Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade Server Version 3.5

Benutzerhandbuch

Anmerkungen und Vorsichtshinweise

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

VORSICHTSHINWEIS: Durch VORSICHTSHINWEISE werden Sie auf potenzielle Gefahrenquellen hingewiesen, die Hardwareschäden oder Datenverlust zur Folge haben könnten, wenn die Anweisungen nicht befolgt werden.

2013 - 03

Inhalt

1

iDRAC6 Enterprise - Übersicht

Der Integrated Dell Remote Access Controller (iDRAC6) Enterprise ist eine Systemverwaltungshardware- und -softwarelösung, die Remote-Verwaltungsfähigkeiten, Wiederherstellung für abgestürzte Systeme sowie Stromsteuerungsfunktionen für Dell PowerEdge-Systeme enthält.

Der iDRAC6 verwendet einen integrierten System-on-Chip-Mikroprozessor für das Remote-Monitor/Steuersystem und befindet sich ebenso wie der PowerEdge-Managed Server auf der Systemplatine. Das Betriebssystem des Servers führt Anwendungsprogramme aus; der iDRAC6 überwacht und verwaltet die Serverumgebung und den Serverzustand außerhalb des Betriebssystems.

Der iDRAC6 kann so konfiguriert werden, dass er bei Warnungen oder Fehlern eine E-Mail oder eine Trap-Warnung des Netzwerk-Verwaltungsprotokolls (SNMP) sendet. Um Ihnen bei der Ursachendiagnose eines Systemabsturzes behilflich zu sein, kann der iDRAC6 Ereignisdaten protokollieren und einen Screenshot erstellen, wenn er einen Systemabsturz feststellt.

Managed Server werden in einem Dell M1000e-Systemgehäuse mit modularen Netzteilen, Kühlungslüftern und einem Gehäuseverwaltungscontroller (CMC) installiert. Der CMC überwacht und verwaltet alle im Gehäuse installierten Komponenten. Fügen Sie einen redundanten CMC hinzu, um bei einem Ausfall des primären CMCs ein Hot-Failover sicherzustellen. Das Gehäuse bietet über seine LCD-Anzeige, Verbindungen der lokalen Konsole sowie seine Webschnittstelle Zugriff auf die iDRAC6-Komponenten. Jedes Blade in einem Gehäuse hat einen iDRAC6. In einem M1000e-Gehäuse können Sie bis zu 16 Blades installieren.

Alle Netzwerkverbindungen zum iDRAC6 laufen über die CMC-Netzwerkschnittstellen (CMC RJ45-Verbindungsanschluss mit der Bezeichnung „GB1“). Der CMC leitet den Datenverkehr über ein privates, internes Netzwerk zu den iDRAC6-Geräten. Dieses private Verwaltungsnetzwerk befindet sich außerhalb des Serverdatenpfads und untersteht nicht der Steuerung des Betriebssystems, d. h. es ist *bandextern*. Die *bandinternen* Netzwerkschnittstellen des verwalteten Servers sind über im Gehäuse installierte E/A-Module (IOMs) zugänglich.

ANMERKUNG: Es wird empfohlen, das Gehäuseverwaltungsnetzwerk, das vom iDRAC6 und vom CMC verwendet wird, von den Produktionsnetzwerken zu isolieren oder abzutrennen. Das Vermischen von Verwaltungs- und Produktions- oder Anwendungs-Netzwerkdatenverkehr kann zu Überlastungen oder Netzwerksättigung führen, woraus sich CMC- und iDRAC6-Kommunikationsverzögerungen ergeben. Diese Verzögerungen können unvorhersehbares Gehäuseverhalten hervorrufen, z. B. CMC-Anzeigen, die besagen, dass der iDRAC6 offline ist, obwohl er ordnungsgemäß funktioniert. Das kann zu weiteren unvorhersehbaren Funktionsweisen führen.

Die iDRAC6-Netzwerkschnittstelle ist standardmäßig deaktiviert. Konfigurieren Sie die iDRAC6-Netzwerkschnittstelle, bevor der iDRAC6 verfügbar gemacht wird. Nachdem der iDRAC6 auf dem Netzwerk aktiviert und konfiguriert wurde, können Sie durch seine zugewiesene IP-Adresse über die iDRAC6-Webschnittstelle, Telnet oder SSH sowie über unterstützte Netzwerkverwaltungsprotokolle, wie die intelligente Plattform-Verwaltungsschnittstelle (IPMI), auf ihn zugreifen.

Was ist neu an dieser Version?

- Unterstützung für DIMM-Konfigurationen und PCI-Karten (siehe Versionshinweise für Details.)
- Unterstützung für Internet Explorer 10 Browser.
- Quell-E-Mail-Konfiguration über RACADM.
- Unterstützung für AMD Abu Dhabi CPU für M915, M910.

IPv6-Ready-Logo-Zertifizierung

Die Mission des IPv6-Ready-Logo-Gremiums besteht darin, die Testspezifikationen für die IPv6-Konformität und Interoperabilitätstestverfahren zu definieren, um Zugriff auf Selbsttest-Hilfsprogramme zu bieten und das IPv6-Ready-Logo zu liefern.

Der iDRAC6 ist zertifiziert für das **Phase-2-IPv6-Ready-Logo** und die Logo-ID lautet **02-C-000380**. Informationen zum IPv6-Ready-Logo-Programm finden Sie unter **URL ipv6ready.org/**.

iDRAC6-Sicherheitsfunktionen

Die folgenden iDRAC-Sicherheitsfunktionen sind verfügbar:

- Benutzerauthentifizierung über Microsoft Active Directory, generischen LDAP-Verzeichnisdienst oder lokal verwaltete Benutzer-IDs und Kennwörter
- Zweifaktor-Authentifizierung, die durch die Smart Card-Anmeldungsfunktion bereitgestellt wird. Die Zweifaktor-Authentifizierung basiert auf dem *Haben* (die Smart Card), und auf dem *Wissen* (die PIN) des Benutzers.
- Rollenbasierte Berechtigung, die einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren
- Benutzer-ID- und Kennwortkonfiguration
- SM-CLP- und Webschnittstellen, die 128-Bit- und 40-Bit-Verschlüsselung unterstützen (für Länder, in denen 128-Bit nicht zulässig ist) und den SSL 3.0-Standard verwenden
- Konfiguration der Sitzungszeitüberschreitung (in Sekunden)
- Konfigurierbare IP-Schnittstellen (wo anwendbar)
- Secure Shell (SSH), die eine verschlüsselte Übertragungsschicht für höhere Sicherheit verwendet
- Beschränkung der Anmeldefehlschläge pro IP-Adresse, mit Anmeldeblockierung der IP-Adresse bei Überschreitung des Grenzwerts
- Konfigurierbarer Client-IP-Adressenbereich für Clients, die an den iDRAC6 angeschlossen werden

iDRAC6 Enterprise und VFlash-Datenträger

iDRAC6 Enterprise verfügt über Schlitze für SD-Karten für vFlash-Medien. Weitere Informationen zu iDRAC6 Enterprise- und vFlash-Medien finden Sie im *Hardware-Benutzerhandbuch* unter **ell.com/support/manuals**.

Tabelle 1-1 listet die Funktionen auf, die für iDRAC6 Enterprise und vFlash-Medien verfügbar sind.

Tabelle 1-1. iDRAC6-Funktionsliste

Funktion	iDRAC6 Enterprise	iDRAC6 Enterprise mit vFlash-Medien
Schnittstellen- und Standardunterstützung		
IPMI 2.0	✓	✓
Internet-GUI	✓	✓
SNMP	✓	✓
WS–MAN	✓	✓
SM-CLP	✓	✓
RACADM-Befehlszeile	✓	✓
Konnektivität		
Netzwerkmodi Freigegeben/Failover	✓	✓
IPv4	✓	✓
VLAN-Tagging	✓	✓
IPv6	✓	✓
Dynamisches DNS	✓	✓
Dedizierte NIC	✓	✓
Sicherheit und Authentifizierung		
Rollenbasierte Berechtigung	✓	✓

Tabelle 1-1. iDRAC6-Funktionsliste *(fortgesetzt)*

Funktion	iDRAC6 Enterprise	iDRAC6 Enterprise mit vFlash-Medien
Local Users (Lokale Benutzer)	✓	✓
Active Directory	✓	✓
Zweifaktor-Authentifizierung	✓	✓
Einmalanmeldung	✓	✓
SSL-Verschlüsselung	✓	✓
Remote-Verwaltung und Störungsbeseitigung		
Remote-Firmware-Aktualisierung	✓	✓
Serverstromregelung	✓	✓
Seriell-über-LAN (mit Proxy)	✓	✓
Seriell-über-LAN (ohne Proxy)	✓	✓
Power Capping (Strombegrenzung)	✓	✓
Erfassung des Bildschirms „Letzter Absturz“	✓	✓
Start-Capture	✓	✓
Virtueller Datenträger	✓	✓
Remote-Dateifreigabe	✓	✓
Virtuelle Konsole	✓	✓
Gemeinsame Nutzung der virtuellen Konsole	✓	✓
vFlash	✗	✓
Überwachung		
Sensorüberwachung und Warnmeldungen	✓	✓
Echtzeit-Stromüberwachung	✓	✓

Tabelle 1-1. iDRAC6-Funktionsliste *(fortgesetzt)*

Funktion	iDRAC6 Enterprise	iDRAC6 Enterprise mit vFlash-Medien
Echtzeit-Stromdiagramme	✓	✓
Historische Stromzähler	✓	✓
Systembestand	✓	✓
Protokollierung		
Systemereignisprotokoll (SEL)	✓	✓
RAC-Protokoll	✓	✓
Ablaufverfolgungsprotokoll	✓	✓
Remote-Syslog	✓	✓
Arbeitsnotizen	✓	✓

✓ = Unterstützt; ✗ = Nicht unterstützt

Unterstützte Plattformen

Die neuesten unterstützten Plattformen finden Sie in der iDRAC6-Infodatei und in der *Dell Systems Software Support-Matrix* unter **dell.com/support/manuals**.

Unterstützte Betriebssysteme

Die neuesten Informationen finden Sie in der iDRAC6-Infodatei und in der *Dell Systems Software Support-Matrix* unter **dell.com/support/manuals**.

Unterstützte Webbrowser

Die neuesten Informationen finden Sie in der Infodatei und in der *Dell Systems Software Support-Matrix* unter **dell.com/support/manuals**.

ANMERKUNG: Aufgrund von Sicherheitslücken wird SSL 2.0 nicht mehr unterstützt. Stellen Sie sicher, dass der Browser zum Aktivieren von SSL 3.0 konfiguriert ist.

Unterstützte Remote-Zugriffsverbindungen

Tabelle 1-2 führt die Verbindungsfunktionen auf.

Tabelle 1-2. Unterstützte Remote-Zugriffsverbindungen

Verbindung	Funktionen
iDRAC6-NIC	• 10 Mbit/s/100 Mbit/s/1 Gbit/s Ethernet über CMC Gbit-Ethernet-Anschluss. • DHCP-Unterstützung. • SNMP-Traps und E-Mail-Ereignisbenachrichtigung. • SM-CLP-Shell und RACADM-Befehle für Vorgänge wie die DRAC6-Konfiguration, Systemstart, Zurücksetzen, Einschalten und Herunterfahren werden über SSH und Telnet unterstützt. • Unterstützung für IPMI-Dienstprogramme wie IPMItool und ipmish.

iDRAC6-Anschlüsse

Tabelle 1-3 führt die Anschlüsse auf, die iDRAC6 nach Verbindungen abhört. Tabelle 1-4 kennzeichnet die Anschlüsse, die der iDRAC6 als Client verwendet. Diese Informationen sind erforderlich, wenn Firewalls für den Remote-Zugriff auf einen iDRAC6 geöffnet werden.

VORSICHTSHINWEIS: iDRAC6 prüft nicht auf Konflikte, die zwischen konfigurierbaren Anschlüssen entstehen können. Überprüfen Sie bei der Einstellung der Anschlusskonfigurationen, dass die Anschlusszuweisungen keine Konflikte verursachen.

Tabelle 1-3. iDRAC6-Server-Abhöranschlüsse

Port Number (Schnittstellennummer)	Funktion
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
3668, 3669	Virtueller Datenträger-Dienst
3670, 3671	Virtueller Datenträger - Sicherer Dienst
5900*	Tastatur/Maus der virtuellen Konsole
5901*	Video über die virtuelle Konsole
5988	Verwendet für WSMAN

* Konfigurierbare Schnittstelle

Tabelle 1-4. iDRAC6-Client-Anschlüsse

Port Number (Schnittstellennummer)	Funktion
25	SMTP
53	DNS
68	DHCP-zugewiesene IP-Adresse
69	TFTP
162	SNMP-Trap
636	LDAPS
3269	LDAPS für globalen Katalog (GC)

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 des iDRAC6 auf dem System.

- Die iDRAC6-Onlinehilfe enthält Informationen zur Verwendung der Webschnittstelle.
- Das *Dell Chassis Management Controller-Benutzerhandbuch* enthält Informationen zur Verwendung des Controllers, der alle Module in dem Gehäuse verwaltet, das den Dell PowerEdge-Server enthält.
- Das *Dell Lifecycle Controller-Benutzerhandbuch* enthält Informationen zu Unified Server Configurator (USC), Unified Server Configurator – Lifecycle Controller Enabled (USC – LCE) und Remote-Diensten.
- Die Dokumente *iDRAC6-CIM-Elementzuweisung* und *iDRAC6 SM-CLP-Eigenschaften-Datenbank*, die im Dell Enterprise Technology Center unter **www.delltechcenter.com** zur Verfügung stehen, enthalten Informationen zur iDRAC6-SM–CLP-Eigenschaften-Datenbank, Zuweisung zwischen WS-MAN-Klassen und SM-CLP-Zielen sowie Details zur Dell Implementierung.
- Das *Dell RACADM-Befehlszeilen-Referenzhandbuch für i*DRAC6 und CMC enthält Informationen zu den RACADM-Unterbefehlen, den unterstützten RACADM-Schnittstellen und Eigenschaftstabellengruppen und Objektdefinitionen für iDRAC6 Enterprise auf Blade-Servern, iDRAC6 Enterprise oder Express auf Rack- und Tower-Servern und zum CMC.
- Die *Dell Systems Software Support-Matrix* bietet Informationen über die verschiedenen Dell Systeme, die durch diese Systemen unterstützten Betriebssysteme und die Dell OpenManage-Komponenten, die auf diesen Systemen installiert werden können.
- Das *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.

- Das *Benutzerhandbuch zur Dell-Verwaltungskonsole* enthält Informationen zur Verwendung der Dell-Verwaltungskonsole.
- Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen über die Installation und Verwendung von Server Administrator.
- Das *Benutzerhandbuch zu Dell Update Packages* enthält Informationen zum Abrufen und Verwenden von Dell Update Packages als Teil der Systemaktualisierungsstrategie.
- Das *Glossar* enthält Informationen zu den in diesem Dokument verwendeten Begriffen.

Die folgenden Systemdokumente sind außerdem erhältlich, um weitere Informationen über das System zur Verfügung zu stellen, auf dem Ihr iDRAC6 installiert ist:

- 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 **www.dell.com/regulatory_compliance**. Garantiebestimmungen können als separates Dokument beigelegt sein.
- Das *Getting Started Guide* (Handbuch zum Einstieg) enthält eine Übersicht über die Systemfunktionen, die Einrichtung des Systems und technische Daten.
- Im *Hardware-Benutzerhandbuch* finden Sie Informationen über Systemfunktionen, Fehlerbehebung im System und zum Installieren oder Austauschen von Systemkomponenten.
- In der Dokumentation zur Systemverwaltungssoftware sind die Merkmale, die Anforderungen, die Installation und die grundlegende Funktion der Software beschrieben.
- In der Dokumentation zum Betriebssystem ist beschrieben, wie das Betriebssystem installiert (sofern erforderlich), konfiguriert und verwendet wird.
- Die Dokumentation für alle separat erworbenen Komponenten enthält Informationen zur Konfiguration und zur Installation dieser Optionen.
- Möglicherweise sind auch Aktualisierungen beigelegt, in denen Änderungen am System, an der Software und/oder an der Dokumentation beschrieben sind.

ANMERKUNG: Lesen Sie diese Aktualisierungen immer zuerst, da sie frühere Informationen gegebenenfalls außer Kraft setzen.

- Im Lieferumfang befindliche Versionsinformationen oder Readme-Dateien geben Auskunft über den letzten Stand der Änderungen am System oder an der Dokumentation oder enthalten fortgeschrittenes technisches Referenzmaterial für erfahrene Benutzer oder IT-Profis.

Zugriff auf Dokumente über Dell Support-Website

So greifen Sie auf die Dokumente von Dell Support-Website zu:

1. Rufen Sie die Website **dell.com/support/manuals** auf.
2. Im Abschnitt **Erzählen Sie uns über Ihr Dell-System** unter **No**, wählen Sie **Aus allen Dell-Produkten auswählen** und klicken Sie auf **Fortfahren**.
3. Klicken Sie im Abschnitt **Produkttyp auswählen** auf **Software**, **Monitore**, **Elektronik und Peripheriegeräte**.
4. Klicken Sie im Abschnitt **Dell Software**, **Monitore**, **Elektronik und Peripheriegeräte auswählen** auf **Software**.
5. Klicken Sie im Abschnitt **Ihre Dell Software auswählen** auf den erforderlichen Link aus dem Fogendem:

- Client System Management
- Enterprise System Management
- Remote Enterprise System Management
- Serviceability Tools

6. Um das Dokument anzuzeigen, klicken Sie auf die erforderliche Produktversion.

Sie können auf die Dokumente mithilfe der folgenden Links zugreifen:

- Für Client System Management-Dokumente — **dell.com/OMConnectionsClient**
- Für Enterprise System Management-Dokumente — **dell.com/openmanagemanuals**
- Für Remote Enterprise System Management-Dokumente — **dell.com/openmanagemanuals**
- Für Serviceability Tools-Dokumente — **dell.com/serviceabilitytools**

2

iDRAC6 Enterprise

Dieser Abschnitt enthält Informationen zum Einrichten des Zugriffs auf iDRAC6 und zur Konfiguration der Verwaltungsumgebung zur Verwendung von iDRAC6.

Bevor Sie beginnen

Legen Sie vor der Konfiguration von iDRAC6 folgende Artikel zurecht:

- *Benutzerhandbuch zur Dell Chassis Management Controller-Firmware*
- DVD *Dell Systems Management Tools and Documentation*

Die DVD *Dell Systems Management Tools and Documentation* enthält die folgenden Komponenten:

- DVD root — Enthält das Dell Systems Build and Update-Dienstprogramm, das Informationen zur Server-Einrichtung und Systeminstallation bereitstellt
- SYSMGMT — Enthält die Systemmanagement-Softwareprodukte einschließlich des Dell OpenManage Server Administrator

Weitere Informationen finden Sie im *Dell OpenManage Server Administrator-Installationshandbuch* und im *Dell OpenManage Management Station Software-Installationshandbuch* auf der Dell Support-Website unter **dell.com/support/manuals**.

Schnittstellen zum Konfigurieren von iDRAC6

Sie können iDRAC6 mit dem iDRAC6- Konfigurationsdienstprogramm, der iDRAC6-Webschnittstelle, der Webschnittstelle des Chassis Management Controller (CMC), dem LCD-Bedienfeld, der lokalen und Remote-RACADM-CLI, iVMCLI oder SM-CLP-CLI konfigurieren. Die lokale RACADM-CLI steht nach der Installation des Betriebssystems und der Dell PowerEdge-Server Management-Software auf dem verwalteten Server zur Verfügung. Tabelle 2-1 beschreibt diese Schnittstellen.

Zur Sicherstellung von mehr Sicherheit sollten Sie über das iDRAC6-Konfigurationshilfsprogramm auf die iDRAC6-Konfiguration zugreifen oder die lokale RACADM CLI über einen Befehl deaktivieren (siehe *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das unter **dell.com/support/manuals**) oder über die GUI (siehe „Lokalen Konfigurationszugriff aktivieren oder deaktivieren“ auf Seite 127 verfügbar ist).

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

Tabelle 2-1. Konfigurationsschnittstellen

Schnittstelle	Beschreibung
iDRAC6-Konfiguration Dienstprogramm	Erfolgt der Zugriff auf das iDRAC6-Konfigurationsdienstprogramm zum Zeitpunkt des Starts, ist es beim Installieren eines neuen Dell PowerEdge-Servers nützlich. Verwenden Sie es zum Einrichten des Netzwerks und grundlegender Sicherheitsfunktionen sowie zum Aktivieren anderer Funktionen.
iDRAC6-Webschnittstelle	Die iDRAC6-Webschnittstelle ist eine browserbasierte Verwaltungsanwendung, die Sie zur interaktiven Verwaltung von iDRAC6 und zur Überwachung des verwalteten Servers verwenden können. Sie stellt die primäre Schnittstelle für alltägliche Aufgaben wie die Überwachung des Systemzustands, die Anzeige des Systemereignisprotokolls, die Verwaltung lokaler iDRAC6-Benutzer und das Starten der CMC-Webschnittstelle und der Virtuelle Konsole-Sitzungen dar.
CMC-Webschnittstelle	Zusätzlich zum Überwachen und Verwalten des Gehäuses können Sie über die CMC-Webschnittstelle den Status eines verwalteten Servers anzeigen, die iDRAC6-Firmware aktualisieren, iDRAC6-Netzwerkeinstellungen konfigurieren, sich an der iDRAC6-Webschnittstelle anmelden sowie den verwalteten Server starten, anhalten oder zurücksetzen.

Tabelle 2-1. Konfigurationsschnittstellen *(fortgesetzt)*

Schnittstelle	Beschreibung
Gehäuse-LCD-Bedienfeld	Über das LCD-Bedienfeld des Gehäuses, welches iDRAC6 enthält, können Sie den High-Level-Status der Server im Gehäuse anzeigen. Während der ursprünglichen Konfiguration des CMC ermöglicht der Konfigurationsassistent, die DHCP-Konfiguration des iDRAC6-Netzwerkbetriebs zu aktivieren.
Lokales und Remote-RACADM	Die Befehlszeilenschnittstelle des lokalen RACADM wird auf dem lokalen Server ausgeführt. Remote-RACADM ist ein Client-Dienstprogramm, das auf einer Management Station ausgeführt wird. Es verwendet die bandexterne Netzwerkschnittstelle, um auf dem verwalteten Server RACADM-Befehle auszuführen. Mit der Option **–r** wird der RACADM-Befehl über ein Netzwerk ausgeführt. RACADM-Befehle bieten Zugriff auf fast alle Funktionen von iDRAC6. Sie können Sensordaten, Protokolleinträge bei Systemereignissen sowie die in iDRAC6 geführten aktuellen Status- und Konfigurationswerte kontrollieren. Sie können iDRAC6-Konfigurationswerte verändern, lokale Benutzer verwalten, Funktionen aktivieren und deaktivieren sowie Stromfunktionen wie das Herunterfahren oder Neustarten des verwalteten Servers ausführen.
iVMCLI	Die iDRAC6-Befehlszeilenschnittstelle des virtuellen Datenträgers (iVMCLI) bietet dem verwalteten Server Zugriff auf Datenträger der Management Station. Sie ist hilfreich beim Entwickeln von Skripts zum Installieren von Betriebssystemen auf mehreren verwalteten Servern.

Tabelle 2-1. Konfigurationsschnittstellen *(fortgesetzt)*

Schnittstelle	Beschreibung
SM-CLP	SM-CLP ist die Implementierung des in iDRAC6 umgesetzten Serververwaltungs-/Workgroup-Serververwaltungs-Befehlszeilenprotokolls. Sie können auf die SM-CLP-Befehlszeile zugreifen, indem Sie sich über Telnet oder SSH am iDRAC6 anmelden und bei der CLI-Eingabeaufforderung `smclp` eingeben. SM-CLP-Befehle setzen einen nützlichen 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.
IPMI	IPMI definiert einen Standard für integrierte Verwaltungssubsysteme wie das iDRAC6, um mit anderen integrierten Systemen und Verwaltungsanwendungen zu kommunizieren. Sie können die iDRAC6-Webschnittstellen-, SM-CLP- oder RACADM-Befehle zum Konfigurieren von IPMI-Plattformereignisfiltern (PEF) und Plattformereignis-Traps (PET) verwenden. PEF bewirken, dass iDRAC6 bestimmte Maßnahmen ausführt (z. B. den Neustart des verwalteten Servers), wenn er einen entsprechenden Zustand feststellt. PET weisen iDRAC6 an, E-Mail- oder IPMI-Warnungen zu senden, wenn bestimmte Ereignisse oder Zustände festgestellt werden. Sie können auch standardmäßige IPMI-Hilfsprogramme wie **IPMItool** und **ipmish** bei iDRAC6 verwenden, wenn Sie IPMI-über-LAN aktivieren.

Konfigurations-Tasks

Dieser Abschnitt stellt eine Übersicht der Konfigurations-Tasks für die Management Station, iDRAC6 und den verwalteten Server dar. Zu den verfügbaren Aufgaben gehören die Konfiguration von iDRAC6 für den Remote-Zugriff, die Konfiguration der gewünschten iDRAC6-Funktionen, die Installation des Betriebssystems auf dem verwalteten Server und die Installation der Verwaltungssoftware in der Management Station und auf dem verwalteten Server.

Die erforderlichen Konfigurationsschritte zum Durchführen der einzelnen Aufgaben sind jeweils neben der Aufgabe aufgeführt.

ANMERKUNG: Installieren Sie vor dem Durchführen der Konfigurationsschritte in diesem Handbuch das CMC- und das E/A-Modul, und bauen Sie den Dell PowerEdge-Server physisch im Gehäuse ein.

Management Station konfigurieren

Richten Sie eine Management Station ein, indem Sie die Dell OpenManage-Software, einen Webbrowser sowie andere Softwaredienstprogramme installieren. Siehe „Konfiguration der Management Station“ auf Seite 69.

iDRAC6-Netzwerkbetrieb konfigurieren

iDRAC6-Netzwerk aktivieren und IP-, Netzmasken-, Gateway- sowie DNS-Adressen konfigurieren.

ANMERKUNG: Greifen Sie über das iDRAC6-Konfigurationshilfsprogramm auf die iDRAC6-Konfiguration zu oder deaktivieren Sie die lokale RACADM CLI über einen Befehl (siehe *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC,* das unter **dell.com/support/manuals**) oder über die GUI (siehe „Lokalen Konfigurationszugriff aktivieren oder deaktivieren“ auf Seite 127 verfügbar ist).

ANMERKUNG: Durch eine Änderung der iDRAC6-Netzwerkeinstellungen werden alle aktuellen Netzwerkverbindungen zum iDRAC6 abgebrochen.

ANMERKUNG: Die Option zum Konfigurieren des Servers über das LCD-Bedienfeld ist *nur* während der ursprünglichen CMC-Konfiguration verfügbar. Nach der Bereitstellung des Gehäuses können Sie über das LCD-Bedienfeld keine iDRAC6-Neukonfiguration mehr vornehmen.

ANMERKUNG: Verwenden Sie das LCD-Bedienfeld nur für die Aktivierung von DHCP im Rahmen der iDRAC6-Netzwerkkonfiguration.

- LCD-Bedienfeld des Gehäuses – Siehe *Benutzerhandbuch zur Dell Chassis Management Controller-Firmware*.
- iDRAC6-Konfigurationsdienstprogramm - Siehe „iDRAC6-Konfigurationshilfsprogramm verwenden“ auf Seite 369.
- CMC-Webschnittstelle – Siehe „Konfigurieren von Netzwerkeinstellungen mit der CMC-Webschnittstelle“ auf Seite 41.
- Remote- und lokales RACADM – Siehe **cfg LanNetworking** im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC* unter **dell.com/support/manuals**.

iDRAC6-Benutzer konfigurieren

Benutzer und Berechtigungen für das lokale iDRAC6 einrichten. iDRAC6 führt eine Tabelle mit sechzehn lokalen Benutzern in der Firmware. Sie können für diese Benutzer Benutzernamen, Kennwörter und Rollen einrichten.

- iDRAC6-Konfigurationsdienstprogramm (konfiguriert nur den Benutzer auf Administratorebene) – Siehe „LAN-Benutzerkonfiguration“ auf Seite 379.
- iDRAC6-Webschnittstelle – Siehe „iDRAC6-Benutzer hinzufügen und konfigurieren“ auf Seite 104.
- Remote- und lokales RACADM – Siehe „iDRAC6-Benutzer hinzufügen“ auf Seite 301.

ANMERKUNG: Wenn Sie iDRAC6 in einer Active Directory-/generischen LDAP-Verzeichnisdienstumgebung benutzen, stellen Sie sicher, dass Ihre Benutzernamen den aktuellen Namenskonventionen für Active Directory bzw. für den generischen LDAP-Verzeichnisdienst entsprechen.

Verzeichnisdienste konfigurieren

Zusätzlich zu den lokalen iDRAC6-Benutzern können Sie Microsoft Active Directory oder den allgemeinen LDAP-Verzeichnisdienst verwenden, um iDRAC6-Benutzeranmeldungen zu authentifizieren.

Weitere Informationen finden Sie unter„Verwendung des iDRAC6-Verzeichnisdiensts“ auf Seite 135.

IP-Filterung und IP-Blockierung konfigurieren

Zusätzlich zur Benutzerauthentifizierung können Sie unbefugte Zugriffe verhindern, indem Sie Verbindungsversuche von IP-Adressen, die sich außerhalb eines definierten Bereichs befinden, zurückweisen, und indem Sie Verbindungen von IP-Adressen blockieren, bei denen die Authentifizierung mehrere Male innerhalb einer konfigurierbaren Zeitspanne fehlgeschlagen ist.

- iDRAC6-Webschnittstelle – Siehe „IP-Filterung und IP-Blockierung konfigurieren“ auf Seite 97.
- RACADM – Siehe „IP-Filterung konfigurieren (IP-Bereich)“ auf Seite 311 und „IP-Blockierung konfigurieren“ auf Seite 314.

Plattformereignisse konfigurieren

Plattformereignisse treten auf, wenn iDRAC6 einen von einem der Sensoren des verwalteten Servers angezeigten Warnungs- oder kritischen Zustand feststellt.

Konfigurieren Sie Plattformereignisfilter (PEF) zum Auswählen der Aktionen, die Sie beim Feststellen eines Ereignisses ausführen möchten, z. B. einen Systemneustart.

- iDRAC6-Webschnittstelle – Siehe „Plattformereignisfilter (PEF) konfigurieren“ auf Seite 100.
- RACADM – Siehe „PEF konfigurieren“ auf Seite 309.

Konfigurieren Sie Plattformereignis-Traps (PET) zum Senden von Warnungsbenachrichtigungen an eine IP-Adresse, wie z. B. eine Management Station mit Verwaltungssoftware, oder zum Senden einer E-Mail an eine festgelegte E-Mail-Adresse.

- iDRAC6-Webschnittstelle – Siehe „Plattformereignis-Traps (PET) konfigurieren“ auf Seite 100.
- RACADM – Siehe „PET konfigurieren“ auf Seite 309.

Lokalen Konfigurationszugriff aktivieren oder deaktivieren

Sie können den Zugriff auf kritische Konfigurationsparameter, wie z. B. Netzwerkkonfiguration und Benutzerberechtigungen, deaktivieren. Sobald er deaktiviert ist, bleibt die Einstellung beim Neustart beständig. Konfigurationsschreibzugriff wird sowohl für das lokale RACADM-Programm als auch für das iDRAC6-Konfigurationsdienstprogramm (beim Start) blockiert. Internetzugriff auf Konfigurationsparameter wird nicht behindert und Konfigurationsdaten stehen immer zur Ansicht zur Verfügung.

Informationen über die iDRAC6-Webschnittstelle finden Sie unter „Lokalen Konfigurationszugriff aktivieren oder deaktivieren“ auf Seite 127. Informationen zu RACADM-Befehlen finden Sie unter **cfgRacTuning** im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das unter **dell.com/support/manuals** verfügbar ist.

iDRAC6-Dienste konfigurieren

Aktivieren oder deaktivieren Sie die iDRAC6-Netzwerkdienste, wie z. B. Telnet, SSH und die Web Server-Schnittstelle, und konfigurieren Sie Schnittstellen und andere Dienstparameter neu.

- iDRAC6-Webschnittstelle – Siehe „iDRAC6-Dienste konfigurieren“ auf Seite 127
- RACADM – Siehe „iDRAC6-Telnet- und SSH-Dienste mittels lokalem RACADM konfigurieren“ auf Seite 316

SSL konfigurieren

SSL für den iDRAC6-Web Server konfigurieren.

- iDRAC6-Webschnittstelle – Siehe „Secure Sockets Layer (SSL)“ auf Seite 113
- RACADM – Siehe cfgRacSecurity, sslcsrgen, sslcertupload, sslcertdownload und sslcertview im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Virtuelle Datenträger konfigurieren

Konfigurieren Sie die Funktion des virtuellen Datenträgers, sodass Sie das Betriebssystem auf dem Dell PowerEdge-Server installieren können. 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.

- iDRAC6-Webschnittstelle – Siehe „Virtuellen Datenträger konfigurieren und verwenden“ auf Seite 281
- iDRAC6-Konfigurationshilfsprogramm - siehe „Konfiguration virtueller Laufwerke“ auf Seite 376

Konfigurieren einer vFlash-Medienkarte

Installieren und Konfigurieren einer vFlash-Medienkarte zur Verwendung bei iDRAC6.

- iDRAC6-Webschnittstelle und Verwendung von RACADM — Siehe „Konfiguration der vFlash-SD-Karte und Verwalten der vFlash-Partitionen“ auf Seite 259

Managed Server-Software installieren

Installieren Sie das Betriebssystem unter Verwendung des virtuellen Datenträgers auf dem Dell PowerEdge-Server, installieren Sie dann die Dell OpenManage-Software auf dem PowerEdge Managed Server und richten Sie die Funktion des Bildschirms Letzter Absturz ein.

- Virtuelle Konsole — Siehe „Softwareinstallation auf dem verwalteten Server“ auf Seite 85
- iVMCLI — Siehe „Befehlszeilendienstprogramm des virtuellen Datenträgers verwenden“ auf Seite 361

Verwalteten Server für die Funktion Bildschirm Letzter Absturz konfigurieren

Richten Sie den verwalteten Server so ein, dass iDRAC6 nach dem Absturz oder Einfrieren eines Betriebssystems einen Screenshot erstellen kann.

- Verwalteter Server — Siehe „Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz“ auf Seite 86 und „Die Windows-Option „Automatischer Neustart“ deaktivieren“ auf Seite 87

Konfigurieren von Netzwerkeinstellungen mit der CMC-Webschnittstelle

ANMERKUNG: Sie müssen Administratorberechtigungen für die Gehäusekonfiguration (Chassis Configuration Administrator) besitzen, um iDRAC6-Netzwerkeinstellungen über den CMC vornehmen zu können.

ANMERKUNG: Der Standardbenutzername für den CMC ist **root**, das Standardkennwort ist **calvin**.

Starten der iDRAC6-Webschnittstelle vom CMC aus

Der CMC bietet eine eingeschränkte Verwaltung individueller Gehäusekomponenten, wie z. B. Server. Zur vollständigen Verwaltung dieser individuellen Komponenten bietet der CMC eine Start-URL für die iDRAC6-Webschnittstelle des Servers.

Zum Starten von iDRAC6 aus CMC:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie **Serverübersicht** in der Systemstruktur. Der Bildschirm **Serverstatus** zeigt die Liste verfügbarer Server an.
3. Klicken Sie auf **iDRAC** für den Server, den Sie verwalten wollen. Die iDRAC GUI wird in einem neuen Browserfenster gestartet.

Starten der iDRAC6-Webschnittstelle für einen einzelnen Server aus CMC:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Erweitern Sie in der Systemstruktur **Server-Übersicht**. Es werden alle Server in der erweiterten Liste der **Server** angezeigt.
3. Klicken Sie auf den Server, den Sie anzeigen möchten. Der Bildschirm **Serverstatus** für den ausgewählten Server wird angezeigt.
4. Klicken Sie auf **iDRAC6-GUI starten**.

Einfache Anmeldung

Mit der Funktion Einzelanmeldung (SSO) können Sie die iDRAC6-Webschnittstelle vom CMC aus starten, ohne sich ein zweites Mal anmelden zu müssen. Die Richtlinien der einfachen Anmeldung werden nachfolgend beschrieben.

- Ein CMC-Benutzer, für den unter **Benutzerberechtigungen** die Option **Serveradministrator** aktiviert ist, wird automatisch mit der Einzelanmeldung bei der iDRAC6-Webschnittstelle angemeldet. Nach der Anmeldung erhält der Benutzer automatisch iDRAC6-Administratorberechtigungen. Dies gilt sogar dann, wenn derselbe Benutzer kein Konto auf iDRAC6 besitzt oder wenn das Konto nicht über Administratorberechtigungen verfügt.

- Ein CMC-Benutzer, für den unter **Benutzerberechtigungen** nicht **Serveradministrator** eingestellt ist, der jedoch dasselbe Konto auf iDRAC6 besitzt, wird automatisch mit der Einzelanmeldung bei iDRAC6 angemeldet. Sobald der Benutzer bei der iDRAC6-Webschnittstelle angemeldet ist, erhält er die Benutzerberechtigungen, die für das iDRAC6-Konto erstellt wurden.

  ANMERKUNG: *„Dasselbe Konto"* bedeutet in diesem Zusammenhang, dass der Benutzer denselben Benutzernamen und dasselbe Kennwort für CMC und für iDRAC6 benutzt. Ein Benutzer, der denselben Benutzernamen, aber ein anderes Kennwort verwendet, wird nicht als zulässiger Benutzer erkannt.

- Ein CMC-Benutzer, für den unter **Benutzerberechtigungen** nicht **Serveradministrator** eingestellt ist und der nicht dasselbe Konto auf iDRAC6 besitzt, wird *nicht* automatisch mit der Einzelanmeldung bei iDRAC6 angemeldet. Dieser Benutzer wird zum iDRAC6-Anmeldungsbildschirm umgeleitet, nachdem er auf **iDRAC6-GUI starten** geklickt hat.

  ANMERKUNG: Wenn iDRAC6-Netzwerk-LAN deaktiviert ist (LAN aktiviert = Nein), ist die Einzelanmeldung nicht verfügbar.

  ANMERKUNG: Wenn der Server vom Gehäuse entfernt wird, die iDRAC6-IP-Adresse geändert wird oder die iDRAC6-Netzwerkverbindung ein Problem aufweist, kann durch Klicken auf das Symbol **iDRAC6-GUI starten** ein Fehlerbildschirm angezeigt werden.

Konfigurieren des Netzwerks für iDRAC6

1. Klicken Sie auf **System→ iDRAC-Einstellungen→ Register Netzwerk/Sicherheit**.
2. Aktivieren oder Deaktivieren von Seriell über LAN:
   a. Klicken Sie auf **Seriell über LAN**.

      Der Bildschirm **Seriell über LAN** wird angezeigt.

   b. Klicken Sie auf das Kontrollkästchen **Seriell über LAN aktivieren**. Außerdem können Sie die Einstellungen **Baudrate** und **Beschränkung der Kanalzugriffsstufe** ändern.

   c. Klicken Sie auf **Anwenden**.
3. Aktivieren oder Deaktivieren von IPMI über LAN:
   a. Klicken Sie auf **Network** (Netzwerk).

      Der Bildschirm **Netzwerk** wird angezeigt.

b Klicken Sie auf **IPMI-Einstellungen**.

c Markieren Sie das Kontrollkästchen **IPMI über LAN aktivieren**. Außerdem können Sie die Einstellungen **Beschränkung der Kanalzugriffsstufe** und **Verschlüsselungsschlüssel** ändern.

d Klicken Sie auf **Anwenden**.

4 Aktivieren oder Deaktivieren von DHCP:

a Klicken Sie auf **Network** (Netzwerk).

Der Bildschirm **Netzwerk** wird angezeigt.

b Markieren Sie im Abschnitt **IPv4-Einstellungen** die Kontrollkästchen **DHCP aktivieren** und **DHCP zum Abrufen von DNS-Serveradressen verwenden**.

c Markieren Sie im Abschnitt **IPv6-Einstellungen** die Kontrollkästchen **AutoConfiguration aktivieren** und **DHCPv6 zum Abrufen von DNS-Serveradressen verwenden**.

d Klicken Sie auf **Anwenden**.

ANMERKUNG: Wenn Sie DHCP nicht aktivieren möchten, müssen Sie die statische IP-Adresse, die Netzmaske und den Standard-Gateway für den Server eingeben.

Verbindungen der FlexAddress-Mezzanine-Kartenarchitektur anzeigen

M1000e enthält FlexAddress, ein erweitertes, mehrstufiges Mehrfachstandard-Netzwerksystem. FlexAddress ermöglicht die Verwendung von beständigen, dem Gehäuse zugewiesenen World-Wide-Namen und MAC-Adressen (WWN/MAC) für jede verwaltete Server-Anschlussverbindung.

ANMERKUNG: Um Fehler zu vermeiden, die zu einer Stromunterversorgung auf dem verwalteten Server führen können, *muss* der richtige Mezzanine-Kartentyp für jede Anschluss- und Architekturverbindung installiert sein.

Die Konfiguration der Funktion FlexAddress wird mithilfe der CMC-Webschnittstelle ausgeführt. Weitere Informationen zur FlexAddress-Funktion und deren Konfiguration finden Sie im *Benutzerhandbuch zu Dell Chassis Management Controller* sowie im Dokument *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification*.

Nachdem Sie die FlexAddress-Funktion aktiviert und für das Gehäuse konfiguriert haben, klicken Sie auf **System**→ Registerkarte **Eigenschaften**→ **WWN/MAC**, damit eine Liste der installierten Mezzanine-Karten, der Strukturen, mit denen sie verbunden sind, des Strukturtyps und der Server- oder Gehäuse-zugewiesenen MAC-Adressen für jede installierte integrierte Ethernet- und optionale Mezzanine-Kartenschnittstelle angezeigt wird.

Die Spalte **Server-zugewiesen** zeigt die vom Server zugewiesenen WWN/MAC-Adressen an, die in der Hardware des Controllers integriert sind. WWN/MAC-Adressen, die „**-**“ anzeigen, weisen darauf hin, dass keine Schnittstelle für die angegebene Struktur installiert ist.

Die Spalte **Gehäuse-zugewiesen** zeigt die vom Gehäuse zugewiesenen WWN/MAC-Adressen an, die für den speziellen Steckplatz verwendet werden. WWN/MAC-Adressen, die „**-**“anzeigen, weisen darauf hin, dass die FlexAddress-Funktion nicht installiert ist.

In der Spalte **Remote zugewiesen** wird die vom Benutzer über WSMAN zugewiesene WWN/MAC-Adresse angezeigt. Diese wird jedoch nur angezeigt, wenn die FlexAddress deaktiviert und die Remote-Verwaltung aktiviert ist. Weitere Informationen finden Sie im *Benutzerhandbuch für Dell Life Cycle Controller* und in der Dokumentation *iDRAC6-CIM-Elementzuweisung*.

Durch ein Häkchen in den Spalten **Server–zugewiesen**, **Gehäuse–zugewiesen** und **Remote zugewiesen** werden die aktiven Adressen angezeigt.

Wenn die Gehäuse-FlexAddress aktiviert ist, wird auf der iDRAC GUI die CMC-zugewiesene MAC-Adresse und nicht die remote zugewiesene MAC-Adresse angezeigt. Die Server-zugewiesene MAC-Adresse wird zwar angezeigt, ist aber nicht aktiv.

Sind die remote zugewiesenen MAC-Adressen aktiv, wird die MAC-Adresse auf der CMC-Webschnittstellenseite für einen bestimmten Steckplatz im Gehäuse als remote verwaltet angezeigt.

Die remote zugewiesenen Adressen werden nur auf der bandexternen iDRAC Out-Of-Band (OOB)-GUI angezeigt und nicht auf anderen Schnittstellen, wie RACADM und IPMI-Hilfsprogrammen.

FlexAddress-MAC für iDRAC6

Die FlexAddress-Funktion ersetzt die Server-zugewiesenen MAC-Adressen durch Gehäuse-zugewiesene MAC-Adressen und wird für den iDRAC6 zusammen mit Blade-LOMs, Mezzanine-Karten und E/A-Modulen eingesetzt. Die iDRAC6-FlexAddress-Funktion unterstützt die Erhaltung steckplatzspezifischer MAC-Adressen für iDRAC6s in einem Gehäuse. Die Gehäuse-zugewiesene MAC-Adresse wird im permanenten CMC-Speicher abgelegt und bei einem iDRAC6-Start oder einer Änderung der CMC-FlexAddress-Seiteneinstellungen an den iDRAC6 gesendet.

Wenn der CMC eine Gehäuse-zugewiesene MAC-Adresse aktiviert, zeigt der iDRAC6 den Wert im Feld **MAC-Adresse** auf den folgenden Bildschirmen an:

- **System**→ Register **Eigenschaften**→ **Systemdetails**→ **iDRAC6-Informationen**
- **System**→ Register **Eigenschaften**→ **WWN/MAC**
- **System**→ **iDRAC-Einstellungen**→ **Register Eigenschaften** → **Remote-Zugriffsinformationen**→ **Netzwerkeinstellungen**
- **System**→ **iDRAC-Einstellungen**→ **Register Netzwerk/Sicherheit** → **Netzwerk**→ **Einstellungen der Netzwerkschnittstellenkarte**

VORSICHTSHINWEIS: Wenn Sie bei aktivierter FlexAddress zwischen Server-zugewiesener MAC-Adresse und Gehäuse-zugewiesener MAC-Adresse umschalten oder umgekehrt, ändert sich auch die iDRAC6-IP-Adresse.

ANMERKUNG: Sie können die iDRAC6-FlexAddress-Funktion nur über den CMC aktivieren oder deaktivieren. Die iDRAC6-GUI meldet lediglich den Status. Etwaige laufende Sitzungen mit virtueller Konsole oder mit virtuellen Medien werden beendet, wenn die Einstellung der FlexAddress auf der CMC-FlexAddress-Seite geändert wird.

FlexAddress durch RACADM aktivieren

Sie können FlexAddress nicht über den iDRAC6 aktivieren. Aktivieren Sie FlexAddress auf einem Steckplatz und auf Strukturebene über CMC.

1 Aktivieren Sie FlexAddress für den Managed Server am Steckplatz über die CMC-Konsole mit dem folgenden RACADM-Befehl:

`racadm setflexaddr -i <slot_no> 1`, wobei *<slot_no>* die Nummer des Steckplatzes ist, auf dem FlexAddress aktiviert werden soll.

2 Aktivieren Sie dann über die CMC-Konsole FlexAddress auf Strukturebene, indem Sie folgenden RACADM-Befehl ausführen:

`racadm setflexaddr -f <fabric_name> 1`, wobei `<fabric_name>` A, B oder C ist.

3 Um FlexAddress für alle iDRAC6s im Gehäuse zu aktivieren, führen Sie über die CMC-Konsole den folgenden RACADM-Befehl aus:

```
racadm setflexaddr -f idrac 1
```

Weitere Informationen zu CMC RACADM-Unterbefehlen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*.

Remote-Syslog

Mit der iDRAC6-Funktion Remote-Syslog können Sie das RAC-Protokoll und das Systemereignisprotokoll (SEL) im Remote-Zugriff auf einen externen syslog-Server schreiben. Sie können sämtliche Protokolle der gesamten Serverfarm von einem zentralen Protokoll aus lesen.

Für das Remote-Syslog-Protokoll ist keine Benutzerauthentifizierung erforderlich. Zur Eingabe von Protokollen im Remote-Syslog-Server, ist sicherzustellen, dass zwischen dem iDRAC6 und dem Remote-Syslog-Server eine ordnungsgemäße Netzwerkkonnektivität besteht, und dass der Remote-Syslog-Server auf demselben Netzwerk ausgeführt wird wie iDRAC6. Bei den Remote-Syslog-Einträgen handelt es sich um UDP-Pakete, die zum syslog-Anschluss des Remote-Syslog-Servers gesendet werden. Treten Netzwerkausfälle auf, sendet der iDRAC6 dasselbe Protokoll nicht erneut. Die Remote-Protokollierung erfolgt in Echtzeit während und wenn die Protokolle im RAC-Protokoll und SEL-Protokoll von iDRAC6 eingetragen werden. Sie können die Einstellungen von iDRAC6-Remote-Syslog auch über den CMC ändern.

So aktivieren Sie Remote-Syslog über die Remote-Webschnittstelle:

1 Öffnen Sie einen unterstützten Webbrowser.

2 Melden Sie sich an der iDRAC6-Webschnittstelle an.

3 Wählen Sie in der Systemstruktur **System**→ Register **Setup**→ **Remote-Syslog-Einstellungen** aus. Der Bildschirm **Remote-Syslog-Einstellungen** wird angezeigt.

Tabelle 2-2 führt die Remote-Syslog-Einstellungen auf.

Tabelle 2-2. Remote-Syslog-Einstellungen

Attribut	Beschreibung
Remote-Syslog aktiviert	Wählen Sie diese Option aus, um die Übertragung und Remote-Erfassung des syslog auf dem festgelegten Server zu aktivieren. Sobald das syslog aktiviert ist, werden neue Protokolleinträge zum Syslog-Server bzw. zu den Syslog-Servern gesendet.
Syslog-Server 1–3	Geben Sie die Adresse des Remote-Syslog-Servers ein, um iDRAC6-Meldungen wie SEL-Protokoll und RAC-Protokoll zu protokollieren. In Syslog-Serveradressen sind alphanumerische Zeichen, -, ., : und _ zulässig.
Port Number (Schnittstellennummer)	Geben Sie die Schnittstellennummer des Remote-Syslog-Servers ein. Geben Sie einen Wert zwischen 1 und 65535 ein. Die Standardeinstellung lautet 514.

ANMERKUNG: Die vom Remote-Syslog-Protokoll definierten Schweregrade unterscheiden sich von den standardmäßigen IPMI-SEL-Schweregraden (Systemereignisprotokoll). Sämtliche iDRAC6-Remote-Syslog-Einträge werden daher im Syslog-Server mit dem Schweregrad **Hinweis** gemeldet.

Das folgende Beispiel zeigt die Konfigurationsobjekte und die Verwendung des RACADM-Befehls zum Ändern der Remote-syslog-Einstellungen:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogEnable [1/0] ; Standardeinstellung
ist 0

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer1 <Servername1> ;
Standardeinstellung ist leer

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer2 <Servername2>;
Standardeinstellung ist leer

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer3 <Servername3>;
Standardeinstellung ist leer

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogPort <Schnittstellennummer>;
Standardeinstellung ist 514
```

Erstes Startlaufwerk

Diese Funktion ermöglicht Ihnen, das erste Startlaufwerk für das System auszuwählen und Einmaliger Start zu aktivieren. Das System startet vom ausgewählten Gerät beim nächsten und darauffolgenden Neustart und verbleibt als erstes Startlaufwerk in der BIOS-Startreihenfolge, bis es erneut entweder über die iDRAC6-GUI oder über die BIOS-Startsequenz geändert wird. Bei Auswahl von „Einmal starten“ startet das System nur einmalig vom ausgewählten Gerät. Danach startet das System gemäß der BIOS-Startreihenfolge.

So wählen Sie das erste Startgerät über die Remote-Webschnittstelle aus:

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der iDRAC6-Webschnittstelle an.
3. Wählen Sie in der Systemstruktur **System**→ Register **Setup** → **Erstes Startlaufwerk** aus. Der Bildschirm **Erstes Startlaufwerk** wird angezeigt.

Tabelle 2-3 führt die Einstellungen für **Erstes Startlaufwerk** auf.

Tabelle 2-3. Erstes Startlaufwerk

Attribut	Beschreibung
Erstes Startlaufwerk	Wählen Sie das erste Startlaufwerk aus der Dropdown-Liste aus. Das System startet beim nächsten Neustart und bei darauffolgenden Neustarts vom ausgewählten Laufwerk.
Einmaliger Start	Ausgewählt = Aktiviert; Markierung aufgehoben = Deaktiviert. Wählen Sie diese Option aus, um beim nächsten Start vom ausgewählten Laufwerk aus zu starten. Im Anschluss daran wird das System vom ersten Startlaufwerk in der BIOS-Startreihenfolge starten.

Remote-Dateifreigabe

Die iDRAC6-Funktion Remote-Dateifreigabe (Remote File Share; RFS) ermöglicht, eine CD/DVD-ISO-Imagedatei festzulegen, die sich auf einer Netzwerkfreigabe befindet, und sie dem Betriebssystem des verwalteten Servers als virtuelles Laufwerk zur Verfügung zu stellen, indem sie mithilfe von NFS oder CIFS als CD oder DVD geladen wird.

ANMERKUNG: Diese Funktion lässt sich nur bei IPv4-Adressen anwenden. IPv6-Adressen werden derzeit nicht unterstützt.

ANMERKUNG: Bei Linux-Distributionen kann diese Funktion einen Befehl zum manuellen Bereitstellen erfordern, wenn es mit runlevel init 3 betrieben wird. Die Syntax für den Befehl lautet:
`mount /dev/OS_specific_device /<benutzerdefinierter Bereitstellungspunkt>`
wobei `<benutzerdefinierter Bereitstellungspunkt>` jedes Verzeichnis ist, das Sie für das Bereitstellen auswählen, ähnlich wie für jeden Bereitstellen-Befehl.
Für RHEL ist das CD-Gerät (virtuelles Gerät **.iso**) **/dev/scd0** und das Floppy-Gerät (virtuelles Gerät **.img**) **/dev/sdc**.
Für SLES ist das CD-Gerät **/dev/sr0** und das Floppy-Gerät **/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`
Hierbei wird der das Gerät identifizierende Text angezeigt (z. B. SCSI-Gerät sdc). Dieses Verfahren gilt auch für virtuelle Medien, wenn Sie Linux-Distributionen in runlevel init 3 verwenden. Standardmäßig werden die virtuellen Medien nicht automatisch in init 3 bereitgestellt.

Das Format des Pfads des freigegebenen CIFS-Image lautet:

```
//<IP-Adresse oder Domänenname>/<Freigabename>/
<Pfad zum Image>
```

Das Format des Pfads des freigegebenen NFS-Image lautet:

```
<IP-Adresse>:/<Pfad zum Image>
```

Wenn ein Benutzername einen Domänennamen enthält, muss der Benutzername im Format *<user name>@<domain>* eingegeben werden. So ist beispielweise **user1@dell.com** ein zulässiger Benutzername, **dell\user1** dagegen nicht.

Ein Dateiname mit der Erweiterung IMG wird als virtuelles Disketten-, ein Dateiname mit der Erweiterung ISO als virtuelles CDROM-Laufwerk umgeleitet. Die Remote-Dateifreigabe unterstützt nur die Imagedateiformate .IMG und .ISO.

Die RFS-Funktion verwendet die zugrunde liegende Implementierung virtueller Datenträger im iDRAC6. Sie müssen über Virtuelle Datenträger-Berechtigungen verfügen, um RFS-Mounting durchführen zu können. Wenn bereits ein virtuelles Laufwerk von Virtueller Datenträger benutzt wird, ist dieses Laufwerk nicht für RFS-Mounting verfügbar und umgekehrt. Um RFS einsetzen zu können, müssen sich Virtuelle Datenträger im iDRAC6 im Modus *Anschließen* oder *Automatisch anschließen* befinden.

Der Verbindungsstatus für RFS ist im iDRAC6-Protokoll verfügbar. Nach einer Verbindung eines per RFS geladenen Laufwerks wird diese Verbindung selbst dann nicht getrennt, wenn Sie sich vom iDRAC6 abmelden. Die RFS-Verbindung wird beendet, wenn der iDRAC6 zurückgesetzt wird oder die Verbindung zum Netzwerk abbricht. GUI- und Befehlszeilenoptionen zum Schließen einer RFS-Verbindung sind für CMC und iDRAC6 ebenfalls verfügbar. Die RFS-Verbindung des CMC hebt immer ein bestehendes RFS-Mounting des iDRAC6 auf.

ANMERKUNG: Zwischen der iDRAC6 vFlash-Funktion und RFS besteht kein Zusammenhang.

Um die Remote-Dateifreigabe über die iDRAC6-Webschnittstelle zu aktivieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der iDRAC6-Webschnittstelle an.
3. Wählen Sie **System**→ Register **Remote-Dateifreigabe** aus.

   Der Bildschirm **Remote-Dateifreigabe** wird angezeigt.

Tabelle 2-4 führt die Einstellungen der Remote-Dateifreigabe auf.

Tabelle 2-4. Einstellungen des Remote-Dateiservers

Attribut	Beschreibung
Benutzername	Benutzername zur Verbindung für NFS/CIFS-Dateisystem.
Kennwort	Kennwort zur Verbindung für NFS/CIFS-Dateisystem.
Image-Dateipfad	Der durch die Remote-Dateifreigabe freigegebene Dateipfad.
Status	**Verbunden**: Die Datei ist freigegeben. **Nicht verbunden**: Die Datei ist nicht freigegeben. **Wird verbunden...**: Verbindung zur Freigabe wird hergestellt

4 Klicken Sie auf **Verbinden** , um eine Dateifreigabeverbindung herzustellen. Die Schaltfläche **Verbinden** wird nach dem erfolgreichen Herstellen einer Verbindung deaktiviert.

ANMERKUNG: Auch wenn Sie die Remote-Dateifreigabe konfiguriert haben, zeigt die GUI die Benutzeranmeldedaten aus Sicherheitsgründen nicht an.

Für Remote-Dateifreigaben lautet der Remote-RACADM-Befehl

`racadm remoteimage`.

`racadm remoteimage <Optionen>`

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` <Imagespeicherort>; Imagespeicherort auf der Netzwerkfreigabe; doppelte Anführungszeichen um Speicherort setzen

`-s` ; aktuellen Status anzeigen

VORSICHTSHINWEIS: Alle Zeichen einschließlich alphanumerischer Zeichen und Sonderzeichen sind als Teil des Benutzernamens, des Kennworts und des Imagespeicherorts zulässig, außer den folgenden Zeichen: ' (Apostroph), " (Anführungszeichen), , (Komma), < (kleiner als) und > (größer als). Bei Verwendung der Remote-Dateifreigabe sind die oben aufgeführten Zeichen als Teil eines Benutzernamens, eines Kennworts oder eines Imagespeicherorts nicht zulässig.

Internes zweifaches SD-Modul

Das interne duale SD-Modul (IDSDM) ist nur auf geeigneten Plattformen verfügbar. Das IDSDM liefert Redundanz auf der Hypervisor-SD-Karte, indem es eine andere SD-Karte verwendet, die den Inhalt der ersten SD-Karte spiegelt. Die iDRAC6 vFlash SD-Karte kann zusammen mit der zweiten SD-Karte auf IDSDM gestellt werden, indem die **Redundanzoption** im Bildschirm **Integrierte Geräte** des BIOS-Setup des Systems auf **Mirror mode** gestellt wird. Wenn die IDSDM-Funktion aktiviert ist, dann ist die vFlash-Funktionalität der iDRAC6 vFlash-SD-Karte nicht verfügbar, und diese Karte wird im IDSDM als sekundäre SD-Karte gesetzt. Weitere Informationen über die BIOS-Optionen für IDSDM finden Sie im *Hardware-Benutzerhandbuch*, das auf der Dell Support-Website unter **dell.com/support/manuals** zur Verfügung steht.

ANMERKUNG: Auf dem Bildschirm **Integrierte Geräte** des BIOS-Setup muss die Option **Interne USB-Schnittstelle** auf **Ein** eingestellt sein. Ist dies auf **Aus** gestellt, ist das IDSDM dem System nicht als ein Startgerät sichtbar.

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. SD2 fungiert als Standby-Karte, sämtliche IDSDM-Dateisystemeinträge werden auf beiden Karten gespeichert; gelesen wird jedoch nur von SD1. Sobald SD1 ausfällt oder entfernt wird, wird SD2 automatisch zur aktiven (Master-) Karte.

Tabelle 2-5. IDSDM-Status

IDSDM – Spiegelungsmodus	SD-Karte	vFlash-SD-Karte
Enabled (Aktiviert)	Aktiv (SD1-Karte)	vFlash inaktiv, Standby SD2
Disabled (Deaktiviert)	Aktiv (SD2-Karte)	Nur vFlash aktiv

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 dem LCD angezeigt, und PET-Warnungen werden erstellt, wenn Warnungen aktiviert sind.

Status des internen zweifachen SD-Moduls unter Verwendung von GUI anzeigen

1. Melden Sie sich an der iDRAC Web GUI an.
2. Klicken Sie in der **Systemstruktur** auf **Wechselbare Flash-Medien**. Die Seite **Wechselbarer vFlash-Datenträger** wird angezeigt. Diese Seite zeigt die beiden folgenden Abschnitte an:

- **Internes zweifaches SD-Modul** – Wird nur angezeigt, wenn das IDSDM im redundanten Modus ist. Der **Redundanzstatus** wird als **Voll** angezeigt. Wenn dieser Abschnitt nicht vorhanden ist, befindet sich die Karte im Zustand des nicht-redundanten Modus. Die gültigen Anzeigen des **Redundanzstatus** sind:
  - **Voll** — SD-Karte 1 und 2 funktionieren ordnungsgemäß.
  - **Verloren** — Entweder eine oder beide SD-Karten funktionieren nicht einwandfrei.
- **Interner Status des SD-Moduls** — Zeigt den Status der SD-Karte für SD1 und SD2 mit den folgenden Informationen an:
  - Status:
    - — Zeigt an, dass die Karte in Ordnung ist.
    - — Zeigt an, dass die Karte offline oder schreibgeschützt ist.
    - — Zeigt an, dass ein Alarm ausgegeben wurde.
  - Position — Position der SD-Karten.
  - Online-Status — Die Karten SD1 und SD2 können sich in einem der Zustände befinden, die unter Tabelle 2-6 aufgelistet sind.

Tabelle 2-6. Zustände der Karten SD1 und SD2

Status	Beschreibung
Boot (Startvorgang)	Der Controller wird hochgefahren.
Aktiv	Die Karte empfängt alle SD-Schreibvorgänge und wird für SD-Lesevorgänge verwendet.
Standby	Die Karte ist die sekundäre Karte. Sie erhält eine Kopie aller SD-Einträge.
Failed (Fehlgeschlagen)	Während eines Lese- oder Schreibvorgangs auf einer SD-Karte wird ein Fehler ausgegeben

Tabelle 2-6. Zustände der Karten SD1 und SD2 *(fortgesetzt)*

Status	Beschreibung
Nicht vorhanden	Keine SD-Karte erkannt
Offline	Beim Hochfahren ist die CID-Signatur der Karte nicht identisch mit dem NV-Speicherwert, oder die Karte ist das Ziel eines laufenden Kopiervorgangs.
Schreibgeschützt	Die Karte ist über den physischen Schieber an der SD-Karte schreibgeschützt. Das IDSDM kann keine schreibgeschützte Karte verwenden.

Aktualisieren der iDRAC6-Firmware

Durch die Aktualisierung der iDRAC6-Firmware wird ein neues Firmware-Image im Flash-Speicher installiert. Die Firmware kann anhand einer der folgenden Methoden aktualisiert werden:

- iDRAC6-Webschnittstelle
- RACADM-CLI
- Dell Update Package (für Linux oder Microsoft Windows)
- DOS-Dienstprogramm zur iDRAC6-Firmware-Aktualisierung
- CMC-Webschnittstelle
- WSMAN-Schnittstelle

Firmware-Paket oder Update Package herunterladen

Laden Sie die Firmware von **support.dell.com** herunter. Das Firmware-Image steht in verschiedenen Formaten zur Verfügung, um die unterschiedlichen verfügbaren Aktualisierungsmethoden zu unterstützen.

Zum Aktualisieren der iDRAC6-Firmware über die iDRAC6-Webschnittstelle oder zur Wiederherstellung des iDRAC6 über die CMC-Webschnittstelle laden Sie das als selbstextrahierendes Archiv verpackte Binär-Image herunter.

Laden Sie zum Aktualisieren der iDRAC6-Firmware vom verwalteten Server aus das betriebssystemspezifische Dell Update Package (DUP) für das Betriebssystem herunter, das auf dem Server ausgeführt wird, dessen iDRAC6 Sie aktualisieren.

Laden Sie zum Aktualisieren der iDRAC6-Firmware mithilfe des DOS-Dienstprogramms sowohl das Dienstprogramm als auch das Binär-Image herunter. Diese Dateien sind in selbstextrahierenden Archiven verpackt.

Ausführen der Firmware-Aktualisierung

ANMERKUNG: Wenn die iDRAC6-Firmware-Aktualisierung beginnt, werden alle bestehenden iDRAC6-Sitzungen abgebrochen. Neue Sitzungen sind erst nach Abschluss des Aktualisierungsvorgangs zulässig.

ANMERKUNG: Während der iDRAC6-Firmware-Aktualisierung laufen die Gehäuselüfter bei 100 % Kapazität. Nach Abschluss der Aktualisierung wird die normale Lüfterdrehzahlregulierung fortgesetzt. Hierbei handelt es sich um eine normale Funktionsweise, die den Server vor Überhitzung schützt, wenn er keine Sensorinformationen an den CMC senden kann.

Führen Sie zum Verwenden eines Dell Update Package für Linux oder Microsoft Windows das betriebssystemspezifische DUP auf dem verwalteten Server aus.

Legen Sie das Binär-Image für die Firmware bei Verwendung der iDRAC6- oder der CMC-Webschnittstelle auf einer Festplatte ab. Auf diese muss die Management Station, von der aus Sie die Webschnittstelle ausführen, zugreifen können. Siehe „iDRAC6-Firmware aktualisieren“ auf Seite 130.

ANMERKUNG: Über die iDRAC6-Webschnittstelle ist es auch möglich, die iDRAC6-Konfiguration auf die Werkseinstellungen zurückzusetzen.

ANMERKUNG: Wenn die Konfiguration während der Firmware-Aktualisierung nicht beibehalten wird, erzeugt der iDRAC6 neue SHA1- und MD5-Schlüssel für das SSL-Zertifikat. Da die Schlüssel von denen im offenen Webbrowser abweichen, müssen alle mit iDRAC6 verbundenen Browserfenster nach der Firmwareaktualisierung geschlossen werden. Wenn die Browserfenster nicht geschlossen sind, wird die Fehlermeldung **Ungültiges Zertifikat** eingeblendet.

Zur Aktualisierung der iDRAC6-Firmware können Sie die CMC-Webschnittstelle oder CMC-RACADM verwenden. Diese Funktion ist verfügbar, wenn sich die iDRAC6-Firmware im Normalmodus befindet, aber auch, wenn sie beschädigt ist. Siehe „iDRAC6-Firmware mithilfe des CMC aktualisieren“ auf Seite 132.

ANMERKUNG: Wenn Sie ein Rollback der iDRAC6-Firmware auf eine ältere Version durchführen, muss das vorhandene Internet Explorer ActiveX Browser-Plugin auf jeder Windows-basierten Management Station gelöscht werden, damit die Firmware eine kompatible Version des ActiveX-Plugin installieren kann.

Überprüfung der Digitalsignatur für Linux-DUPs

Eine Digitalsignatur wird dazu verwendet, die Identität des Unterzeichners einer Datei zu beglaubigen und zu bescheinigen, dass der ursprüngliche Inhalt der Datei seit der Unterzeichnung nicht modifiziert wurde.

Falls der GNU Privacy Guard (GPG) noch nicht auf dem System installiert ist, installieren Sie ihn jetzt, damit Digitalsignaturen verifiziert werden können.

Zur Verwendung des Standardüberprüfungsverfahrens führen Sie folgende Schritte durch:

1. Laden Sie den öffentlichen Dell Linux-GnuPG-Schlüssel herunter, indem Sie zu **lists.us.dell.com** wechseln und auf den Link **Dell Public GPG key** klicken. Speichern Sie die Datei auf Ihr lokales System. Der Standardname lautet **linux-security-publickey.txt**.
2. Importieren Sie den öffentlichen Schlüssel zur vertrauenswürdigen GPF-Datenbank, indem Sie folgenden Befehl ausführen:

   ```
   gpg --import <Dateiname des öffentlichen Schlüssels>
   ```

3. Um eine Warnung bzgl. eines nicht vertrauenswürdigen Schlüssels zu verhindern, ändern Sie die Vertrauensstufe für den öffentlichen Dell-GPG-Schlüssel.
   a. Geben Sie folgenden Befehl ein:

      ```
      gpg --edit-key 23B66A9D
      ```

   b. Geben Sie im GPG-Schlüsseleditor `fpr` ein. Die folgende Meldung wird angezeigt:

      ```
      pub 1024D/23B66A9D 2001-04-16 Dell, Inc.
      (Produktgruppe) <linux-security@dell.com>
      Primärer Schlüsselfingerabdruck: 4172 E2CE 955A
      1776 A5E6 1BB7 CA77 951D 23B6 6A9D
      ```

      Stimmt der Fingerabdruck des importierten Schlüssels mit dem oben aufgeführten überein, besitzen Sie eine korrekte Kopie des Schlüssels.

c Während Sie sich im GPG-Schlüsselbearbeitungsprogramm befinden, geben Sie `trust` ein. Das folgende Menü wird angezeigt:

```
Bitte geben Sie an, wie vertrauenswürdig Sie
diesen Benutzer einstufen, die Schlüssel
anderer Benutzer korrekt zu verifizieren (durch
Einsehen von Passports, Überprüfen von
Fingerabdrücken unterschiedlicher Quellen usw.)

  1 = Ich weiß nicht oder möchte keine Aussage
  machen
  2 = Ich habe KEIN Vertrauen
  3 = Ich habe geringfügiges Vertrauen
  4 = Ich habe volles Vertrauen
  5 = Ich habe absolutes Vertrauen
  m = zurück zum Hauptmenü

Ihre Entscheidung?
```

d Geben Sie `5` ein, und drücken Sie die Eingabetaste. Die folgende Eingabeaufforderung wird angezeigt:

```
Möchten Sie diesen Schlüssel wirklich auf
absolutes Vertrauen einstellen? (y/n)
```

e Geben Sie `y` <Eingabe> ein, um die Auswahl zu bestätigen.

f Geben Sie `quit` <Eingabe> ein, um das GPG-Schlüsselbearbeitungsprogramm zu beenden.

Der öffentliche Schlüssel muss nur einmal importiert und bestätigt werden.

4 Laden Sie sich das erforderliche Paket (z. B. das Linux-DUP oder das selbstextrahierende Archiv) sowie die zugehörige Signaturdatei von der Dell Support-Website unter **support.dell.com/support/downloads** herunter.

ANMERKUNG: Jedes Linux-Aktualisierungspaket enthält eine separate Signaturdatei, die auf derselben Webseite wie das Aktualisierungspaket angezeigt wird. Sie benötigen sowohl das Aktualisierungspaket als auch die zugehörige Signaturdatei zur Verifizierung. Standardmäßig hat die Signaturdatei denselben Namen wie die DUP-Datei, mit der Erweiterung **.sign**. So verfügt das iDRAC6-Firmware-Image beispielsweise über eine zugeordnete **.sign**-Datei (**IDRAC_FRMW_LX_2.2.BIN.sign**), die im selbstextrahierenden Archiv mit dem Firmware-Image (**IDRAC_FRMW_LX_2.2.BIN**) enthalten ist. Zum Herunterladen der Dateien klicken Sie mit der rechten Maustaste auf die **Download**-Verknüpfung und verwenden Sie die Dateioption **„Ziel speichern unter"**.

5 Überprüfen Sie das Aktualisierungspaket:

```
gpg --verify <Linux-Aktualisierungspaket-
Signaturdateiname> <Linux-Aktualisierungspaket-
Dateiname>
```

Im folgenden Beispiel werden die Schritte zum Überprüfen eines Dell PowerEdge M610 iDRAC6-Aktualisierungspakets beschrieben:

1 Laden Sie die beiden folgenden Dateien von **support.dell.com** herunter:

- IDRAC_FRMW_LX_2.2.BIN.sign
- IDRAC_FRMW_LX_2.2.BIN

2 Importieren Sie den öffentlichen Schlüssel durch Ausführen des folgenden Befehls:

```
gpg --import <Linux-Sicherheit-öffentlicher
Schlüssel.txt>
```

Die folgende Ausgabemeldung wird angezeigt:

```
gpg: Schlüssel 23B66A9D: „Dell Computer
Corporation (Linux Systems Group) <linux-
security@dell.com>" nicht verändert
gpg: Gesamtzahl verarbeitet: 1
gpg: unverändert: 1
```

3 Legen Sie die GPG-Vertrauensstufe für den öffentlichen Dell Schlüssel fest, falls dies nicht bereits geschehen ist.

a Geben Sie folgenden Befehl ein:

```
gpg --edit-key 23B66A9D
```

b Geben Sie in der Befehlsaufforderung den folgenden Befehl ein:

```
fpr
trust
```

c Geben Sie `5` ein, und drücken Sie dann die Eingabetaste, um `Ich habe absolutes Vertrauen` aus dem Menü auszuwählen.

d Geben Sie `y` <Eingabe> ein, um die Auswahl zu bestätigen.

e Geben Sie `quit` <Eingabe> ein, um das GPG-Schlüsselbearbeitungsprogramm zu beenden.

Damit ist die Validierung des öffentlichen Schlüssels von Dell abgeschlossen.

4 Überprüfen Sie die Digitalsignatur des Dell PowerEdge M610 iDRAC6-Pakets, indem Sie folgenden Befehl ausführen:

```
gpg --verify IDRAC_FRMW_LX_2.2.BIN.sign
IDRAC_FRMW_LX_2.2.BIN
```

Die folgende Ausgabemeldung wird angezeigt:

```
gpg: Signatur erstellt am Freitag, 11. Juli
2008 um 15:03:47 CDT (Central-Sommerzeit)
mithilfe der DSA-Schlüssel-ID 23B66A9D
gpg: Gute Signatur von „Dell, Inc.
(Produktgruppe) <linux-security@dell.com>"
```

Falls der Schlüssel noch nicht wie in Schritt 3 gezeigt überprüft wurde, werden Sie zusätzliche Meldungen erhalten:

```
gpg: WARNUNG: Dieser Schlüssel wurde nicht durch eine
vertrauenswürdige Signatur bestätigt!
gpg: Es gibt keinen Hinweis darauf, dass die Signatur
dem Besitzer gehört.
Primärer Schlüsselfingerabdruck: 4172 E2CE 955A 1776
A5E6 1BB7 CA77 951D 23B6 6A9D
```

Verwenden der iDRAC6-Webschnittstelle

ANMERKUNG: Eine Unterbrechung der iDRAC6-Firmware-Aktualisierung vor ihrem Abschluss kann dazu führen, dass die iDRAC6-Firmware beschädigt wird. In solchen Fällen können Sie den iDRAC6 über die CMC-Webschnittstelle wiederherstellen.

ANMERKUNG: Die Firmware-Aktualisierung behält standardmäßig die aktuellen iDRAC6-Einstellungen bei. Während des Aktualisierungsprozesses haben Sie die Option, die iDRAC6-Konfigurationen auf den Herstellerstandard zurückzusetzen. Wenn Sie die Konfiguration auf die Werkseinstellungen einstellen, wird der Zugriff auf das externe Netzwerk nach Abschluss der Aktualisierung deaktiviert. Das Netzwerk muss unter Verwendung des iDRAC6-Konfigurationsdienstprogramms aktiviert und konfiguriert werden.

1. Starten Sie die iDRAC6-Webschnittstelle.
2. Wählen Sie in der Systemstruktur **System→ iDRAC-Einstellungen** aus.
3. Klicken Sie auf die Registerkarte **Aktualisieren**.

   Die Seite **Firmwaraktualisierung** wird angezeigt.

   ANMERKUNG: Damit die Firmware aktualisiert werden kann, muss der iDRAC6 in den Aktualisierungsmodus versetzt werden. Sobald sich der iDRAC6 in diesem Modus befindet, wird er automatisch zurückgesetzt, selbst wenn Sie den Aktualisierungsvorgang abbrechen.
4. Klicken Sie im Abschnitt **Hochladen** auf **Durchsuchen**, um das heruntergeladene Firmware-Image zu suchen. Der standardmäßige Firmware-Imagename lautet **firmimg.imc**.
5. Klicken Sie auf **Hochladen**.

   Die Dateien werden zu iDRAC6 hochgeladen. This may take several minutes to complete.

   ANMERKUNG: Während des Hochladens kann der Firmware-Aktualisierungsprozess durch Klicken auf **Abbrechen** abgebrochen werden. Wenn Sie auf **Abbrechen** klicken, wird iDRAC6 in den normalen Betriebsmodus zurückgesetzt.

   Wenn der Hochladevorgang vollständig ist, wird der Bildschirm **Hochladen (Schritt 2 von 3)** angezeigt.

   - Wenn die Image-Datei erfolgreich hochgeladen wurde und alle Überprüfungsvorgänge bestanden hat, wird eine Meldung angezeigt, die bestätigt, dass das Firmware-Image überprüft wurde.

- Wenn das Image nicht erfolgreich hochgeladen wurde oder die Überprüfungsvorgänge nicht bestanden hat, wechselt die Firmware-Aktualisierung zum Bildschirm **Firmware-Aktualisierung** zurück. Sie können versuchen, iDRAC6 erneut zu aktualisieren, oder auf **Abbrechen** klicken, um iDRAC6 in den normalen Betriebsmodus zurückzusetzen.

ANMERKUNG: Wenn Sie die Markierung für das Kontrollkästchen **Konfiguration beibehalten** aufheben, wird iDRAC6 auf die Standardeinstellungen zurückgesetzt. Das LAN ist in den Standardeinstellungen deaktiviert, und Sie können sich nicht an der iDRAC6-Webschnittstelle anmelden. Sie müssen die LAN-Einstellungen während des BIOS-POST oder über den CMC mit dem **iDRAC6-Konfigurationsdienstprogramm** neu konfigurieren.

6 Standardmäßig ist das Kontrollkästchen **Konfiguration sichern** aktiviert (markiert), um die aktuellen Einstellungen auf dem iDRAC6 nach einer Erweiterung zu sichern. Wenn die Einstellungen nicht beibehalten werden sollen, entfernen Sie die Markierung im Kontrollkästchen **Konfiguration beibehalten**.

7 Klicken Sie auf **Aktualisierung starten**, um den Aktualisierungsvorgang zu starten. Unterbrechen Sie den Aktualisierungsvorgang nicht.

8 Auf der Seite **Hochladen (Schritt 3 von 3)** können Sie den Status des Hochladevorgangs einsehen. Der Fortschritt der Firmwareaktualisierung wird als Prozentsatz in der Spalte **Fortschritt** angezeigt.

9 Sobald die Firmware-Aktualisierung vollständig ist, wird das Fenster **Hochladen (Schritt 3 von 3)** mit dem Ergebnis neu angezeigt, und iDRAC6 wird automatisch zurückgesetzt. Sie müssen das aktuelle Browserfenster schließen und eine neue iDRAC6-Verbindung in einem neuen Browserfenster herstellen.

Die iDRAC6-Firmware über RACADM aktualisieren

Sie können die iDRAC6-Firmware unter Verwendung von remote-RACADM aktualisieren.

1 Laden Sie das iDRAC6-Firmware-Image von der Dell Support-Website unter **www.support.dell.com** auf den TFTP-Server herunter.

Zum Beispiel:

C:\downloads\firmimg.imc

2 Führen Sie den folgenden RACADM-Befehl aus:

Zum Beispiel:

```
racadm -r <iDRAC6-IP-Adresse> -u <Benutzername> -p
<Kennwort> fwupdate -g -u -a <Pfad>
```

wobei *Pfad* der Speicherort auf dem TFTP-Server ist, auf dem **firmimg.imc** gespeichert ist.

DOS-Aktualisierungsdienstprogramm verwenden

Starten Sie zum Aktualisieren der iDRAC6-Firmware mit dem DOS-Aktualisierungsdienstprogramm den verwalteten Server zu DOS und führen Sie den Befehl **idrac16d** aus. Die Syntax für den Befehl lautet:

```
idrac16d [-f] [-i=<Dateiname>] [-l=<Protokolldatei>]
```

Wenn der Befehl **idrac16d** ohne Optionen ausgeführt wird, aktualisiert er die iDRAC6-Firmware unter Verwendung der Firmware-Imagedatei **firmimg.imc** im aktuellen Verzeichnis.

Die Optionen sind wie folgt:

- `-f` - Erzwingt die Aktualisierung. Die Option `-f` kann dazu verwendet werden, die Firmware auf ein früheres Image *zurückzustufen*.
- `-i=<Dateiname>` - Bestimmt den Dateinamen, den das Firmware-Image enthält. Diese Option ist erforderlich, wenn der Firmware-Dateiname geändert wurde und jetzt vom Standardnamen **firmimg.imc** abweicht.
- `-l=<Protokolldatei>` - Protokolliert die Ausgabe der Aktualisierungsaktivität. Diese Option wird für das Debuggen verwendet.

ANMERKUNG: Wenn Sie zum Befehl **idrac16d** falsche Argumente eingeben oder die Option `-h` angeben, könnten Sie feststellen, dass in der Gebrauchsausgabe eventuell eine zusätzliche Option, `-nopresconfig`, auftritt. Diese Option wird zum Aktualisieren der Firmware ohne Bewahren von Konfigurationsinformationen verwendet. Es wird empfohlen, diese Option **nicht** zu benutzen, da sie sämtliche Ihrer iDRAC6-Konfigurationsinformationen wie IP-Adressen, Benutzer und Kennwörter *löscht*.

WSMAN-Schnittstelle verwenden

Informationen zum Aktualisieren der Firmware über WSMAN finden Sie in der Dokumentation im Dell Enterprise Technology Center unter **www.delltechcenter.com**.

Aktualisieren des USC-Reparaturpakets

Informationen zur Aktualisierung des USC-Reparaturpakets über die iDRAC6-Webschnittstelle finden Sie im *Dell Lifecycle Controller-Benutzerhandbuch*.

iDRAC6 zur Verwendung mit IT Assistant konfigurieren

Dell OpenManage IT Assistant kann verwaltete Geräte ermitteln, die die Anforderungen für das einfache Netzwerkverwaltungsprotokoll (SNMP) v1 und v2c sowie die intelligente Plattform-Verwaltungsschnittstelle (IPMI) v2.0 erfüllen.

iDRAC6 erfüllt die Anforderungen für IPMI v2.0. In diesem Abschnitt werden die Schritte zum Konfigurieren von iDRAC6 zur Ermittlung und Überwachung durch IT Assistant beschrieben. Sie können dies auf zwei verschiedene Arten ausführen: Durch das iDRAC6-Konfigurationsdienstprogramm und durch die grafische Webschnittstelle von iDRAC6.

iDRAC6-Konfigurationsdienstprogramm zum Aktivieren von Ermittlung und Überwachung verwenden

Um iDRAC6 für die IPMI-Ermittlung sowie das Senden von Warnungs-Traps auf der Stufe des iDRAC6-Konfigurationsdienstprogramms einzurichten, müssen Sie Ihren verwalteten Server (Blade) neu starten und das Hochfahren über die virtuelle Konsole sowie entweder einen Remote-Monitor und eine Konsolentastatur oder eine SOL-Verbindung (Seriell über LAN) beobachten. Wenn `<Strg-E> für Setup im Remote-Zugriff` angezeigt wird, drücken Sie auf <Strg><E>.

Wenn der Bildschirm iDRAC6-**Konfigurationsdienstprogramm** angezeigt wird, blättern Sie mit den Pfeiltasten nach unten.

1. Aktivieren Sie **IPMI über LAN**.
2. Geben Sie, falls verwendet, den **Verschlüsselungsschlüssel für RMCP+** Ihrer Site ein.

   ANMERKUNG: Wenden Sie sich an den leitenden Netzwerkadministrator oder CIO, um das Einführen dieser Option zu besprechen, da sie wertvollen zusätzlichen Sicherheitsschutz bietet und standortweit eingesetzt werden muss, um ordnungsgemäß funktionieren zu können.
3. Drücken Sie bei **LAN-Parameter** die <Eingabetaste>, um den Unterbildschirm aufzurufen. Verwenden Sie zum Navigieren die Aufwärts- und Abwärtstasten.
4. Schalten Sie **LAN-Warnung aktiviert** mit der Leertaste auf **Ein**.
5. Geben Sie die IP-Adresse der Management Station unter **Warnungsziel 1** ein.
6. Geben Sie unter Verwendung einer im gesamten Datencenter einheitlich befolgten Namenskonventionen eine Namenszeichenkette unter **iDRAC6-Name** ein. Die Standardeinstellung lautet `iDRAC6-{`*`Service-Tag-Nummer`*`}`.

Beenden Sie das iDRAC6-Konfigurationsdienstprogramm, indem Sie <Esc>, <Esc> und dann die <Eingabetaste> drücken, um Ihre Änderungen zu speichern. Ihr Server wird jetzt zum normalen Betrieb gestartet und während der nächsten geplanten Ermittlungsphase von IT Assistant ermittelt.

ANMERKUNG: Sie können auch die Dell-Verwaltungskonsole – die One-to-Many-Systemverwaltungsanwendung der nächsten Generation – verwenden, um Ermittlung und Überwachung zu aktivieren. Weitere Informationen finden Sie im *Benutzerhandbuch zur Dell-Verwaltungskonsole* auf der Dell Support-Website unter **dell.com/support/manuals**.

iDRAC6-Webschnittstelle zum Aktivieren von Ermittlung und Überwachung verwenden

Die IPMI-Ermittlung kann auch über die Remote-Webschnittstelle aktiviert werden:

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich mit einem Anmeldenamen und Kennwort mit Administratorberechtigungen an der iDRAC6-Webschnittstelle an.
3. Wählen Sie in der Systemstruktur **System→ iDRAC-Einstellungen→ Register Netzwerk/Sicherheit** aus.

   Der Bildschirm **Netzwerk** wird angezeigt.
4. Stellen Sie sicher, dass im Abschnitt **IPMI-Einstellungen** das Kontrollkästchen **IPMI über LAN aktivieren** ausgewählt (markiert) ist.
5. Wählen Sie im Drop-Down-Menü **Beschränkung der Kanalberechtigungsebene** die Option **Administrator** aus.
6. Geben Sie, falls verwendet, den **Verschlüsselungsschlüssel für RMCP+** Ihrer Site ein.
7. Klicken Sie auf **Anwenden**, falls Sie in dem Bildschirm Änderungen vorgenommen haben.
8. Wählen Sie in der Systemstruktur **System→ Ρεγιστερ Warnungsverwaltung→ Plattformereignisse** aus.

   Der Bildschirm **Plattformereignisse** wird angezeigt und enthält eine Liste der Ereignisse, für die Sie iDRAC6 zum Generieren von Warnungen konfigurieren können.
9. Aktivieren Sie Warnungen für ein oder mehrere Ereignisse, indem Sie das Kontrollkästchen in der Spalte **Warnung erstellen** markieren.
10. Klicken Sie auf **Anwenden**, falls Sie in dem Bildschirm Änderungen vorgenommen haben.
11. Klicken Sie auf **Trap-Einstellungen**. Der Bildschirm **Trap-Einstellungen** wird eingeblendet.
12. Markieren Sie im Abschnitt **IPv4-Ziel-Liste** im ersten verfügbaren Feld **Ziel-IP-Adresse** das Kontrollkästchen **Aktiviert**, und geben Sie anschließend die IP-Adresse Ihrer Management Station ein.

13 Wiederholen Sie Schritt 12 für den Abschnitt **IPv6-Ziel-Liste**.

14 Klicken Sie auf **Anwenden**. Wenn Sie auf **Senden** klicken, wird eine Test-Trap-Warnung gesendet.

15 Klicken Sie auf **E-Mail-Warnungseinstellungen**. Der Bildschirm **E-Mail-Warnungseinstellungen** wird angezeigt.

16 Geben Sie im Abschnitt **Ziel-E-Mail-Adressen** im ersten verfügbaren Feld **E-Mail-Warnung** die E-Mail-Adresse ein, an die Warnungsmeldungen gesendet werden sollen, und klicken Sie anschließend auf **Anwenden**.

17 Wenn Sie auf **Senden** klicken, wird eine Test-E-Mail-Warnung gesendet.

Es wird dringen empfohlen, zu Sicherheitszwecken für IPMI-Befehle einen separaten Benutzer mit eigenem Benutzernamen, IPMI-über-LAN-Berechtigungen und Kennwort einzurichten:

1 Wählen Sie in der Systemstruktur **System→ iDRAC-Einstellungen** aus.

2 Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Benutzer**.

Der Bildschirm **Benutzer** wird eingeblendet und zeigt eine Liste aller Benutzer (definiert oder undefiniert) an.

3 Klicken Sie auf die **Benutzer-ID** eines undefinierten Benutzers.

Der Bildschirm **Benutzerkonfiguration** für die ausgewählte Benutzer-ID wird angezeigt.

4 Markieren Sie das Kontrollkästchen **Benutzer aktivieren**, und geben Sie dann den Benutzernamen und das Kennwort ein.

5 Stellen Sie sicher, dass im Abschnitt **IPMI-LAN-Berechtigung** die Option **Maximale LAN-Benutzerberechtigung gewährt** auf **Administrator** eingestellt ist.

6 Legen Sie die Benutzerberechtigungen nach Bedarf fest.

7 Klicken Sie auf **Anwenden**, um die Einstellungen für den neuen Benutzer zu speichern.

IT Assistant zum Anzeigen von iDRAC6-Status und -Ereignissen verwenden

Nachdem die Ermittlung abgeschlossen ist, werden die iDRAC6-Geräte in der **Server**-Kategorie des Bildschirms **Details zu ITA-Geräten** eingeblendet und die iDRAC6-Informationen können durch Klicken auf den iDRAC6-Namen angezeigt werden. Dies ist anders als bei DRAC5-Systemen, bei denen die Verwaltungskarte in der RAC-Gruppe angezeigt wird.

iDRAC6-Fehler- und Warnungs-Traps werden jetzt im primären **Warnungsprotokoll** des IT Assistant sichtbar. Sie werden in der Kategorie **Unbekannt** angezeigt, doch die Trap-Beschreibung und der Schweregrad sind korrekt.

Weitere Informationen zur Verwendung von IT Assistant zum Verwalten des Datencenters stehen Ihnen im *Benutzerhandbuch zu Dell OpenManage IT Assistant* zur Verfügung.

ANMERKUNG: Sie können auch die Dell-Verwaltungskonsole – die One-to-Many-Systemverwaltungsanwendung der nächsten Generation – verwenden, um den iDRAC6-Status und iDRAC6-Ereignisse anzuzeigen. Weitere Informationen finden Sie im *Benutzerhandbuch zur Dell-Verwaltungskonsole* auf der Dell Support-Website unter **dell.com/support/manuals**.

3

Konfiguration der Management Station

Eine Management Station ist ein Computer zum Überwachen und Verwalten der Dell PowerEdge-Server und anderer Module im Gehäuse. In diesem Abschnitt werden Softwareinstallations- und Konfigurationsaufgaben beschrieben, über die eine Management Station zum Arbeiten mit iDRAC6 Enterprise eingerichtet wird. Befolgen Sie vor dem Konfigurieren des iDRAC6 die in diesem Abschnitt beschriebenen Anweisungen, um sicherzustellen, dass die benötigten Extras installiert und konfiguriert sind.

Schritte zum Einrichten der Management Station

Führen Sie zum Einrichten der Management Station folgende Schritte aus:

1. Richten Sie das Netzwerk für Management Station ein.
2. Installieren und konfigurieren Sie einen unterstützten Internet-Browser.
3. Installieren Sie eine Java-Laufzeitumgebung (Runtime Environment, JRE) (erforderlich bei Verwendung des Plug-In-Typs Java).
4. Installieren Sie Telnet- oder SSH-Clients, falls erforderlich.
5. Installieren Sie einen TFTP-Server, falls erforderlich.
6. Installieren Sie Dell OpenManage IT Assistant (optional).
7. Installieren Sie die Dell-Verwaltungskonsole (optional).

Netzwerkvoraussetzungen für die Management Station

Damit die Management Station auf den iDRAC6 zugreifen kann, muss sie sich auf demselben Netzwerk wie der mit „GB1“ bezeichnete CMC RJ45-Verbindungsanschluss befinden. Es ist möglich, das CMC-Netzwerk von dem Netzwerk zu isolieren, auf dem sich der verwaltete Server befindet, sodass die Management Station zwar LAN-Zugriff auf den iDRAC6, aber nicht auf den verwalteten Server haben kann.

Durch die Verwendung der iDRAC6-Virtuelle Konsole-Funktion (siehe „Seriell über LAN konfigurieren und verwenden“ auf Seite 209) