolenumleitung über den externen seriellen Anschluss mit direkter Verbindung zum System über ein serielles Kabel wird die Anmeldeaufforderung `localhost.localdomain` angezeigt, nachdem der Server auf das Betriebssystem gestartet wurde.

3 Melden Sie sich unter Verwendung des Betriebssystembenutzernamens und -kennworts an.

4 Sollte die S-Abf-Taste nicht aktiviert sein, aktivieren Sie sie über `echo 1 >/proc/sys/kernel/sysrq`

5 Verwenden Sie die magische Taste, um die S-Abf-Funktion zu aktivieren. Durch den folgenden Befehl wird beispielsweise der Server neu gestartet:

```
echo b > /proc/sysrq-trigger
```

ANMERKUNG: Sie müssen die Break-Sequenz erst nach der Verwendung der magischen S-Abf-Tasten ausführen.

ActiveX-basierte Sitzung für virtuelle Konsole, die auf dem Windows-Betriebssystem ausgeführt wird

Das Verhalten der Funktion „Alle Tastenanschläge an den Server senden“ in einer ActiveX-basierten Sitzung für die virtuelle Konsole, die unter dem Windows-Betriebssystem ausgeführt wird, ähnelt dem Verhalten, das in Bezug auf die Java-basierte Sitzung für die virtuelle Konsole erläutert wurde, die auf der Windows-Management Station ausgeführt wird. Es gelten allerdings die folgenden Ausnahmen:

- Wenn die Funktion „Alle Tastenanschläge senden“ deaktiviert ist, wird durch Drücken der Taste F1 die Hilfe-Anwendung auf der Management Station und auf dem Managed System gestartet, und es wird die folgende Meldung angezeigt:

  `Click Help on the Virtual Console page to view the online Help`

- Die Datenträger-Tasten sind möglicherweise nicht ausdrücklich blockiert.
- Die Tastenkombinationen <Alt + Leer>, <Strg + Alt + +> und <Strg + Alt + -> werden nicht an das Managed System gesendet und werden durch das Betriebssystem auf der Management Station interpretiert.

15

Virtuelle Datenträger verwalten

Der virtuelle Datenträger ermöglicht dem verwalteten Server, auf Datenträgergeräte der Management Station oder auf ISO-CD/DVD-Images einer Netzwerkfreigabe zuzugreifen, als wären sie Geräte auf dem verwalteten Server.

Über die Funktion für den virtuellen Datenträger können Sie die folgenden Schritte ausführen:

- Remote auf Datenträger zugreifen, die über das Netzwerk mit einem Remote-System verbunden sind
- Anwendungen installieren
- Treiber aktualisieren
- Ein Betriebssystem auf dem Managed System installieren

Hierbei handelt es sich um eine Lizenzfunktion für Rack- und Tower-Server. Sie ist standardmäßig für Blade-Server verfügbar.

Zentrale Funktionen:

- Der virtuelle Datenträger unterstützt virtuelle optische Laufwerke (CD/DVD), Floppy-Laufwerke (einschließlich USB-basierte Laufwerke) und USB-Flash-Laufwerke.
- Sie können nur ein Floppy-Laufwerk, ein USB-Flash-Laufwerk, ein Image oder einen Schlüssel und nur ein optisches Laufwerk auf der Management Station mit einem Managed System verbinden. Unterstützte Floppy-Laufwerke umfassen ein Floppy-Image oder ein verfügbares Floppy-Laufwerk. Unterstützte optische Laufwerke umfassen maximal ein verfügbares optisches Laufwerk oder eine einzige ISO-Imagedatei.

  Die folgende Abbildung zeigt ein typisches Setup für einen virtuellen Datenträger.
- Es ist nicht möglich, über virtuelle Computer auf den virtuellen Floppy-Datenträger von iDRAC zuzugreifen.
- Alle verbundenen virtuellen Datenträger emulieren ein physisches Laufwerk auf dem Managed System.
- Auf Windows-basierten, verwalteten Systemen werden die Laufwerke der virtuellen Datenträger automatisch geladen, wenn sie angeschlossen und mit einem Laufwerkbuchstaben konfiguriert sind.
- Auf Linux-basierten Managed Systems mit bestimmten Konfigurationen werden die virtuellen Datenträgerlaufwerke nicht automatisch gemountet. Verwenden Sie zum manuellen Mounten der Laufwerke den Mount-Befehl.
- Alle Zugriffsanforderungen werden auf den virtuellen Datenträger vom verwalteten System über das Netzwerk zur Management Station geleitet.
- Die virtuellen Geräte werden als zwei Laufwerke auf dem Managed System angezeigt, ohne dass der Datenträger auf den Laufwerken installiert ist.
- Sie können zwar das (schreibgeschützte) CD/DVD-Laufwerk zwischen zwei Managed Systems auf der Management Station freigeben, nicht aber den USB-Datenträger.
- Virtuelle Datenträger erfordern eine verfügbare Netzwerkbandbreite von mindestens 128 Kbit/s.
- Wenn LOM- oder NIC-Failovers auftreten, wird die Sitzung für den virtuellen Datenträger möglicherweise getrennt.

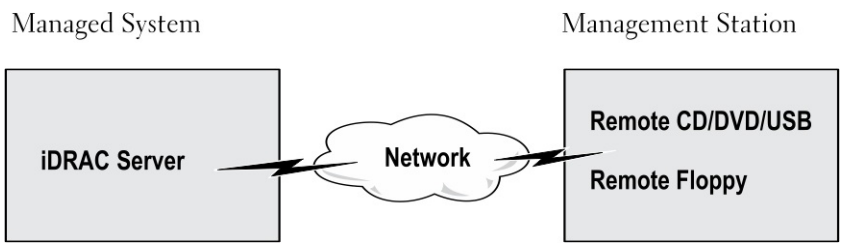


Abbildung 4. Setup für den virtuellen Datenträger

Themen:

Unterstützte Laufwerke und Geräte

Die folgende Tabelle listet die Laufwerke auf, die durch den virtuellen Datenträger unterstützt werden.

Tabelle 41. Unterstützte Laufwerke und Geräte

Laufwerk	Unterstützte Speichermedien
Virtuelle optische Laufwerke	• 1,44 Zoll Legacy-Diskettenlaufwerk mit 1,44 Zoll-Diskette • CD-ROM • DVDs • CD-RW • Kombinationslaufwerk mit dem CD-ROM-Datenträger
Virtuelle Floppy-Laufwerke	• CD-ROM/DVD-Imagedatei im Format ISO9660 • Floppy-Imagedatei im ISO9660-Format
USB-Flash-Laufwerke	• USB-CD-ROM-Laufwerk mit CD-ROM-Datenträger • USB-Schlüssel-Image im ISO9660-Format

Virtuellen Datenträger konfigurieren

Bevor Sie die Einstellungen für den virtuellen Datenträger konfigurieren, müssen Sie sicherstellen, dass Sie zuvor Ihren Web-Browser für die Verwendung des Java- oder ActiveX-Plugins konfigurieren.

Zugehöriger Link

Web-Browser für die Verwendung der virtuellen Konsole konfigurieren

Konfigurieren von virtuellen Datenträgern über die iDRAC-Webschnittstelle

So konfigurieren Sie die Einstellungen für den virtuellen Datenträger:

VORSICHT: Setzen Sie iDRAC nicht zurück, während eine Sitzung für einen virtuellen Datenträger ausgeführt wird, da dieser Vorgang unerwünschte Folgen nach sich ziehen könnte, z. B. Datenverlust.

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **Server** > **Verbundener Datenträger**.
2. Nehmen Sie die gewünschten Einstellungen vor. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Virtuelle Datenträger über RACADM konfigurieren

Verwenden Sie zum Konfigurieren des virtuellen Datenträgers den Befehl **set** bei den Objekten in der Gruppe **iDRAC.VirtualMedia**.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Virtuelle Datenträger über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

Sie können virtuelle Datenträger über das Dienstprogramm für die iDRAC-Einstellungen verbinden, trennen und automatisch verbinden. Gehen Sie dazu wie folgt vor:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Datenträger- und USB-Port-Einstellungen**.

Die Seite **iDRAC-Einstellungen für Media und USB-Schnittstelleneinstellungen** wird angezeigt.

2 Wählen Sie im Abschnitt **Virtueller Datenträger** je nach Anforderung die Optionen **Trennen**, **Verbinden** oder **Automatisch verbinden** aus. Weitere Informationen zu den Optionen finden Sie in der *iDRAC Settings Utility Online Help* (Online-Hilfe für das Dienstprogramm zu den iDRAC-Einstellungen).

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Einstellungen des virtuellen Datenträgers werden konfiguriert.

Status des verbundenen Datenträgers und Systemantwort

Die folgende Tabelle beschreibt die Systemantwort auf der Basis der Einstellungen des verbundenen Datenträgers.

Tabelle 42. Status des verbundenen Datenträgers und Systemantwort

Status des verbundenen Datenträgers	Systemreaktion
Trennen	Image konnte dem System nicht zugeordnet werden.
Verbinden	Der Datenträger wird verbunden, auch wenn die **Client-Ansicht** geschlossen wird.
Automatisch verbinden	Der Datenträger wird verbunden, wenn die **Client-Ansicht** geöffnet wird. Er wird getrennt, wenn die **Client-Ansicht** geschlossen wird.

Server-Einstellungen für das Anzeigen virtueller Geräte im virtuellen Datenträger

Sie müssen die folgenden Einstellungen in der Verwaltungsstation konfigurieren, um die Sichtbarkeit von leeren Laufwerken zu ermöglichen. Klicken Sie dazu in Windows Explorer im Menü **Organisieren** auf **Ordner- und Suchoptionen**. Klicken Sie auf die Registerkarte **Ansicht** , deaktivieren Sie die Option **Leere Laufwerke im Ordner „Computer“ ausblenden**, und klicken Sie auf **OK**.

Auf virtuellen Datenträger zugreifen

Sie können auf den virtuellen Datenträger mit oder ohne Verwendung der virtuellen Konsole zugreifen. Bevor Sie auf den virtuellen Datenträger zugreifen, müssen Sie zuvor Ihre Web-Browser konfigurieren.

Virtual Media und RFS schließen sich gegenseitig aus. Falls die RFS-Verbindung aktiv ist und Sie versuchen, den virtuellen Datenträger-Client zu starten, wird die folgende Fehlermeldung angezeigt: *Virtueller Datenträger ist zurzeit nicht verfügbar. Eine virtuelle Datenträger- oder Remote-Dateifreigabe-Sitzung wird gerade verwendet.*

Wenn die RFS-Verbindung nicht aktiv ist, und wenn Sie versuchen, den Client des virtuellen Datenträgers zu starten, wird der Client erfolgreich gestartet. Sie können dann den Client des virtuellen Datenträgers nutzen, um Geräte und Dateien auf die virtuellen Laufwerke der virtuellen Datenträger abzubilden.

Zugehöriger Link

Web-Browser für die Verwendung der virtuellen Konsole konfigurieren
Virtuellen Datenträger konfigurieren

Virtuellen Datenträger über die virtuelle Konsole starten

Bevor Sie den virtuellen Datenträger über die virtuelle Konsole starten können, müssen Sie Folgendes sicherstellen:

- Die virtuelle Konsole ist aktiviert.
- Das System ist so konfiguriert, dass leere Laufwerke eingeblendet werden. Gehen Sie im Windows Explorer zu **Ordneroptionen**, deaktivieren Sie das Kontrollkästchen **Leere Laufwerke im Ordner „Computer“ ausblenden**, und klicken Sie auf **OK**.

So greifen Sie über die virtuelle Konsole auf den virtuellen Datenträger zu:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Virtuelle Konsole**.
Daraufhin wird die Seite **Virtuelle Konsole** angezeigt.

2 Klicken Sie auf **Virtuelle Konsole starten**.
Der **Virtuelle Konsole-Viewer** wird gestartet.

> **ANMERKUNG: Unter Linux ist Java der Standard-Plug-In-Typ für den Zugriff auf die virtuelle Konsole. Öffnen Sie unter Windows die Datei .jnlp, um die virtuelle Konsole mithilfe von Java zu starten.**

3 Klicken Sie auf **Virtueller Datenträger** > **Virtuellen Datenträger verbinden**.
Die Sitzung des virtuellen Datenträgers wird hergestellt, und das Menü **Virtueller Datenträger** zeigt die Liste der für die Zuordnung verfügbaren Geräte an.

> **ANMERKUNG: Das Fenster Virtuelle Konsole-Viewer muss während des Zugriffs auf den virtuellen Datenträger aktiviert bleiben.**

Zugehöriger Link

Web-Browser für die Verwendung der virtuellen Konsole konfigurieren
Virtuellen Datenträger konfigurieren
Deaktivieren von Warnmeldungen beim Starten der Virtuellen Konsole oder Virtueller Datenträger mit dem Java- oder ActiveX-Plug-In

Virtuelle Datenträger ohne virtuelle Konsole starten

Bevor Sie bei deaktivierter **virtueller Konsole** den virtuellen Datenträger starten, müssen Sie Folgenden sicherstellen:

- Der virtuelle Datenträger befindet sich im Status *Verbunden*.
- Das System ist so konfiguriert, dass leere Laufwerke eingeblendet werden. Gehen Sie dazu im Windows Explorer zu **Ordneroptionen**, deaktivieren Sie das Kontrollkästchen **Leere Laufwerke im Ordner „Computer“ ausblenden**, und klicken Sie auf **OK**.

So starten Sie den virtuellen Datenträger bei deaktivierter virtueller Konsole:

1 Wechseln Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Virtuelle Konsole**.
Daraufhin wird die Seite **Virtuelle Konsole** angezeigt.

2 Klicken Sie auf **Virtuelle Konsole starten**.
Die folgende Meldung wird angezeigt:
```
Virtual Console has been disabled. Do you want to continue using Virtual Media redirection?
```

3 Klicken Sie auf **OK**.
Daraufhin wird das Fenster **Virtuelle Datenträger** angezeigt.

4 Klicken Sie im Menü **Virtuelle Datenträger** auf **CD/DVD zuordnen** oder auf **Wechseldatenträger zuordnen**.
Weitere Informationen finden Sie im Abschnitt Virtuelles Laufwerk zuordnen.

ANMERKUNG: Die Laufwerkbuchstaben der virtuellen Komponente auf dem verwalteten System entsprechen nicht den Buchstaben des physikalischen Laufwerks auf der Management Station.

ANMERKUNG: Der virtuelle Datenträger funktioniert u. U. nicht ordnungsgemäß auf Clients des Windows-Betriebssystems, die mit Internet Explorer Enhanced Security konfiguriert wurden. Um dieses Problem zu lösen, schlagen Sie in der Dokumentation zum Microsoft-Betriebssystem nach oder wenden Sie sich an den Systemadministrator.

ANMERKUNG: Das HTML5-Plugin wird nicht für eigenständige virtuelle Datenträger unterstützt.

Zugehöriger Link

Virtuellen Datenträger konfigurieren

Deaktivieren von Warnmeldungen beim Starten der Virtuellen Konsole oder Virtueller Datenträger mit dem Java- oder ActiveX-Plug-In

Images von virtuellen Datenträgern hinzufügen

Sie können ein Datenträger-Abbild des Remote-Ordners erstellen und dieses als USB-angeschlossenes Gerät zum Server-Betriebssystem bereitstellen. So fügen Sie virtuelle Datenträger-Abbilder hinzu:

1 Klicken Sie auf **Virtueller Datenträger** > **Abbild erstellen...**.

2 Klicken Sie im Feld **Quell-Ordner** auf **Durchsuchen**, und navigieren Sie zu dem Ordner oder Verzeichnis, der als Quelle für die Abbild-Datei verwendet werden soll. Die Abbild-Datei befindet sich auf der Management-Station oder dem Laufwerk C: des verwalteten Systems.

3 Der Standardpfad zur Speicherung der erstellten Abbild-Dateien (normalerweise das Desktop-Verzeichnis) wird im Feld **Imagedateiname** angezeigt. Um diesen Standort zu ändern, klicken Sie auf **Durchsuchen** und gehen Sie auf einen Standort.

4 Klicken Sie auf **Abbild erstellen**.
Die Abbild-Erstellung beginnt. Falls der Standort der Abbild-Datei sich innerhalb des Quellordners befindet, wird eine Warnmeldung angezeigt, die besagt, dass die Abbild-Erstellung nicht fortgesetzt werden kann, weil der Standort der Abbild-Datei im Quellordner eine Endlosschleife verursacht. Falls sich der Standort der Abbild-Datei nicht im Quellordner befindet, wird die Erstellung des Abbilds fortgesetzt.

Nach der Erstellung des Abbildes wird eine Erfolgsmeldung angezeigt.

5 Klicken Sie auf **Fertigstellen**.
Das Abbild wird erstellt.

Wenn ein Ordner als Abbild hinzugefügt wird, wird eine **.img**-Datei auf dem Desktop der Management-Station erstellt, über die diese Funktion verwendet wird. Wenn diese **.img**-Datei verschoben oder gelöscht wird, kann der entsprechende Eintrag für diesen Ordner im Menü **Virtueller Datenträger** nicht verwendet werden. Daher wird empfohlen, die **.img**-Datei weder zu verschieben, noch zu löschen, während das *Abbild* verwendet wird. Die **.img**-Datei kann jedoch entfernt werden, nachdem die Auswahl für den entsprechenden Eintrag zunächst aufgehoben und der Eintrag anschließend über die Option **Abbild entfernen** entfernt wurde.

Details zum virtuellen Gerät anzeigen

Klicken Sie zum Anzeigen der Details des virtuellen Geräts auf **Tools** > **Statistik**. Im Fenster **Statistik** werden im Abschnitt **Virtuelle Datenträger** auch die zugeordneten virtuellen Geräte und die Lese-/Schreibaktivität für die einzelnen Geräte angezeigt. Wenn ein virtueller Datenträger angeschlossen ist, werden diese Informationen angezeigt. Wenn der virtuelle Datenträger nicht angeschlossen ist, wird die Meldung „virtueller Datenträger ist nicht angeschlossen“ angezeigt.

Wenn der virtuelle Datenträger ohne die virtuelle Konsole gestartet wird, dann wird der Abschnitt **Virtueller Datenträger** als Dialogfeld angezeigt, das Informationen über die zugeordneten Geräte enthält.

USB-Gerät zurücksetzen

So setzen Sie das USB-Gerät zurück:

1 Klicken Sie im Viewer der virtuellen Konsole auf **Tools** > **Statistik**.

Das Fenster **Statistik** wird angezeigt.

2 Klicken Sie unter **Virtueller Datenträger**auf **USB-Reset**.

Es wird eine Meldung angezeigt, über die der Benutzer gewarnt wird, dass sich das Zurücksetzen der USB-Verbindung auf den gesamten Input für das Zielgerät auswirken kann, einschließlich des virtuellen Datenträgers und der Maus.

3 Klicken Sie auf **Ja**.

Das USB-Gerät wird zurückgesetzt.

> **ANMERKUNG: Der virtuelle iDRAC-Datenträger wird nicht beendet, auch wenn Sie sich von der Sitzung für die iDRAC-Webschnittstelle abgemeldet haben.**

Virtuelles Laufwerk zuordnen

So ordnen Sie das virtuelle Laufwerk zu:

> **ANMERKUNG: Während Sie den ActiveX-basierten virtuellen Datenträger verwenden, benötigen Sie Administratorberechtigungen für das Zuordnen einer Betriebssystem-DVD oder eines USB-Flash-Laufwerks das mit der Management Station verbunden ist. Starten Sie zum Zuordnen der Laufwerke IE als Administrator, oder fügen Sie die iDRAC-IP-Adresse zur Liste der vertrauenswürdigen Sites hinzu.**

1 Klicken Sie zum Einrichten einer Virtual-Media-Sitzung im Menü **Virtueller Datenträger** auf **Virtuellen Datenträger verbinden**.

Für jedes Gerät, das für die Zuordnung vom Hostserver her bereit steht, wird ein Menüelement unter dem Menü **Virtueller Datenträger** angezeigt. Das Menüelement wird nach dem Gerätetyp benannt, wie z. B.:

- CD/DVD zuordnen
- Entfernbare Festplatte zuordnen
- Diskette zuordnen

> **ANMERKUNG: Die Menüoption Diskettenlaufwerk zuordnen wird in der Liste angezeigt, wenn die Option Diskettenemulation auf der Seite Angehängte Datenträger aktiviert ist. Wenn Diskettenemulation aktiviert ist, wird Wechseldatenträger zuordnen ersetzt durch Diskettenlaufwerk zuordnen.**

Die Option **DVD/CD zuordnen** kann für ISO-Dateien verwendet werden und die Option **Wechseldatenträger zuordnen** kann für Abbilder verwendet werden.

> **ANMERKUNG: Sie können keine physischen Datenträger, wie USB-basierte Laufwerke, CDs oder DVSs, unter Verwendung der virtuellen HTML5-Konsole zuordnen.**

2 Klicken Sie auf den Gerätetyp, den Sie zuordnen möchten.

ANMERKUNG: Die aktive Sitzung zeigt an, ob eine Sitzung von der gegenwärtigen Web-Schnittstellensitzung, einer anderen Web-Schnittstellensitzung oder von VMCLI aus aktiv ist.

3 Wählen Sie im Feld **Laufwerk/Abbilddatei** das Gerät aus der Dropdown-Liste aus.

Die Liste enthält alle verfügbaren (nicht zugeordneten) Geräte, die Sie zuordnen können (CD/DVD, entfernbare Festplatte, Diskette), und Abbilddateitypen, die Sie zuordnen können (ISO oder IMG). Die Abbilddateien befinden sich im Standardverzeichnis für Abbilddateien (normalerweise dem Desktop des Benutzers). Falls das Gerät nicht in der Dropdown-Liste verfügbar ist, klicken Sie auf **Durchsuchen**, um das Gerät anzugeben.

Der richtige Dateityp ist ISO für CD/DVD und IMG für Wechseldatenträger und Disketten.

Wenn das Abbild im Standard-Dateipfad (Desktop) erstellt wird, wenn Sie die Option **Wechseldatenträger zuordnen** auswählen, so ist das erstellte Abbild zur Auswahl im Dropdown-Menü verfügbar.

Wenn das Abbild an einem anderen Speicherort erstellt wird, wenn Sie die Option **Wechseldatenträger zuordnen** auswählen, so ist das erstellte Abbild nicht zur Auswahl im Dropdown-Menü verfügbar. Klicken Sie in diesem Falle auf **Durchsuchen**, um das Abbild festzulegen.

4 Wählen Sie **Schreibgeschützt** aus, um beschreibbare Geräte schreibgeschützt zuzuordnen.

Für CD/DVD-Laufwerke ist diese Option standardmäßig aktiviert und kann nicht deaktiviert werden.

ANMERKUNG: Wenn Sie für die Zuordnung die virtuelle, HTML5-basierte Konsole verwenden, werden ISO- und IMG-Dateien als schreibgeschützte Dateien zugeordnet.

5 Klicken Sie auf **Gerät zuordnen,** um das Gerät dem Hostserver zuzuordnen.

Nach der Zuordnung des Geräts/der Datei ändert sich der Name des zugehörigen Menüelements **Virtueller Datenträger**, um den Gerätenamen anzugeben. Falls das CD/DVD-Gerät beispielsweise einer Abbilddatei mit Namen **foo.iso** zugeordnet ist, wird das CD/DVD-Menüelement im Menü „Virtueller Datenträger“ **foo.iso zugeordnet zu CD/DVD** genannt. Ein Häkchen bei diesem Menüelement gibt an, dass es zugeordnet ist.

Zugehöriger Link

Korrekte virtuelle Laufwerke für die Zuordnung anzeigen

Images von virtuellen Datenträgern hinzufügen

Korrekte virtuelle Laufwerke für die Zuordnung anzeigen

Auf einer Linux-basierten Management Station zeigt das Fenster **Client** für den virtuellen Datenträger möglicherweise entfernbare Festplatten und Floppy-Laufwerke an, die nicht Teil der Management Station sind. Um sicherzustellen, dass die korrekten virtuellen Laufwerke zum Zuordnen verfügbar sind, müssen Sie die Schnittstelleneinstellung für die verbundene SATA-Festplatte aktivieren. Gehen Sie dazu wie folgt vor:

1 Starten Sie das Betriebssystem auf der Management Station neu. Drücken Sie während des POST auf die Taste <F2> oder die Taste <F12>, um das **System-Setup**-Programm aufzurufen.

2 Gehen Sie zu **SATA-Einstellungen**. Dort werden die Schnittstellendetails angezeigt.

3 Aktivieren Sie die Schnittstellen, die derzeit tatsächlich vorhanden und mit der Festplatte verbunden sind.

4 Rufen Sie das Fenster **Client** für den virtuellen Datenträger auf. Es wird mit den Laufwerken angezeigt, die zugeordnet werden können.

Zugehöriger Link

Virtuelles Laufwerk zuordnen

Zuordnung für virtuelles Laufwerk aufheben

So heben Sie die Zuordnung für ein virtuelles Laufwerk auf:

1 Wählen Sie im Menü **Virtuelle Datenträger** einen der folgenden Schritte aus:

- Klicken Sie auf das Gerät, dessen Zuweisung aufgehoben werden soll.

- Klicken Sie auf **Virtuelle Datenträger trennen**.

Eine Bestätigungsmeldung wird angezeigt.

2 Klicken Sie auf **Yes** (Ja).

Die Markierung für das Menüelement wird nicht angezeigt, was darauf hinweist, dass es nicht dem Host-Server zugeordnet sind.

ANMERKUNG: Nach dem Aufheben der Zuweisung eines an vKVM angeschlossenen USB-Geräts von einem Client-System mit dem Macintosh-Betriebssystem aus steht das nicht zugeordnete Gerät auf dem Client eventuell nicht zur Verfügung. Starten Sie das System neu oder stellen Sie das Gerät auf dem Client-System manuell bereit, damit das Gerät angezeigt wird.

Startreihenfolge über das BIOS festlegen

Über das Dienstprogramm für die System-BIOS-Einstellungen können Sie das Managed System so konfigurieren, dass es von virtuellen optischen Laufwerken oder virtuellen Floppy-Laufwerken gestartet wird.

ANMERKUNG: Werden virtuelle Datenträger geändert, während sie verbunden sind, kann dies ggf. zum Anhalten der System-Startsequenz führen.

So aktivieren Sie das Managed System für den Startvorgang:

1 Starten Sie das verwaltete System.
2 Drücken Sie die Taste <F2>, um die Seite **System-Setup** aufzurufen.
3 Gehen Sie zu **System-BIOS-Einstellungen** > **Starteinstellungen** > **BIOS-Starteinstellungen** > **Startsequenz**.

Im Popup-Fenster werden die virtuellen optischen Laufwerke und virtuellen Diskettenlaufwerke mit den Standard-Startgeräten aufgeführt.

4 Stellen Sie sicher, dass das virtuelle Laufwerk aktiviert und als erstes Gerät mit startfähigem Datenträger aufgelistet wird. Falls erforderlich, folgen Sie den Bildschirmanleitungen zur Änderung der Startreihenfolge.
5 Klicken Sie auf **OK**, navigieren Sie zurück zur Seite mit den **System-BIOS-Einstellungen**, und klicken Sie dann auf **Fertigstellen**.
6 Klicken Sie auf **Ja**, um die Änderungen zu speichern und die Seite zu schließen.

Das verwaltete System wird neu gestartet.

Das verwaltete System versucht, basierend auf der Startreihenfolge, von einem startfähigen Gerät zu starten. Wenn das virtuelle Gerät angeschlossen ist und es ist ein startfähiger Datenträger vorhanden, startet das System zum virtuellen Gerät. Ansonsten ignoriert das System das Gerät - ähnlich wie ein physisches Gerät ohne startfähigen Datenträger.

Einmalstart für virtuelle Datenträger aktivieren

Sie können die Startreihenfolge für den Start nur einmal ändern, nachdem Sie das virtuelle Remote-Datenträgergerät verbunden haben.

Bevor Sie die Einmalstart-Option aktivieren, müssen Sie Folgendes sicherstellen:

- Sie verfügen über die Berechtigung *Benutzer konfigurieren*.
- Ordnen Sie die lokalen oder virtuellen Laufwerke (CD/DVD, Floppy oder das USB-Flash-Gerät) dem startfähigen Datenträger oder dem Image über die Optionen für den virtuellen Datenträger zu.
- Der virtuelle Datenträger befindet sich im Status *Verbunden*, damit die virtuellen Laufwerke in der Startsequenz angezeigt werden.

So aktivieren Sie die Einmalstartoption und starten das Managed System über den virtuellen Datenträger:

1 Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **Server** > **Verbundener Datenträger**.
2 Wählen Sie unter **Virtueller Datenträger** die Option **Einmalstart aktivieren** aus, und klicken Sie dann auf **Anwenden**.
3 Schalten Sie das Managed System ein und drücken Sie **<F2>** während des Startens.
4 Ändern Sie die Startreihenfolge zum Starten vom virtuellen Datenträgergerät.
5 Starten Sie den Server neu.

Das Managed System startet einmalig vom virtuellen Datenträger.

Zugehöriger Link

Virtuelles Laufwerk zuordnen

Virtuellen Datenträger konfigurieren

16

VMCLI-Dienstprogramm installieren und verwenden

Das Dienstprogramm Virtual Media Command Line Interface (VMCLI) ist eine Schnittstelle, die die Funktionen des virtuellen Datenträgers von der Management Station zum iDRAC auf dem verwalteten System bereitstellt. Mit diesem Dienstprogramm können Sie auf die Funktionen von virtuellen Datenträgern zugreifen, darunter Image-Dateien und physische Laufwerke, um ein Betriebssystem auf mehreren Remote-Systemen innerhalb eines Netzwerks bereitzustellen.

ANMERKUNG: VMCLI-unterstützt nur das TLS-1.0-Sicherheitsprotokoll.

Das VMCLI-Dienstprogramm unterstützt folgende Funktionen:

- Austauschbare Geräte oder Images verwalten, auf die Sie über virtuelle Datenträger zugreifen können.
- Sitzungen automatisch beenden, wenn die iDRAC-Firmware-Option **Einmalstart** aktiviert ist.
- Sichere Datenübertragung zum iDRAC mittels SSL-Verschlüsselung.
- Führen Sie die VMCLI-Befehle so lange aus, bis:
  - Die Verbindungen automatisch beendet werden.
  - Ein Betriebssystem den Prozess beendet.

ANMERKUNG: Verwenden Sie zum Beenden des Prozesses unter Windows den Task Manager.

Themen:

VMCLI installieren

Das VMCLI-Dienstprogramm ist auf der *Dell Systems Management Tools and Documentation*-DVD enthalten.

So installieren Sie das VMCLI-Dienstprogramm:

1. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk der Verwaltungsstation ein.
2. Folgen Sie zum Installieren der DRAC-Tools den Anweisungen auf dem Bildschirm.
3. Überprüfen Sie nach der erfolgreichen Installation den Ordner **install\Dell\SysMgt\rac5**, um sicherzustellen, dass die Datei **vmcli.exe** vorhanden ist. Überprüfen Sie in gleicher Weise den entsprechenden Pfad für UNIX.

   Das VMCLI-Dienstprogramm ist damit auf dem System installiert.

VMCLI-Dienstprogramm ausführen

- Wenn das Betriebssystem bestimmte Berechtigungen oder eine Gruppenmitgliedschaft benötigt, benötigen Sie ähnliche Berechtigungen für das Ausführen von VMCLI-Befehlen.
- Auf Windows-Systemen benötigen Nicht-Administratoren zum Ausführen des VMCLI-Dienstprogramms Berechtigungen als **Hauptbenutzer**.

- Auf Linux-Systemen müssen Nicht-Administratoren für den Zugriff auf iDRAC, für das Ausführen des VMCLI-Dienstprogramms oder zum Protokollieren von Benutzerbefehlen den VMCLI-Befehlen das Präfix `sudo` voranstellen. Zum Hinzufügen oder Bearbeiten von Benutzern in der VMCLI-Administratorengruppe müssen Sie den Befehl `visudo` verwenden.

VMCLI-Syntax

Die VMCLI-Schnittstelle ist auf Windows- und Linux-Systemen identisch. Die VMCLI-Syntax lautet:

```
VMCLI [parameter] [operating_system_shell_options]
```

Beispiel: `vmcli -r iDRAC-IP-address:iDRAC-SSL-port`

Der *Parameter* aktiviert VMCLI für den Verbindungsaufbau zum angegebenen Server, für den Zugriff auf iDRAC und für die Zuordnung zum angegebenen virtuellen Datenträger.

ANMERKUNG: Bei der Eingabe der VMCLI-Syntax müssen Sie auf die Groß- und Kleinschreibung achten.

Zur Gewährleistung der Sicherheit wird empfohlen, die folgenden VMCLI-Parameter zu verwenden:

- `vmcli -i` – Aktiviert ein interaktives Verfahren für den Start von VMCLI. Mit diesem Verfahren ist sichergestellt, dass Benutzername und Kennwort nicht angezeigt werden, wenn Prozesse von anderen Benutzern überprüft werden.
- vmcli `-r <iDRAC-IP-address[:iDRAC-SSL-port]> -S -u <iDRAC-user-name> -p <iDRAC-user-password> -c {< device-name > | < image-file >}` – Zeigt an, ob das iDRAC-Zertifizierungsstellenzertifikat gültig ist. Wenn das Zertifikat nicht gültig ist, wird bei Ausführung dieses Befehls eine Warnmeldung angezeigt. Der Befehl wird jedoch erfolgreich ausgeführt, und die VMCLI-Sitzung wird aufgebaut. Weitere Informationen zu VMCLI-Parametern finden Sie in der *VMCLI-Hilfe* oder auf den entsprechenden Seiten im *VMCLI-Benutzerhandbuch*.

Zugehöriger Link

VMCLI-Befehle für den Zugriff auf virtuelle Datenträger
VMCLI: Betriebssystem-Shell-Optionen

VMCLI-Befehle für den Zugriff auf virtuelle Datenträger

Die folgende Tabelle enthält die VMCLI-Befehle, die für den Zugriff auf verschiedene virtuelle Datenträger erforderlich sind.

Tabelle 43. VMCLI-Befehle

Virtueller Datenträger	Befehl
Diskettenlaufwerk	`vmcli -r [RAC IP or hostname] -u [iDRAC user name] -p [iDRAC user password] -f [device name]`
Startfähiges Floppy- oder USB-Schlüssel-Image	`vmcli -r [iDRAC IP address] [iDRAC user name] -p [iDRAC password] -f [floppy.img]`
CD-Laufwerk über die Option „-f“	`vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -f [device name]|[image file]-f [cdrom - dev ]`
Startfähiges CD/DVD-Image	`vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -c [DVD.img]`

Wenn die Datei nicht schreibgeschützt ist, kann der virtuelle Datenträger in die Imagedatei schreiben. So stellen Sie sicher, dass der virtuelle Datenträger nicht auf den Datenträger schreibt:

- Konfigurieren Sie das Betriebssystem so, dass eine Disketten-Imagedatei, die nicht überschrieben werden darf, mit einem Schreibschutz versehen wird.
- Verwenden Sie Schreibschutzfunktion auf dem Gerät.

Beim Virtualisieren von schreibgeschützten Imagedateien können sich mehrere Sitzungen dieselben Imagedatenträger teilen.

Beim Virtualisieren von physischen Laufwerken kann zu einem bestimmten Zeitpunkt jeweils nur eine Sitzung auf ein gegebenes physisches Laufwerk zugreifen.

VMCLI: Betriebssystem-Shell-Optionen

VMCLI verwendet Shell-Optionen, um die folgenden Betriebssystemfunktionen zu aktivieren:

- stderr/stdout-Umleitung - leitet jede gedruckte Dienstprogrammausgabe zu einer Datei um.

  Bei Verwendung des Größer-als-Zeichens (>), gefolgt von einem Dateinamen, wird die angegebene Datei mit der gedruckten Ausgabe des VMCLI-Dienstprogramms überschrieben.

ANMERKUNG: Das VMCLI-Dienstprogramm liest keine Daten aus der Standardeingabe (stdin). Daher ist keine stdin-Umleitung erforderlich.

- Ausführung im Hintergrund: Standardmäßig wird das VMCLI-Dienstprogramm im Vordergrund ausgeführt. Verwenden Sie die Shell-Funktionen des Betriebssystems, um das Dienstprogramm im Hintergrund auszuführen.

  Unter einem Linux-Betriebssystem wird das Programm z. B. durch das Und-Zeichen (&) und den entsprechenden Befehl als neuer Hintergrundprozess gestartet. Diese Methode ist bei Skriptprogrammen nützlich, da das Skript nach dem Starten eines neuen Vorgangs für den VMCLI-Befehl weiter ausgeführt werden kann (andernfalls würde das Skript blockieren, bis das VMCLI-Programm beendet ist).

  Wenn mehrere VMCLI-Sitzungen gestartet werden, verwenden Sie die Betriebssystem-spezifischen Funktionen zum Auflisten oder Beenden von Prozessen.

17

vFlash SD-Karte verwalten

Die vFlash SD-Karte ist eine Secure Digital (SD)-Karte, die in den vFlash SD-Kartensteckplatz eines Systems eingeführt wird. Sie können Karten mit einer Speicherkapazität von bis zu 16 GB verwenden. Nachdem Sie die Karten eingeführt haben, müssen Sie die vFlash-Funktion aktivieren, um Partitionen erstellen und verwalten zu können. vFlash ist eine Lizenzfunktion.

Wenn die Karte im vFlash SD-Kartensteckplatz des Systems nicht erkannt wird, wird die folgende Fehlermeldung in der iDRAC-Web-Schnittstelle unter **Übersicht** > **Server** > **vFlash** angezeigt:

```
SD card not detected. Please insert an SD card of size 256MB or greater.
```

ANMERKUNG: Stellen Sie sicher, dass Sie ausschließlich eine vFlash-kompatible SD-Karte in den iDRAC vFlash-Kartensteckplatz einführen. Wenn Sie eine nicht-kompatible SD-Karte einführen, wird beim Initialisieren der Karte die folgende Fehlermeldung angezeigt: *Während der Initialisierung der SD-Karte ist ein Fehler aufgetreten.*

Zentrale Funktionen:

- Bereitstellung von Speicherplatz und Emulation von USB-Gerät(en).
- Erstellung von bis zu 16 Partitionen. Diese Partitionen werden dem System, wenn angeschlossen, je nach ausgewähltem Emulationsmodus als Floppy-Laufwerk, als Festplatte oder CD/DVD-Laufwerk bereitgestellt.
- Erstellung von Partitionen aus unterstützten Dateisystemtypen. Unterstützt das **.img**-Format für Floppy-Emulationstypen, das **.iso**-Format für CD/DVD-Emulationstypen und die **.iso**- und **.img**-Formate für Festplatten-Emulationstypen.
- Erstellung von startfähigen USB-Geräten
- Einmalstart auf ein emuliertes USB-Gerät

  ANMERKUNG: Es ist möglich, dass eine vFlash-Lizenz während eines vFlash-Vorgangs ausläuft. In diesem Fall werden die laufenden vFlash-Vorgänge vollständig abgeschlossen.

ANMERKUNG: Wenn der FIPS-Modus aktiviert ist, können Sie keine vFlash-Aktionen ausführen.

Themen:

Konfigurieren der vFlash-SD-Karte

Stellen Sie vor der Konfiguration von vFlash sicher, dass die vFlash-SD-Karte auf dem System installiert ist. Informationen zur Installation und Enfernung der Karte aus Ihrem System finden Sie im *Hardware Owner's Manual* (Hardware-Benutzerhandbuch) des Systems unter **dell.com/support/manuals**.

ANMERKUNG: Sie müssen über die Berechtigung für den Zugriff auf virtuelle Datenträger verfügen, um die vFlash-Funktion aktivieren oder deaktivieren und die Karte initialisieren zu können.

Zugehöriger Link

Eigenschaften der vFlash-SD-Karte anzeigen
Aktivieren oder Deaktivieren der vFlash-Funktionalität
vFlash SD-Karte initialisieren

Eigenschaften der vFlash-SD-Karte anzeigen

Nachdem die vFlash-Funktion aktiviert wurde, können Sie die SD-Karteneigenschaften über die iDRAC-Webschnittstelle oder über RACADM anzeigen.

vFlash SD-Karteneigenschaften über die Web-Schnittstelle anzeigen

Um die Eigenschaften der vFlash SD-Karte anzuzeigen, gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **vFlash**. Daraufhin wird die Seite **SD-Karteneigenschaften** angezeigt. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

vFlash SD-Karteneigenschaften über RACADM anzeigen

Um die Eigenschaften der vFlash SD-Karte unter Verwendung von RACADM anzuzeigen, verwenden Sie den Befehl `get` mit den folgenden Objekten:

- iDRAC.vflashsd.AvailableSize
- iDRAC.vflashsd.Health
- iDRAC.vflashsd.Licensed
- iDRAC.vflashsd.Size
- iDRAC.vflashsd.WriteProtect

Weitere Informationen zu diesen Objekten finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* unter **dell.com/idracmanuals**.

vFlash SD-Karteneigenschaften über das Dienstprogramm für die iDRAC-Einstellungen anzeigen

Um die vFlash SD-Karteneigenschaften anzuzeigen, gehen Sie im **Dienstprogramm für die iDRAC-Einstellungen** zu **Datenträger und USB-Port-Einstellungen**. Die Seite **Datenträger und USB-Port-Einstellungen** zeigt die Eigenschaften an. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

Aktivieren oder Deaktivieren der vFlash-Funktionalität

Zum Ausführen der Partitionsverwaltung muss die vFlash-Funktionalität aktiviert sein.

vFlash-Funktionen über die Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die vFlash-Funktion:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **vFlash**.
   Die Seite **Eigenschaften der SD-Karte** wird angezeigt.
2. Wählen oder löschen Sie die Option **vFlash aktiviert**, um die VFlash-Medienkarte zu aktivieren. Wenn eine vFlash-Partition verbunden wird, ist es nicht möglich, vFlash zu deaktivieren, und es wird eine Fehlermeldung angezeigt.

   ANMERKUNG: Wenn die vFlash-Funktion deaktiviert ist, werden die SD-Karteneigenschaften nicht angezeigt.
3. Klicken Sie auf **Anwenden**. Die vFlash-Funktion wird entsprechend Ihrer Auswahl aktiviert oder deaktiviert.

vFlash-Funktionen über RACADM aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die vFlash-Funktion über RACADM:

```
racadm set iDRAC.vflashsd.Enable [n]
```

n=0	Disabled (Deaktiviert)
n=1	Enabled (Aktiviert)

ANMERKUNG: Die RACADM-Befehlsfunktionen sind nur verfügbar, wenn eine vFlash SD-Karte vorhanden ist. Wenn keine solche Karte vorhanden ist, wird die folgende Meldung angezeigt: *FEHLER: SD-Karte nicht vorhanden*.

vFlash-Funktionen über das Dienstprogramm für die iDRAC-Einstellungen aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die vFlash-Funktion:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Datenträger- und USB-Port-Einstellungen**.
   Die Seite **iDRAC-Einstellungen . Datenträger- und USB-Port-Einstellungen** wird angezeigt.
2. Wählen Sie im Abschnitt **vFlash-Datenträger** die Option **Aktiviert** aus, um die vFlash-Funktion zu aktivieren, oder wählen Sie **Deaktiviert** aus, um die vFlash-Funktion zu deaktivieren.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die vFlash-Funktion wird auf der Basis Ihrer Auswahl aktiviert oder deaktiviert.

vFlash SD-Karte initialisieren

Durch den Initialisierungsvorgang wird die SD-Karte neu formatiert, und die anfänglichen vFlash-Systeminformationen auf der Karte werden konfiguriert.

ANMERKUNG: Wenn die SD-Karte schreibgeschützt ist, wird die Option „Initialisieren“ deaktiviert.

vFlash SD-Karte über die Web-Schnittstelle initialisieren

So initialisieren Sie die vFlash SD-Karte:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **vFlash**.
   Die Seite **Eigenschaften der SD-Karte** wird angezeigt.
2. Aktivieren Sie **vFLASH**, und klicken Sie auf **Initialisieren**.
   Alle vorhandenen Inhalt werden entfernt, und die Karte wird mit den neuen vFlash-Systeminformationen formatiert.

   Wenn eine vFlash-Partition verbunden wird, schlägt der Initialisierungsvorgang fehl, und es wird eine Fehlermeldung angezeigt.

Initialisieren der vFlash-SD-Karte mithilfe von RACADM

So initialisieren Sie die vFlash-SD-Karte mithilfe von RACADM:

```
racadm set iDRAC.vflashsd.Initialized 1
```

Sämtliche vorhandenen Partitionen werden gelöscht, und die Karte wird erneut formatiert.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

vFlash SD-Karte über das Dienstprogramm für die iDRAC-Einstellungen initialisieren

So initialisieren Sie die vFlash SD-Karte über das Dienstprogramm für die iDRAC-Einstellungen:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Datenträger- und USB-Port-Einstellungen**.
Die Seite **iDRAC-Einstellungen . Datenträger- und USB-Port-Einstellungen** wird angezeigt.
2 Klicken Sie auf **vFlash initialisieren**.
3 Klicken Sie auf **Ja**. Daraufhin wird die Initialisierung gestartet.
4 Klicken Sie auf **Zurück** , und navigieren Sie zur Seite **iDRAC-Einstellungen . Datenträger- und USB-Port-Einstellungen**, um die Erfolgsmeldung anzuzeigen.
Alle vorhandenen Inhalt werden entfernt, und die Karte wird mit den neuen vFlash-Systeminformationen formatiert.

Aktuellen Status über RACADM abrufen

So rufen Sie den Status des zuletzt an die vFlash SD-Karte gesendeten Initialisierungsbefehls ab:

1 Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2 Geben Sie den folgenden Befehl ein: `racadm vFlashsd status`
Daraufhin wird der Status der an die SD-Karte gesendeten Befehle angezeigt.
3 Verwenden Sie zum Abrufen des aktuellen Status für alle vFlash-Partitionen den folgenden Befehl: `racadm vflashpartition status -a`
4 Verwenden Sie zum Abrufen des aktuellen Status für eine bestimmte Partition den folgenden Befehl: `racadm vflashpartition status -i (index)`

ANMERKUNG: Wenn iDRAC zurückgesetzt wird, geht der Status des letzten Partitionsvorgangs verloren.

vFlash-Partitionen verwalten

Sie können die folgenden Schritte über die iDRAC-Web-Schnittstelle oder RACADM ausführen:

ANMERKUNG: Als Administrator können Sie alle Aufgaben auf den vFlash-Partitionen ausführen. Ansonsten benötigen Sie die Berechtigung Auf virtuelle Datenträger zugreifen, um die Inhalte auf der Partition erstellen, löschen, formatieren, verbinden, trennen oder kopieren zu können.

- Leere Partition erstellen
- Partition unter Verwendung einer Imagedatei erstellen
- Partition formatieren
- Verfügbare Partitionen anzeigen
- Partition modifizieren
- Partitionen verbinden oder trennen
- Vorhandene Partitionen löschen
- Partitionsinhalte herunterladen
- In eine Partition starten

ANMERKUNG: Wenn Sie auf den vFlash-Seiten auf eine beliebige Option klicken, wenn eine Anwendung wie WS-MAN, das Dienstprogramm für die iDRAC-Einstellungen oder RACADM vFlash verwendet, oder wenn Sie zu einer anderen Seite in der GUI navigieren, zeigt iDRAC möglicherweise die folgende Meldung an: `vFlash is currently in use by another process. Try again after some time.`

vFlash ist in der Lage, eine schnelle Partitionserstellung auszuführen, wenn keine anderen laufenden vFlash-Vorgänge aktiv sind, z. B. Formatieren, Partitionen verbinden, usw. Daher wird empfohlen, zunächst alle Partitionen zu erstellen, bevor Sie andere einzelne Partitionsvorgänge durchführen.

Leere Partition erstellen

Eine leere Partition, die mit dem System verbunden ist, verhält sich ähnlich wie ein leeres USB-Flash-Laufwerk. Sie können leere Partitionen auf einer vFlash-SD-Karte erstellen. Sie können Partitionen des Typs *Floppy* oder *Festplatte* anlegen. Der Partitionstyp „CD“ wird nur im Rahmen der Erstellung von Partitionen auf der Basis von Images unterstützt.

Stellen Sie vor dem Erstellen einer leeren Partition Folgendes sicher:

- dass Sie über die Berechtigung **Zugriff auf virtuellen Datenträger** verfügen.
- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.

Leere Partition über die Web-Schnittstelle erstellen

So erstellen Sie eine leere vFlash-Partition:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **vFlash** > **Leere Partition erstellen**.

Die Seite **Leere Partition erstellen** wird angezeigt.

2 Geben Sie die erforderlichen Informationen an, und klicken Sie auf **Anwenden**. Weitere Informationen zu diesen Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Es wird eine neue, unformatierte, leere Partition erstellt, die standardmäßig schreibgeschützt ist. Es wird eine Seite angezeigt, auf der der Verarbeitungsprozentsatz angezeigt wird. In den folgenden Fällen wird eine Fehlermeldung angezeigt:

- Die Karte ist schreibgeschützt.
- Der Kennzeichnungsname stimmt mit der Kennzeichnung einer vorhandenen Partition überein.
- Ein nicht ganzzahliger Wert wurde als Partitionsgröße eingegeben, der Wert übersteigt den auf der Karte verfügbaren Speicherplatz oder die Partition ist größer als 4 GB.
- Auf der Karte wird ein Initialisierungsvorgang ausgeführt.

Leere Partition über RACADM erstellen

So erstellen Sie eine leere Partition:

1 Melden Sie sich über Telnet, SSH oder serielle Konsole bei Ihrem System an.

2 Geben Sie den folgenden Befehl ein:

```
racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s [n]
```

wobei `[n]` die Partitionsgröße ist.

Standardmäßig wird eine leere Partition als editierbare Partition erstellt.

Partition unter Verwendung einer Imagedatei erstellen

Sie können auf der vFlash-SD-Karte mithilfe einer Imagedatei eine neue Partition erstellen. Dabei werden die folgenden Image-Dateiformate unterstützt: **.img** oder **.iso**. Die Partitionen liegen in den folgenden Emulationstypen vor: Diskette (**.img**), Festplatte (**.img**) oder CD (**.iso**). Die Größe der erstellen Partition entspricht der Größe der Image-Datei.

Vor der Erstellung einer Partition über eine Imagedatei müssen Sie Folgendes sicherstellen:

- Sie haben Berechtigungen für den Zugriff auf den virtuellen Datenträger.
- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.

ANMERKUNG: Das hochgeladene Image und der Emulationstyp stimmen überein. Es treten Probleme auf, wenn iDRAC ein Gerät mit einem falschen Imagetyp emuliert. Beispiel: Wenn die Partition unter Verwendung eines ISO-Images erstellt wird und der Emulationstyp als Festplatte festgelegt ist, wird das BIOS nicht in der Lage sein, über dieses Image zu starten.

- Der Imagetyp und der Emulationstyp stimmen überein.
- Die Größe der Image-Datei ist geringer als der auf der Karte verfügbare Speicherplatz oder gleich diesem Speicherplatz.
- Die Größe der Image-Datei beträgt höchstens 4 GB, da dies die maximale Partitionsgröße ist. Bei der Erstellung einer Partition über einen Webbrowser muss die Größe der Image-Datei jedoch unter 2 GB liegen.

ANMERKUNG: Die vFlash-Partition ist eine Image-Datei auf einem FAT32-Dateisystem. Für die Image-Datei gilt daher die 4-GB-Einschränkung.

Partition unter Verwendung einer Imagedatei mithilfe der Webschnittstelle erstellen

So erstellen Sie eine vFlash-Partition über eine Imagedatei:

1 Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **Server** > **vFlash** > **Aus Image erstellen**.

Die Seite **Partition über Imagedatei erstellen** wird angezeigt.

2 Geben Sie die angeforderten Informationen ein, und klicken Sie auf **Anwenden.** Weitere Informationen über die Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Es wird eine neue Partition erstellt. Beim CD-Emulationstyp wird eine schreibgeschützte Partition erstellt. Bei den Floppy- oder Festplatten-Emulationstypen wird eine editierbare Partition erstellt. In den folgenden Fällen wird eine Fehlermeldung angezeigt:

- Die Karte ist schreibgeschützt.
- Der Kennzeichnungsname stimmt mit der Kennzeichnung einer vorhandenen Partition überein.
- Die Imagedatei ist größer als 4 GB oder übersteigt den auf der Karte verfügbaren Speicherplatz.
- Die Imagedatei existiert nicht oder die Erweiterung der Imagedatei ist weder .img noch .iso.
- Auf der Karte wird bereits ein Initialisierungsvorgang ausgeführt.

Partition unter Verwendung einer Imagedatei mithilfe von RACADM erstellen

So erstellen Sie eine Partition aus einer Imagedatei über RACADM:

1 Melden Sie sich über Telnet, SSH oder serielle Konsole bei Ihrem System an.

2 Geben Sie den Befehl ein

```
racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/
foo.iso -u root -p mypassword
```

Die erstellte Partition ist schreibgeschützt. Dieser Befehl unterscheidet bei der Image-Dateinamenerweiterung zwischen Groß- und Kleinschreibung. Wird beispielsweise die Dateinamenerweiterung in Großbuchstaben (FOO.ISO) statt in Kleinbuchstaben (FOO.iso) angegeben, gibt der Befehl einen Syntaxfehler aus.

ANMERKUNG: Diese Funktion wird im lokalen RACADM nicht unterstützt.

ANMERKUNG: Die Erstellung einer vFlash-Partition aus einer Imagedatei, die sich auf dem CFS oder der für NFS IPv6 aktivierten Netzwerkfreigabe befindet, wird nicht unterstützt.

Partition formatieren

Sie können eine vorhandene Partition auf der vFlash-SD-Karte auf Grundlage des Dateisystemtyps formatieren. Die unterstützten Dateisystemtypen sind EXT2, EXT3, FAT16 und FAT32. Sie können nur eine Partition des Typs Festplatte oder Diskette, aber nicht CD, anlegen. Schreibgeschützte Partitionen können nicht formatiert werden.

Vor der Erstellung einer Partition über eine Imagedatei stellen Sie Folgendes sicher:

- Sie haben Berechtigungen für den **Zugriff auf den virtuellen Datenträger**.
- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.

So formatieren Sie eine vFlash-Partition:

1 Wechseln Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **vFlash** > **Formatieren**.
Die Seite **Partition formatieren** wird angezeigt.

2 Geben Sie die erforderlichen Informationen ein und klicken Sie auf **Anwenden**.
Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Es wird eine Warnungsmeldung angezeigt, die darauf hinweist, dass alle Daten auf der Partition gelöscht werden.

3 Klicken Sie auf **OK**.
Die ausgewählte Partition wird gemäß dem festgelegten Dateisystemtyp formatiert. Es wird eine Fehlermeldung angezeigt, wenn Folgendes zutrifft:
   - Die Karte ist schreibgeschützt.
   - Auf der Karte wird bereits ein Initialisierungsvorgang ausgeführt.

Verfügbare Partitionen anzeigen

Stellen Sie sicher, dass die vFlash-Funktion aktiviert ist, damit die Liste der verfügbaren Partitionen angezeigt wird.

Verfügbare Partitionen über die Web-Schnittstelle anzeigen

Um die verfügbaren vFlash-Partitionen anzuzeigen, gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **vFlash** > **Verwalten**. Die Seite **Partitionen verwalten** wird angezeigt und zeigt die verfügbaren Partitionen und die verknüpften Informationen für jede einzelnen Partition an. Weitere Informationen zu den Partitionen finden Sie in der *iDRAC-Online-Hilfe*.

Verfügbare Partitionen über RACADM anzeigen

So zeigen Sie die verfügbaren Partitionen und die dazugehörigen Eigenschaften über RACADM an:

1 Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2 Geben Sie die folgenden Befehle ein:
   - So listen Sie alle vorhandenen Partitionen und deren Eigenschaften auf:
     ```
     racadm vflashpartition list
     ```
   - So rufen Sie den Status des Vorgangs auf Partition 1 ab:
     ```
     racadm vflashpartition status -i 1
     ```
   - So rufen Sie den Status sämtlicher vorhandener Partitionen ab:
     ```
     racadm vflashpartition status -a
     ```

     ANMERKUNG: Die Option „-a“ ist nur mit der Statusaktion gültig.

Partition modifizieren

Sie können den Schreibschutz für eine schreibgeschützte Partition aktivieren oder deaktivieren. Vor dem Ändern einer Partition müssen Sie Folgendes sicherstellen:

- Die vFlash-Funktion ist aktiviert.
- Sie haben Berechtigungen für den **Zugriff auf den virtuellen Datenträger**.

ANMERKUNG: Standardmäßig wird eine schreibgeschützte Partition erstellt.

Partition über die Web-Schnittstelle ändern

So ändern Sie eine Partition:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **vFlash** > **Verwalten**.
   Die Seite **Partitionen verwalten** wird angezeigt.
2 Führen Sie in der Spalte **Nur-Lesen** die folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie für den Wechsel in den schreibgeschützten Modus auf **Anwenden**.
   - Deaktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie für den Wechsel des schreibgeschützten Modus auf **Anwenden**.

     Auf Grundlage der entsprechenden Auswahl werden die Partitionen zu Nur-Lesen oder Lesen-Schreiben geändert.

     ANMERKUNG: Ist die Partition vom Typ CD, ist der Status schreibgeschützt. Sie können den Zustand nicht in den Schreibstatus ändern. Wenn die Partition verbunden ist, ist das Kontrollkästchen grau unterlegt.

Partition über RACADM ändern

So zeigen Sie die verfügbaren Partitionen und Eigenschaften auf der Karte an:

1 Melden Sie sich über Telnet, SSH oder serielle Konsole bei Ihrem System an.
2 Verwenden Sie eine der folgenden Optionen:
   - Verwenden Sie den Befehl `set` zum Ändern des Lese-Schreib-Status der Partition:
     - So ändern Sie eine schreibgeschützte Partition zu Lesen-Schreiben:
       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 1
       ```
     - So ändern Sie eine Lesen-Schreiben-Partition zu Nur-Lesen:
       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 0
       ```
   - Verwenden Sie den Befehl `set` zum Festlegen des Emulationstyps:
     ```
     racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or CD-DVD>
     ```

Partitionen verbinden oder trennen

Wenn Sie eine oder mehrere Partitionen verbinden, werden diese gegenüber dem Betriebssystem und dem BIOS als USB-Massenspeichergeräte angezeigt. Wenn Sie mehrere Partitionen verbinden, werden diese auf der Basis des zugewiesenen Index in aufsteigender Reihenfolge im Betriebssystem und im BIOS-Startreihenfolgemenü angezeigt.

Wenn Sie eine Partition trennen, wird diese nicht mehr im Betriebssystem und im BIOS-Startreihenfolgemenü angezeigt.

Wenn Sie eine Partition verbinden oder trennen, wird der USB-Bus auf dem Managed System zurückgesetzt. Dies wirkt sich auch auf die Anwendungen aus, die vFlash verwenden. Außerdem werden die Sitzungen für die virtuellen iDRAC-Datenträger getrennt.

Vor dem Verbinden und Trennen einer Partition müssen Sie Folgendes sicherstellen:

- Die vFlash-Funktion ist aktiviert.
- Es wird nicht bereits ein Initialisierungsvorgang auf der Karte ausgeführt.
- Sie haben Berechtigungen für den **Zugriff auf den virtuellen Datenträger**.

Partitionen über die Web-Schnittstelle verbinden oder trennen

So werden Partitionen verbunden oder abgetrennt:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **vFlash** > **Verwalten**.
   Die Seite **Partitionen verwalten** wird angezeigt.
2 Führen Sie in der Spalte **Verbunden** die folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie zum Verbinden der Partition(en) auf **Anwenden**.
   - Aktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie zum Trennen der Partition(en) auf **Anwenden**.
     Auf Grundlage der entsprechenden Auswahl werden die Partitionen verbunden oder abgetrennt.

Partitionen über RACADM verbinden oder trennen

So werden Partitionen verbunden oder abgetrennt:

1 Melden Sie sich über Telnet, SSH oder serielle Konsole bei Ihrem System an.
2 Verwenden Sie die folgenden Befehle:

- So verbinden Sie eine Partition:
  ```
  racadm set iDRAC.vflashpartition.<index>.AttachState 1
  ```
- So trennen Sie eine Partition ab:
  ```
  racadm set iDRAC.vflashpartition.<index>.AttachState 0
  ```

Verhalten des Betriebssystems bei verbundenen Partitionen

Windows- und Linux-Betriebssysteme:

- Das Betriebssystem kontrolliert die Laufwerksbuchstaben und weist sie den angeschlossenen Partitionen zu.
- Schreibgeschützte Partitionen sind schreibgeschützte Laufwerke auf dem Betriebssystem.
- Das Betriebssystem muss das Dateisystem einer angeschlossenen Partition unterstützen. Ansonsten können Sie die Inhalte der Partition über das Betriebssystem weder lesen noch ändern. In einer Windows-Umgebung kann das Betriebssystem beispielsweise den Partitionstyp EXT2 nicht lesen, da es sich hierbei um einen Linux-eigenen Typ handelt. In einer Linux-Umgebung kann das Betriebssystem wiederum den Partitionstyp NTFS nicht lesen, da es sich hierbei um einen Windows-eigenen Typ handelt.
- Die Beschriftung der vFlash-Partition weicht vom Volume-Namen des Dateisystems auf dem emulierten USB-Gerät ab. Sie können den Volume-Namen des emulierten USB-Geräts von dem Namen auf dem Betriebssystem ändern. Auf den Namen der Partitionsbeschriftung, der in iDRAC gespeichert wird, hat dies jedoch keine Auswirkung.

Vorhandene Partitionen löschen

Stellen Sie vor dem Löschen vorhandener Partitionen Folgendes sicher:

- Die vFlash-Funktion ist aktiviert.
- Die Karte ist nicht schreibgeschützt.
- Die Partition ist nicht verbunden.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.

Vorhandene Partitionen über die Web-Schnittstelle löschen

Löschen einer bestehenden Partition:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **vFlash** > **Verwalten**.
Die Seite **Partitionen verwalten** wird angezeigt.
2 Klicken Sie in der Spalte **Löschen** auf das Symbol zum Löschen, um die gewünschte Partition zu löschen.
Es wird eine Meldung angezeigt, aus der hervorgeht, dass die Partition durch diese Maßnahme endgültig gelöscht wird.
3 Klicken Sie auf **OK**.
Die Partition ist damit gelöscht.

Vorhandene Partitionen über RACADM löschen

So löschen Sie Partitionen:

1 Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2 Geben Sie die folgenden Befehle ein:
- So löschen Sie eine Partition:
  ```
  racadm vflashpartition delete -i 1
  ```
- Zum Löschen sämtlicher Partitionen ist die vFlash-SD-Karte erneut zu initialisieren.

Partitionsinhalte herunterladen

Sie können die Inhalte einer vFlash-Partition in den folgenden Formaten herunterladen: **.img** oder **.iso**:

- Managed System (über das iDRAC ausgeführt wird)
- Netzwerkstandort, der mit einer Management Station verknüpft ist.

Vor dem Herunterladen der Partitionsinhalte müssen Sie Folgendes sicherstellen:

- Sie haben Berechtigungen für den Zugriff auf den virtuellen Datenträger.
- Die vFlash-Funktion ist aktiviert.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.
- Wenn eine Lesen-Schreiben-Partition vorliegt, darf diese nicht verbunden sein.

So laden Sie die Inhalte der vFlash-Partition herunter:

1 Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **Server** > **vFlash** > **Herunterladen**.
Die Seite **Partition herunterladen** wird angezeigt.

2 Wählen Sie aus dem Drop-Down-Menü **Kennzeichnung** eine Partition aus, die Sie herunterladen möchten, und klicken Sie auf **Herunterladen**.

ANMERKUNG: Alle vorhandenen Partitionen (mit Ausnahme der verbundenen Partitionen) werden in der Liste angezeigt. Es wird standardmäßig die erste Partition ausgewählt.

3 Legen Sie den Speicherort fest, an dem die Datei gespeichert werden soll.
Der Inhalt der ausgewählten Partition wird an den festgelegten Speicherort heruntergeladen.

ANMERKUNG: Wenn nur der Ordnerspeicherort angegeben ist, wird die Partitionsbezeichnung mit dem Dateinamen und außerdem bei CD- und Festplattenpartitionen mit der Dateierweiterung .iso und bei Floppy- und Festplattenpartitionen mit der Dateierweiterung .img gekennzeichnet.

Zu einer Partition starten

Sie können eine verbundene vFlash-Partition als Startgerät für den nächsten Startvorgang einrichten.

Vor dem Starten einer Partition müssen Sie Folgendes sicherstellen:

- Die vFlash-Partition enthält ein startfähiges Image (in den Formaten **.img** oder **.iso**), um einen Start vom Gerät zu ermöglichen.
- Die vFlash-Funktion ist aktiviert.
- Sie haben Berechtigungen für den Zugriff auf den virtuellen Datenträger.

Über die Web-Schnittstelle auf eine Partition starten

Weitere Informationen zum Festlegen der vFlash-Partition als ein erstes Startlaufwerk finden Sie unter Erstes Startlaufwerk einrichten.

ANMERKUNG: Wenn die verbundene(n) vFlash-Partition(en) nicht im Drop-Down-Menü Erstes Startlaufwerk gelistet ist/sind, müssen Sie sicherstellen, dass das BIOS in der aktuellen Version vorliegt.

Über RACADM auf eine Partition starten

Um eine vFlash-Partition als erstes Startgerät einzustellen, verwenden Sie das Objekt **iDRAC.ServerBoot**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

ANMERKUNG: Wenn Sie diesen Befehl ausführen, wird die Kennzeichnung der vFlash-Partition automatisch auf Einmalstart eingestellt (`iDRAC.ServerBoot.BootOnce` ist auf `1` eingestellt). Der Einmalstart startet das Gerät auf der Partition nur einmal und behält es nicht dauerhaft als erstes Gerät in der Startreihenfolge.

18

SMCLP verwenden

Die Spezifikation des Server Management Command Line Protocol (SMCLP) ermöglicht CLI-basierte Systemverwaltung. Sie definiert ein Protokoll zur Verwaltung von Befehlen, die über Standardzeichen-Datenströme übermittelt werden. Dieses Protokoll greift auf einen Common Information Model Object Manager (CIMOM) zu, der ein menschliches Befehlsset verwendet. Das SMCLP ist eine Subkomponente der Distributed Management Task Force (DMTF) SMASH-Initiative zum Optimieren der Systemverwaltung auf mehreren Plattformen. Die SMCLP-Spezifikation beschreibt, zusammen mit der Managed-Element-Addressing-Spezifikation und zahlreichen Profilen zu den SMCLP-Zuordnungsspezifikationen, die standardmäßigen Verben und Ziele für verschiedene Verwaltungstaskausführungen.

ANMERKUNG: Es wird angenommen, dass Sie mit der SMASH-Initiative (Systemverwaltungsarchitektur für Serverhardware) und den SMWG SMCLP-Angaben vertraut sind.

Das SM-CLP ist eine Unterkomponente der DMTF (Distributed Management Task Force) SMASH-Initiative zum Rationalisieren der Serververwaltung über mehrere Plattformen. In Verbindung mit der Spezifikation für verwaltete Elementadressierung und zahlreichen Profilen zu SM-CLP-Zuordnungsspezifikationen beschreibt die SM-CLP-Spezifikation die Standard-Verben und -Ziele zum Ausführen verschiedener Verwaltungsaufgaben.

Das SMCLP wird von der iDRAC-Controller-Firmware aus gehostet und unterstützt Telnet, SSH und seriell-basierte Schnittstellen. Die iDRAC-SMCLP-Schnittstelle basiert auf der SMCLP-Spezifikation Version 1.0, bereitgestellt von der DMTF-Organisation.

ANMERKUNG: Informationen zu den Profilen, Erweiterungen und MOFs können unter delltechcenter.com abgerufen werden, und die gesamten DMTF-Informationen können von dmtf.org/standards/profiles/ abgerufen werden.

SM-CLP-Befehle setzen einen Teilsatz der Befehle des lokalen RACADM um. Diese Befehle eignen sich gut für das Scripting, da sie über eine Befehlszeile der Management Station ausgeführt werden können. Sie können die Befehlsausgabe in eindeutigen Formaten, einschließlich XML, abrufen, wodurch das Scripting und die Integration mit vorhandenen Berichterstattungs- und Verwaltungshilfsprogrammen erleichtert wird.

Themen:

System-Verwaltungsfunktionen über SMCLP

Mit iDRAC SMCLP können Sie die folgenden Funktionen ausführen:

- Serverenergieverwaltung – System einschalten, herunterfahren oder neu starten
- Verwaltung des Systemereignisprotokolls (SEL) – SEL-Datensätze anzeigen oder löschen
- iDRAC-Benutzerkonto verwalten
- Systemeigenschaften anzeigen

SMCLP-Befehle ausführen

Sie können die SMCLP-Befehle über die SSH- oder Telnet-Schnittstelle ausführen. Öffnen Sie eine SSH- oder Telnet-Schnittstelle, und melden Sie sich als Administrator bei iDRAC an. Daraufhin wird die SMCLP-Befehlseingabe (admin ->) angezeigt.

SMCLP-Befehlseingaben:

- yx1x-Blade-Server verwenden `-$`.
- yx1x-Rack- und Tower-Server verwenden `admin->`.
- yx2x-Blade-, Rack- und Tower-Server verwenden `admin->`.

Hier steht „y“ für ein alphanumerisches Zeichen wie „M“ (für Blade-Server), „R“ (für Rack-Server) und „T“ (für Tower-Server) und „x“ für eine Zahl. Diese Zahl dient der Kennzeichnung der Dell PowerEdge-Server-Generation.

ANMERKUNG: Skripte, die `-$` verwenden, können diese für yx1x-Systeme verwenden, aber beginnend bei yx2x-Systemen kann ein Skript mit `admin->` für Blade-, Rack- und Tower-Server verwendet werden.

iDRAC-SMCLP-Syntax

iDRAC SMCLP verwendet das Konzept von Verben und Zielen und stellt Systemverwaltungsfunktionen über die CLI bereit. Das Verb gibt den auszuführenden Vorgang an und das Ziel bestimmt die Einheit (oder das Objekt), die den Vorgang ausführt.

Die SMCLP Befehlszeilensyntax:

```
<verb> [<options>] [<target>] [<properties>]
```

Die folgende Tabelle zeigt die Verben sowie ihre Definitionen.

Tabelle 44. SMCLP-Verben

Verb	Definition
cd	Navigiert durch den MAP mittels der Shell.
set	Stellt eine Eigenschaft auf einen bestimmten Wert ein.
Hilfe	Zeigt die Hilfe für ein bestimmtes Ziel an.
reset	Setzt das Ziel zurück.
show	Zeigt die Zieleigenschaften, Verben und Unterziele an.
start	Schaltet ein Ziel ein.
stop	Fährt ein Ziel herunter.
exit	Beendet die SMCLP-Shell-Sitzung
Version	Zeigt die Versionsattribute eines Ziels an.
load	Lädt ein Binärbild von einer URL zu einer bestimmten Zieladresse.

Die folgende Tabelle enthält eine Liste mit Zielen.

Tabelle 45. SMCLP-Ziele

Ziel	Definitionen
admin1	admin domain
admin1/profiles1	Registrierte Profile in iDRAC
admin1/hdwr1	Hardware
admin1/system1	Ziel des verwalteten Systems
admin1/system1/capabilities1	SMASH-Erfassungsfunktionen des verwalteten Systems
admin1/system1/capabilities1/pwrcap1	Funktionen zur Energienutzung des verwalteten Systems
admin1/system1/capabilities1/elecap1	Zielfunktionen des verwalteten Systems
admin1/system1/logs1	Datensatzprotokoll-Erfassungsziel
admin1/system1/logs1/log1	Systemereignisprotokoll (SEL) Datensatzeintrag
admin1/system1/logs1/log1/record*	Eine einzelne SEL-Datensatzinstanz auf dem verwalteten System
admin1/system1/settings1	SMASH-Erfassungseinstellungen des verwalteten Systems
admin1/system1/capacities1	SMASH-Erfassung der verwalteten Systemkapazitäten
admin1/system1/consoles1	SMASH-Erfassung der verwalteten Systemkonsolen
admin1/system1/sp1	Serviceprozessor
admin1/system1/sp1/timesvc1	Zeitansage des Serviceprozessors
admin1/system1/sp1/capabilities1	SMASH-Erfassung der Serviceprozessorfunktionen
admin1/system1/sp1/capabilities1/clpcap1	CLP-Dienstfunktionen
admin1/system1/sp1/capabilities1/pwrmgtcap1	Dienstfunktionen der Stromzustandsverwaltung auf dem System
admin1/system1/sp1/capabilities1/acctmgtcap*	Dienstfunktionen der Kontoverwaltung
admin1/system1/sp1/capabilities1/rolemgtcap*	Lokale rollenbasierte Verwaltungsfunktionen
admin1/system1/sp1/capabilities/PwrutilmgtCap1	Energienutzung-Verwaltungsfunktionen
admin1/system1/sp1/capabilities1/elecap1	Authentifizierungsfunktionen
admin1/system1/sp1/settings1	Sammlung von Serviceprozessoreinstellungen
admin1/system1/sp1/settings1/clpsetting1	CLP-Dienst-Einstellungsdaten
admin1/system1/sp1/clpsvc1	CLP-Dienst-Protokolldienst
admin1/system1/sp1/clpsvc1/clpendpt*	CLP-Dienst-Protokollendpunkt

Ziel	Definitionen
admin1/system1/sp1/clpsvc1/tcpendpt*	CLP-Dienst-Protokoll-TCP-Endpunkt
admin1/system1/sp1/jobq1	Auftragswarteschlange des CLP-Dienst-Protokolls
admin1/system1/sp1/jobq1/job*	CLP-Dienst-Protokollaufgabe
admin1/system1/sp1/pwrmgtsvc1	Stromzustandsverwaltungsdienst
admin1/system1/sp1/account1-16	Lokales Benutzerkonto
admin1/sysetm1/sp1/account1-16/identity1	Identitätskonto des lokalen Benutzers
admin1/sysetm1/sp1/account1-16/identity2	IPMI-Identitätskonto (LAN)
admin1/sysetm1/sp1/account1-16/identity3	IPMI-Identitätskonto (seriell)
admin1/sysetm1/sp1/account1-16/identity4	CLP-Identitätskonto
admin1/system1/sp1/acctsvc1	Verwaltungsdienst für lokales Benutzerkonto
admin1/system1/sp1/acctsvc2	IPMI-Kontoverwaltungsdienst
admin1/system1/sp1/acctsvc3	CLP-Kontoverwaltungsdienst
admin1/system1/sp1/rolesvc1	Lokaler rollenbasierter Authentifizierungsdienst (RBA)
admin1/system1/sp1/rolesvc1/Role1-16	Lokale Rolle
admin1/system1/sp1/rolesvc1/Role1-16/privilege1	Lokale Rollenberechtigung
admin1/system1/sp1/rolesvc2	IPMI-RBA-Dienst
admin1/system1/sp1/rolesvc2/Role1-3	IPMI-Rolle
admin1/system1/sp1/rolesvc2/Role4	IPMI Seriell-über-LAN-Rolle (SOL)
admin1/system1/sp1/rolesvc3	CLP-RBA-Dienst
admin1/system1/sp1/rolesvc3/Role1-3	CLP-Rolle
admin1/system1/sp1/rolesvc3/Role1-3/privilege1	CLP-Rollenberechtigung

Zugehöriger Link

SMCLP-Befehle ausführen
Anwendungsbeispiele

MAP-Adressbereich navigieren

Objekte, die mit dem SM-CLP verwaltet werden können, werden durch Ziele repräsentiert, die in einem hierarchischen Bereich, Adressbereich des Verwaltungszugriffspunkts (Manageability Access Point = MAP) genannt, angeordnet sind. Ein Adresspfad legt den Pfad vom Adressbereichsstamm zu einem Objekt im Adressbereich fest.

Das root-Ziel wird durch einen Schrägstrich (/) oder einen umgekehrten Schrägstrich (\) dargestellt. Es ist der standardmäßige Ausgangspunkt, wenn Sie sich am iDRAC anmelden. Wechseln Sie von root abwärts, indem Sie das Verb `cd` verwenden.

ANMERKUNG: Auf SM-CLP-Adresspfaden sind der Schrägstrich (/) und der umgekehrte Schrägstrich (\) untereinander austauschbar. Mit einem umgekehrten Schrägstrich am Ende einer Befehlszeile wird jedoch der Befehl in der nächsten Zeile fortgesetzt und der Schrägstrich wird ignoriert, wenn der Befehl geparst wird.

Wenn Sie z. B. zum dritten Eintrag des Systemereignisprotokolls (SEL) wechseln möchten, geben Sie den folgenden Befehl ein:

```
->cd /admin1/system1/logs1/log1/record3
```

Geben Sie das Verb `cd` ohne Ziel ein, um Ihren aktuellen Standort im Adressbereich zu finden. Die Abkürzungen `..` und `.` funktionieren auf dieselbe Weise wie unter Windows und Linux: `..` bezieht sich auf die übergeordnete Ebene und `.` bezieht sich auf die aktuelle Ebene.

Verb „show“ verwenden

Verwenden Sie zum Anzeigen weiterer Informationen zu einem Ziel das Verb `show`. Durch dieses Verb werden die Eigenschaften der Ziele, der Unterziele, der Verknüpfungen und eine Liste der SM-CLP-Verben angezeigt, die an einem bestimmten Standort zulässig sind.

Option -display verwenden

Anhand der Option `show -display` können Sie die Befehlsausgabe auf eines oder mehrere der folgenden Elemente einschränken: Eigenschaften, Ziele, Zuordnungen und Verben. Wenn Sie z. B. nur die Eigenschaften und Ziele des aktuellen Orts anzeigen möchten, verwenden Sie den folgenden Befehl:

```
show -display properties,targets
```

Wenn Sie nur bestimmte Eigenschaften aufführen möchten, qualifizieren Sie sie, wie im folgenden Befehl gezeigt wird:

```
show -d properties=(userid,name) /admin1/system1/sp1/account1
```

Wenn Sie nur eine Eigenschaft anzeigen möchten, können Sie die Klammern auslassen.

Option -level verwenden

Die Option `show -level` führt den Befehl `show` über weitere Ebenen neben dem angegebenen Ziel aus. Verwenden Sie zum Anzeigen aller Ziele und Eigenschaften im Adressbereich die Option `-l all`.

Option -output verwenden

Die Option `-output` legt eins von vier Formaten für die Ausgabe von SM-CLP-Verben fest: **text**, **clpcsv**, **keyword** und **clpxml**.

Das Standardformat ist **text**, die am einfachsten lesbare Ausgabe. Das **Format clpcsv** ist ein Format, bei dem Werte durch Kommas getrennt werden. Es eignet sich zum Laden in ein Tabellenkalkulationsprogramm. Das Format **keyword** gibt Informationen als Liste von keyword = value-Paaren (eins pro Zeile) aus. Das Format **clpxml** ist ein XML-Dokument, das ein **response** -XML-Element enthält. Die DMTF hat die Formate **clpcsv** und **clpxml** festgelegt, deren Spezifikationen auf der DMTF-Website unter **dmtf.org** verfügbar sind.

Das folgende Beispiel zeigt, wie der Inhalt des SEL in XML ausgegeben werden kann:

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

Anwendungsbeispiele

In diesem Abschnitt werden die Fallbeispiele für SMCLP dargestellt:

- Server-Energieverwaltung
- SEL-Verwaltung
- MAP-Zielnavigation

Server-Energieverwaltung

Die folgenden Beispiele stellen die Verwendung von SMCLP für die Ausführung von Energieverwaltungsaufgaben auf einem Managed System dar.

Geben Sie die folgenden Befehle an der SMCLP-Befehlseingabe ein:

- Ausschalten des Servers:
  ```
  stop /system1
  ```
  Die folgende Meldung wird angezeigt:
  ```
  system1 has been stopped successfully
  ```
- Einschalten des Servers:
  ```
  start /system1
  ```
  Die folgende Meldung wird angezeigt:
  ```
  system1 has been started successfully
  ```
- Neustart des Servers:
  ```
  reset /system1
  ```
  Die folgende Meldung wird angezeigt:
  ```
  system1 has been reset successfully
  ```

SEL-Verwaltung

Die folgenden Beispiele stellen die Verwendung von SMCLP für die Ausführung von SEL-bezogenen Aufgaben auf dem verwalteten System dar. Geben Sie die folgenden Befehle an der SMCLP-Befehlseingabe ein:

- So zeigen Sie das Systemereignisprotokoll (SEL) an:
  ```
  show/system1/logs1/log1
  ```
  Die folgende Ausgabe wird angezeigt:
  ```
  /system1/logs1/log1

  Targets:

  Record1

  Record2
  ```

```
Record3

Record4

Record5

Properties:

InstanceID = IPMI:BMC1 SEL Log

MaxNumberOfRecords = 512

CurrentNumberOfRecords = 5

Name = IPMI SEL

EnabledState = 2

OperationalState = 2

HealthState = 2

Caption = IPMI SEL

Description = IPMI SEL

ElementName = IPMI SEL

Commands:

cd

show

help

exit

version
```

- Zum Anzeigen des SEL-Datensatzes:
  `show/system1/logs1/log1`

  Die folgende Ausgabe wird angezeigt:

```
/system1/logs1/log1/record4

Properties:

LogCreationClassName= CIM_RecordLog

CreationClassName= CIM_LogRecord

LogName= IPMI SEL

RecordID= 1

MessageTimeStamp= 20050620100512.000000-000
```

```
Description= FAN 7 RPM: fan sensor, detected a failure

ElementName= IPMI SEL Record

Commands:

cd

show

help

exit

version
```

- Zum Löschen von SEL:
  `delete /system1/logs1/log1/record*`

  Die folgende Ausgabe wird angezeigt:

  ```
  All records deleted successfully
  ```

MAP-Zielnavigation

Die folgenden Beispiele stellen die Verwendung des Befehls „cd verb“ für die Navigation des MAP dar. In allen Beispielen wird angenommen, dass das anfängliche Standardziel „/“ ist.

Geben Sie die folgenden Befehle an der SMCLP-Befehlseingabe ein:

- Anhand des folgenden Befehls navigieren Sie für einen Neustart zum Systemziel:
  cd system1 reset – Das aktuelle Ziel lautet „/“.
- So wechseln Sie zum SEL-Ziel und zeigen die Protokolldatensätze an:
  `cd system1`

  `cd logs1/log1`

  `show`
- So zeigen Sie das aktuelle Ziel an:
  Geben Sie `cd .` ein.
- So gehen Sie eine Ebene nach oben:
  Geben Sie `cd ..` ein.
- So schließen Sie die Befehlseingabe:
  `exit`

19

Verwenden des iDRAC Service Module

Das iDRAC Service Module ist eine Software-Anwendung, die auf dem Server installiert werden sollte (sie ist nicht standardmäßig installiert). Es ergänzt iDRAC durch Überwachungsinformationen vom Betriebssystem. Es ergänzt iDRAC durch zusätzliche Daten für die Arbeit mit iDRAC-Schnittstellen wie z. B. für die Webschnittstelle, RACADM und WSMAN. Sie können die durch das iDRAC Service Module überwachten Funktionen für die Steuerung der auf dem Betriebssystem des Servers verbrauchten CPU- und Arbeitsspeicherkapazität konfigurieren.

ANMERKUNG: Sie können das iDRAC Service Module nur dann verwenden, wenn Sie die iDRAC Express- oder iDRAC Enterprise-Lizenz installiert haben.

Stellen Sie vor der Verwendung des iDRAC-Service-Moduls Folgendes sicher:

- Sie verfügen über die Berechtigung zum Anmelden, Konfigurieren und zur Serversteuerung in iDRAC, sodass Sie die Funktionen des iDRAC-Servicemoduls aktivieren und deaktivieren können.
- Deaktivieren Sie nicht die Option **iDRAC-Konfiguration über lokale RACADM-Schnittstelle**.
- Der Betriebssystem-zu-iDRAC-Passthrough-Kanal wurde über den internen USB-Bus in iDRAC aktiviert.

ANMERKUNG:

- Wenn das iDRAC Service Module zum ersten Mal ausgeführt wird, wird standardmäßig der Passthrough-Kanal zwischen Betriebssystem und iDRAC aktiviert. Wenn Sie diese Funktion deaktivieren, nachdem Sie das iDRAC Service Module installiert haben, müssen Sie sie manuell in iDRAC aktivieren.
- Wenn der Passthrough-Kanal zwischen Betriebssystem und iDRAC über LOM in iDRAC aktiviert wird, können Sie das iDRAC Service Module nicht verwenden.

Themen:

Installieren des iDRAC Service Module

Sie können das iDRAC Service Module von **dell.com/support** herunterladen und installieren. Sie müssen über Administratorberechtigungen für das Server-Betriebssystem verfügen, um das iDRAC Service Module installieren zu können. Weitere Informationen zur Installation finden Sie im *iDRAC Service Module Installation Guide* (Installationshandbuch zum iDRAC Service Module) unter **dell.com/support/manuals**.

ANMERKUNG: Diese Funktion gilt nicht für Dell Precision PR7910-Systeme.

Unterstützte Betriebssysteme für das iDRAC Service Module

Eine Liste der Betriebssysteme, die vom iDRAC-Servicemodul unterstützt werden, finden Sie im Installationshandbuch zum iDRAC-Servicemodul *iDRAC Service Module Installation Guide*, das unter **dell.com/openmanagemanuals** verfügbar ist.

Überwachungsfunktionen des iDRAC-Servicemoduls

Das iDRAC Service Module (iSM) bietet die folgenden Überwachungsfunktionen:

- Unterstützung des Redfish-Profils für Netzwerkattribute
- Remote-iDRAC-Hardware-Reset
- iDRAC-Zugriff über Host-BS (experimentelle Funktion)
- Bandinterne iDRAC-SNMP-Warnungen
- Anzeigen von Informationen zum Betriebssystem (BS)
- Replizieren von Lifecycle Controller-Protokollen zu den Betriebssystemprotokollen
- Automatische Systemwiederherstellung ausführen
- WMI (Windows Management Instrumentation) -Management-Provider bestücken
- Integration mit SupportAssist-Sammlung. Dieses Paket ist nur anwendbar, wenn Version 2.0 oder höher des iDRAC Service Module installiert ist. Weitere Informationen hierzu finden Sie unter Generieren der SupportAssist-Erfassung.
- Bereiten Sie das Entfernen der NVMe-PCIe-SSD vor. Weitere Informationen finden Sie unter Idracug_Vorbereiten auf das Entfernen einer NVMe-PCIe-SSD.

ANMERKUNG: Funktionen, wie Windows Management Instrumentation Provider, Vorbereiten zum Entfernen von NVMe PCIe SSDs über iDRAC und Automatisieren der SupportAssist-Betriebssystemerfassung, werden nur auf Dell PowerEdge-Servern mit einer Firmware-Version ab Version 2.00.00.00 unterstützt.

Unterstützung des Redfish-Profils für Netzwerkattribute

Das iDRAC Service Module v2.3 bietet zusätzliche Netzwerkattribute für iDRAC, die über mithilfe der REST-Clients über iDRAC abgerufen werden können. Weitere Informationen finden Sie unter „Unterstützung für das iDRAC-Redfish-Profil“.

Betriebssystem-Informationen

OpenManage Server Administrator gibt derzeit Betriebssysteminformationen und Hostnamen an iDRAC weiter. Das iDRAC Service Module stellt iDRAC ähnliche Informationen, wie beispielsweise BS-Name, BS-Version und FQDN (Fully Qualified Domain Name), bereit. Diese Überwachungsfunktion ist standardmäßig aktiviert. Diese Option ist nicht deaktiviert, wenn OpenManage Server Administrator auf dem Hostbetriebssystem installiert ist.

Bei Version 2.0 oder höher des iDRAC Service Module wurde die Funktion für Betriebssysteminformationen durch die Überwachung der BS-Netzwerkschnittstelle ergänzt. Wenn Version 2.0 oder höher des iDRAC Service Module mit iDRAC 2.00.00.00 verwendet wird, startet es die Überwachung der Betriebssystem-Netzwerkschnittstellen. Sie können diese Informationen über die iDRAC-Webschnittstelle, RACADM oder WSMAN abrufen. Weitere Informationen finden Sie unter Anzeigen der auf dem Hostbetriebssystem verfügbaren Netzwerkschnittstellen.

Wenn ein iDRAC-Servicemodul ab Version 2.0 mit einer iDRAC-Version verwendet wird, die niedriger als Version 2.00.00.00 ist, bietet die Informationsfunktion des Betriebssystems keine Überwachung der BS-Netzwerkschnittstelle an.

Replizieren von Lifecycle-Protokollen zum BS-Protokoll

Sie können eine Replikation der Lifecycle Controller-Protokolle in die Protokolle des Betriebssystems durchführen, sobald die Funktion in iDRAC aktiviert wird. Dies ist ähnlich wie bei der System Event Log (SEL)-Replikation von OpenManage Server Administrator. Alle Ereignisse, bei der die Option **OS Log** (**BS-Protokoll)** als das Ziel ausgewählt ist (auf der Seite **Alerts (Warnungen)** oder in den entsprechenden RACADM- oder WSMAN-Schnittstellen), werden unter Verwendung des iDRAC Service Module in das BS-Protokoll

repliziert. Der Standardsatz von Protokollen, die in die Betriebssystemprotokolle aufgenommen werden sollten, ist derselbe, der auch für SNMP-Warnungen oder -Traps konfiguriert wird.

Das iDRAC Service Module protokolliert auch die Ereignisse, die während der Ausfallzeiten des Betriebssystems aufgetreten sind. Die BS-Protokollierung des iDRAC Service Module erfolgt gemäß den IETF-Syslog-Standards für Linux-basierte Betriebssysteme.

ANMERKUNG: Ab iDRAC Service Module Version 2.1 kann der Replikationsspeicherort für die Lifecycle Controller-Protokolle im Windows-BS unter Verwendung des iDRAC Service Module-Installationsprogramms konfiguriert werden. Sie können während der Installation des iDRAC Service Module oder der Bearbeitung des iDRAC Service Module-Installationsprogramms den Speicherort festlegen.

Wenn OpenManage Server Administrator installiert ist, ist diese Überwachungsfunktion zur Vermeidung doppelter SEL-Einträge in der BS-Protokolldatei deaktiviert.

ANMERKUNG: Unter Microsoft Windows starten Sie den Windows Ereignisprotokolldienst neu oder starten das Host-BS neu, wenn iSM-Ereignisse unter Systemprotokollen anstelle der Anwendungsprotokolle protokolliert wird.

Optionen zur automatischen Systemwiederherstellung

Die automatische Systemwiederherstellungsfunktion ist ein Hardware-basierter Zeitgeber. Wenn ein Hardwarefehler auftritt, kann der Health Monitor aufgerufen werden, der Server wird jedoch genauso zurückgesetzt, als wenn der Netzschalter betätigt worden wäre. Die Implementierung von ASR erfolgt über einen „Heartbeat"-Zeitgeber, der kontinuierlich abwärts zählt. Der Health Monitor lädt den Zähler in regelmäßigen Abständen neu, um zu verhindern, dass er auf Null herunterzählt. Wenn der ASR bis auf Null herunterzählt, wird davon ausgegangen, dass das Betriebssystem gesperrt wurde. In diesem Fall versucht das System automatisch, einen Neustart durchzuführen.

Sie können Optionen zur automatischen Systemwiederherstellung wie z. B. Neustart, Aus-/Einschalten oder Ausschalten des Servers nach einem festgelegten Zeitintervall ausführen. Diese Funktion ist nur dann aktiviert, wenn der Watchdog-Zeitgeber des Betriebssystems deaktiviert ist. Wenn OpenManage Server Administrator installiert ist, ist diese Überwachungsfunktion zur Vermeidung doppelter Watchdog-Zeitgeber deaktiviert.

Windows Management Instrumentation-Provider

Bei WMI handelt es sich um eine Gruppe von Erweiterungen des Windows-Treibermodells, die eine Betriebssystemschnittstelle bereitstellt, über die instrumentierte Komponenten Informationen und Benachrichtigungen zur Verfügung stellen. WMI ist die Microsoft-Implementierung des Web-Based Enterprise Management (WBEM) und Common Information Model (CIM) der Distributed Management Task Force (DMTF) für die Verwaltung von Serverhardware, Betriebssystemen und Anwendungen. WMI-Anbieter helfen bei der Integration mit Systemverwaltungskonsolen wie Microsoft System Center und ermöglichen die Erstellung von Skripten zur Verwaltung von Microsoft Windows Server-Lösungen.

Sie können die WMI-Option in iDRAC aktivieren oder deaktivieren. iDRAC gibt die WMI-Klassen über das iDRAC Service Module weiter und stellt so Informationen zum Serverstatus bereit. Standardmäßig ist die WMI-Informationsfunktion aktiviert. Das iDRAC Service Module stellt die von WSMAN überwachten Klassen in iDRAC über WMI zur Verfügung. Die Klassen werden im Namespace **root/cimv2/dcim** verfügbar gemacht.

Auf die Klassen können Sie mithilfe einer beliebigen Standard-WMI-Client-Schnittstelle zugreifen. Weitere Informationen finden Sie in den Profildokumenten.

Die folgenden Beispiele verwenden die Klasse DCIM_account, um die Möglichkeiten zu illustrieren, die die WMI-Informationsfunktion im iDRAC Service Module bietet. Weitere Informationen zu den unterstützten Klassen und Profilen finden Sie in der WSMAN-Profildokumentation im Dell TechCenter.

Tabelle 46. Beispiele:

CIM-Schnittstelle	WinRM	WMIC	PowerShell
Aufzählen von Instanzen einer Klasse	`winrm e wmi/root/cimv2/dcim/dcim_account`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account`	`Get-WmiObject dcim_account -namespace root/cimv2/dcim`
Entscheiden Sie sich für eine bestimmte Instanz einer Klasse	`winrm g wmi/root/cimv2/dcim/DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.2+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name="iDRAC.Embedded.1#Users.16"`	`Get-WmiObject -Namespace root\cimv2\dcim -Class dcim_account -filter "Name='iDRAC.Embedded.1#Users.16'"`
Get-zugeordnete Instanzen einer Instanz	`winrm e wmi/root/cimv2/dcim/* -dialect:association -filter:{object=DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc}`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name='iDRAC.Embedded.1#Users.2' ASSOC`	`Get-Wmiobject -Query "ASSOCIATORS OF {DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace root/cimv2/dcim`
Get-Referenzen einer Instanz	`winrm e wmi/root/cimv2/dcim/* -dialect:association -associations -filter:{object=DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc}`	Nicht anwendbar	`Get-Wmiobject -Query "REFERENCES OF {DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace root/cimv2/dcim`

Remote-iDRAC-Hardware-Reset

Durch die Verwendung von iDRAC können Sie die unterstützten Server auf kritische Probleme mit der Systemhardware, -firmware oder -software überwachen. Manchmal reagiert iDRAC ggf. aus verschiedenen Gründen nicht mehr. Während solcher Szenarien müssen Sie den Server ausschalten und iDRAC zurücksetzen. Um die iDRAC-CPU zurückzusetzen, müssen Sie den Server bzw. das System aus- und wieder einschalten.

Durch die Verwendung der iDRAC-Funktion für einen Remote-Hard-Reset, wenn iDRAC nicht mehr reagiert, können Sie iDRAC remote zurücksetzen, ohne das System aus- und wieder einzuschalten. Um iDRAC remote zurückzusetzen, stellen Sie sicher, dass Sie über Administratorrechte auf dem Host-Betriebssystem verfügen. Standardmäßig ist die iDRAC-Funktion für den Remote-Hard-Reset aktiviert. Sie können den Hard-Reset für iDRAC über die iDRAC-Webschnittstelle, RACADM und WS-MAN durchführen.

ANMERKUNG: Diese Funktion wird nicht auf Dell PowerEdge R930-Servern unterstützt, sondern nur auf Dell PowerEdge-Servern ab der 13. Generation.

Befehlsverwendung

Dieser Abschnitt enthält Informationen zur Befehlsverwendung auf Windows-, Linux- und ESXi-Betriebssystemen zur Durchführung eines iDRAC-Hardware-Resets.

- **Windows**
  - Unter Verwendung der lokalen Windows Management Instrumentation (WMI):

    ```
    winrm  i  iDRACHardReset wmi/root/cimv2/dcim/DCIM_iSMService?
    InstanceID="iSMExportedFunctions"
    ```

  - Unter Verwendung der Remote-WMI-Schnittstelle:

    ```
    winrm i iDRACHardReset wmi/root/cimv2/dcim/dcim_ismservice -u:<admin-username> -p:<admin-
    passwd> -r: http://<remote-hostname OR IP>/wsman -a:Basic -encoding:utf-8 -skipCACheck -
    skipCNCheck
    ```

  - Unter Verwendung des Windows PowerShell-Skripts mit und ohne force-Option:

    ```
    Invoke-iDRACHardReset -force
    ```

    ```
    Invoke-iDRACHardReset
    ```

  - Unter Verwendung der Verknüpfung **Programmmenü**:

    Zur Vereinfachung bietet iSM eine Verknüpfung im **Programm-Menü** des Windows-Betriebssystems. Wenn Sie die Option **Remote iDRAC Hard Reset (Remote-Hard-Reset für iDRAC)** auswählen, werden Sie dazu aufgefordert, das Zurücksetzen von iDRAC zu bestätigen. Nach der Bestätigung wird iDRAC zurückgesetzt und das Ergebnis des Vorgangs wird angezeigt.

    ANMERKUNG: Die folgende Warnmeldung wird im Event Viewer (Ereignisanzeige) unter der Kategorie Application Logs (Anwendungsprotokolle) angezeigt. Bei dieser Warnung sind keine weiteren Maßnahmen erforderlich.

    ```
    A provider, ismserviceprovider, has been registered in the Windows Management
    Instrumentation namespace Root\CIMV2\DCIM to use the LocalSystem account. This account
    is privileged and the provider may cause a security violation if it does not correctly
    impersonate user requests.
    ```

- **Linux**

  iSM stellt einen ausführbaren Befehl auf allen iSM-unterstützten Linux-Betriebssystemen bereit. Sie können diesen Befehl durch die Anmeldung beim Betriebssystem mithilfe von SSH (oder gleichwertig) ausführen.

  ```
  Invoke-iDRACHardReset
  ```

  ```
  Invoke-iDRACHardReset -f
  ```

- **ESXi**

  Auf allen von iSM unterstützten ESXi-Betriebssystemen unterstützt iSM Version 2.3 einen CMPI-Methodenanbieter (Common Management Programming Interface), um den iDRAC-Reset remote unter Verwendung der WinRM-Remote-Befehle durchzuführen.

  ```
  winrm i iDRACHardReset http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/
  DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=
  iSMExportedFunctions -u:<root-username> -p:<passwd> -r:https://<Host-IP>:443/wsman -a:basic -
  encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck
  ```

ANMERKUNG: Das VMware ESXi-Betriebssystem fordert den Benutzer nicht auf, den Reset des iDRAC vor dem Durchführen zu bestätigen.

ANMERKUNG: Aufgrund von Einschränkungen des VMware ESXi-Betriebssystems wird die iDRAC-Konnektivität nach dem Zurücksetzen nicht vollständig wiederhergestellt. Stellen Sie sicher, dass Sie iDRAC manuell zurücksetzen. Weitere Informationen finden Sie unter "Remote-Hard-Reset für iDRAC" in diesem Dokument.

Fehlerbehandlung

Tabelle 47. Fehlerbehandlung

Ergebnis	Beschreibung
0	Erfolgreich
1	Nicht unterstützte BIOS-Version für iDRAC-Reset
2	Nicht unterstützte Plattform
3	Zugriff verweigert
4	iDRAC-Reset fehlgeschlagen

Bandinterne Unterstützung für iDRAC-SNMP-Warnungen

Bei Verwendung des iDRAC-Servicemoduls in Version 2.3 können Sie SNMP-Benachrichtigungen vom Host-Betriebssystem empfangen, die den vom iDRAC generierten Benachrichtigungen ähneln.

Sie können die iDRAC-SNMP-Warnungen auch ohne Konfiguration von iDRAC überwachen und den Server remote durch Konfigurieren der SNMP-Traps und -Ziele auf dem Host-Betriebssystem verwalten. In iDRAC Service Module v2.3 oder höher konvertiert diese Funktion alle in die Betriebssystemprotokolle replizierten Lifecycle-Protokolle in SNMP-Traps.

ANMERKUNG: Diese Funktion ist nur dann aktiv, wenn die Replikationsfunktion der Lifecycle-Protokolle aktiviert ist.

ANMERKUNG: Auf Linux-Betriebssystemen erfordert diese Funktion ein aktiviertes Master- oder BS-SNMP mit SNMP-Multiplexing-Protokoll (SMUX).

Standardmäßig ist diese Funktion deaktiviert. Obwohl der In-Band-SNMP-Warnmechanismus mit dem iDRAC-SNMP-Warnmechanismus koexistieren kann, verfügen die aufgezeichneten Protokolle möglicherweise über redundante SNMP-Warnungen von beiden Quellen. Es wird empfohlen, entweder die In-Band- oder Out-of-Band-Option anstelle von beiden zu verwenden.

Befehlsverwendung

Dieser Abschnitt enthält Informationen zur Befehlsverwendung auf Windows-, Linux- und ESXi-Betriebssystemen.

- **Windows-Betriebssystem**
  - Unter Verwendung der lokalen Windows Management Instrumentation (WMI):

    ```
    winrm i EnableInBandSNMPTraps
    wmi/root/cimv2/dcim/DCIM_iSMService?InstanceID="iSMExportedFunctions" @{state="[0/1]"}
    ```

  - Unter Verwendung der Remote-WMI-Schnittstelle:

    ```
    winrm i EnableInBandSNMPTraps wmi/root/cimv2/dcim/DCIM_iSMService?
    InstanceID="iSMExportedFunctions" @{state="[0/1]"}
    -u:<admin-username> -p:<admin-passwd> -r:http://<remote-hostname OR IP>/wsman  -a:Basic -
    encoding:utf-8 -skipCACheck -skipCNCheck
    ```

- **LINUX-Betriebssystem**

  Auf allen iSM-unterstützten Linux-Betriebssystemen stellt iSM einen ausführbaren Befehl bereit. Sie können diesen Befehl durch die Anmeldung beim Betriebssystem mithilfe von SSH (oder gleichwertig) ausführen.

  Beginnend mit iSM 2.4.0 können Sie Agent-x als das Standardprotokoll für die bandinternen iDRAC-SNMP-Alarme unter Verwendung des folgenden Befehls konfigurieren:

  ```
  ./Enable-iDRACSNMPTrap.sh 1/agentx -force
  ```

Wenn `–force` nicht angegeben ist, stellen Sie sicher, dass net-SNMP konfiguriert ist, und starten den snmpd-Dienst neu.

- Gehen Sie wie folgt vor, um diese Funktion zu aktivieren:

```
Enable-iDRACSNMPTrap.sh 1
```

```
Enable-iDRACSNMPTrap.sh enable
```

- Gehen Sie wie folgt vor, um diese Funktion zu deaktivieren:

```
Enable-iDRACSNMPTrap.sh 0
```

```
Enable-iDRACSNMPTrap.sh disable
```

ANMERKUNG: Die Option --force konfiguriert Net-SNMP für die Weiterleitung der Traps. Sie müssen jedoch das Trap-Ziel konfigurieren.

- **VMware ESXi-Betriebssystem**

  Auf allen von iSM unterstützten ESXi-Betriebssystemen unterstützt iSM Version 2.3 einen CMPI-Methodenanbieter (Common Management Programming Interface), um diese Funktion remote unter Verwendung der WinRM-Remote-Befehle zu aktivieren.

```
winrm i EnableInBandSNMPTraps http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:<user-name> -p:<passwd> -r:https://<remote-host-name
```

```
ip-address>:443/wsman -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck @{state="[0/1]"}
```

ANMERKUNG: Sie müssen die systemweiten VMware ESXi-SNMP-Einstellungen für Traps überprüfen und konfigurieren.

ANMERKUNG: Weitere Einzelheiten finden Sie im technischen Whitepaper zu bandinternen SNMP-Benachrichtigungen In-Band SNMP Alerts, das unter http://en.community.dell.com/techcenter/extras/m/white_papers verfügbar ist.

iDRAC-Zugriff über Host-BS (experimentelle Funktion)

Mithilfe dieser Funktion können Sie die Hardwareparameter über die iDRAC-Webschnittstelle, WS-MAN und die Redfish-Schnittstellen unter Verwendung der Host-IP-Adresse und ohne Konfiguration der iDRAC-IP-Adresse konfigurieren und überwachen. Sie können die iDRAC-Anmeldeinformationen verwenden, wenn der iDRAC-Server nicht konfiguriert ist, oder weiterhin dieselben iDRAC-Anmeldeinformationen nutzen, wenn der iDRAC-Server zuvor schon konfiguriert wurde.

iDRAC-Zugriff über Windows-Betriebssysteme

Sie können diese Aufgabe mithilfe der folgenden Methoden durchführen:

- Installieren Sie die iDRAC-Zugriffsfunktion unter Verwendung des Webpack.
- Konfiguration unter Verwendung des iSM-PowerShell-Skripts

Installation unter Verwendung von MSI

Sie können diese Funktion unter Verwendung des web-pack installieren. Diese Funktion ist bei einer typischen iSM-Installation deaktiviert. Falls diese Funktion aktiviert ist, lautet die standardmäßige Überwachungsportnummer 1266. Sie können diese Portnummer innerhalb des Bereichs von 1024 und 65535 ändern. iSM leitet die Verbindung zu iDRAC weiter. iSM erstellt dann einen eingehende Firewall-Regel, OS2iDRAC. Die Überwachungsportnummer wird zur OS2iDRAC-Firewall-Regel im Hostbetriebssystem hinzugefügt, wodurch eingehende Verbindungen ermöglicht werden. Die Firewall-Regel wird automatisch aktiviert, wenn diese Funktion aktiviert ist.

Beginnend mit iSM 2.4.0 können Sie den aktuellen Status und die Überwachungsportkonfiguration durch Verwendung des folgenden PowerShell-cmdlet abrufen:

```
Enable-iDRACAccessHostRoute –status get
```

Die Ausgabe dieses Befehls gibt an, ob diese Funktion aktiviert oder deaktiviert ist. Wenn diese Funktion aktiviert ist, wird die Überwachungsportnummer angezeigt.

ANMERKUNG: Die Microsoft IP-Hilfsdienste müssen auf Ihrem System ausgeführt werden, damit diese Funktion funktioniert.

Verwenden Sie für den Zugriff auf die iDRAC-Webschnittstelle das Format `https://<host-name>` oder `OS-IP>:443/login.html` im Browser, wobei Folgendes gilt:

- `<host-name>`: vollständiger Hostname des Servers, auf dem iSM für den iDRAC-Zugriff über die Betriebssystemfunktion installiert und konfiguriert ist. Sie können die BS-IP-Adresse verwenden, wenn der Hostname nicht vorhanden ist.
- `443`: die standardmäßige iDRAC-Portnummer. Diese wird als Verbindungsportnummer bezeichnet, an die alle eingehenden Verbindungen auf der Überwachungsportnummer umgeleitet werden. Sie können die Portnummer über die iDRAC-Webschnittstelle, WS-MAN und die RACADM-Schnittstellen ändern.

Konfiguration unter Verwendung von iSM-PowerShell-cmdlet

Falls diese Funktion während der Installation von iSM deaktiviert ist, können Sie sie unter Verwendung des folgenden, von iSM bereitgestellten Windows PowerShell-Befehls aktivieren:

```
Enable-iDRACAccessHostRoute
```

Falls die Funktion bereits konfiguriert wurde, können Sie sie deaktivieren oder modifizieren, indem Sie den PowerShell-Befehl mit den entsprechenden Optionen verwenden. Folgende Optionen sind verfügbar:

- **Status**: Dieser Parameter ist obligatorisch. Bei den Werten wird nicht zwischen Groß- und Kleinschreibung unterschieden. Mögliche Werte sind **true**, **false** oder **get**.
- **Port**: Dies ist die Überwachungsportnummer. Wenn Sie keine Portnummer angeben, wird die standardmäßige Portnummer 1266 verwendet. Wenn der Parameterwert für **Status** FALSE ist, können Sie die restlichen Parameter ignorieren. Sie müssen eine neue Portnummer eingeben, die nicht bereits für diese Funktion konfiguriert ist. Die neuen Portnummereinstellungen überschreiben die vorhandene, eingehende OS2iDRAC-Firewall-Regel und Sie können die neue Portnummer für die Verbindung mit iDRAC verwenden. Der Wertebereich liegt zwischen 1024 und 65535.
- **IPRange**: Dieser Parameter ist optional und liefert einen Bereich von IP-Adressen, die eine Verbindung zu iDRAC über das Hostbetriebssystem herstellen dürfen. Der IP-Adressbereich liegt im Classless Inter-Domain Routing (CIDR)-Format vor – einer Kombination aus IP-Adresse und Subnetzmaske. Beispiel: 10.94.111.21/24. Der Zugriff auf iDRAC ist für IP-Adressen, die nicht innerhalb dieses Bereichs liegen, beschränkt.

ANMERKUNG: Diese Funktion unterstützt nur IPv4-Adressen.

iDRAC-Zugriff über Linux-Betriebssysteme

Sie können diese Funktion mithilfe der Datei **setup.sh** installieren, die im Rahmen des Web-Pack verfügbar ist. Diese Funktion ist bei einer standardmäßigen oder typischen iSM-Installation deaktiviert. Verwenden Sie zum Abrufen des Status dieser Funktion den folgenden Befehl:

```
Enable-iDRACAccessHostRoute get-status
```

Um diese Funktion zu installieren, aktivieren und konfigurieren, verwenden Sie den folgenden Befehl:

```
./Enable-iDRACAccessHostRoute <Enable-Flag> [ <source-port> <source-IP-range/source-ip-range-mask>]
```

<Enable-Flag>=0	Disable (Deaktivieren) `<source-port>` und `<source-IP-range/source-ip-range-mask>` sind nicht erforderlich.
<Enable-Flag>=1	Aktivieren `<source-port>` ist erforderlich und `<source-ip-range-mask>` ist optional.
<source-IP-range>	IP-Bereich im Format *<IP-Adresse/Subnetzmaske>*. Beispiel: 10.95.146.98/24

Koexistenz von OpenManage Server Administrator mit dem iDRAC Service Module

In einem System können OpenManage Server Administrator und das iDRAC Service Module gleichzeitig und unabhängig voneinander funktionieren.

Wenn Sie die Überwachungsfunktionen während der Installation des iDRAC Service Module aktiviert haben, deaktiviert das iDRAC Service Module nach Abschluss der Installation und Erkennung von OpenManage Server Administrator jene Überwachungsfunktionen, die sich überschneiden. Wenn OpenManage Server Administrator ausgeführt wird, deaktiviert das iDRAC Service Module die sich überschneidenden Überwachungsfunktionen nach Anmeldung beim Betriebssystem und bei iDRAC.

Wenn Sie diese Überwachungsfunktionen zu einem späteren Zeitpunkt mithilfe der iDRAC-Schnittstellen erneut aktivieren, werden die gleichen Prüfungen durchgeführt, und die Funktionen werden abhängig davon aktiviert, ob OpenManage Server Administrator ausgeführt wird oder nicht.

Verwendung des iDRAC Servicemoduls über die iDRAC-Webschnittstelle

So verwenden Sie das iDRAC Servicemodul über die iDRAC-Webschnittstelle:

1 Gehen Sie zu **Übersicht** > **Server** > **Service Module**.

Die Seite **iDRAC Service Module-Setup** wird geöffnet.

2 Sie können Folgendes anzeigen:

- Die auf dem Host-Betriebssystem installierte Version des iDRAC-Servicemoduls.
- Den Verbindungsstatus des iDRAC Service Module mit iDRAC.

3 Wählen Sie zum Ausführen bandexterner Überwachungsfunktionen eine oder mehrere der folgenden Optionen aus:

- **BS-Information** – Informationen zum Betriebssystem anzeigen.
- **Lifecycle-Protokoll in BS-Protokoll replizieren** – Lifecycle Controller-Protokolle in Betriebssystemprotokolle einbeziehen. Diese Option ist deaktiviert, wenn OpenManage Server Administrator auf dem System installiert ist.
- **WMI-Informationen** – Schließt WMI-Informationen ein.
- **Automatische Systemwiederherstellung** – Ausführen der automatischen Systemwiederherstellung nach einer festgelegten Zeit (in Sekunden):
  - **Neustarten**
  - **System ausschalten**
  - **System aus- und einschalten**

  Diese Option ist deaktiviert, wenn OpenManage Server Administrator auf dem System installiert ist.

Verwenden des iDRAC Servicemodul von RACADM

Zur Verwendung des iDRAC-Servicemoduls über RACADM verwenden Sie die Objekte in der Gruppe **ServiceModule**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Unter Verwendung des iDRAC-Servicemoduls unter BS Windows Nano

Installationsanleitungen finden Sie im *iDRAC Service Module Installation Guide (iDRAC-Servicemodul-Installationshandbuch)*.

Um zu überprüfen, ob der iSM-Dienst ausgeführt wird, verwenden Sie den folgenden Befehl „cmdlet“:

```
Get-Service "iDRAC Service Module"
```

Sie können die replizierten Lifecycle-Protokolle mithilfe von WMI oder Windows PowerShell-Abfrage einsehen:

```
GetCimInstance –Namespace root/cimv2 – className win32_NTLogEvent
```

Standardmäßig sind die Protokolle unter **Ereignis-Viewer** > **Anwendungs- und Dienstprotokolle** > **System** verfügbar.

20

Verwendung der USB-Schnittstelle für das Server-Management

Bei Dell PowerEdge Servern der 12. Generation sind alle USB-Ports für den Server vorgesehen. Bei Servern der 13. Generation wird einer der USB-Ports der Frontblende vom iDRAC für Verwaltungszwecke wie z. B. Vorabbereitstellung und Beheben von Störungen verwendet. Der Port ist mit einem Symbol versehen, das kennzeichnet, dass es sich um einen Verwaltungsport handelt. Alle Server der 13. Generation mit LCD-Bildschirm unterstützen diese Funktion. Dieser Port ist nicht verfügbar bei einigen Variationen der Modelle 200–500 ohne LCD. In solchen Fällen können Sie diese Ports auch für das Betriebssystem des Servers verwenden.

ANMERKUNG: Diese Funktion wird nicht auf PowerEdge R930-Servern unterstützt.

Wenn der USB-Anschluss von iDRAC verwendet wird:

- Die USB-Netzwerkschnittstelle ermöglicht die Verwendung vorhandener bandexterner Remote-Management-Tools von einem tragbaren Gerät wie einem Notebook mithilfe eines USB-Kabels des Typs A/A, das mit iDRAC verbunden ist. Dem iDRAC wird die IP-Adresse 169.254.0.3 zugewiesen und dem Verwaltungsgerät wird die IP-Adresse 169.254.0.4 zugewiesen.
- Sie können ein Server-Konfigurationsprofil in dem USB-Gerät speichern und die Server-Konfiguration von dem USB-Gerät aktualisieren.

ANMERKUNG: Diese Funktion wird unterstützt auf:

- USB-Geräten, die ein FAT-Dateisystem und eine einzelne Partition aufweisen.
- Allen Dell Tablets mit Windows 8 und Windows RT, einschließlich des XPS 10 und des Venue Pro 8. Verwenden Sie auf Geräten mit USB-Mini-Anschluss, wie z. B. dem XPS 10 und dem Venue Pro 8, den On-the-Go (OTG)-Dongle und ein Kabel des Typs A/A.

Themen:

Zugehöriger Link

Konfigurieren von iDRAC über das Server-Konfigurationsprofil auf dem USB-Gerät
Zugriff auf die iDRAC-Schnittstelle über eine direkte USB-Verbindung

Zugriff auf die iDRAC-Schnittstelle über eine direkte USB-Verbindung

Mit der iDRAC Direct-Funktion können Sie eine direkte Verbindung zwischen Ihrem Notebook und dem iDRAC-USB-Port herstellen. Diese Funktion ermöglicht Ihnen die direkte Interaktion mit den iDRAC-Schnittstellen wie z. B. der Webschnittstelle, RACADM und WSMan für erweiterte Serververwaltung und -wartung.

Verwenden Sie ein Kabel des Typs A/A zum Anschluss des Notebooks an den Server.

Wenn iDRAC als USB-Laufwerk fungiert und der Verwaltungsportmodus auf **Automatic (Automatisch)** eingestellt ist, verwendet iDRAC immer den USB-Port. Der Port wechselt nicht automatisch zum Betriebssystem.

Eine Liste der unterstützten Browser und Betriebssysteme finden Sie in den Versionshinweisen unter Dell.com/idracmanuals.

ANMERKUNG: Wenn Sie Windows-Betriebssysteme verwenden, müssen Sie möglicherweise einen RNDIS-Treiber installieren, um diese Funktion verwenden zu können.

Zum Zugriff auf die iDRAC-Schnittstelle über den USB-Anschluss:

1 Schalten Sie alle Wireless-Netzwerke ab, und trennen Sie die Verbindung zu allen anderen kabelgebundenen Netzwerken.
2 Stellen Sie sicher, dass der USB-Port aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren der USB-Verwaltungsschnittstelle.
3 Schließen Sie ein Kabel des Typs A/A vom Laptop an den USB-Anschluss von iDRAC an.
   Die Management-LED (falls vorhanden) wechselt zu Grün und bleibt zwei Sekunden lang eingeschaltet.
4 Warten Sie, bis das Notebook und iDRAC die IP-Adressen 169.254.0.4 und 169.254.0.3 erhalten. Es kann einige Sekunden dauern, bis die IP-Adressen zugewiesen werden.
5 Beginnen Sie mit der Verwendung der iDRAC-Netzwerkschnittstellen, wie z. B. der Webschnittstelle, RACADM oder WSMan.
6 Wenn iDRAC den USB-Port verwendet, blinkt die LED zur Anzeige von Aktivität. Der Blinkintervall beträgt vier pro Sekunde.
7 Nach Abschluss der gewünschten Aktionen trennen Sie das USB-Kabel vom System.
   Danach schaltet sich die LED aus.

Konfigurieren von iDRAC über das Server-Konfigurationsprofil auf dem USB-Gerät

Mit der neuen iDRAC Direkt-Funktion können Sie iDRAC direkt am Server konfigurieren. Zuerst müssen Sie die USB-Verwaltungsport-Einstellungen in iDRAC konfigurieren, setzen Sie dann das USB-Gerät mit dem Server-Konfigurationsprofil ein und importieren Sie das Server-Konfigurationsprofil vom USB-Gerät in iDRAC.

ANMERKUNG: Sie können die USB-Verwaltungsschnittstelle unter Verwendung der iDRAC-Schnittstellen nur dann festlegen, wenn kein USB-Gerät mit dem Server verbunden ist.

ANMERKUNG: Auf PowerEdge-Servern ohne LCD und LED-Bedienfeld wird der USB-Schlüssel nicht unterstützt.

Zugehöriger Link

Konfigurieren der USB-Verwaltungsschnittstelle
Importieren der Server-Konfiguration vom USB-Gerät

Konfigurieren der USB-Verwaltungsschnittstelle

Sie können den USB-Anschluss in iDRAC konfigurieren:

- Aktivieren oder Deaktivieren eines Server-USB-Anschlusses unter Verwendung des BIOS-Setup-Programms. Wenn Sie diesen entweder auf **Alle Schnittstellen ausgeschaltet** oder **Anschlüsse an der Vorderseite ausgeschaltet** einstellen, deaktiviert iDRAC auch den verwalteten USB-Anschluss. Sie können den Schnittstellen/Status unter Verwendung der iDRAC-Schnittstellen anzeigen. Wenn der Status deaktiviert ist:
  - verarbeitet iDRAC keine USB-Geräte oder Hosts, die mit den verwalteten USB-Anschluss verbunden sind.
  - Sie können die verwalteten USB-Konfiguration verändern, aber die Einstellungen haben keine Auswirkungen, bis die Frontblenden-USB-Anschlüsse im BIOS aktiviert sind.
- Stellen Sie den USB-Port-Modus ein, der bestimmt, ob der USB-Anschluss von iDRAC, oder von dem Server-Betriebssystem verwendet wird:
  - Automatisch (Standard): Wenn ein USB-Gerät nicht von iDRAC unterstützt wird, oder wenn das Server-Profil auf dem Gerät nicht anwesend ist, wird der USB-Anschluss von iDRAC abgetrennt und mit dem Server verbunden. Wenn ein Gerät aus dem Server entfernt wird, wird die Schnittstellenkonfiguration zurückgesetzt, und für die Verwendung von iDRAC bestimmt.
  - Standard-Betriebssystemverwendung: Das USB-Gerät wird immer vom Betriebssystem verwendet.
  - Nur iDRAC Direkt: Das USB-Gerät wird immer vom iDRAC verwendet.

Sie müssen zum Konfigurieren der USB-Verwaltungsschnittstelle über die Berechtigung zur Server-Steuerung verfügen.

Wenn ein USB-Gerät angeschlossen ist, zeigt die Seite System-Bestandsaufnahme die USB-Geräteinformationen unter dem Abschnitt Hardware-Bestandsaufnahme an.

Ein Ereignis wird im Lifecycle Controller-Protokoll protokolliert, wenn:

- das Gerät sich im automatischen oder iDRAC-Modus befindet und das USB-Gerät angeschlossen oder entfernt wird
- der USB-Verwaltungsanschlussmodus geändert wird
- das Gerät automatisch von iDRAC auf BS schaltet
- das Gerät von iDRAC oder dem Betriebssystem ausgeworfen wird.

Wenn ein Gerät seine Leistungsanforderungen an die Stromversorgung übersteigt, wie von USB-Spezifikation erlaubt, wird das Gerät getrennt, und ein Überstromereignis wird mit den folgenden Eigenschaften generiert:

- Kategorie: „Systemfunktionszustand“
- Typ: USB-Gerät
- Schweregrad: Warnung
- Zulässige Benachrichtigungen: E-Mail, SNMP-Trap, Remote Syslog- und WS-Ereignisse.
- Maßnahmen: Keine.

Eine Fehlermeldung wird angezeigt, und im Lifecycle Controller-Protokoll protokolliert wenn:

- Sie versuchen, den USB-Verwaltungsanschluss ohne Benutzerberechtigung für die Serversteuerung zu konfigurieren.
- Ein USB-Gerät wird von iDRAC verwendet und Sie versuchen, den USB-Verwaltungsanschlussmodus zu ändern.
- Ein USB-Gerät wird von iDRAC verwendet und Sie entfernen das Gerät.

Konfigurieren der USB-Verwaltungsschnittstelle über die Webschnittstelle

So konfigurieren Sie die USB-Schnittstelle:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Hardware** > **USB-Verwaltungsschnittstelle**.
Die Seite **Konfigurieren der USB-Verwaltungsschnittstelle** wird angezeigt.

2 Wählen Sie aus dem Drop-Down-Menü **Modus USB-Verwaltungsschnittstelle** eine der folgenden Optionen:
- **Automatisch** – USB-Schnittstelle wird vom iDRAC oder dem Betriebssystem des Servers verwendet.
- **Standardnutzung des Betriebssystems** – USB-Schnittstelle wird von dem Betriebssystem des Servers verwendet.
- **Nur iDRAC Direct** – USB-Schnittstelle wird von iDRAC verwendet.

3 Von iDRAC verwaltet: USB XML-Konfiguration Drop-Down-Menü, wählen Sie die Optionen aus, um einen Server zu konfigurieren, indem Sie XML-Konfigurationsdateien importieren, die auf einem USB-Laufwerk gespeichert sind:
- **Deaktiviert**
- **Nur aktiviert, wenn der Server standardmäßige Anmeldeinformationseinstellungen hat**
- **Aktiviert**

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

4 Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

Konfigurieren der USB-Verwaltungsschnittstelle über RACADM

Zum Konfigurieren der USB-Verwaltungsschnittstelle verwenden Sie die folgenden RACADM-Unterbefehle und -Objekte:

- So zeigen Sie den Status der USB-Schnittstelle an:
```
racadm get iDRAC.USB.ManagementPortStatus
```
- So zeigen Sie die Konfiguration der USB-Schnittstelle an:
```
racadm get iDRAC.USB.ManagementPortMode
```
- So ändern Sie die Konfiguration der USB-Schnittstelle:
```
racadm set iDRAC.USB.ManagementPortMode <Automatic|Standard OS Use|iDRAC|>
```

ANMERKUNG: Stellen Sie sicher, dass Sie das Standard-BS-Attribut bei der Verwendung im RACADM-Befehlssatz in einfache Anführungszeichen setzen.

- So zeigen Sie die USB-Gerätebestandsaufnahme an:

```
racadm hwinventory
```

- So richten Sie die Konfiguration von Überstromalarm ein:

```
racadm eventfilters
```

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Konfigurieren der USB-Verwaltungsschnittstelle über das Dienstprogramm für iDRAC-Einstellungen

So konfigurieren Sie die USB-Schnittstelle:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Medien und USB-Schnittstelleneinstellungen**.
   Die Seite **iDRAC-Einstellungen für Media und USB-Schnittstelleneinstellungen** wird angezeigt.
2. Führen Sie von dem Drop-Down-Menü **USB-Verwaltungsschnittstellenmodus** die folgenden Schritte aus:
   - **Automatisch** – USB-Schnittstelle wird vom iDRAC oder dem Betriebssystem des Servers verwendet.
   - **Standardnutzung des Betriebssystems** – USB-Schnittstelle wird von dem Betriebssystem des Servers verwendet.
   - **Nur iDRAC Direct** – USB-Schnittstelle wird von iDRAC verwendet.
3. Wählen Sie vom Drop-Down-Menü **iDRAC-Direct: USB-Konfigurations-XML** die Optionen zur Konfiguration eines Servers, indem Sie das Server-Konfigurationsprofil auf einem USB-Laufwerk speichern:
   - **Deaktiviert**
   - **Aktiviert, wenn der Server nur standardmäßige Anmeldeinformationseinstellungen besitzt**
   - **Aktiviert**

   Weitere Informationen zu den verfügbaren Feldern finden Sie in der *iDRAC Settings Utility Online Help* (Online-Hilfe des Dienstprogramms für iDRAC-Einstellungen).
4. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**. Die Einstellungen sind damit gespeichert.

Importieren der Server-Konfiguration vom USB-Gerät

Stellen Sie sicher, dass Sie im Stammverzeichnis des USB-Geräts mit Namen System_Configuration_XML ein Verzeichnis erstellen, in dem sowohl die config.xml- und die control.xml-Dateien enthalten sind:

- DAS Serverkonfigurationsprofil ist im System_Configuration_XML-Unterverzeichnis unter dem Stammverzeichnis des USB-Geräts enthalten. Diese Datei enthält alle Attribut-Wert-Paare des Servers. Dies schließt Attribute von iDRAC, PERC, RAID und BIOS ein. Sie können diese Datei bearbeiten, um ein bestehendes Attribut auf dem Server zu konfigurieren. Der Name kann <servicetag>-config.xml, <modelnumber>-config.xml, oder config.xml sein.
- Steuerungs-XML-Datei – Schließt die Parameter zur Steuerung des Importvorgangs ein und verfügt nicht über die Attribute des iDRAC oder einer anderen Komponente im System. Diese Steuerungsdatei enthält die folgenden drei Parameter:
  - ShutdownType – Ordentliches Herunterfahren, erzwungen, Kein Neustart.
  - TimeToWait (in Sekunden) – mindestens 300 und höchstens 3600.
  - EndHostPowerState – aktiviert oder deaktiviert.

Beispiel für control.xml-Datei:

```
<InstructionTable> <InstructionRow> <InstructionType>Configuration XML import Host control
Instruction</InstructionType> <Instruction>ShutdownType</Instruction> <Value>NoReboot</Value>
<ValuePossibilities>Graceful,Forced,NoReboot</ValuePossibilities> </InstructionRow>
<InstructionRow> <InstructionType>Configuration XML import Host control Instruction</
InstructionType> <Instruction>TimeToWait</Instruction> <Value>300</Value>
```

```
<ValuePossibilities>Minimum value is 300 -Maximum value is 3600 seconds.</ValuePossibilities> </
InstructionRow> <InstructionRow> <InstructionType>Configuration XML import Host control
Instruction</InstructionType> <Instruction>EndHostPowerState</Instruction> <Value>On</Value>
<ValuePossibilities>On,Off</ValuePossibilities> </InstructionRow></InstructionTable>
```

Sie müssen zum Ausführen dieses Vorgangs über die Berechtigung zur Serversteuerung verfügen.

ANMERKUNG: Das Ändern der USB-Verwaltungseinstellungen in der XML-Datei während des Imports des Serverkonfigurationsprofils führt zu fehlgeschlagenen Aufträgen oder mit Fehlern abgeschlossen Aufträgen. Sie können Attribute in der XML-Datei zur Vermeidung der Fehler auskommentieren.

So importieren Sie das Server-Konfigurationsprofil vom USB-Gerät zu iDRAC:

1 Konfigurieren der USB-Verwaltungsschnittstelle
   - Stellen Sie den **USB-Verwaltungsanschlussmodus** auf **Automatisch** oder **iDRAC**.
   - Stellen Sie **iDRAC-Verwaltet: USB XML-Konfiguration** auf **Aktiviert mit Standard-Anmeldeinformationen** oder **Aktiviert** ein.
2 Stecken Sie den USB-Speicherstick (der die Dateien **configuration.xml** und **control.xml** enthält) in die iDRAC-USB-Schnittstelle ein.
3 Das Server-Konfigurationsprofil wird auf dem USB-Gerät im Unterverzeichnis **System_Configuration_XML** im Stammverzeichnis des USB-Geräts ermittelt. Es wird in der folgenden Reihenfolge ermittelt:
   - **<servicetag>-config.xml**
   - **<modelnum>-config.xml**
   - **config.xml**
4 Ein Server-Import-Job wird gestartet.

   Wenn das Profil nicht ermittelt wird, wird der Vorgang beendet.

   Wenn **iDRAC-Verwaltet: USB XML-Konfiguration** auf **Aktiviert mit Standard-Anmeldeinformationen** eingestellt wurde und das BIOS-Setup-Kennwort nicht Null ist, oder wenn eines der iDRAC-Benutzerkontos geändert wurde, wird eine Fehlermeldung angezeigt und der Vorgang wird beendet.
5 LCD-Anzeige und LED (falls vorhanden) zeigen den Status an, dass ein Import-Job gestartet wurde.
6 Wenn Sie über eine Konfiguration verfügen, die bereitgestellt werden muss, und der **Herunterfahren-Typ** in der Kontrolldatei als **Kein Neustart** angegeben ist, müssen Sie den Server neu starten, damit die Einstellungen konfiguriert werden können. Andernfalls wird der Server neu gestartet wird, und die Konfiguration wird angewendet. Nur wenn der Server bereits ausgeschaltet war, wird die bereitgestellte Konfiguration angewendet, und zwar auch dann, wenn die Option **Kein Neustart** angegeben wurde.
7 Nachdem Sie den Job-Import abgeschlossen haben, zeigen die LCDs/LEDs an, dass der Auftrag abgeschlossen ist. Falls ein Neustart erforderlich ist, wird auf dem LCD-Display der Job-Status als „Unterbrochen – Warten auf Neustart“ angegeben.
8 Wenn das USB-Gerät weiterhin mit dem Server verbunden ist, wird das Ergebnis des Importvorgangs in der Datei **results.xml** des USB-Geräts aufgezeichnet.

LCD-Meldungen

Wenn das LCD-Bedienfeld verfügbar ist, werden die folgenden Meldungen in einer Reihenfolge angezeigt:

1 Importieren – Wenn Sie das Server-Konfigurationsprofil aus dem USB-Gerät kopiert wird.
2 Anwenden – Wenn der Job ausgeführt wird.
3 Abgeschlossen – Wenn der Job erfolgreich abgeschlossen wurde.
4 Mit Fehlern beendet – Wenn der Job mit Fehlern abgeschlossen wurde.
5 Fehlgeschlagen – Wenn der Job fehlgeschlagen ist.

Weitere Details finden Sie in der Ergebnis-Datei auf dem USB-Gerät.

Verhalten der LED-Blinkfunktion

Wenn die USB-LED vorhanden ist, bedeutet dies Folgendes:

- Dauerhaft grün – Wenn Sie das Server-Konfigurationsprofil von dem USB-Gerät kopiert wird.
- Grün blinkend – Wenn der Job ausgeführt wird.
- Dauerhaft grün – Wenn der Job erfolgreich abgeschlossen wurde.

Protokolle und Ergebnis-Datei

Die folgenden Informationen werden für den Importvorgang protokolliert:

- Das automatische Importieren aus USB wird in der Lifecycle Controller-Protokolldatei protokolliert.
- Wenn das USB-Gerät eingesetzt bleibt, werden die Job-Ergebnisse in der Ergebnis-Datei, die sich im USB-Stick befindet, aufgezeichnet.

Eine Ergebnis-Datei namens **Results.xml**, wird in dem Unterverzeichnis mit den folgenden Informationen aktualisiert oder erstellt:

- Service-Tag-Nummer – Die Daten werden aufgezeichnet , nachdem der Importvorgang entweder eine Job-ID oder einen Fehler zurückgegeben hat.
- Job-ID – Die Daten werden aufgezeichnet , nachdem der Importvorgang eine Job-ID zurückgegeben hat.
- Startdatum und Uhrzeit des Jobs – Die Daten werden aufgezeichnet , nachdem der Importvorgang eine Job-ID zurückgegeben hat.
- Status – Die Daten werden aufgezeichnet, wenn der Import-Vorgang einen Fehler zurückgibt oder wenn die Job-Ergebnisse verfügbar sind.

21

Verwenden von iDRAC Quick Sync

Einige Dell PowerEdge Server der 13. Generation verfügen über eine Quick Sync-Blende, welche die Quick Sync-Funktion unterstützt. Diese Funktion ermöglicht die Verwaltung am Server mit einem mobilen Gerät. Dadurch können Sie Bestands- und Überwachungsinformationen mithilfe des mobilen Geräts anzeigen und grundlegende iDRAC-Einstellungen konfigurieren (z. B. Einrichtung und Konfiguration von Root-Anmeldeinformationen für das erste Startgerät).

Sie können iDRAC Quick Sync-Zugriff für Ihr mobiles Gerät (z. B. OpenManage Mobile) in iDRAC konfigurieren. Sie müssen die OpenManage Mobile-Anwendung auf dem mobilen Gerät installieren, um den Server über die iDRAC Quick Sync-Schnittstelle zu verwalten.

ANMERKUNG: Diese Funktion wird derzeit auf mobilen Geräten mit Android Betriebssystem unterstützt.

In der aktuellen Version steht diese Funktion nur für die Dell PowerEdge R730, R730xd und R630 Rack-Server zur Verfügung. Für diese Server können Sie optional eine Blende erwerben. Daher handelt es sich um ein Hardware-Up-Sell und die Funktionen sind nicht abhängig von der iDRAC-Softwarelizenzierung.

Die iDRAC Quick Sync-Hardware enthält die folgenden Elemente:

- Aktivierungstaste: Sie müssen auf diese Taste drücken, um die Quick Sync-Schnittstelle zu aktivieren. In einer eng gestapelten Rack-Infrastruktur trägt dies dazu bei, den Server, der das Kommunikationsziel ist, zu identifizieren und zu aktivieren. Die Quick Sync-Funktion wird deaktiviert, nachdem sie eine konfigurierbare Zeitdauer nicht genutzt wird (der Standardwert beträgt 30 Sekunden) oder wenn Sie die Taste zum Deaktivieren drücken.
- Aktivitäts-LED: Wenn Quick Sync deaktiviert ist, blinkt die LED eine Weile und geht dann aus. Wenn der konfigurierbare Inaktivitätszeitgeber ausgelöst wird, schaltet sich die LED aus und deaktiviert die Schnittstelle.

Wenn Sie nach der Konfiguration der iDRAC Quick Sync-Einstellungen in iDRAC das mobile Gerät in einem Abstand von maximal zwei Zentimetern halten, können Sie die einschlägigen Informationen zum Server ablesen und iDRAC-Konfigurationseinstellungen vornehmen.

Mit dem OpenManage Mobile können Sie:

- Bestandsaufnahme-Informationen anzeigen:
- Überwachungsinformationen anzeigen:
- Die grundlegende iDRAC-Netzwerkeinstellungen konfigurieren

Weitere Informationen über OpenManage Mobile finden Sie im *Benutzerhandbuch für OpenManage Mobile* unter **dell.com/manuals**.

Themen:

Zugehöriger Link

Konfigurieren von iDRAC Quick Sync
Verwenden vom Mobile-Gerät zum Anzeigen von iDRAC-Informationen

Konfigurieren von iDRAC Quick Sync

Mithilfe der iDRAC-Web-Schnittstelle oder RACADM können Sie die iDRAC Quick Sync-Funktion konfigurieren, um auf das mobile Gerät zugreifen zu können:

- Zugriff – Sie können eine der folgenden Optionen zum Konfigurieren des Zugriffs auf den Status der iDRAC Quick Sync-Funktion festlegen:
  - Lese-/Schreibvorgang – Standardstatus.
  - Lese-Schreib-Zugriff – Ermöglicht die Konfiguration der grundlegenden iDRAC-Einstellungen.
  - Nur-Lese-Zugriff – Ermöglicht das Anzeigen der Bestandsaufnahme und Überwachung von Informationen.
  - Deaktivierter Zugriff – Lässt kein Anzeigen von Informationen und Konfigurieren von Einstellungen zu.
- Zeitüberschreitung – Sie können den iDRAC Quick Sync-Zeitgeber für Inaktivität aktivieren oder deaktivieren:
  - Aktiviert – Sie können eine Dauer festlegen, nach der der Quick Sync-Modus abgeschaltet wird. Drücken Sie zum Einschalten erneut die Aktivierungstaste.
  - Deaktiviert – Der Zeitgeber lässt nicht zu, dass Sie eine Zeitüberschreitungsperiode eingeben.
- Beschränkung für Zeitüberschreitung – Mit dieser Option können Sie die Dauer festlegen, nach der der Quick Sync-Modus deaktiviert wird. Der Standardwert ist 30 Sekunden.

Zum Konfigurieren der Einstellungen müssen Sie über die Berechtigung zur Server-Steuerung verfügen. Damit die Einstellungen wirksam werden, ist kein Server-Neustart erforderlich.

Wenn die Konfiguration geändert wird, wird ein Eintrag im Lifecycle Controller-Protokoll eingetragen.

Konfigurieren von iDRAC Quick Sync-Einstellungen unter Verwendung der Webschnittstelle

Zur Konfiguration von iDRAC Quick Sync:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Hardware-** > **Frontblende**.

2 Wählen Sie im Abschnitt **iDRAC Quick Sync** aus dem Drop-Down-Menü **Zugriff** eine der folgenden Optionen für die Bereitstellung des Zugriffs auf das mobile Andriod-Gerät aus:
   - Lesen-Schreiben
   - Nur-Lesen
   - Deaktiviert

3 Aktivieren Sie den Zeitgeber.

4 Geben Sie den Timeout-Wert an.

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

5 Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

Konfigurieren von iDRAC Quick Sync-Einstellungen über RACADM

Verwenden Sie zum Konfigurieren der iDRAC Quick Sync-Funktion die racadm-Objekte in der Gruppe **System.QuickSync**. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Konfigurieren von iDRAC Quick Sync-Einstellungen über das Dienstprogramm für iDRAC-Einstellungen

Zur Konfiguration von iDRAC Quick Sync:

1 Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Frontblendensicherheit**.

Die Seite **iDRAC-Einstellungen – Frontblendensicherheit** wird angezeigt.

2 Im **iDRAC Quick Sync-**Abschnitt:

- Geben Sie die Zugriffsebene an.
- Aktivieren Sie Timeout.
- Geben Sie die Benutzerdefinierte Zeitüberschreitungsbegrenzung (15 Sekunden bis 3600 Sekunden) an.

Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

3 Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Einstellungen werden angewendet.

Verwenden vom Mobile-Gerät zum Anzeigen von iDRAC-Informationen

Weitere Informationen zum Anzeigen von iDRAC-Informationen von dem mobilen Gerät finden Sie im *OpenManage Mobile User's Guide* (OpenManage-Mobile-Benutzerhandbuch) unter **dell.com/support/manuals**.

22

Betriebssysteme bereitstellen

Sie können die folgenden Dienstprogramme verwenden, um Betriebssysteme auf Managed Systemen bereitzustellen:

- Remote-Dateifreigabe
- Konsole für virtuelle Datenträger

Themen:

Zugehöriger Link

Betriebssystem über eine Remote-Dateifreigabe bereitstellen
Betriebssystem über virtuelle Datenträger bereitstellen

Betriebssystem über eine Remote-Dateifreigabe bereitstellen

Bevor Sie das Betriebssystem über eine Remote-Dateifreigabe (RFS, Remote File Share) bereitstellen, müssen Sie Folgendes sicherstellen:

- Die iDRAC-Berechtigungen **Benutzer konfigurieren** und **Zugriff auf virtuelle Datenträger** sind für den Benutzer aktiviert.
- Die Netzwerkfreigabe enthält Treiber und eine startfähige Imagedatei für das Betriebssystem in einem branchenüblichen Standardformat, wie z. B. **.img** oder **.iso**.

  ANMERKUNG: Folgen Sie während der Erstellung der Imagedatei den standardmäßigen, netzwerkbasierten Installationsvorgängen, und markieren Sie das Bereitstellungsimage als schreibgeschütztes Image, um sicherzustellen, dass jedes Zielsystem gestartet werden kann und gemäß dem gleichen Bereitstellungsverfahren ausgeführt wird.

So stellen Sie ein Betriebssystem mithilfe von RFS bereit:

1. Stellen Sie unter Verwendung der Remote-Dateifreigabe (RFS) die ISO- oder IMG-Imagedatei über NFS oder CIFS im verwalteten System bereit.
2. Wechseln Sie zu **Übersicht** > **Setup** > **Erstes Startlaufwerk**.
3. Legen Sie die Startreihenfolge in der Drop-Down-Liste **Erstes Startgerät** fest, um einen virtuellen Datenträger wie z. B. Floppy, CD, DVD oder ISO auszuwählen.
4. Wählen Sie die Option **Einmalstart** aus, um das Managed System für den Neustart über die Imagedatei nur für die nächste Instanz zu aktivieren.
5. Klicken Sie auf **Anwenden**.
6. Starten Sie das Managed System neu, und folgen Sie den Anweisungen auf dem Bildschirm, um die Bereitstellung abzuschließen.

Zugehöriger Link

Verwalten der Remote-Dateifreigabe (Remote File Share)
Erstes Startlaufwerk einstellen

Verwalten der Remote-Dateifreigabe (Remote File Share)

Mit der Remote-Dateifreigabe (Remote File Share, RFS) können Sie eine ISO- oder IMG-Image-Datei auf einer Netzwerkfreigabe festlegen und diese dem Betriebssystem des verwalteten Servers als virtuelles Laufwerk zur Verfügung stellen, indem sie mithilfe von NFS oder CIFS als CD oder DVD geladen wird. Die RFS-Funktion ist lizenziert.

ANMERKUNG: CIFS unterstützt IPv4- und IPv6-Adressen, NFS jedoch nur IPv4-Adressen.

Die Remote-Dateifreigabe unterstützt nur **.img-** und **.iso**-Image-Dateiformate. Eine **.img**-Datei wird als virtuelle Diskette umgeleitet und eine **.iso-**Datei wird als virtuelle CDROM umgeleitet.

Sie müssen über Virtuelle Datenträger-Berechtigungen verfügen, um RFS-Mounting durchführen zu können.

ANMERKUNG: Wenn ESXi auf dem verwalteten System ausgeführt wird und Sie ein Floppy-Abbild (.img) über die Remote-Dateifreigabe bereitstellen, ist das verbundene Floppy-Abbild auf dem ESXi-Betriebssystem nicht verfügbar.

RFS und Funktionen des virtuellen Datenträgers schließen sich gegenseitig aus.

- Falls der virtuelle Datenträger-Client nicht aktiv ist und Sie versuchen, eine RFS-Verbindung herzustellen, wird die Verbindung hergestellt, und das Remote-Abbild steht dem Hostbetriebssystem zur Verfügung.
- Wenn der Client des virtuellen Datenträgers aktiv ist und Sie versuchen, eine RFS-Verbindung einzurichten, wird die folgende Fehlermeldung angezeigt:

  Der virtuelle Datenträger wird abgetrennt oder für das ausgewählte virtuelle Laufwerk umgeleitet.

Der Verbindungsstatus für RFS ist im iDRAC-Protokoll verfügbar. Nach einer Verbindung eines per RFS geladenen Laufwerks wird diese Verbindung selbst dann nicht getrennt, wenn Sie sich von iDRAC abmelden. Die RFS-Verbindung wird beendet, wenn iDRAC zurückgesetzt wird oder die Verbindung zum Netzwerk abbricht. Die Webschnittstelle und Befehlszeilenoptionen zum Schließen einer RFS-Verbindung im CMC und in iDRAC ebenfalls verfügbar. Die RFS-Verbindung des CMC hebt immer ein bestehendes RFS-Mounting in iDRAC auf.

ANMERKUNG: Zwischen der iDRAC vFlash-Funktion und RFS besteht kein Zusammenhang.

Wenn Sie die iDRAC-Firmware von Version 1.30.30 auf 1.50.50 während einer aktiven RFS-Verbindung aktualisieren und gleichzeitig der Virtual Media-Attach-Modus auf **Anhängen** oder **Automatisch anhängen** gesetzt ist, dann versucht iDRAC, die RFS-Verbindung erneut herzustellen, nachdem die Firmware-Aktualisierung abgeschlossen ist und iDRAC neu gestartet wird.

Wenn Sie die iDRAC-Firmware von Version 1.30.30 auf 1.50.50 während einer aktiven RFS-Verbindung aktualisieren und gleichzeitig der Virtual Media-Attach-Modus auf **Entfernen** gesetzt ist, dann versucht iDRAC nicht, die RFS-Verbindung erneut herzustellen, nachdem die Firmware-Aktualisierung abgeschlossen ist und iDRAC neu gestartet wird.

Remote-Dateifreigabe über die Web-Schnittstelle konfigurieren

So aktivieren Sie die Remote-Dateifreigabe:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Overview (Übersicht)** > **Server** > **Attached Media (Verbundener Datenträger)**.
Daraufhin wird die Seite **Verbundener Datenträger** angezeigt.
2 Wählen Sie unter **Verbundener Datenträger** die Option **Verbinden** oder **Automatisch Verbinden**aus.
3 Legen Sie unter **Remote File Share (Remote-Dateifreigabe)** den Dateipfad für das Image, den Domänennamen, Benutzernamen und das Kennwort fest. Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
Beispiel für einen Dateipfad:

- CIFS - //<IP zur Verbindung für CIFS-Dateisystem>/<Dateipfad>/<Image-Name>
- NFS —< IP zur Verbindung für NFS-Dateisystem>/<Dateipfad>/<Imagename>

ANMERKUNG: Für den Dateipfad kann sowohl das Zeichen '/' als auch '\' verwendet werden.

CIFS unterstützt IPv4- und IPv6-Adressen, NFS jedoch nur IPv4-Adressen.

Bei einer NFS-Freigabe muss der genaue <Dateipfad> und <Imagename> eingegeben werden, da zwischen Groß- und Kleinschreibung unterschieden wird.

ANMERKUNG: Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern.

ANMERKUNG: Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen.

4 Klicken Sie auf **Anwenden** und dann auf **Verbinden**.

Nachdem die Verbindung eingerichtet wird, wird der **Verbindungsstatus** als **Verbunden** angezeigt.

ANMERKUNG: Auch wenn Sie die Remote-Dateifreigabe konfiguriert haben, zeigt die Webschnittstelle die Benutzeranmeldedaten aus Sicherheitsgründen nicht an.

Bei Linux-Distributionen kann diese Funktion beim Betrieb mit runlevel init 3 einen Befehl zum manuellen Bereitstellen erfordern. Die Syntax für den Befehl lautet:

```
mount /dev/OS_specific_device / user_defined_mount_point
```

wobei `user_defined_mount_point` jedes Verzeichnis ist, das Sie für das Bereitstellen auswählen, ähnlich wie für jeden Bereitstellen-Befehl.

Für RHEL ist das CD-Gerät (virtuelles **.iso-**Gerät) `/dev/scd0` und das Diskettengerät (virtuelles **.img**-Gerät) `/dev/sdc`.

Für SLES ist das CD-Gerät `/dev/sr0` und das Diskettengerät /dev/sdc. Um beim Anschluss des virtuellen Gerätes die Verwendung des richtigen Gerätes sicherzustellen (jeweils SLES oder RHEL), müssen Sie auf dem Linux-Betriebssystem sofort folgenden Befehl ausführen:

```
tail /var/log/messages | grep SCSI
```

Dadurch wird der Text zur Identifizierung des Geräts angezeigt (z. B. SCSI device sdc). Dieses Verfahren gilt auch für virtuelle Datenträger, wenn Sie Linux-Distributionen in runlevel init 3 verwenden. Standardmäßig werden die virtuellen Datenträger nicht automatisch in init 3 bereitgestellt.

Remote-Dateifreigabe über RACADM konfigurieren

Verwenden Sie die folgenden Befehle, um die Remote-Dateifreigabe über RACADM zu konfigurieren:

```
racadm remoteimage
```

```
racadm remoteimage <options>
```

Optionen sind:

`-c` ; Verbindung zu Image herstellen

`-d` ; Verbindung zu Image abbrechen

`-u` <Benutzername>; Benutzername zum Zugriff auf die Netzwerkfreigabe

`-p` <Kennwort>; Kennwort zum Zugriff auf die Netzwerkfreigabe

`-l` <Speicherort_Image>: Imagespeicherort in der Netzwerkfreigabe. Setzen Sie den Speicherort zwischen (doppelte) Anführungszeichen. Beispiele für Imagedateipfade finden Sie im Abschnitt „Remote-Dateifreigabe über die Web-Schnittstelle konfigurieren“.

`-s` ; aktuellen Status anzeigen

ANMERKUNG: Alle Zeichen einschließlich alphanumerischer Zeichen und Sonderzeichen sind als Teil des Benutzernamens, des Kennworts und des Imagespeicherorts zulässig, mit Ausnahme der folgenden Zeichen: ’ (Apostroph), ” (Anführungszeichen), , (Komma), < (kleiner als) und > (größer als).

Betriebssystem über virtuelle Datenträger bereitstellen

Bevor Sie das Betriebssystem über einen virtuellen Datenträger bereitstellen können, müssen Sie Folgendes sicherstellen:

- Der virtuelle Datenträger befindet sich im Status *Verbunden*, damit die virtuellen Laufwerke in der Startsequenz angezeigt werden.
- Wenn sich ein virtueller Datenträger im Modus *Automatisch verbunden* befindet, müssen Sie zunächst die Anwendung für den virtuellen Datenträger starten, bevor das System gestartet wird.
- Die Netzwerkfreigabe enthält Treiber und eine startfähige Imagedatei für das Betriebssystem in einem branchenüblichen Standardformat, wie z. B. **.img** oder **.iso**.

So stellen Sie ein Betriebssystem über den virtuellen Datenträger bereit:

1 Führen Sie einen der folgenden Vorgänge aus:
   - Legen Sie eine Betriebssystem-Installations-CD- oder DVD in das CD- oder DVD-Laufwerk der Management Station ein.
   - Verbinden Sie das Betriebssystem-Image.
2 Wählen Sie das Laufwerk auf der Management Station mit dem Image aus, mit dem eine Verknüpfung hergestellt werden soll.
3 Verwenden Sie eines der folgenden Verfahren, um das benötigte Gerät zu starten:
   - Legen Sie die Startreihenfolge so fest, dass über die iDRAC-Web-Schnittstelle einmal vom **virtuellen Floppy**- oder vom **virtuellen CD/DVD/ISO**-Laufwerk aus gestartet wird.
   - Legen Sie die Startreihenfolge über **System-Setup** > **System-BIOS-Einstellungen** fest, indem Sie während des Startvorgangs auf <F2> drücken.
4 Starten Sie das Managed System neu, und folgen Sie den Anweisungen auf dem Bildschirm, um die Bereitstellung abzuschließen.

Zugehöriger Link

Virtuellen Datenträger konfigurieren
Erstes Startlaufwerk einstellen
iDRAC konfigurieren

Betriebssystem über mehrere Festplatten bereitstellen

1 Lösen Sie die bestehende CD/DVD-Verbindung.
2 Legen Sie die nächste CD/DVD in das optische Remote-Laufwerk ein.
3 Weisen Sie das CD/DVD-Laufwerk neu zu.

Integriertes Betriebssystem auf SD-Karte bereitstellen

So installieren Sie einen eingebetteten Hypervisor auf eine SD-Karte:

1 Setzen Sie zwei SD-Karten in die Steckplätze für das interne Dual-SD-Modul (IDSDM) auf dem System ein.
2 Aktivieren Sie das SD-Modul und die Redundanz (falls erforderlich) im BIOS.
3 Überprüfen Sie, ob die SD-Karte auf einem der Laufwerke verfügbar ist, indem Sie während des Startvorgangs auf die Taste <F11> drücken.

4 Stellen Sie das eingebettete Betriebssystem bereit, und folgen Sie den Anweisungen zur Installation des Betriebssystems.

Zugehöriger Link

Über IDSDM

SD-Modul und Redundanz im BIOS aktivieren

SD-Modul und Redundanz im BIOS aktivieren

So aktivieren Sie das SD-Modul und die Redundanz im BIOS:

1 Drücken Sie während des Startvorgangs auf <F2>.
2 Gehen Sie zu **System-Setup** > **System-BIOS-Einstellungen** > **Integrierte Geräte**.
3 Setzen Sie die **interne USB-Schnittstelle** auf **Ein**. Wenn sie auf **Aus** gesetzt ist, kann IDSDM nicht als Startgerät verwendet werden.
4 Wenn Redundanz nicht benötigt wird (einzelne SD-Karte), setzen Sie die **interne SD-Kartenschnittstelle** auf **Ein** und die **interne SD-Kartenredundanz** auf **Deaktiviert**.
5 Wenn Redundanz benötigt wird (zwei SD-Karten), setzen Sie die **interne SD-Kartenschnittstelle** auf **Ein** und die **interne SD-Kartenredundanz** auf **Spiegelung**.
6 Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
7 Klicken Sie zum Speichern der Einstellungen auf **Ja**, und drücken Sie auf <Esc>, um das **System-Setup** zu beenden.

Über IDSDM

Das interne zweifache SD-Modul (IDSDM) ist nur auf geeigneten Plattformen verfügbar. IDSDM bietet Redundanz auf der Hypervisor-SD-Karte, indem eine andere SD-Karte verwendet wird, die den Inhalt der ersten SD-Karte spiegelt.

Eine der beiden SD-Karten kann Master sein. Wenn z. B. zwei neue SD-Karten in das IDSDM eingesetzt werden, wird SD1 die aktive oder Master-Karte und SD2 die Standby-Karte. Die Daten werden auf den beiden Karten geschrieben, aber die Daten werden von SD1 gelesen. Immer wenn SD1 ausfällt oder entfernt wird, wird SD2 automatisch zur aktiven (Master-) Karte.

Unter Verwendung des iDRAC können Sie den Status, den Funktionszustand sowie die Verfügbarkeit von IDSDM anzeigen. Der Redundanzstatus der SD-Karte sowie Fehlerereignisse werden zum SEL protokolliert und auf der Frontblende angezeigt, und PET-Warnungen werden erstellt, wenn Warnungen aktiviert sind.

Zugehöriger Link

Sensorinformationen anzeigen

23

Fehler auf Managed System über iDRAC beheben

Sie können Fehler auf einem Remote-Managed-System wie folgt analysieren und beheben:

- Diagnosekonsole
- POST-Code
- Videos zur Start- und Absturzerfassung
- Bildschirm zum letzten Absturz
- Systemereignisprotokolle
- Lifecycle-Protokolle
- Status auf der Frontblende
- Problemanzeigen
- Systemzustand

Themen:

Zugehöriger Link

Diagnosekonsole verwenden
Planen von Automatischer Remote-Diagnose
POST-Codes anzeigen
Videos zum Startvorgang und zur Absturzerfassung anzeigen
Protokolle anzeigen
Bildschirm „Letzter Systemabsturz“ anzeigen
Status der Anzeige auf der Frontblende anzeigen
Anzeigen für Hardwareprobleme
Systemzustand anzeigen
Generieren der SupportAssist-Erfassung

Diagnosekonsole verwenden

iDRAC bietet einen Standardsatz mit Netzwerkdiagnose-Tools, die den Tools auf Microsoft Windows- oder Linux-basierten Systemen ähneln. Über die iDRAC-Webschnittstelle können Sie auf die Netzwerk-Debugging-Tools zugreifen.

So rufen Sie die Diagnosekonsole auf:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Fehlerbehebung** > **Diagnose**.

2 Geben Sie in das Textfeld **Befehl** einen Befehl ein, und klicken Sie dann auf **Senden**. Weitere Informationen zu den verfügbaren Befehlen finden Sie in der *iDRAC-Online-Hilfe*.

Die Ergebnisse werden auf der gleichen Seite angezeigt.

Planen von Automatischer Remote-Diagnose

Sie können im Remote-Zugriff die automatisierte Offline-Diagnose auf einem Server als einmaliges Ereignis auf- und die Ergebnisse abrufen. Falls ein Neustart erforderlich ist, können Sie diesen sofort ausführen oder auf einen nachfolgenden Neustart- oder Wartungszyklus planen (ähnlich wie bei Aktualisierungen). Die Diagnoseergebnisse werden gesammelt und im internen iDRAC-Speicher gespeichert. Sie können die Ergebnisse dann in eine NFS- oder CIFS Netzwerkfreigabe exportieren, indem Sie den RACADM-Befehl `diagnostics export` verwenden. Sie können die Diagnose auch mit den entsprechenden WSMAN-Befehlen ausführen. Weitere Informationen finden Sie in der WSMAN-Dokumentation.

Sie müssen über die iDRAC Express-Lizenz verfügen, um die automatische Remote-Diagnose verwenden zu können.

Sie können die Diagnose entweder sofort ausführen oder auf einen bestimmten Tag und eine Uhrzeit planen, wobei Sie auch die Art der Diagnose und den Neustarttyp festlegen können.

Für den Zeitplan können Sie Folgendes festlegen:

- Startzeit – Ausführen der Diagnose zu einem zukünftigen Datum und Uhrzeit. Wenn Sie TIME NOW (SOFORT) angeben, wird die Diagnose beim nächsten Neustart ausgeführt.
- Endzeit – Ausführen der Diagnose bis zu einem bestimmten Datum und Uhrzeit nach der Startzeit. Wenn die Diagnose mit Eintreten der Endzeit nicht gestartet ist, wird sie als fehlgeschlagen mit abgelaufener Endzeit gekennzeichnet. Wenn Sie TIME NA (ZEIT NICHT ANWENDBAR) angeben, ist keine Wartezeit anwendbar.

Die verfügbaren Diagnosetypen sind:

- Schnelltest
- Erweiterter Test
- Beide in einer bestimmten Reihenfolge

Die verfügbaren Neustarttypen sind:

- System aus- und einschalten
- Ordentliches Herunterfahren (Warten, bis das Betriebssystem herunterfährt, bevor der Neustart des Systems beginnt)
- Erzwungenes Ordentliches Herunterfahren (signalisiert dem Betriebssystem, dass es herunterfahren soll und räumt eine Wartezeit von 10 Minuten ein. Wenn das Betriebssystem nicht heruntergefahren ist, schaltet iDRAC das System aus und wieder ein)

Es kann jeweils nur eine Diagnose ausgeführt werden. Eine Diagnose kann erfolgreich, mit Fehlern oder nicht erfolgreich abgeschlossen werden. Die Diagnose-Ereignisse einschließlich der Ergebnisse werden im Lifecycle Controller-Protokoll aufgezeichnet. Sie können die Ergebnisse der letzten Ausführung der Diagnose mithilfe von Remote-RACADM oder WS-MAN abrufen.

Sie können die Diagnoseergebnisse der letzten remote geplanten und abgeschlossenen Diagnose auf eine Netzwerkfreigabe wie z. B. CIFS oder NFS exportieren. Die maximal zulässige Dateigröße ist 5 MB.

Sie können eine Diagnose abbrechen, wenn der Job-Status „Nicht geplant“ oder „Geplant“ lautet. Wenn die Diagnose ausgeführt wird, können Sie das System neu starten, um den Job abzubrechen.

Stellen Sie vor dem Ausführen des Remote-Diagnose Folgendes sicher:

- Lifecycle Controller ist aktiviert.
- Sie verfügen über Anmelde- und Serversteuerungsberechtigungen.

Planen von Automatischer Remote-Diagnose unter Verwendung von RACADM

- Verwenden Sie zum Ausführen der Remote-Diagnose und zum Speichern der Ergebnisse auf dem lokalen System den folgenden Befehl:
  ```
  racadm diagnostics run -m <Mode> -r <reboot type> -s <Start Time> -e <Expiration Time>
  ```
- Verwenden Sie zum Exportieren der Ergebnisse der zuletzt ausgeführten Remote-Diagnose den folgenden Befehl:
  ```
  racadm diagnostics export -f <file name> -l <NFS / CIFS share> -u <username> -p <password>
  ```

Weitere Informationen zu diesen Optionen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC8)* unter **dell.com/idracmanuals**.

POST-Codes anzeigen

POST-Codes zeigen den Fortschritt des System-BIOS an, kennzeichnen verschiedene Phasen der Startsequenz von Power-on-Reset und ermöglichen, Fehler bezüglich des Systemstarts zu diagnostizieren. Die Seite POST-Code zeigt den letzten **POST-Code** des Systems vor dem Start des Betriebssystems an.

Gehen Sie zum Anzeigen von POST-Codes zu **Übersicht** > **Server** > **Fehlerbehebung** > **POST-Code**.

Die Seite **POST-Code** blendet die Systemzustandsanzeige, einen Hexadezimalcode sowie eine Beschreibung des Codes ein.

Videos zum Startvorgang und zur Absturzerfassung anzeigen

Sie können die folgenden Videoaufzeichnungen anzeigen:

- Letzte drei Startzyklen – Ein Video zum Startzyklus protokolliert die Sequenz der Ereignisse für einen Startzyklus. Bei den Videos zum Startzyklus wird das jeweils neueste Video zuerst angezeigt.
- Video zum letzten Absturz – Ein Video zum letzten Absturz protokolliert die Sequenz der Ereignisse, die zum Ausfall geführt haben.

Dies ist eine lizenzierte Funktion.

iDRAC zeichnet zum Zeitpunkt des Starts 50 Frames auf. Die Wiedergabe der Startbildschirme tritt mit einer Rate von 1 Frame pro Sekunde auf. Wenn iDRAC zurückgesetzt wird, ist das Systemstartvideo nicht mehr verfügbar, da dieses im RAM gespeichert und gelöscht wird.

ANMERKUNG:

- Sie müssen über Berechtigungen für den Zugriff auf die virtuelle Konsole oder über Administratorberechtigungen verfügen, um die Videos zum Startvorgang und zu Abstürzen abzuspielen.
- Die Videoerfassungszeit im iDRAC-GUI-Videogerät kann von der Videoerfassungszeit, die auf anderen Videogeräten angezeigt wird, abweichen. Das iDRAC-GUI-Videogerät zeigt die Zeit in der iDRAC-Zeitzone an, während alle anderen Videogeräte die Zeit in den Zeitzonen des jeweiligen Betriebssystems anzeigen.

Um den Bildschirm **Systemstartprotokoll** anzuzeigen, klicken Sie auf **Übersicht** > **Server** > **Fehlerbehebung** > **Videoerfassung**.

Der Bildschirm **Videoerfassung** zeigt die Videoaufzeichnungen an. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Konfigurieren der Videoerfassungs-Einstellungen

So konfigurieren Sie die Videoerfassungs-Einstellungen:

1 Gehen Sie in der iDRAC-Webschnittstelle auf **Übersicht** > **Server** > **Fehlerbehebung** > **Videoerfassung**.
Die Seite **Videoerfassung** wird angezeigt.
2 Wählen Sie aus dem Drop-Down-Menü **Videoerfassungs-Einstellungen** eine der folgenden Optionen:
- **Deaktivieren** – Die Starterfassung ist deaktiviert.
- **Erfassen, bis Puffer voll** – Die Startreihenfolge wird erfasst, bis die Größe des Pufferspeichers erreicht wird.
- **Erfassen bis zum Ende des POST** – Die Startreihenfolge wird erfasst, bis das Ende des POST-Vorgangs erreicht wird.

3 Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

Protokolle anzeigen

Sie können die Systemereignisprotokolle (SELs) und die Lifecycle-Protokolle anzeigen. Weitere Informationen finden Sie unter Systemereignisprotokoll anzeigen und Lifecycle-Protokoll anzeigen.

Bildschirm „Letzter Systemabsturz“ anzeigen

Die Funktion „Bildschirm Letzter Absturz“ erfasst einen Screenshot des letzten Systemabsturzes, speichert diesen und zeigt ihn in iDRAC an. Dies ist eine Lizenzfunktion.

So zeigen Sie den Bildschirm „Letzter Absturz“ an:

1 Stellen Sie sicher, dass die Funktion „Bildschirm Letzter Absturz“ aktiviert ist.
2 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Fehlerbehebung** > **Bildschirm „Letzter Absturz“**.
Auf der Seite **Bildschirm „Letzter Absturz“** wird der Bildschirm für den letzten Absturz auf dem Managed System angezeigt.

Klicken Sie auf **Löschen**, um den Bildschirm für den letzten Absturz zu löschen.

Zugehöriger Link

Bildschirm „Letzter Absturz“ aktivieren

Status der Anzeige auf der Frontblende anzeigen

Die Frontblende auf dem Managed System fasst den Status der folgenden Systemkomponenten zusammen:

- Batterien
- Lüfter
- Eingriff
- Netzteile
- Wechselbarer Flash-Datenträger
- Temperaturen
- Spannungen

Sie können den Status der Frontblende auf dem Managed System wie folgt abrufen:

- Bei Rack- und Tower-Servern: Über den Status der LC-Anzeige auf der Frontblende und die System-ID-LED oder über den Status der LE-Anzeige auf der Frontblende und die System-ID-LED.
- Bei Blade-Servern: Nur über die System-ID-LEDs.

Status der LC-Anzeige auf der Frontblende des Systems anzeigen

Um den Status des LCD auf der Frontblende für die jeweiligen Rack- und Tower-Server anzuzeigen, gehen Sie in der iDRAC-Webschnittstelle zu **Overview (Übersicht)** > **Hardware** > **Front Panel (Frontblende)**. Die Seite **Front Panel (Frontblende)** wird angezeigt. Im Abschnitt **Live Front Panel Feed (Live-Frontblenden-Feed)** wird der Live-Status der Meldungen angezeigt, die derzeit auf dem LCD der Frontblende angezeigt werden. Wenn das System normal ausgeführt wird (gekennzeichnet durch eine stetig blaue Anzeige auf dem LCD auf der Frontblende), sind die beiden Optionen **Hide Error (Fehler ausblenden)** und **UnHide Error (Fehler einblenden)** ausgegraut.

ANMERKUNG: Sie können die Fehler nur für Rack- und Tower-Server ein- und ausblenden.

Zum Anzeigen des Status des LCD auf der Frontblende über RACADM, verwenden Sie die Objekte in der Gruppe **System.LCD**. Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Zugehöriger Link

LCD-Einstellung konfigurieren

Status der LE-Anzeige auf der Frontblende des Systems anzeigen

Um den Status der aktuellen System-ID-LED anzuzeigen, gehen Sie in der iDRAC-Webschnittstelle zu**Übersicht** > **Hardware** > **Frontblende**. Daraufhin wird der Abschnitt **Live-Status der Frontblende** mit dem aktuellen Status der Frontblende angezeigt:

- Dauerhaft blau – Auf dem Managed System liegen keine Probleme vor.
- Blau blinkend – Der Identifizierungsmodus ist aktiviert (unabhängig davon, ob ein Fehler auf dem Managed System vorhanden ist).
- Dauerhaft gelb – Das Managed System befindet sich im Failsafe-Modus.
- Gelb blinkend – Auf dem Managed System sind Fehler vorhanden.

Wenn das System normal ausgeführt wird (erkennbar am blauen Statussymbol auf der LED auf der Frontblende), werden die Optionen **Fehler ausblenden** und **Fehler einblenden** ausgegraut dargestellt. Sie können die Fehleranzeige nur auf Rack- und Tower-Servern ein- und ausblenden.

Um den Status der System-ID-LED unter Verwendung von RACADM anzuzeigen, verwenden Sie den Befehl **getled**.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Zugehöriger Link

LED-Einstellung für die System-ID konfigurieren

Anzeigen für Hardwareprobleme

Die Hardware-bezogenen Probleme lauten:

- Gerät kann nicht hochgefahren werden
- Laute Lüfter
- Verlust der Netzwerkkonnektivität
- Festplattenfehler
- Fehler des USB-Datenträgers

- Physischer Schaden

Verwenden Sie auf der Basis des Problems die folgenden Verfahren, um das Problem zu beheben:

- Setzen Sie das Modul oder die Komponente neu ein, und starten Sie das System neu.
- Setzen Sie bei einem Blade-Server das Modul in einen anderen Schacht des Gehäuses ein.
- Tauschen Sie die Festplatten oder die USB-Flash-Laufwerke aus.
- Schließen Sie die Strom- und Netzwerkkabel erneut an, oder tauschen Sie sie aus

Sollte das Problem fortbestehen, finden Sie weitere Informationen zum Beheben von spezifischen Fehlern auf dem Hardware-Gerät im *Hardware-Benutzerhandbuch*.

VORSICHT: Sie dürfen nur Fehlerbehebungsmaßnahmen ausführen und einfache Reparaturen vornehmen, wenn dies in Ihrer Produktdokumentation genehmigt ist oder wenn Sie online bzw. telefonisch von einem Service- und Support-Team entsprechende Anleitungen erhalten. Schäden durch nicht von Dell genehmigte Wartungsversuche werden nicht durch die Garantie abgedeckt. Lesen und befolgen Sie die zusammen mit dem Produkt gelieferten Sicherheitshinweise.

Systemzustand anzeigen

Die Webschnittstellen für iDRAC und CMC (für Blade-Server) zeigen den Status für die folgenden Komponenten an:

- Batterien
- Gehäuse-Controller-Status
- Lüfter
- Eingriff
- Netzteile
- Wechselbarer Flash-Datenträger
- Temperaturen
- Spannungen
- CPU

Wechseln Sie in der iDRAC-Webschnittstelle zum Abschnitt **Übersicht** > **Server** > **Systemzusammenfassung** > **Serverzustand** .

Wechseln Sie zum Anzeigen des CPU-Zustands zu **Übersicht** > **Hardware** > **CPU**.

Die Anzeichen für den System-Zustand lauten wie folgt:

-  – Weist auf einen normalen Status hin.
-  – Weist auf einen Warnstatus hin.
-  – Weist auf einen Ausfallstatus hin.
-  – Weist auf einen unbekannten Status hin.

Klicken Sie einen beliebigen Komponentennamen im Abschnitt **Server-Zustand**, um die Details zu den jeweiligen Komponenten anzuzeigen.

Generieren der SupportAssist-Erfassung

Wenn Sie zusammen mit dem technischen Support ein Problem mit einem Server beheben müssen, Ihre Sicherheitsrichtlinien aber keine direkte Internetverbindung zulassen, können Sie dem technischen Support die notwendigen Daten zur Behebung des Problems zukommen lassen, ohne Software installieren oder Hilfsprogramme von Dell herunterladen zu müssen und ohne über Zugang zum Internet über das Betriebssystem oder iDRAC zu verfügen. Sie können die Daten von einem anderen System senden und sich darauf verlassen, dass die von Ihrem Server erfassten Daten während der Übertragung an den technischen Support nicht für nicht autorisierte Personen sichtbar sind.

Sie können außerdem einen Zustandsbericht für den Server generieren und den Bericht anschließend in eine Management Station (lokal) oder Netzwerkfreigabe exportieren (z. B. Common Internet File System (CIFS) oder Network File Share (NFS)). Sie können diesen Bericht

dann direkt für den technischen Support freigeben. Für den Export in eine Netzwerkfreigabe, wie z. B. CIFS oder NFS, ist eine direkte Netzwerkverbindung zum freigegebenen oder dedizierten iDRAC-Netzwerkport erforderlich.

Der Report wird im Standard-ZIP-Format erstellt. Der Report enthält Informationen, die den Informationen im DSET-Report ähnlich sind, wie z. B.:

- Hardware-Bestandsaufnahme für alle Komponenten
- System, Lifecycle Controller und Komponentenattribute
- Betriebssystem- und Anwendungsinformationen
- Aktive Lifecycle Controller-Protokolle (archivierte-Einträge sind nicht eingeschlossen)
- PCIe SSD-Protokolle
- Speicher-Controller-Protokolle

ANMERKUNG: Die TTYLog-Erfassung für PCIe SSDs unter Verwendung der SupportAssist-Funktion wird auf Dell PowerEdge-Servern der 12· Generation nicht unterstützt.

Nachdem die Daten erstellt wurden, können Sie sie anzuzeigen. Sie enthalten eine Reihe von XML-Dateien und Protokolldateien. Die Daten müssen für den technischen Support freigegeben werden, um das Problem zu beheben.

Jedes Mal, wenn eine Datenerfassung durchgeführt wird, wird ein Ereignis im Lifecycle Controller-Protokoll aufgezeichnet. Das Ereignis enthält Informationen wie beispielsweise die verwendete Schnittstelle, Datum und Uhrzeit des Exports und den iDRAC-Benutzernamen.

Es gibt es zwei Vorgehensweisen, die BS-Anwendung und Protokolle zu erstellen:

- Automatisch – Verwendung des iDRAC Service Module, das das Betriebssystem-Collector-Tool automatisch aufruft.
- Manuell: durch manuelles Ausführen des OS Collector (ausführbar über das Betriebssystem des Servers). iDRAC stellt die ausführbare OS Collector-Datei im Betriebssystem des Servers als USB-Gerät mit der Bezeichnung DRACRW dar.

ANMERKUNG:

- Das BS-Collector-Tool ist nicht für Dell Precision PR7910-Systeme anwendbar.
- Die BS-Protokollerfassungs-Funktion wird auf CentOS Betriebssystemen nicht unterstützt.
- Bei Servern mit Windows 2016 Nano Edition wird das Viewer-Protokoll HardwareEvent.evtx nicht vom OS Collector-Tool erzeugt. Um das Viewer-Protokoll HardwareEvent.evtx zu erstellen, führen Sie den Befehl ~New-Item -Path HKLM:\SYSTEM \ControlSet001\Services\EventLog\HardwareEvents~ aus, bevor Sie das OS Collector-Tool ausführen.

Stellen Sie vor dem Generieren eines Funktionszustandreports Folgendes sicher:

- Lifecycle Controller ist aktiviert.
- Die Funktion Systembestandsaufnahme beim Neustart erfassen (CSIOR) ist aktiviert.
- Sie verfügen über Anmelde- und Serversteuerungsberechtigungen.

Zugehöriger Link

Automatisches Generieren der SupportAssist-Erfassung
Manuelles Generieren der SupportAssist-Erfassung

Automatisches Generieren der SupportAssist-Erfassung

Wenn das iDRAC-Servicemodul installiert ist und ausgeführt wird, können Sie die SupportAssist-Erfassung automatisch generieren. Das iDRAC-Servicemodul ruft die entsprechende OS Collector-Datei auf dem Host-Betriebssystem auf, erfasst die Daten und überträgt sie an den iDRAC. Anschließend können Sie die Daten am erforderlichen Speicherort ablegen.

Automatisches Generieren der SupportAssist-Erfassung unter Verwendung der iDRAC-Webschnittstelle

So generieren Sie die SupportAssist-Erfassung automatisch:

1 Wechseln Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Fehlerbehebung** > **SupportAssist**.

Daraufhin wird die Seite **SupportAssist** angezeigt.

2 Wählen Sie die Optionen aus, für die Sie Daten erfassen möchten:

- **Hardware**
- **Betriebssystem- und Anwendungsdaten**

  ANMERKUNG: Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen.

- Klicken Sie auf **Erweiterte Exportoptionen**. Folgende zusätzliche Optionen stehen zur Verfügung:
  - **RAID Controller-Protokoll**
  - **Filtern von Berichten aktivieren** unter **Betriebssystem- und Anwendungsdaten**

Basierend auf den ausgewählten Optionen wird die Zeit, die zur Sammlung der Daten verwendet wurde, neben diesen Optionen angezeigt.

3 Wählen Sie **Ich stimme der Verwendung dieser Daten durch SupportAssist zu** aus, und klicken Sie auf **Exportieren**.

4 Wenn das iDRAC Service Modul die Übertragung des Betriebssystems und der Anwendungsdaten auf iDRAC abgeschlossen hat, wird es zusammen mit den Hardware-Daten gepackt und der endgültig Bericht wird erstellt. Eine Meldung wird angezeigt, um den Bericht zu speichern.

5 Geben Sie den Speicherort an, an dem die SupportAssist-Erfassung gespeichert werden soll.

Manuelles Generieren der SupportAssist-Erfassung

Wenn iSM nicht installiert ist, können Sie das OS Collector-Tool manuell ausführen, um die SupportAssist-Erfassung zu generieren. Sie müssen das OS Collector-Tool auf dem Serverbetriebssystem ausführen, um die Betriebssystem- und Anwendungsdaten zu exportieren. Ein virtuelles USB-Gerät mit der Bezeichnung DRACRW wird im Serverbetriebssystem angezeigt. Dieses Gerät enthält die für das Hostbetriebssystem spezifische OS Collector-Datei. Führen Sie die Datei über das Server-BS aus, um die Daten zu erfassen und zu iDRAC zu übertragen. Sie können die Daten dann an einen lokalen oder einen freigegebenen Netzwerkspeicherort exportieren.

Bei Dell PowerEdge-Servern der 13. Generation wird das OS Collector-DUP werkseitig installiert. Wenn Sie jedoch feststellen, dass OS Collector nicht im iDRAC vorhanden ist, dann können Sie die DUP-Datei von der Dell Support-Website herunterladen und dann die Datei unter Verwendung des Firmware-Update-Vorgangs auf iDRAC hochladen.

Bevor Sie die SupportAssist-Erfassung manuell unter Verwendung des OS Collector Tools generieren, führen Sie die folgenden Schritte auf dem Host-Betriebssystem aus:

- Auf einem Linux-Betriebssystem: Überprüfen Sie, ob der IPMI-Dienst ausgeführt wird. Wenn er nicht ausgeführt wird, müssen Sie den Dienst manuell starten. Die folgende Tabelle enthält die Befehle, die Sie verwenden können, um den IPMI-Dienststatus zu überprüfen und den Dienst (falls erforderlich) für jedes Linux-Betriebssystem zu starten.

Tabelle 48. Linux-Betriebssystem und Befehl zum Überprüfen des IPMI-Dienstes

LINUX-Betriebssystem	Befehl zum Aktivieren des IPMI-Dienst-Status	Der Befehl zum Starten des IPMI-Diensts
Red Hat Enterprise Linux 5 64-Bit	`$ service ipmi status`	`$ service ipmi start`
Red Hat Enterprise Linux 6		

LINUX-Betriebssystem	Befehl zum Aktivieren des IPMI-Dienst-Status	Der Befehl zum Starten des IPMI-Diensts
SUSE Linux Enterprise Server 11		
CentOS 6		
Oracle VM		
Oracle Linux 6.4		
Red Hat Enterprise Linux 7	`$ systemctl status ipmi.service`	`$ systemctl start ipmi.service`

ANMERKUNG:

- CentOS wird nur für iDRAC Service Module 2.0 oder höher unterstützt.
- Wenn die IPMI-Module nicht vorhanden sind, können Sie die jeweiligen Module aus den BS-Installationsmedien installieren. Der Dienst wird gestartet, sobald die Installation abgeschlossen ist.

- Auf Windows-Betriebssystemen:
  - Überprüfen Sie, ob der WMI-Dienst ausgeführt wird:
    - Wenn WMI angehalten wird, startet der OS Collector automatisch die WMI und fährt mit der Sammlung fort.
    - Wenn WMI deaktiviert ist, hält die OS Collector-Sammlung mit einer Fehlermeldung an.
  - Überprüfen Sie die entsprechenden Berechtigungsebenen, und stellen Sie sicher, dass keine Firewall- oder Sicherheitseinstellungen verhindern, dass die Registrierungs- oder Software-Daten abgerufen werden.

Manuelles Generieren der SupportAssist-Erfassung unter Verwendung der iDRAC-Webschnittstelle

So generieren Sie die SupportAssist-Erfassung manuell:

1. Wechseln Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Fehlerbehebung** > **SupportAssist**.

   Daraufhin wird die Seite **SupportAssist** angezeigt.
2. Wählen Sie die Optionen aus, für die Sie Daten erfassen möchten:
   - **Hardware** zum Exportieren des Berichts an einen Speicherort auf dem lokalen System.
   - **Betriebssystem- und Anwendungsdaten** zum Exportieren des Berichts an eine Netzwerkfreigabe und zum Festlegen der Netzwerkeinstellungen.

     ANMERKUNG: Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen.
   - Klicken Sie auf **Erweiterte Exportoptionen**. Folgende zusätzliche Optionen stehen zur Verfügung:
     - **RAID Controller-Protokoll**
     - **Filtern von Berichten aktivieren** unter **Betriebssystem- und Anwendungsdaten**

   Basierend auf den ausgewählten Optionen wird die Zeit, die zur Sammlung der Daten verwendet wurde, neben diesen Optionen angezeigt.

   Wenn das OS Collector Tool nicht auf dem System ausgeführt wurde, wird die Option „Betriebssystem- und Anwendungsdaten“ ausgeblendet und kann nicht gewählt werden. Die Meldung „BS- und Anwendungsdaten (Zeitstempel: Nie)“ wird angezeigt.

   Wenn OS Collector in der Vergangenheit auf dem System ausgeführt wurde, zeigt der Zeitstempel an, wann die Betriebssystem- und Anwendungsdaten zuletzt erfasst wurden: Last Collected: <timestamp> (Zuletzt erfasst: <Zeitstempel>)
3. Klicken Sie auf **Mit BS-Collector verbinden**.

   Sie werden zum Zugriff auf das Host-Betriebssystem aufgefordert. Eine Nachricht wird angezeigt, die Sie zum Starten der virtuellen Konsole auffordert.
4. Klicken Sie ach dem Start der virtuellen Konsole auf die Popup-Meldung, um das OS Collector-Tool auszuführen und zu verwenden, um die Daten zu erfassen.

5 Navigieren Sie zum virtuellen DRACRW USB-Gerät das dem System durch den iDRAC zur Verfügung gestellt wird.
6 Rufen Sie die OS Collector-Datei für das geeignete Host-Betriebssystem auf:
   - Führen Sie für Windows **Windows_OSCollector_Startup.bat** aus.
   - Führen Sie für Linux **Linux_OSCollector_Startup.exe** aus.
7 Nachdem der OS Collector die Übertragung der Daten auf iDRAC abgeschlossen hat, wird das USB-Gerät automatisch von iDRAC entfernt.
8 Kehren Sie zurück zur Seite **SupportAssist**, und klicken Sie auf das Symbol für **Aktualisieren**, um den neuen Zeitstempel anzupassen.
9 Um die Daten zu exportieren, wählen Sie unter **Export-Speicherort Lokal** oder **Netzwerk** aus.
10 Falls Sie **Netzwerk** ausgewählt haben, geben Sie die Details zum Netzwerk-Speicherort an.
11 Wählen Sie **Ich stimme der Verwendung dieser Daten durch SupportAssist zu** aus, und klicken Sie auf **Exportieren**, um die Daten am angegebenen Speicherort zu speichern.

Manuelles Generieren der SupportAssist-Erfassung unter Verwendung von RACADM

Zum Generieren der SupportAssist-Erfassung unter Verwendung von RACADM, verwenden Sie den Unterbefehl **techsupreport**. Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Serverstatusbildschirm auf Fehlermeldungen überprüfen

Wenn eine gelbe LED zu blinken beginnt und ein bestimmter Server einen Fehler aufweist, kennzeichnet der Hauptserverstatusbildschirm auf dem LCD den betroffenen Server in Orange. Verwenden Sie die Navigationsschaltflächen des LCD, um den betroffenen Server zu kennzeichnen, und klicken Sie dann auf die Schaltfläche in der Mitte. Fehler- und Warnmeldungen werden jetzt in der zweiten Zeile angezeigt. Eine Liste der im LCD-Feld angezeigten Fehlermeldungen finden Sie im Server-Benutzerhandbuch.

iDRAC-Neustart

Sie können einen harten oder weichen iDRAC-Neustart ausführen, ohne den Server auszuschalten:

- Harter Neustart – Halten Sie auf dem Server die LED-Schaltfläche für 15 Sekunden gedrückt.
- Weicher Neustart – Über die iDRAC-Webschnittstelle oder RACADM.

Zurücksetzen des iDRAC über die iDRAC-Webschnittstelle

Führen Sie zum Zurücksetzen von iDRAC einen der folgenden Schritte über die iDRAC-Webschnittstelle aus:

- Gehen Sie zu **Übersicht** > **Server** > **Zusammenfassung**. Klicken Sie unter **Schnellstart-Tasks** auf **iDRAC zurücksetzen**.
- Gehen Sie zu **Übersicht** > **Server** > **Fehlerbehebung** > **Diagnose**. Klicken Sie auf **iDRAC zurücksetzen**.

Zurücksetzen des iDRAC über RACADM

Für den Neustart von iDRAC verwenden Sie den Befehl **racreset**. Weitere Informationen finden Sie im *RACADM-Referenzhandbuch für iDRAC und CMC* unter **dell.com/support/manuals**.

Löschen von System- und Benutzerdaten

Sie können System-Komponente(n) und die Benutzerdaten für diese Komponenten löschen. Das System umfasst u. a. die folgenden Komponenten:

- Lifecycle-Controller-Daten
- Integrierte Diagnosefunktionen
- Integriertes BS-Treiberpaket
- Zurücksetzen des BIOS auf die Standardeinstellungen
- Zurücksetzen des iDRAC auf die Standardeinstellungen

Stellen Sie vor der Durchführung einer Systemlöschung Folgendes sicher:

- Sie verfügen über iDRAC-Serversteuerung-Berechtigungen.
- Lifecycle Controller ist aktiviert.

Die Option „Lifecycle-Controller-Daten“ löscht jeden Inhalt, wie z. B. das LC-Protokoll, die Konfigurations-Datenbank, die Werk-Protokolle wie ab Werk geliefert und die Konrigurations-Informationen aus dem FP-SPI (oder die Verwaltungs-Riser).

ANMERKUNG: Das Lifecycle Controller-Protokoll enthält die Informationen über die Anfrage zur Systemlöschung und alle Informationen, die erzeugt werden, wenn der iDRAC neu startet. Alle vorherigen Informationen werden entfernt.

Sie können einzelne oder mehrere Systemkomponenten mithilfe des **SystemErase**-Befehls löschen:

```
racadm systemErase <BIOS | DIAG | DRVPACK | LCDATA | IDRAC >
```

wobei

- BIOS – BIOS wird auf die Standardeinstellung zurückgesetzt
- DIAG – Integrierte Diagnosefunktionen
- DRVPACK – Integriertes BS-Treiberpaket
- LCDATA – Löscht die Lifecycle-Controller-Daten
- IDRAC – iDRAC wird auf die Standardeinstellung zurückgesetzt

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

ANMERKUNG: Der Dell Tech Center-Link wird in der iDRAC-GUI auf Systemen der Marke Dell angezeigt. Wenn Sie Systemdaten unter Verwendung des WS-Man-Befehls löschen und möchten, dass der Link wieder angezeigt wird, starten Sie den Host manuell neu und warten Sie, bis CSIOR ausgeführt wird.

Zurücksetzen des iDRAC auf die Standardeinstellungen

Sie können iDRAC mithilfe des Dienstprogramms für die iDRAC-Einstellungen oder der iDRAC-Webschnittstelle auf die Werkseinstellungen zurücksetzen.

Zurücksetzen von iDRAC auf die Standardwerkseinstellungen unter Verwendung der iDRAC-Webschnittstelle

So setzen Sie iDRAC mithilfe der iDRAC-Webschnittstelle auf die Standardwerkseinstellungen zurück:

1 Gehen Sie zu **Übersicht** > **Server** > **Fehlerbehebung** > **Diagnose**.
Daraufhin wird die Seite **Diagnoseprogramm Konsole** angezeigt.

2 Klicken Sie auf **iDRAC auf Standardeinstellungen zurücksetzen**.
Der Status der Fertigstellung wird in Prozent angezeigt. iDRAC startet neu und wird zurück auf die Werkseinstellungen gesetzt. Die iDRAC-IP wird zurückgesetzt und es kann nicht darauf zugegriffen werden. Sie können die IP mithilfe der Frontblende oder des BIOS konfigurieren.

Zurücksetzen von iDRAC auf die Standardwerkseinstellungen unter Verwendung des Dienstprogramms für iDRAC-Einstellungen

So setzen Sie iDRAC über das Dienstprogramm für die iDRAC-Einstellungen auf die werksseitigen Standardeinstellungen zurück:

1 Gehen Sie zu **iDRAC Konfigurationen auf Standard zurücksetzen**.
Daraufhin wird die Seite **iDRAC-Einstellungen – iDRAC-Konfigurationen auf Standardeinstellungen zurücksetzen** angezeigt.

2 Klicken Sie auf **Ja**.
Die iDRAC Zurücksetzung startet.

3 Klicken Sie auf **Zurück**, und navigieren Sie erneut zur Seite **iDRAC-Einstellungen – iDRAC-Konfigurationen auf Standardeinstellungen zurücksetzen**, um die Erfolgsmeldung anzuzeigen.

24

Häufig gestellte Fragen

In diesem Abschnitt werden häufig gestellte Fragen zu den folgenden Themen aufgelistet:

- System-Ereignisprotokoll
- Netzwerksicherheit
- Active Directory
- Einfache Anmeldung
- Smart Card-Anmeldung
- Virtuelle Konsole
- Virtueller Datenträger
- vFlash-SD-Karte
- SNMP-Authentifizierung
- Speichergeräte
- iDRAC Service Module
- RACADM
- Verschiedenes

Themen:

- System-Ereignisprotokoll
- Netzwerksicherheit
- Active Directory
- Einfache Anmeldung
- Smart Card-Anmeldung
- Virtuelle Konsole
- Virtueller Datenträger
- vFlash-SD-Karte
- SNMP-Authentifizierung
- Speichergeräte
- iDRAC Service Module
- RACADM
- Verschiedenes

System-Ereignisprotokoll

Warum verwendet SEL während der Verwendung der iDRAC-Webschnittstelle über den Internet Explorer nicht die Option „Speichern unter“?

Der Grund dafür liegt in einer Browser-Einstellung. So können Sie das Problem lösen:

1 Wechseln Sie im Internet Explorer zu **Tools** > **Internetopionen** > **Sicherheit** und wählen Sie die Zone, in die Sie versuchen herunterzuladen.

Wenn sich das iDRAC-Gerät z. B. in Ihrem lokalen Intranet befindet, wählen Sie **Lokales Intranet** und klicken Sie auf **Stufe anpassen**....

2 Im Fenster **Sicherheitseinstellungen** müssen unter **Downloads** die folgenden Optionen aktiviert sein:
   - Automatische Eingabeaufforderung für Datei-Downloads (falls diese Option verfügbar ist)
   - Dateien herunterladen

VORSICHT: Um sicherzustellen, dass der Computer, der für den Zugriff auf iDRAC verwendet wird, sicher ist, aktivieren Sie unter Verschiedenes nicht die Option Anwendungen und unsichere Dateien starten.

Netzwerksicherheit

Während des Zugriffs auf die iDRAC-Webschnittstelle wird eine Sicherheitswarnung angezeigt, aus der hervorgeht, dass das durch die Zertifizierungsstelle ausgestellte SSL-Zertifikat nicht vertrauenswürdig ist.

iDRAC ist mit einem standardmäßigen iDRAC-Server-Zertifikat ausgestattet, das die Netzwerksicherheit gewährleistet, während der Zugriff über die Web-Schnittstelle oder ein Remote-RACADM erfolgt. Dieses Zertifikat wurde durch eine nicht vertrauenswürdige Zertifizierungsstelle ausgestellt. Um dieses Problem zu beheben, laden Sie ein iDRAC-Server-Zertifikat hoch, das durch eine vertrauenswürdige Zertifizierungsstelle ausgestellt wurde (z. B. Microsoft Certificate Authority, Thawte oder Verisign).

Warum führt der DNS-Server keine Registrierung von iDRAC durch?

Einige DNS-Server registrieren ausschließlich iDRAC-Namen mit bis zu 31 Zeichen.

Wenn Sie auf die iDRAC-Webschnittstelle zugreifen, wird eine Sicherheitswarnung angezeigt, aus der hervorgeht, dass der SSL-Zertifikat-Host-Name nicht mit dem iDRAC-Host-Namen übereinstimmt.

iDRAC ist mit einem standardmäßigen iDRAC-Server-Zertifikat ausgestattet, das die Netzwerksicherheit gewährleistet, während der Zugriff über die Web-Schnittstelle oder ein Remote-RACADM erfolgt. Wenn dieses Zertifikat verwendet wird, zeigt der Web-Browser eine Sicherheitswarnung an, da das für iDRAC ausgestellte Standardzertifikat nicht mit dem iDRAC-Host-Namen übereinstimmt (z. B. mit der IP-Adresse).

Um dieses Problem zu lösen, laden Sie ein iDRAC-Server-Zertifikat hoch, das auf die IP-Adresse oder den iDRAC-Host-Namen ausgestellt wurde. Im Rahmen der Generierung der Zertifikatsignierungsanforderung (für die Ausstellung des Zertifikats) müssen Sie sicherstellen, dass der allgemeine Name (CN) der Zertifikatsignierungsanforderung mit der iDRAC-IP-Adresse (wenn auf die IP-Adresse ausgestellt) oder mit dem registrierten DNS-iDRAC-Namen (wenn auf den registrierten iDRAC-Namen ausgestellt) übereinstimmt.

So stellen Sie sicher, dass die Zertifikatsignierungsanforderung mit dem registrierten DNS-iDRAC-Namen übereinstimmt:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk**. Daraufhin wird die Seite **Netzwerk** angezeigt.
2 Im Abschnitt **Allgemeine Einstellungen**:
   - Wählen Sie die Option **iDRAC auf DNS registrieren** aus.
   - Geben Sie den iDRAC-Namen in das Feld **DNS-iDRAC-Name** ein.
3 Klicken Sie auf **Anwenden**.

Active Directory

Meine Active Directory-Anmeldung ist gescheitert. Wie kann ich dieses Problem lösen?

Um das Problem zu diagnostizieren, klicken Sie auf der Seite **Active Directory-Konfiguration und -Verwaltung** auf die Option **Einstellungen testen**. Überprüfen Sie die Testergebnisse, und beheben Sie das Problem. Ändern Sie die Konfiguration, und führen Sie den Test aus, bis der Test den Authorisierungsschritt erfolgreich bestanden hat.

Überprüfen Sie allgemein die folgenden Aspekte:

- Stellen Sie während des Anmeldens sicher, dass Sie den richtigen Benutzerdomänennamen und nicht den NetBIOS-Namen verwenden. Wenn Sie ein lokales iDRAC-Benutzerkonto haben, melden Sie sich auf dem iDRAC mit den lokalen Anmeldeinformationen an. Überprüfen Sie nach der Anmeldung Folgendes:
  - Die Option **Active Directory aktivieren** ist auf der Seite **Aktive Directory-Konfiguration und -Verwaltung** markiert.
  - Die DNS-Einstellung auf der **iDRAC-Netzwerkkonfigurationsseite** ist korrekt.
  - Sie haben das richtige Stamm-CA-Zertifikat des Active Directory auf den iDRAC hochgeladen, falls Überprüfung des Zertifikats aktiviert wurde.
  - Der iDRAC-Name und der iDRAC-Domänenname stimmen mit der Active Directory-Umgebungskonfiguration überein, wenn Sie das erweiterte Schema verwenden.
  - Der Gruppenname und der Gruppendomänenname stimmen mit der Active Directory-Konfiguration überein, wenn Sie das Standardschema verwenden.
  - Wenn der Benutzer und das iDRAC-Objekt sich in einer anderen Domäne befinden, dann wählen Sie nicht die Option **Benutzerdomäne von Anmeldung** aus. Stattdessen wählen Sie die Option **Eine Domäne angeben** aus, und geben Sie den Namen der Domäne ein, in der sich das iDRAC-Objekt befindet.
- Überprüfen Sie die SSL-Zertifikate des Domänen-Controllers, um sicherzustellen, dass die iDRAC-Zeit innerhalb der Gültigkeitsdauer des Zertifikats liegt.

Die Anmeldung bei Active Directory schlägt selbst dann fehl, wenn die Zertifikatüberprüfung aktiviert ist. Die Testergebnisse zeigen die folgende Fehlermeldung an. Warum tritt dieses Verhalten auf, und wie kann es gelöst werden?

```
ERROR: Can't contact LDAP server, error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct
Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if the
iDRAC date is within the valid period of the certificates and if the Domain Controller Address
configured in iDRAC matches the subject of the Directory Server Certificate.
```

Wenn die Zertifikatsüberprüfung aktiviert ist, sobald der iDRAC die SSL-Verbindung zum Verzeichnisserver herstellt, verwendet iDRAC das hochgeladene Zertifizierungsstellenzertifikat, um das Zertifikat des Verzeichnisservers zu überprüfen. Die häufigsten Gründe für eine fehlgeschlagene Zertifikatsüberprüfung sind Folgende:

- Das Gültigkeitsdatum des iDRAC liegt nicht innerhalb des Gültigkeitszeitraums des Serverzertifikats oder des Zertifizierungsstellenzertifikats. Überprüfen Sie die Gültigkeit des iDRAC-Zertifikats und Ihres Zertifikats.
- Die in iDRAC konfigurierten Domänen-Controller-Adressen stimmen nicht mit dem Servernamen oder alternativen Servernamen im Directory-Server-Zertifikat überein. Falls Sie eine IP-Adresse verwenden, lesen Sie bitte die folgende Frage. Wenn Sie einen FQDN verwenden, stellen Sie bitte sicher, dass Sie den FQDN des Domänen-Controllers verwenden und nicht den der Domäne selbst, zum Beispiel **servername.example.com** anstelle von **example.com**.

Die Zertifikatüberprüfung schlägt fehl, auch wenn die IP-Adresse als Domänen-Controller-Adresse verwendet wird. Wie kann dieses Verhalten gelöst werden?

Prüfen Sie das Feld Servername oder alternativer Servername Ihres Domänen-Controller-Zertifikats. Normalerweise verwendet Active Directory den Host-Namen und nicht die IP-Adresse des Domänen-Controllers im Feld Servername oder alternativer Servername des Domänen-Controller-Zertifikats. Um das Problem zu lösen, führen Sie einen der folgenden Schritte aus:

- Konfigurieren Sie den Hostnamen (FQDN) des Domänen-Controllers als *Adresse(n) des Domänen-Controllers* auf dem iDRAC, damit er mit dem Servernamen oder alternativen Servernamen des Server-Zertifikats übereinstimmt.
- Erstellen Sie das Server-Zertifikat erneut, damit im Feld "Servername" oder "Alternativer Servername" eine IP-Adresse verwendet wird, die auf dem iDRAC konfiguriert ist.
- Deaktivieren Sie die Überprüfung des Zertifikats, wenn Sie dem Domänen-Controller beim SSL-Handshake ohne diese Überprüfung vertrauen.

Wie werden die Domänen-Controller-Adressen konfiguriert, wenn das erweiterte Schema in einer Umgebung mit mehreren Domänen verwendet wird?

Es musste der Host-Name (FQDN) oder die IP-Adresse des Domänen-Controllers sein, der die Domäne bedient, in der sich das iDRAC-Objekt befindet.

Wann muss ich Adressen des globalen Katalogs konfigurieren?

Wenn Sie das Standardschema verwenden und die Benutzer und Rollengruppen verschiedenen Domänen angehören, sind Adressen des globalen Katalogs erforderlich. In diesem Fall können Sie nur die Universalgruppe benutzen.

Wenn Sie das Standardschema verwenden und alle Benutzer und Rollengruppen derselben Domäne angehören, sind keine Adressen des globalen Katalogs erforderlich.

Wenn Sie ein erweitertes Schema verwenden, wird die Adresse des globalen Katalogs nicht verwendet.

Wie funktioniert die Abfrage im Standardschema?

iDRAC verbindet sich zuerst mit den konfigurierten Domänen-Controller-Adressen, wenn sich die Benutzer und Rollengruppen in dieser Domäne befinden. Die Berechtigungen werden gespeichert.

Wenn Global Controller-Adressen konfiguriert werden, fragt iDRAC6 weiterhin den Global Catalog ab. Wenn zusätzliche Berechtigungen vom Global Catalog erfasst werden, werden diese Berechtigungen aufgespeichert.

Verwendet iDRAC immer LDAP über SSL?

Ja. Der gesamte Transfer erfolgt über den geschützten Anschluss 636 und/oder 3269. Unter Einstellungen testen führt iDRAC einen LDAP CONNECT durch, um das Problem zu isolieren, er führt jedoch keinen LDAP BIND auf einer unsicheren Verbindung aus.

Warum ist in der Standardkonfiguration des iDRAC die Überprüfung des Zertifikats aktiviert?

iDRAC setzt eine hohe Sicherheit durch, um die Identität des Domänen-Controllers, mit dem iDRAC eine Verbindung herstellt, sicherzustellen. Ohne Überprüfung des Zertifikats kann ein Hacker über einen vorgetäuschten Domänen-Controller die SSL-Verbindung übernehmen. Wenn Sie allen Domänen-Controllern in Ihrem Sicherheitsbereich ohne Überprüfung des Zertifikats vertrauen, können Sie die Überprüfung durch die Web-Schnittstelle oder RACADM deaktivieren.

Unterstützt iDRAC den NetBIOS-Namen?

Nicht in dieser Version.

Warum dauert es bis zu vier Minuten, sich über die Active Directory-basierte Einmal- oder Smart Card-Anmeldung bei iDRAC anzumelden?

Die Active Directory-Einmal- oder die Smart Card-Anmeldung dauert in der Regel weniger als 10 Sekunden; die Anmeldung kann allerdings bis zu vier Minuten dauern, wenn Sie den bevorzugten DNS-Server und den alternativen DNS-Server angegeben haben und der bevorzugte DNS-Server fehlschlägt. DNS-Zeitüberschreitungen werden erwartet, wenn ein DNS-Server heruntergefahren ist. iDRAC meldet Sie unter Verwendung des alternativen DNS-Servers an.

Das Active Directory für eine vorhandene Domäne ist in Windows Server 2008 Active Directory kofiguriert. Eine untergeordnete Domäne bzw. Subdomäne ist für die Domäne vorhanden, der Benutzer und die Gruppe sind in derselben untergeordneten Domäne vorhanden und der Benutzer ist ein Mitglied dieser Gruppe. Bei dem Versuch, sich unter Verwendung des Benutzers, der sich in der untergeordneten Domäne befindet, am iDRAC anzumelden, schlägt das Einmalige Anmelden über Active Directory fehl.

Dies kann möglicherweise auf den falschen Gruppentyp zurückzuführen sein. Im Active Directory-Server gibt es zwei Arten von Gruppentypen:

- Sicherheit – Sicherheitsgruppen ermöglichen Ihnen, den Benutzer- und Computerzugriff auf freigegebene Ressourcen zu verwalten und Gruppenrichtlinieneinstellungen zu filtern.
- Verteilung – Verteilungsgruppen sind nur als E-Mail-Verteilerlisten vorgesehen.

Stellen Sie immer sicher, dass der Gruppentyp Sicherheit lautet. Sie können zum Zuweisen von Berechtigungen für Objekte keine Verteilergruppen verwenden, verwenden Sie diese jedoch zum Filtern von Gruppenrichtlinieneinstellungen.

Einmaliges Anmelden

Die SSO-Anmeldung schlägt auf Windows Server 2008 R2 x64 fehl. Welche Einstellungen sind zum Lösen dieses Problems erforderlich?

1 Führen Sie **http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** für den Domänen-Controller und die Domänenregel aus.

2 Konfigurieren Sie die Computer zur Verwendung der DES-CBC-MD5-Cipher-Suite.

Diese Einstellungen haben möglicherweise Einfluss auf die Kompatibilität mit Client-Computern oder -Diensten und Anwendungen in Ihrer Umgebung. Die Regeleinstellung Für Kerberos zulässige Verschlüsselungstypen konfigurieren ist unter **Computer-Konfiguration** > **Sicherheitseinstellungen** > **Lokale Richtlinien** > **Sicherheitsoptionen** gespeichert.

3 Stellen Sie sicher, dass die Domänen-Clients über das aktualiserte GPO verfügen.

4 Geben Sie in der Befehlszeile den Befehl `gpupdate /force` ein und löschen Sie die alte Keytab mit Befehl `klist purge`.

5 Nachdem das GPO aktualisiert wurde, erstellen Sie die neue Keytab.

6 Laden Sie das Keytab zu iDRAC hoch.

Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Warum scheitert die SSO-Anmeldung bei Active Directory-Benutzern auf Windows 7 und Windows Server 2008 R2?

Sie müssen die Verschlüsselungstypen für Windows 7 und Windows Server 2008 R2 aktivieren. So aktivieren Sie die Verschlüsselungstypen:

1 Melden Sie sich als Administrator oder als Benutzer mit Administratorrechten an.

2 Wechseln Sie zu **Start** und führen Sie **gpedit.msc** aus. Das Fenster **Editor für lokale Gruppenrichtlinien** wird angezeigt.

3 Wechseln Sie zu **Lokale Computereinstellungen** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Lokale Richtlinien** > **Sicherheitsoptionen**.

4 Klicken Sie mit der rechten Maustaste auf **Netzwerksicherheit: Für Kerberos genehmigte Verschlüsselungstypen konfigurieren** und wählen Sie **Eigenschaften** aus.

5 Aktivieren Sie alle Optionen.

6 Klicken Sie auf **OK**. Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Führen Sie die folgenden zusätzlichen Einstellungen für das erweiterte Schema aus:

1 Navigieren Sie im Fenster **Editor für lokale Gruppenrichtlinien** zu **Einstellungen des lokalen Computers** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Lokale Richtlinien** > **Sicherheitsoptionen**.

2 Klicken Sie mit der rechten Maustaste auf **Netzwerksicherheit: NTLM einschränken: Ausgehender NTLM-Verkehr zu Remote-Server** und wählen Sie **Eigenschaften** aus.

3 Wählen Sie **Alle zulassen**, klicken Sie auf **OK** und schließen Sie das Fenster **Editor für lokale Gruppenrichtlinien**.

4 Gehen Sie zu **Start**, und führen Sie den Befehl „cmd“ aus. Daraufhin wird das Fenster mit der Windows-Befehlseingabe angezeigt.

5 Führen Sie den Befehl `gpupdate /force` aus. Die Gruppenrichtlinien werden daraufhin aktualisiert. Schließen Sie das Fenster für die Befehlseingabe.

6 Gehen Sie zu **Start**, und führen Sie den Befehl „lregedit“ aus. Daraufhin wird der **Registrierungs-Editor** aufgerufen.

7 Navigieren Sie zu **HKEY_LOCAL_MACHINE** > **System** > **CurrentControlSet** > **Control** > **LSA** .

8 Klicken Sie mit der rechten Maustaste in den rechten Fensterbereich und wählen Sie **Neu** > **DWORD (32-Bit) Wert** aus.

9 Geben Sie dem neuen Schlüssel den Namen **SuppressExtendedProtection**.

10 Klicken Sie mit der rechten Maustaste auf **SuppressExtendedProtection** und klicken Sie dann auf **Ändern.**.

11 Geben Sie in das Feld **Wertdaten** die Zahl **1** ein und klicken Sie auf **OK**.

12 Schließen Sie das Fenster **Registrierungseditor**. Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Wenn Sie die SSO für iDRAC aktiviert haben und Internet Explorer zum Anmelden an iDRAC verwenden, schlägt die SSO fehl, und Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben. Wie beheben Sie das Problem?

Stellen Sie sicher, dass die iDRAC-IP-Adresse unter **Extras** > **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Sites**aufgelistet ist. Wenn sie nicht aufgelistet ist, schlägt die SSO fehl, und Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben. Klicken Sie auf **Abbrechen** und fahren Sie fort.

Smart Card-Anmeldung

Bei Verwendung der Active Directory Smart-Card-Anmeldung dauert es vbs zu vier Minuten, um sich am iDRAC anzumelden.

Die normale Active Directory-Smart Card oder die Smart Card-Anmeldung dauert in der Regle weniger als 10 Sekunden; die Anmeldung kann allerdings bis zu vier Minuten dauern, wenn Sie den bevorzugten DNS-Server und den alternativen DNS-Server auf der Seite **Netzwerk** angegeben haben und der bevorzugte DNS-Server fehlschlägt. DNS-Zeitüberschreitungen werden erwartet, wenn ein DNS-Server heruntergefahren ist. iDRAC meldet Sie unter Verwendung des alternativen DNS-Servers an.

Das ActiveX-Plugin kann das Smart Card-Laufwerk nicht erkennen.

Stellen Sie sicher, dass die Smart Card auf dem Microsoft Windows-Betriebssystem unterstützt wird. Windows unterstützt eine beschränkte Anzahl von Cryptographic Service Providers (CSP) für die Smart Card.

Sie können generell überprüfen, ob die Smart Card-CSPs auf einem bestimmten Client vorhanden sind, indem Sie die Smart Card beim Windows-Anmeldebildschirm (Strg-Alt-Entf) in das Laufwerk einlegen, um zu sehen, ob Windows die Smart Card erkennt und das PIN-Dialogfeld einblendet.

Falsche Smart Card-PIN

Prüfen Sie, ob die Smart Card aufgrund übermäßiger Versuche mit einer falschen PIN gesperrt wurde. In solchen Fällen kann Ihnen der Aussteller der Smart Card in der Organisation helfen, eine neue Smart Card zu beschaffen.

Virtuelle Konsole

Die Sitzung für die virtuelle Konsole ist aktiv, auch wenn Sie sich von der iDRAC-Webschnittstelle abgemeldet haben. Ist dies das erwartete Verhalten?

Ja. Schließen Sie das Fenster mit dem Viewer für die virtuelle Konsole, um sich von der entsprechenden Sitzung abzumelden.

Kann eine neue Remote-Konsolenvideositzung gestartet werden, wenn das lokale Video auf dem Server ausgeschaltet ist?

Ja.

Warum dauert es 15 Sekunden, um das lokale Video auf dem Server auszuschalten, nachdem eine Aufforderung zum Ausschalten des lokalen Videos eingereicht wurde?

Hierdurch wird einem lokalen Benutzer die Gelegenheit gegeben, Maßnahmen durchzuführen, bevor das Video ausgeschaltet wird.

Tritt beim Einschalten des lokalen Videos eine Zeitverzögerung auf?

Nein. Sobald der iDRAC eine Anforderung zum Einschalten des lokalen Videos erhält, wird das Video sofort eingeschaltet.

Kann der lokale Benutzer das Video aus- oder einschalten?

Wenn die lokale Konsole deaktiviert ist, kann der lokale Benutzer das Video nicht aus- oder einschalten.

Werden beim Ausschalten des lokalen Videos auch die lokale Tastatur und Maus ausgeschaltet?

Nein.

Wird durch das Ausschalten der lokalen Konsole auch das Video der Remote-Konsolensitzung ausgeschaltet?

Nein, das Ein- oder Ausschalten des lokalen Videos ist von der Remote-Konsolensitzung unabhängig.

Welche Berechtigungen sind für einen iDRAC-Benutzer erforderlich, um das lokale Server-Video ein- oder auszuschalten?

Sämtliche Benutzer mit iDRAC-Konfigurationsberechtigungen können die lokale Konsole ein- oder ausschalten.

Wie kann ich den aktuellen Status des lokalen Servervideos abrufen?

Der Status wird auf der Seite „Virtuelle Konsole“ angezeigt.

Verwenden Sie zur Anzeige des Status des Objekts den folgenden Befehl: `iDRAC.VirtualConsole.AttachState`.

```
racadm get idrac.virtualconsole.attachstate
```

Verwenden Sie alternativ den folgenden Befehl über eine Telnet-, SSH- oder eine Remote-Sitzung:

```
racadm -r (iDrac IP) -u (username) -p (password) get iDRAC.VirtualConsole.AttachState
```

Der Status wird auch auf der OSCAR-Anzeige der virtuellen Konsole angezeigt. Wenn die lokale Konsole aktiviert ist, wird neben dem Servernamen ein grüner Status angezeigt. Wenn sie deaktiviert ist, zeigt ein gelber Punkt an, dass iDRAC die lokale Konsole gesperrt hat.

Warum wird der untere Bereich des Systembildschirms nicht im Fenster für die virtuelle Konsole angezeigt?

Stellen Sie sicher, dass die Bildschirmauflösung der Management Station auf 1280x1024 eingestellt ist.

Warum wird das Fenster für den Viewer der virtuellen Konsole auf Linux-Betriebssystemen unkenntlich dargestellt?

Für den Konsolen-Viewer ist unter Linux ein UTF-8-Zeichensatz erforderlich. Überprüfen Sie Ihre Spracheinstellungen und setzen Sie den Zeichensatz bei Bedarf zurück.

Warum wird die Maus unter der Linux-Textkonsole in Lifecycle Controller nicht synchronisiert?

Die virtuelle Konsole benötigt den USB-Maustreiber, der USB-Maustreiber ist jedoch nur im X-Window-Betriebssystem verfügbar. Führen Sie im Viewer für die virtuelle Konsole die folgenden Schritte aus:

- Gehen Sie zur Registerkarte **Tools** > **Session Options (Sitzungsoptionen)** > **Mouse (Maus)**. Wählen Sie unter **Mouse Acceleration (Mausbeschleunigung) Linux** aus.
- Wählen Sie im Menü **Extras** die Option **Einzel-Cursor** aus.

Wie kann der Mauszeiger im Fenster für den Viewer für die virtuelle Konsole synchronisiert werden?

Bevor Sie eine Sitzung für eine virtuelle Konsole starten, stellen Sie sicher, dass Sie die richtige Maus für Ihr Betriebssystem ausgewählt haben.

Stellen Sie außerdem sicher, dass die Option **Single Cursor (Einzel-Cursor)** unter **Tools (Extras)** im Menü für die virtuelle iDRAC-Konsole auf dem Client für die Konsole ausgewählt ist. Standardmäßig ist der Zwei-Cursor-Modus eingestellt.

Kann eine Tastatur oder eine Maus verwendet werden, während ein Microsoft-Betriebssystem remote über die virtuelle Konsole installiert wird?

Nein. Wenn Sie remote ein unterstütztes Microsoft-Betriebssystem auf einem System installieren, auf dem die virtuelle Konsole im BIOS aktiviert ist, wird eine EMS-Verbindungsnachricht gesendet, bei der Sie remote **OK** auswählen müssen. Sie müssen entweder **OK** auf dem lokalen System auswählen oder den remote verwalteten Server neu starten, eine Neuinstallation vornehmen und die virtuelle Konsole im BIOS deaktivieren.

Diese Nachricht wird durch Microsoft erstellt, um den Benutzer darauf hinzuweisen, dass die virtuelle Konsole aktiviert ist. Um sicherzustellen, dass diese Meldung nicht angezeigt wird, müssen Sie die virtuelle Konsole im Dienstprogramm für die iDRAC-Einstellungen ausschalten, bevor Sie ein Betriebssystem remote installieren.

Warum zeigt die Nummernblockanzeige auf der Management Station nicht den Status des Nummernblocks auf dem Remote-Server an?

Wenn Sie über iDRAC auf den Nummernblock auf der Management Station zugreifen, stimmt dieser nicht unbedingt mit dem Status des Nummernblocks auf dem Remote-Server überein. Der Status des Nummernblocks hängt von der Einstellung zum Zeitpunkt der Verbindungsherstellung der Remote-Sitzung ab. Dabei ist der Status des Nummernblocks auf der Management Station nicht von Belang.

Warum werden mehrere Session Viewer-Fenster eingeblendet, wenn vom lokalen Host aus eine Sitzung der virtuellen Konsole aufgebaut wird?

Sie konfigurieren eine virtuelle Konsole über das lokale System. Dieser Vorgang wird nicht unterstützt.

Wenn eine Sitzung für eine virtuelle Konsole aktiv ist und ein lokaler Benutzer auf den Managed Server zugreift, wird dem ersten Benutzer eine Warnmeldung angezeigt?

Nein. Wenn ein lokaler Benutzer auf das System zugreift, haben beide Kontrolle über das System.

Wie viel Bandbreite ist für die Ausführung einer Sitzung für eine virtuelle Konsole erforderlich?

Für eine gute Leistung wird eine Verbindung mit einer Bandbreite von 5 Mbit/s empfohlen. Eine Verbindung mit einer Bandbreite von 1 Mbit/s stellt die Mindestanforderung dar.

Was sind die Mindestsystemanforderungen der Management Station zum Ausführen der virtuellen Konsole?

Die Management Station benötigt einen Intel Pentium III 500-MHz-Prozessor mit mindestens 256 MB RAM.

Warum zeigt das Fenster mit dem Viewer für die virtuelle Konsole manchmal die Meldung „Kein Signal“ an?

Diese Meldung wird angezeigt, da das iDRAC-Plug-in für die virtuelle Konsole das Remote-Server-Desktop-Video nicht empfängt. Im Allgemeinen kann dieses Verhalten auftreten, wenn der Remote-Server ausgeschaltet ist. Manchmal wird diese Meldung aufgrund einer Empfangsfehlfunktion des Remote-Server-Desktop-Videos angezeigt.

Warum zeigt das Fenster für den Viewer der virtuellen Konsole gelegentlich die Meldung „Außerhalb des Bereichs“ an?

Diese Meldung wird möglicherweise angezeigt, weil ein Parameter, der für die Videoerfassung erforderlich ist, sich außerhalb des Bereichs befindet, für den iDRAC das Video erfassen kann. Wenn bestimmte Parameter, z. B. die Anzeigeauflösung oder die Bildwiederholfrequenz, zu hoch eingestellt sind, ist es möglich, dass die Meldung „Out of range“ (Außerhalb des Bereichs) angezeigt wird. In der Regel wird der maximale Bereich der Parameter durch physische Begrenzungen definiert, wie z. B. die Größe des Videospeichers oder der Bandbreite.

Warum wird, wenn eine Sitzung für eine virtuelle Konsole von der iDRAC-Web-Schnittstelle aus gestartet wird, ein ActiveX-Sicherheits-Popup-Fenster angezeigt?

iDRAC ist möglicherweise nicht in der Liste der vertrauenswürdigen Sites enthalten. Um zu verhindern, dass das Sicherheits-Popup-Fenster bei jedem Start einer Sitzung einer virtuellen Konsole aufgerufen wird, fügen Sie iDRAC wie folgt zur Liste der vertrauenswürdigen Sites im Client-Browser hinzu:

1 Klicken Sie auf **Extras** > **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Sites**.
2 Klicken Sie auf **Sites**, und geben Sie die IP-Adresse oder den DNS-Namen des iDRAC ein.
3 Klicken Sie auf **Hinzufügen**.
4 Klicken Sie auf **Stufe anpassen**.
5 Wählen Sie im Fenster **Sicherheitseinstellungen** die Option **Bestätigen** unter **Unsignierte ActiveX-Steuerelemente herunterladen** aus.

Warum ist das Fenster für den Viewer der virtuellen Konsole leer?

Wenn Sie über Berechtigungen für virtuelle Datenträger verfügen, nicht aber für die virtuelle Konsole, können Sie den Viewer für den Zugriff auf die Funktion für virtuelle Datenträger starten, die Konsole des verwalteten Servers wird jedoch nicht angezeigt.

Warum wird die Maus nicht unter DOS synchronisiert, wenn die virtuelle Konsole ausgeführt wird?

Das Dell BIOS emuliert den Maustreiber als PS/2-Maus. Die PS/2-Maus ist so konzipiert, dass sie die relative Position für den Mauszeiger verwendet, was die Verzögerung in der Synchronisation verursacht. iDRAC verfügt über einen USB-Maustreiber, mit dem eine absolute Position und damit eine engere Verfolgung des Mauszeigers möglich ist. Selbst wenn iDRAC die absolute Position der USB-Maus an das Dell BIOS weiterleitet, konvertiert die BIOS-Emulation sie zurück in die relative Position und das Verhalten bleibt unverändert. Um dieses Problem zu beheben, stellen Sie auf dem Bildschirm „Configuration“ (Konfiguration) den Mausmodus auf „USC/Diags“ ein.

Wenn die virtuelle Konsole mit dem Java-Plug-in unter RHEL 7.3 MS gestartet wird, steht die Schaltfläche zum Schließen für die Fenster „Instant Messaging“, „Performance“ (Leistung) und „Stat“ (Status) eventuell nicht zur Verfügung.

Verwenden Sie die Tastenkombination Alt+F4, um das Fenster zu schließen.

Nach dem Start der virtuellen Konsole ist der Mauszeiger auf der virtuellen Konsole aktiv, jedoch nicht auf dem lokalen System. Warum tritt dieses Verhalten auf und wie kann es behoben werden?

Dieser Fehler tritt auf, wenn für **Mouse Mode (Mausmodus) USC/Diags** eingestellt ist. Drücken Sie die Tastenkombination **Alt+M**, um die Maus auf dem lokalen System zu verwenden. Drücken Sie **Alt+M** erneut, um die Maus auf der virtuellen Konsole zu verwenden.

Warum tritt eine Zeitüberschreitung auf der GUI-Sitzung auf, wenn die iDRAC-Webschnittstelle kurz nach dem Start der virtuellen Konsole über die CMC-Web-Schnittstelle gestartet wird?

Wenn die virtuelle Konsole über die CMC-Webschnittstelle für iDRAC gestartet wird, wird ein Popup-Fenster zum Starten der virtuellen Konsole geöffnet. Dieses Popup-Fenster wird kurz nach dem Öffnen der virtuellen Konsole geschlossen.

Wenn sowohl die GUI als auch die virtuelle Konsole auf das gleiche iDRAC-System auf einer Management Station gestartet werden, tritt eine Sitzungszeitüberschreitung für die iDRAC-GUI auf, wenn die GUI vor dem Schließen des Popup-Fensters gestartet wird. Wenn die iDRAC-GUI über die CMC-Webschnittstelle nach dem Schließen des Popup-Fensters der virtuellen Konsole gestartet wird, tritt dieses Problem nicht auf.

Warum kann der Linux S-Abf-Schlüssel nicht mit Internet Explorer verwendet werden?

Das Verhalten der S-Abf-Taste ändert sich, wenn die virtuelle Konsole über Internet Explorer verwendet wird. Um die S-Abf-Taste zu nutzen, drücken Sie die Taste **Druck** und lassen Sie sie los, während Sie die Tasten **Strg** und **Alt** gedrückt halten. So nutzen Sie die S-Abf-Taste für einen Remote-Linux-Server über iDRAC bei Verwendung des Internet Explorers:

1. Aktivieren Sie die Funktion für die magische Taste auf dem Remote-Linux-Server. Sie können den folgenden Befehl verwenden, sie auf dem Linux-Terminal zu aktivieren:
   ```
   echo 1 > /proc/sys/kernel/sysrq
   ```
2. Aktivieren Sie den Tastaturdurchgangsmodus von Active X Viewer.
3. Drücken Sie **Strg+Alt+Druck**.
4. Lassen Sie nur die Taste **Druck** wieder los.
5. Drücken Sie die Tastenkombination **Druck+Strg+Alt**.

ANMERKUNG: Die S-Abf-Funktion wird derzeit nicht für Internet Explorer und Java unterstützt.

Warum wird die Meldung „Verknüpfung unterbrochen“ unten auf der virtuellen Konsole angezeigt?

Wenn Sie während des Neustarts eines Servers den freigegebenen Netzwerkport verwenden, wird iDRAC getrennt, während das BIOS die Netzwerkkarte zurücksetzt. Dieser Vorgang dauert auf Karten mit 10 Gbit länger und dauert außerdem außergewöhnlich lange, wenn auf dem angeschlossenen Netzwerk-Switch das Spanning Tree Protocol (STP) aktiviert ist. In diesem Fall wird empfohlen, die Option „portfast“ für den Switch-Port zu verwenden, der mit dem Server verbunden ist. In den meisten Fällen stellt sich die virtuelle Konsole selbst wieder her.

Das Starten der virtuellen Konsole mit HTML5 schlägt fehl, wenn der Browser für die ausschließliche Verwendung von TLS 1.0 eingestellt ist.

Stellen Sie sicher, dass der Browser für die Verwendung von TLS 1.1 oder höher eingestellt ist.

Virtueller Datenträger

Warum wird die Verbindung mit dem Client für den virtuellen Datenträger manchmal getrennt?

- Wenn eine Netzwerk-Zeitüberschreitung eintritt, trennt die iDRAC-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Datenträger.
- Wenn die virtuelle Konsole deaktiviert ist, kann es zur Trennung der Sitzung des virtuellen Datenträgers kommen. Durch das Deaktivieren der TLS-Zertifikatsperrüberprüfung können Sie das Trennen der Verbindung vermeiden. So deaktivieren Sie die Zertifikatsperrüberprüfung:
  a Starten Sie das **Java-Systemsteuerung**.
  b Klicken Sie auf die Registerkarte **Erweitert**.
  c Machen Sie die Option **Check for TLS certificate revocations check on (TLS-Zertifikatsperrüberprüfung prüfen)** ausfindig und wählen Sie **Do not check (Nicht überprüfen)** aus.
  d Klicken Sie auf **Apply (Anwenden)** und dann auf **OK**. Das Fenster **Java Control Panel (Java-Systemsteuerung)** wird geschlossen.
- Wenn Sie die CD im Clientsystem ändern, verfügt die neue CD eventuell über eine Autostart-Funktion. Wenn dies der Fall ist, kann für die Firmware eine Zeitüberschreitung eintreten und die Verbindung wird unterbrochen, wenn es zu lange dauert, bis das Clientsystem die CD liest. Wenn eine Verbindung verloren geht, können Sie sie über die GUI wieder herstellen und mit dem vorherigen Vorgang fortfahren.
- Wenn die Konfigurationseinstellungen des virtuellen Datenträgers in der iDRAC-Webschnittstelle oder durch Befehle des lokalen RACADM geändert werden, wird die Verbindung aller verbundener Datenträger bei Übernahme der Konfigurationsänderung unterbrochen.
- Verwenden Sie zum erneuten Verbinden des virtuellen Datenträgers das Fenster „Virtueller Datenträger – **Client-Ansicht**“.

Warum dauert eine Windows-Betriebssysteminstallation über einen virtuellen Datenträger länger?

Wenn Sie das Windows-Betriebssystem mithilfe der DVD *Dell Systems Management Tools and Documentation* (Dell Systemverwaltungstools und Dokumentation) und über eine langsame Netzwerkverbindung installieren, kann es sein, dass das Installationsverfahren aufgrund von Netzwerklatenz für den Zugriff auf die iDRAC-Webschnittstelle mehr Zeit erfordert. Das Installationsfenster zeigt den Installationsfortschritt nicht an.

Wie kann das virtuelle Gerät als Startlaufwerk konfiguriert werden?

Greifen Sie auf dem verwalteten System auf das BIOS-Setup zu und wechseln Sie zum Startmenü. Machen Sie die virtuelle CD, die virtuelle Diskette oder vFlash ausfindig und ändern Sie die Gerätestartreihenfolge nach Bedarf. Machen Sie außerdem den virtuellen Datenträger startfähig, indem Sie im CMOS-Setup während der Startsequenz die Leertaste drücken. Um z. B. von einem CD-Laufwerk aus zu starten, konfigurieren Sie das CD-Laufwerk als erstes Laufwerk in der Startreihenfolge.

Welche Datenträgertypen können als Startlaufwerk festgelegt werden?

Mit dem iDRAC können Sie von den folgenden startfähigen Datenträgern aus starten:

- CD-ROM/DVD-Datenträger
- ISO 9660-Image
- 1,44 Zoll-Diskette oder Disketten-Image
- USB-Schlüssel, der vom Betriebssystem als Wechsellaufwerk erkannt wird
- Ein USB-Schlüssel-Image

Wie kann der USB-Schlüssel in ein Startlaufwerk umkonfiguriert werden?

Sie können auch über eine Windows 98-Startdiskette starten und Systemdateien von der Startdiskette auf den USB-Stick kopieren. Geben Sie z. B. an der DOS-Eingabeaufforderung den folgenden Befehl ein:

```
sys a: x: /s
```

wobei „x:“ für den USB-Schlüssel steht, der als Startlaufwerk konfiguriert werden soll.

Der virtuelle Datenträger ist angeschlossen und mit der Remote-Diskette verbunden. Ich kann mein virtuelles Disketten-/CD-Laufwerk auf einem System mit dem Betriebssystem Red Hat Enterprise Linux oder SUSE Linux nicht finden. Wie kann ich dieses Problem lösen?

Bei einigen Linux-Versionen werden virtuelle Diskettenlaufwerke und virtuelle CD-Laufwerke nicht in gleicher Weise automatisch geladen. Um das virtuelle Diskettenlaufwerk zu laden, machen Sie den Geräteknoten ausfindig, den Linux dem virtuellen Diskettenlaufwerk zuweist. Um das virtuelle Diskettenlaufwerk zu laden, gehen Sie folgendermaßen vor:

1 Öffnen Sie eine Linux-Eingabeaufforderung, und führen Sie den folgenden Befehl aus:
```
grep "Virtual Floppy" /var/log/messages
```
2 Machen Sie den letzten Eintrag zu dieser Meldung ausfindig, und notieren Sie die Zeit.
3 Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:
```
grep "hh:mm:ss" /var/log/messages
```
wobei, hh:mm:ss der Zeitstempel der Meldung ist, die von grep in Schritt 1 zurückgegeben wurde.
4 Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls und finden Sie den Gerätenamen, der dem virtuellen Diskettenlaufwerk zugeordnet wurde.
5 Stellen Sie sicher, dass das virtuelle Diskettenlaufwerk angeschlossen ist und eine Verbindung dazu besteht.
6 Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:
```
mount /dev/sdx /mnt/floppy
```
wobei `/dev/sdx` für den in Schritt 4 ermittelten Gerätenamen steht und `/mnt/floppy` der Mount-Punkt ist.

Um das virtuelle CD-Laufwerk zu laden, machen Sie den Geräteknoten ausfindig, den Linux dem virtuellen CD-Laufwerk zuweist. Um das virtuelle CD-Laufwerk zu laden, gehen Sie folgendermaßen vor:

1 Öffnen Sie eine Linux-Eingabeaufforderung, und führen Sie den folgenden Befehl aus:
```
grep "Virtual CD" /var/log/messages
```
2 Machen Sie den letzten Eintrag zu dieser Meldung ausfindig, und notieren Sie die Zeit.
3 Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:
```
grep "hh:mm:ss" /var/log/messages
```
wobei, hh:mm:ss der Zeitstempel der Meldung ist, die von grep in Schritt 1 zurückgegeben wurde.
4 Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls und machen Sie den Gerätenamen ausfindig, der der *virtuellen Dell-CD* zugeordnet wurde.
5 Stellen Sie sicher, dass das virtuelle CD-Laufwerk vorhanden und verbunden ist.
6 Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:
```
mount /dev/sdx /mnt/CD
```
wobei `/dev/sdx` für den in Schritt 4 ermittelten Gerätenamen steht und `/mnt/floppy` der Mount-Punkt ist.

Warum werden die mit dem Server verbundenen virtuellen Laufwerke nach einer Remote-Firmware-Aktualisierung über die iDRAC-Webschnittstelle entfernt?

Firmware-Aktualisierungen führen zu einem Reset des iDRAC, einem Abbruch der Remote-Verbindung sowie zum Entladen der virtuellen Laufwerke. Die Laufwerke werden wieder angezeigt, wenn der iDRAC-Reset-Vorgang abgeschlossen ist.

Warum werden nach dem Anschließen eines USB-Geräts alle USB-Geräte abgetrennt?

Virtuelle Datenträgergeräte und vFlash-Geräte werden als Composite-USB-Gerät am Host-USB-BUS angeschlossen und verwenden einen gemeinsamen USB-Port. Immer wenn ein virtuelles Datenträgergerät oder vFlash-USB-Gerät an den Host-USB-BUS angeschlossen oder davon getrennt wird, werden alle virtuellen Datenträger- und vFlash-Geräte vorübergehend vom Host-USB-Bus getrennt und danach wieder verbunden. Wenn ein virtuelles Datenträgergerät vom Hostbetriebssystem verwendet wird, müssen Sie das Verbinden bzw. Abtrennen eines oder mehrerer virtueller Datenträger- oder vFlash-Geräte vermeiden. Es wird empfohlen, zuerst alle erforderlichen USB-Geräte anzuschließen, bevor Sie sie verwenden.

Welche Funktion hat das USB-Reset?

Sie setzt die Remote- und lokalen USB-Geräte zurück, die an den Server angeschlossen sind.

Wie lässt sich die Leistung des virtuellen Datenträgers maximieren?

Starten Sie zum Maximieren der Leistung des virtuellen Datenträgers den virtuellen Datenträger bei deaktivierter virtueller Konsole, oder führen Sie eine der folgenden Schritte aus:

- Stellen Sie den Schieberegler für die Leistung auf die maximale Geschwindigkeit.
- Deaktivieren Sie die Verschlüsselung sowohl für den virtuellen Datenträger als auch für die virtuelle Konsole.

ANMERKUNG: In diesem Fall wird die Datenübertragung zwischen dem verwalteten Server und iDRAC für den virtuellen Datenträger und für die virtuelle Konsole nicht gesichert.

- Wenn Sie ein Windows Server-Betriebssystem verwenden, halten Sie den Windows-Dienst mit der Bezeichnung Windows Event Collector an. Hierfür gehen Sie auf **Start** > **Verwaltungstools** > **Dienste**. Klicken Sie mit der rechten Maustaste auf **Windows Event Collector** und klicken Sie auf **Stop (Beenden)**.

Während der Betrachtung der Inhalte eines Diskettenlaufwerks oder eines USB-Schlüssels wird ein Verbindungsfehler angezeigt, wenn das gleiche Laufwerk über den virtuellen Datenträger angeschlossen ist. Warum?

Ein gleichzeitiger Zugriff auf virtuelle Diskettenlaufwerke ist nicht erlaubt. Vor dem Versuch, das Laufwerk zu virtualisieren, ist die Anwendung zum Anzeigen des Laufwerkinhalts zu schließen.

Welche Dateisystemtypen werden auf dem virtuellen Diskettenlaufwerk unterstützt?

Ihr virtuelles Diskettenlaufwerk unterstützt FAT16- oder FAT32-Dateisysteme.

Warum wird eine Fehlermeldung angezeigt, wenn man versucht, ein DVD-Laufwerk/einen USB-Schlüssel über einen virtuellen Datenträger zu verbinden, auch wenn der virtuelle Datenträger derzeit nicht verwendet wird?

Diese Fehlermeldung wird angezeigt, wenn zusätzlich eine Remote-Dateifreigabe (Remote File Share, RFS) verwendet wird. Die Funktionen für die RFS und den virtuellen Datenträger können nicht gleichzeitig verwendet werden.

Das Starten des virtuellen Datenträgers mit HTML5 schlägt fehl, wenn der Browser für die ausschließliche Verwendung von TLS 1.0 eingestellt ist.

Stellen Sie sicher, dass der Browser für die Verwendung von TLS 1.1 oder höher eingestellt ist.

vFlash-SD-Karte

Wann ist die vFlash SD-Karte gesperrt?

Die vFlash SD-Karte ist gesperrt, wenn ein Vorgang läuft, z. B. während der Initialisierung eines Vorgangs.

SNMP-Authentifizierung

Warum wird die Meldung „Remote-Zugriff: SNMP-Authentifizierungsfehler“ angezeigt?

Als ein Teil der Ermittlung versucht IT Assistant, die Community-Namen get und set des Geräts zu überprüfen. Im IT Assistant ist der Get-Community-Name = public und der Set-Community-Name = private. Standardmäßig ist der Community-Name für den iDRAC-Agenten public. Wenn IT Assistant eine Set-Anforderung sendet, erstellt der iDRAC-Agent den SNMP-Authentifizierungsfehler, weil er nur Anforderungen von Community = public akzeptiert.

Um zu verhindern, dass SNMP-Authentifizierungsfehler erstellt werden, müssen Sie Community-Namen eingeben, die vom Agenten akzeptiert werden. Da der iDRAC nur einen einzigen Community-Namen zulässt, müssen Sie den gleichen Get- und Set-Community-Namen für das IT Assistant-Ermittlungs-Setup eingeben.

Speichergeräte

Es werden nicht alle Informationen zu allen Speichergeräten angezeigt, die mit dem System verbunden sind, und OpenManage Storage Management zeigt mehr Speichergeräte an, als auf iDRAC vorhanden sind. Warum?

iDRAC zeigt Informationen nur für die von Comprehensive Embedded Management (CEM) unterstützten Geräte an.

iDRAC Service Module

Sollte vor der Installation und dem Ausführen des iDRAC Service Module der Open Manage Server Administrator deinstalliert werden?

Nein, Sie müssen Server Administrator nicht deinstallieren. Stellen Sie vor der Installation oder Ausführung des iDRAC Service Module sicher, dass Sie die Funktionen von Server Administrator, die das iDRAC Service Module bereitstellt, gestoppt haben.

Wie wird überprüft, ob das iDRAC Service Module auf dem System installiert ist?

Um herauszufinden, ob das iDRAC Service Module auf Ihrem System installiert ist, gehen Sie folgendermaßen vor:

- Auf Systemen, die Windows ausführen:
  Öffnen Sie die **Systemsteuerung**, und überprüfen Sie, ob das iDRAC-Service-Modul in der Liste der installierten Programme angezeigt wird.
- Auf Systemen, die Linux ausführen:
  Führen Sie den folgenden Befehl aus: `rpm –qi dcism`. Wenn das iDRAC Service Module installiert ist, wird der Status **Installed (Installiert)** angezeigt.

ANMERKUNG: Um zu überprüfen, ob das iDRAC Service Module unter RedHat Enterprise Linux 7 installiert ist, verwenden Sie den Befehl `systemctl status dcismeng.service` anstelle des Befehls `init.d`.

Wie wird die Versionsnummer des iDRAC Service Module überprüft, die im System installiert ist?

Zum überprüfen der Version des iDRAC Service Module im System führen Sie eine der folgenden Aktionen aus:

- Klicken Sie auf **Start** > **Systemsteuerung** > **Programme und Funktionen**. Die Version des installierten iDRAC Service Module wird auf der Registerkarte **Version** aufgeführt.
- Gehen Sie zu **Arbeitsplatz** > **Programm deinstallieren oder ändern**.

Welche Berechtigungsebene muss ein Benutzer mindestens haben, um das iDRAC Service Module installieren zu können?

Zum Installieren des iDRAC Service Module müssen Sie über Administratorrechte verfügen.

Auf dem iDRAC Service Module 2.0 und früher wird während der Installation des iDRAC Service Module eine Fehlermeldung angezeigt, die besagt, dass es sich um einen nicht unterstützten Server handelt. Weitere Informationen über die unterstützten Server finden Sie im Benutzerhandbuch. Wie kann ich dieses Problem lösen?

Stellen Sie vor der Installation des iDRAC Service Module sicher, dass der Server ein PowerEdge-Server der 12. Generation oder höher ist. Stellen Sie außerdem sicher, dass Sie ein 64-Bit-System haben.

Die folgende Meldung wird in der BS-Protokolldatei angezeigt, selbst wenn das Passthrough vom Betriebssystem zu iDRAC über USBNIC ordnungsgemäß konfiguriert ist. Warum?

Das iDRAC Service Module kann nicht mit iDRAC über den Passthrough-Kanal zwischen Betriebssystem und iDRAC kommunizieren

Das iDRAC Service Module verwendet die Funktion für Passthrough vom Betriebssystem zu iDRAC über die USB-NIC, um die Kommunikation mit iDRAC herzustellen. Gelegentlich kann es vorkommen, dass die Kommunikation nicht hergestellt werden kann, obwohl die USB-NIC-Schnittstelle mit den korrekten IP-Endpunkten konfiguriert ist. Dieser Fall kann eintreten, wenn die Hostbetriebssystem-

Routing-Tabelle mehrere Einträge für dieselbe Zielmaske hat und das USB-NIC-Ziel nicht als das erste Ziel in der Routing-Reihenfolge aufgeführt ist.

Tabelle 49. iDRAC-Service-Modul

Ziel	Gateway	Genmask	Flags	Metrik	Ref.	Iface verwenden
Standardeinstellung	10.94.148.1	0.0.0.0	UG	1024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	B	0	0	0 em1
Link-lokal	0.0.0.0	255.255.255.0	B	0	0	0 em1
Link-lokal	0.0.0.0	255.255.255.0	B	0	0	0 enp0s20u12u3

In diesem Beispiel ist **enp0s20u12u3** die USB-NIC-Schnittstelle. Die Zielmaske „link-local“ wird wiederholt und die USB-NIC ist nicht die erste in der Reihenfolge. Dies führt zu dem Konnektivitätsproblem zwischen dem iDRAC Service Module und iDRAC über das Passthrough vom Betriebssystem zu iDRAC. Um das Konnektivitätsproblem zu beheben, stellen Sie sicher, dass die iDRAC-USBNIC-IPv4-Adresse (die Standardeinstellung lautet 169.254.0.1) über das Hostbetriebssystem erreichbar ist.

Wenn nicht:

- Ändern Sie die iDRAC-USBNIC-Adresse auf einer eindeutigen Ziel-Maske.
- Löschen Sie die Einträge, die Sie nicht benötigen, aus der Routingtabelle, um sicherzustellen, dass die USB-NIC durch die Route ausgewählt wird, wenn der Host die iDRAC-USB-NIC-IPv4-Adresse erreichen möchte.

Beim Deinstallieren eines iDRAC Service Module von einem VMware ESXi-Server auf einem iDRAC Service Module 2.0 wird der virtuelle Switch auf dem vSphere-Client als vSwitchiDRACvusb und die Port-Gruppe als iDRAC-Netzwerk benannt. Wie können sie gelöscht werden?

Während der Installation eines iDRAC Service Module-VIB auf einem VMware ESXi-Server erstellt das iDRAC Service Module den vSwitch und die Portgruppe, um mit iDRAC über den Passthrough zwischen Betriebssystem und iDRAC im USB-NIC-Modus zu kommunizieren. Nach Abschluss der Deinstallation werden der virtuelle Switch **vSwitchiDRACvusb** und die Portgruppe **iDRAC Network (iDRAC-Netzwerk)** nicht gelöscht. Um sie manuell zu löschen, führen Sie einen der folgenden Schritte aus:

- Gehen Sie zum Assistenten für die Konfiguration des vSphere-Clients, und löschen Sie die Einträge.
- Wechseln Sie zur Esxcli, und geben Sie die folgenden Befehle ein:
  - Zum Entfernen der Portgruppe: `esxcfg-vmknic -d -p "iDRAC Network"`
  - Zum Entfernen des vSwitch: `esxcfg-vswitch -d vSwitchiDRACvusb`

ANMERKUNG: Sie können das iDRAC-Service-Modul auf dem VMware ESXi-Server neu installieren, da es sich dabei für den Server nicht um ein funktionsbezogenes Problem handelt.

Wo befindet sich das replizierte Lifecycle-Protokoll im Betriebssystem?

So zeigen Sie die replizierten Lifecycle-Protokolle an:

Tabelle 50. Lifecycle-Protokolle

Betriebssystem	Location (Speicherort)
Microsoft Windows	**Ereignisanzeige** > **Windows-Protokolle** > **System**. Alle iDRAC Service Module Lifecycle-Protokolle werden unter dem Quellnamen des **iDRAC Service Module** repliziert. **ANMERKUNG: In iSM Version 2.1 und höher werden Lifecycle-Protokolle unter dem Quellnamen des Lifecycle Controller-Protokolls repliziert. In iSM-Version 2.0 und früher werden die Protokolle unter dem Quellnamen des iDRAC Service Module repliziert.**

Betriebssystem	Location (Speicherort)
	ANMERKUNG: Der Speicherort des Lifecycle-Protokolls kann über das iDRAC Service Module-Installationsprogramm konfiguriert werden. Sie können während der Installation des iDRAC Service Module oder der Bearbeitung des Installationsprogramms den Speicherort festlegen.
Red Hat Enterprise Linux, SUSE Linux, CentOS und Citrix XenServer	/var/log/messages
VMware ESXi	/var/log/syslog.log

Was sind die abhängigen Linux-Pakete oder ausführbaren Dateien, die während der Vollendung der Linux-Installation verfügbar sind?

Die Liste der abhängigen Linux-Pakete finden Sie im Abschnitt *Linux-Abhängigkeiten* im *iDRAC Service Module Installation Guide (Installationshandbuch zum iDRAC Service Module)*.

RACADM

Wenn nach dem Zurücksetzen eines iDRAC (über den Befehl „racadm racreset“) ein Befehl eingegeben wird, wird die folgende Meldung angezeigt. Wofür steht diese Meldung?

```
ERROR: Unable to connect to RAC at specified IP address
```

Die Meldung gibt an, dass Sie warten müssen, bis der iDRAC-Reset abgeschlossen ist, bevor Sie einen anderen Befehl ausgeben.

Wenn Sie RACADM-Befehle und -Unterbefehle verwenden, werden einige Fehler nicht behoben.

Bei der Verwendung von RACADM-Befehlen können ein oder mehrere der folgenden Fehler auftreten:

- Lokale RACADM-Fehlermeldungen - Probleme wie Syntax, typografische Fehler und falsche Namen.
- Remote RACADM-Fehlermeldungen – Probleme wie falsche IP-Adresse, falscher Benutzername oder falsches Kennwort.

Wenn während eines PING-Tests auf dem iDRAC der Netzwerkmodus von „Dediziert“ in „Freigegeben“ geändert wird, wird keine PING-Antwort generiert.

Löschen Sie die ARP-Tabelle auf dem System.

Remote-RACADM ist nicht in der Lage, eine Verbindung zu iDRAC über SUSE Linux Enterprise Server (SLES) 11 SP1 herzustellen.

Stellen Sie sicher, dass Sie die offiziellen openssl- und libopenssl-Versionen installiert haben. Führen Sie den folgenden Befehl aus, um die RPM-Pakete zu installieren:

```
rpm -ivh --force < filename >
```

Hierbei ist `filename` die openssl- oder libopenssl rpm-Paketdatei.

Beispiel:

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
rpm -ivh --force libopenssl0_9_8-0.9.8h-30.22.21.1.x86_64.rpm
```

Warum sind die Remote-RACADM- und webbasierten Dienste nach einer Eigenschaftsänderung nicht verfügbar?

Es kann eine Weile dauern, bis die Remote-RACADM-Dienste und die webbasierte Schnittstelle nach einem Reset des iDRAC-Web Servers verfügbar sind.

Der iDRAC Web-Server wird zurückgesetzt, wenn:

- Die Netzwerkkonfiguration oder Netzwerk-Sicherheitseigenschaften werden mittels der webbasierten iDRAC-Benutzeroberfläche geändert.
- Die Eigenschaft „iDRAC.Webserver.HttpsPort“ wird geändert; auch dann, wenn eine Änderung durch `racadm set -f <config file>` erfolgt.
- Der Befehl **racresetcfg** wird verwendet.
- iDRAC wurde zurückgesetzt.
- Ein neues SSL-Serverzertifikat wird hochgeladen.

Warum wird eine Fehlermeldung angezeigt, wenn Sie versuchen, eine Partition zu löschen, nachdem Sie sie über den lokalen RACADM erstellt haben?

Dies tritt auf, da der Partitionserstellungsvorgang noch nicht abgeschlossen ist. Die Partition wird jedoch nach einer Weile gelöscht und der Löschvorgang durch eine entsprechende Meldung bestätigt. Falls nicht, warten Sie, bis der Partitionserstellungsvorgang abgeschlossen ist, und löschen Sie die Partition anschließend.

Verschiedenes

Wie kann man eine iDRAC-IP-Adresse für einen Blade-Server ausfindig machen?

- **Mit der CMC-Webschnittstelle**.
  Gehen Sie zu **Chassis (Gehäuse)** > **Servers (Server)** > **Setup** > **Deploy (Bereitstellen)**. In der angezeigten Tabelle wird die IP-Adresse für den Server angezeigt.
- **Über die virtuelle Konsole**: Starten Sie den Server neu, um die iDRAC-IP-Adresse im Rahmen eines POST zu betrachten. Wählen Sie im OSCAR die „Dell CMC“-Konsole aus, um sich über eine lokale serielle Verbindung am CMC anzumelden. CMC-RACADM-Befehle können über diese Verbindung gesendet werden.
  Weitere Informationen zu CMC-RACADM-Befehlen finden Sie im Referenzhandbuch für die CMC-RACADM-Befehlszeilenschnittstelle, das unter **dell.com/cmcmanuals** verfügbar ist.

  Weitere Informationen zu iDRAC-RACADM-Befehlen finden Sie im iDRAC-RACADM-Referenzhandbuch für die Befehlszeilenoberfläche *iDRAC RACADM Command Line Interface Reference Guide*, das unter **dell.com/idracmanuals** verfügbar ist.
- **Unter Verwendung lokaler RACADM**
  Verwenden Sie den Befehl: `racadm getsysinfo` Zum Beispiel:

```
$ racadm getniccfg -m server-1
DHCP Enabled = 1
IP Address   = 192.168.0.1
Subnet Mask  = 255.255.255.0
Gateway      = 192.168.0.1
```

- **LCD verwenden**:
  Markieren Sie im Hauptmenü den Server, klicken Sie auf die Schaltfläche zum Markieren, wählen Sie den gewünschten Server aus und klicken Sie auf die Schaltfläche zum Markieren.

Wie kann man die CMC-IP-Adresse ausfindig machen, die sich auf den Blade-Server bezieht?

- **Von der iDRAC-Webschnittstelle**:
  Gehen Sie zu **Overview (Übersicht)** > **iDRAC Settings (iDRAC-Einstellungen)** > **CMC**. Die Seite **CMC Summary (CMC-Zusammenfassung)** zeigt die CMC-IP-Adresse an.
- **Von der virtuellen Konsole**:

Wählen Sie im OSCAR die „Dell CMC“-Konsole aus, um sich über eine lokale serielle Verbindung am CMC anzumelden. CMC-RACADM-Befehle können über diese Verbindung ausgegeben werden.

```
$ racadm getniccfg -m chassis
NIC Enabled         = 1
DHCP Enabled        = 1
Static IP Address   = 192.168.0.120
Static Subnet Mask  = 255.255.255.0
Static Gateway      = 192.168.0.1
Current IP Address  = 10.35.155.151
Current Subnet Mask = 255.255.255.0
Current Gateway     = 10.35.155.1
Speed               = Autonegotiate
Duplex              = Autonegotiate
```

ANMERKUNG: Sie können diesen Vorgang außerdem über den Remote-RACADM ausführen.

Weitere Informationen zu CMC-RACADM-Befehlen finden Sie im Referenzhandbuch für die CMC-RACADM-Befehlszeilenschnittstelle, das unter **dell.com/cmcmanuals** verfügbar ist.

Weitere Informationen zu iDRAC-RACADM-Befehlen finden Sie im iDRAC-RACADM-Referenzhandbuch für die Befehlszeilenoberfläche *iDRAC RACADM Command Line Interface Reference Guide*, das unter **dell.com/idracmanuals** verfügbar ist.

Wie kann man die iDRAC-IP-Adresse für Rack- und Tower-Server ausfindig machen?

- **Von der iDRAC-Webschnittstelle**:
  Gehen Sie zu **Overview (Übersicht)** > **Server** > **Properties (Eigenschaften)** > **Summary (Zusammenfassung)**. Die Seite **System Summary (Systemzusammenfassung)** zeigt die iDRAC-IP-Adresse an.
- **Von lokalem RACADM**:
  Verwenden Sie den Befehl **racadm getsysinfo**.
- **Über die LCD**:
  Verwenden Sie auf dem physischen Server zum Anzeigen der iDRAC-IP-Adresse die Navigationsschaltflächen auf dem LCD-Display. Gehen Sie zu **Setup View (Setup-Ansicht)** > **View (Anzeigen)** > **iDRAC IP (iDRAC-IP-Adresse)** > **IPv4** oder **IPv6** > **IP (IP-Adresse)**.
- **Vom OpenManage Server Administrator**:
  Wechseln Sie in der Server Administrator-Web-Schnittstelle zu **Modulares Gehäuse** > **System-/Server-Modul** > **Hauptsystemgehäuse/Hauptsystem** > **Remote-Zugriff**.

Die iDRAC-Netzwerkverbindung funktioniert nicht.

Für Blade-Server:

- Stellen Sie sicher, dass das LAN-Kabel am CMC angeschlossen ist.
- Stellen Sie sicher, dass NIC-Einstellungen, IPv4- oder IPv6-Einstellungen und entweder Statisch oder DHCP für das Netzwerk aktiviert sind.

Für Rack- und Tower-Server:

- Stellen Sie im freigegebenen Modus sicher, dass das LAN-Kabel mit der NIC-Schnittstelle verbunden ist, die mit einem Schraubenschlüsselsymbol gekennzeichnet ist.
- Stellen Sie im dedizierten Modus sicher, dass das LAN-Kabel mit der iDRAC-LAN-Schnittstelle verbunden ist.
- Stellen Sie sicher, dass NIC-Einstellungen, IPv4- und IPv6-Einstellungen und entweder „Statisch“ oder „DHCP“ für das Netzwerk aktiviert sind.

Der Blade-Server wurde in das Gehäuse eingesetzt, der EIN-/AUS-Schalter wurde gedrückt, der Server konnte jedoch nicht eingeschaltet werden.

- iDRAC benötigt bis zu 2 Minuten zum Initialisieren, bevor der Server hochgefahren werden kann.
- Überprüfen Sie den Energiehaushalt des CMC. Der Grenzwert für den Energiehaushalt des Gehäuses wurde möglicherweise überschritten.

Wie ruft man einen iDRAC-Administrator-Benutzernamen und das zugehörige Kennwort ab?

Sie müssen die Standardeinstellungen von iDRAC wiederherstellen. Weitere Informationen finden Sie unter Zurücksetzen von iDRAC auf die Standardeinstellungen.

Wie kann man den Namen des Steckplatzes für das System in einem Gehäuse ändern?

1 Melden Sie sich bei der CMC-Web-Schnittstelle an, und gehen Sie zu **Gehäuse** > **Server** > **Setup**.
2 Geben Sie den neuen Namen für den Steckplatz in die Zeile für den Server ein und klicken Sie auf **Anwenden**.

Der iDRAC auf Blade-Server reagiert während des Startvorgangs nicht.

Enfernen Sie den Server und setzen Sie ihn erneut ein.

Überprüfen Sie die CMC-Webschnittstelle, um zu sehen, ob iDRAC als aktualisierbare Komponente angezeigt wird. Ist dies der Fall, folgen Sie den Anweisungen unter Aktualisieren von Firmware über die CMC-Webschnittstelle.

Falls das Problem weiterhin besteht, kontaktieren Sie den technischen Support.

Beim Versuch, den verwalteten Server zu starten, ist die Betriebsanzeige grün, aber es ist kein POST bzw. kein Video vorhanden.

Dies kann eintreten, wenn einer oder mehrere der folgenden Zustände zutreffen:

- Speicher ist nicht installiert oder ist unzugänglich.
- Die CPU ist nicht installiert oder ist unzugänglich.
- Die Video-Riser-Karte fehlt oder ist falsch eingesteckt.

Weitere Informationen finden Sie, wenn Sie über die iDRAC-Webschnittstelle oder die Server-LC-Anzeige die Fehlermeldungen im iDRAC-Protokoll aufrufen.

25

Anwendungsszenarien

In diesem Abschnitt erhalten Sie Erläuterungen zum Navigieren zu bestimmten Abschnitten innerhalb des Handbuchs, um typische Anwendungsszenarien auszuführen.

Themen:

Fehler auf einem Managed System beheben, auf das nicht zugegriffen werden kann

Nach dem Eingang von Warnungen aus OpenManage Essentials, Dell Management Console oder einem lokalen Trap-Kollektor sind fünf Server in einem Rechenzentrum aufgrund von Problemen wie einem nicht mehr reagierenden Betriebssystem oder Server nicht mehr zugänglich. Es ist daher erforderlich, den Grund für diesen Fehler zu ermitteln, um den Fehler zu beheben und den Server über iDRAC zu reaktivieren.

Bevor der Fehler in Bezug auf ein nicht zugreifbares System behoben werden kann, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Bildschirm „Letzter Absturz“ ist aktiviert
- Warnungen auf iDRAC sind aktiviert

Um den Grund für den Fehler zu identifizieren, müssen Sie Folgendes auf der iDRAC-Web-Schnittstelle überprüfen und die Verbindung zum System wiederherstellen:

ANMERKUNG: Wenn Sie nicht auf die iDRAC-Webschnittstelle zugreifen können, gehen Sie zum Server, rufen Sie das LCD-Bedienfeld auf, notieren Sie sich die IP-Adresse oder den Host-Namen, und führen Sie von Ihrer Management-Station aus die folgenden Vorgänge über die iDRAC-Webschnittstelle aus:

- Server-LED-Status – Blinkt gelb oder leuchtet dauerhaft gelb.
- LCD-Bedienfeld auf der Frontblende oder Fehlermeldung – Gelbe LC-Anzeige oder Fehlermeldung.
- Betriebssystem-Image wird in der virtuellen Konsole angezeigt. Wenn das Image angezeigt wird, starten Sie das System über einen Warmstart neu, und melden Sie sich wieder an. Wenn die Anmeldung erfolgreich war, ist der Fehler behoben.

- Bildschirm „Letzter Absturz“
- Capture-Video beim Startvorgang
- Absturzvideo-Capture
- Serverzustand – Rote *x*-Symbole für die Systemkomponenten, bei denen Fehler vorliegen.
- Speicher-Array-Status – Array möglicherweise offline oder ausgefallen
- Lifecycle-Protokoll für kritische Ereignisse in Bezug auf die Hardware und die Firmware auf dem System und die Protokolleinträge, die beim Systemabsturz erfasst wurden.
- Tech Support-Report erstellen und die erfassten Daten anzeigen.
- Verwenden Sie die vom iDRAC Service Module bereitgestellten Überwachungsfunktionen.

Zugehöriger Link

Vorschau der virtuellen Konsole
Videos zum Startvorgang und zur Absturzerfassung anzeigen
Systemzustand anzeigen
Protokolle anzeigen
Generieren der SupportAssist-Erfassung
Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen
Verwenden des iDRAC Service Module

Systeminformationen abrufen und Systemzustand bewerten

So rufen Sie Systeminformationen ab und bewerten den Systemzustand:

- Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Systemzusammenfassung**, um die Systeminformationen anzuzeigen und um auf bestimmte Links auf dieser Seite zuzugreifen, um den Systemstatus zu bewerten. Sie können beispielsweise den Zustand des Gehäuselüfters überprüfen.
- Sie können außerdem die Gehäuseortungs-LED konfigurieren und auf der Basis der Farbe den Systemzustand bewerten.
- Wenn das iDRAC Service Module installiert ist, werden die Host-Informationen zum Betriebssystem angezeigt.

Zugehöriger Link

Systemzustand anzeigen
Verwenden des iDRAC Service Module
Generieren der SupportAssist-Erfassung

Einrichten von Warnungen und Konfigurieren von E-Mail-Warnungen

So richten Sie Warnungen ein und konfigurieren E-Mail-Warnungen:

1 Aktivieren Sie Warnungen.
2 Konfigurieren Sie die E-Mail-Warnung und markieren Sie die Schnittstellen.
3 Führen Sie einen Neustart aus, schalten Sie das Gerät aus, oder führen Sie einen Aus- und Einschaltvorgang auf dem Managed System durch.
4 Senden Sie die Testwarnung.

Lifecycle-Protokoll und Systemereignisprotokoll anzeigen und exportieren

So zeigen Sie das Lifecycle-Protokoll und das Systemereignisprotokoll (SEL) an und exportieren diese:

1 Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Protokolle**, um das SEL anzuzeigen. Gehen Sie zu **Übersicht** > **Server** > **Protokolle** > **Lifecycle-Protokoll**, um das Lifecycle-Protokoll anzuzeigen.

ANMERKUNG: Das SEL wird außerdem im Lifecycle-Protokoll angezeigt. Über die Filteroptionen können Sie das SEL anzeigen.

2 Exportieren Sie das SEL oder das Lifecycle-Protokoll im XML-Format an einen externen Speicherort (Management Station, USB-Schlüssel, Netzwerkfreigabe, usw.). Alternativ können Sie die Remote-System-Protokollierung aktivieren, so dass alle Protokolle, die in das Lifecycle-Protokoll geschrieben werden, gleichzeitig auch auf die konfigurierten Remote-Server geschrieben werden.

3 Wenn Sie das iDRAC-Servicemodul verwenden, exportieren Sie das Lifecycle-Protokoll in das Betriebssystemprotokoll. Weitere Informationen finden Sie unter Verwenden des iDRAC Service Module.

Schnittstellen zum Aktualisieren der iDRAC-Firmware

Verwenden Sie zum Aktualisieren der iDRAC-Firmware die folgenden Schnittstellen:

- iDRAC-Web-Schnittstelle
- RACADM-Befehlszeilenschnittstelle (iDRAC und CMC)
- Dell Update Package (DUP)
- CMC-Webschnittstelle
- Lifecycle-Controller–Remote-Dienste
- Lifecycle-Controller
- Dell Remote Access Configuration Tool (DRACT)

Ordnungsgemäßes Herunterfahren durchführen

Um ein ordnungsgemäßes Herunterfahren durchzuführen, gehen Sie in der iDRAC-Webschnittstelle zu einem der folgenden Standorte:

- **Übersicht** > **Server** > **Stromversorgung/Thermisch** > **Stromversorgungskonfiguration** > **Stromsteuerung**. Daraufhin wird die Seite **Stromsteuerung** angezeigt. Wählen Sie **Ordnungsgemäßes Herunterfahren** aus, und klicken Sie auf **Anwenden**.
- **Übersicht** > **Server** > **Stromversorgung/Thermisch** > **Stromversorgungsüberwachung**. Wählen Sie aus dem Dropddown-Menü **Stromsteuerung** die Option **Ordnungsgemäßes Herunterfahren** aus, und klicken Sie dann auf **Anwenden**.

ANMERKUNG: Alle Power-Optionen hängen vom Host-Betriebssystem ab. Damit die Optionen richtig funktionieren, müssen Sie erforderliche Änderungen am Betriebssystem vornehmen. Zum Beispiel Gnom-Optimierung-Tool in RHEL 7.2.

Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Neues Administratorbenutzerkonto erstellen

Sie können das standardmäßige lokale Administratorbenutzerkonto ändern oder ein neues Administratorbenutzerkonto erstellen. Weitere Informationen zum Ändern des lokalen Administratorbenutzerkontos finden Sie unter Lokale Administratorkontoeinstellungen ändern.

Weitere Informationen zum Erstellen eines neuen Administratorkontos finden Sie in den folgenden Abschnitten:

- Lokale Benutzer konfigurieren
- Konfigurieren von Active Directory-Benutzern
- Generische LDAP-Benutzer konfigurieren

Starten der Server-Remote-Konsole und Mounten eines USB-Laufwerks

So starten Sie die Remote-Konsole und mounten ein USB-Laufwerk:

1 Schließen Sie ein USB-Flash-Laufwerk (mit dem erforderlichen Image) an die Management Station an.

2 Starten Sie die virtuelle Konsole über eine der folgenden Möglichkeiten über die iDRAC-Webschnittstelle:

- Gehen Sie auf **Übersicht** > **Server** > **Virtuelle Konsole**, und klicken Sie auf **Virtuelle Konsole starten**.
- Gehen Sie zu **Übersicht** > **Server** > **Eigenschaften**, und klicken Sie auf die Option **Starten**, die sich unter **Virtuelle Konsole – Vorschau** befindet.

Daraufhin wird der **Viewer für die virtuelle Konsole** angezeigt.

3 Klicken Sie über das Menü **File (Datei)** auf **Virtual Media (Virtueller Datenträger)** > **Launch Virtual Media (Virtuellen Datenträger starten)**.

4 Klicken Sie auf **Image hinzufügen**, und wählen Sie das Image aus, das sich auf dem USB-Flash-Laufwerk befindet.

Das Image wird zur Liste der verfügbaren Laufwerke hinzugefügt.

5 Wählen Sie das Laufwerk aus, das zugeordnet werden soll. Das Image auf dem USB-Flash-Laufwerk wird dem verwalteten System zugeordnet.

Bare Metal-Betriebssystem über verbundenen virtuellen Datenträger und Remote-Dateifreigabe installieren

Weitere Informationen zu diesem Schritt finden Sie unter Betriebssystem über eine Remote-Dateifreigabe bereitstellen.

Rack-Dichte verwalten

Derzeit sind die beiden Server in einem Rack installiert. Um zwei weitere Server hinzuzufügen, müssen Sie bestimmen, wie viel Kapazität im Rack noch verfügbar ist.

So bewerten Sie die Kapazität eines Rack in Bezug auf das Hinzufügen weiterer Server:

1 Zeigen Sie die aktuellen und historischen Stromverbrauchsdaten für die Server an.

2 Aktivieren Sie auf der Basis dieser Daten, der Stromversorgungsinfrastruktur und der Kühlungsbeschränkungen für das System die Strombegrenzungsrichtlinie, und legen Sie die Strombegrenzungswerte fest.

> **ANMERKUNG: Es wird empfohlen, die Begrenzung nahe des zulässigen Höchstwertes festzulegen und über diese begrenzte Stufe dann die verbliebene Kapazität auf dem Rack für das Hinzufügen weiterer Server zu bestimmen.**

Neue elektronische Lizenz installieren

Weitere Informationen finden Sie unter Lizenzvorgänge.

Anwenden der E/A-Identitätskonfigurationseinstellungen für mehrere Netzwerkkarten bei einem Neustart eines einzelnen Hostsystems

Wenn Sie in einem Server, der Teil einer Storage Area Network (SAN)-Umgebung ist, über mehrere Netzwerkkarten verfügen und Sie andere virtuelle Adressen sowie Initiator- und Zielkonfigurationseinstellungen auf diese Karten anwenden möchten, verwenden Sie die Funktion zur E/A-Identitätsoptimierung, um den Zeitaufwand für die Konfiguration dieser Einstellungen zu reduzieren. Führen Sie dazu folgende Schritte durch:

1 Stellen Sie sicher, dass BIOS, iDRAC und Netzwerk-Karten auf die neueste Firmware aktualisiert sind.
2 Aktivieren Sie die E/A-Identitätsoptimierung.
3 Exportieren Sie die XML-Konfigurationsdatei von iDRAC.
4 Bearbeiten Sie die E/A-Identitätsoptimierungseinstellungen in der XML-Datei.
5 Importieren Sie die XML-Konfigurationsdatei nach iDRAC.

Zugehöriger Link

Aktualisieren der Gerätefirmware
Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung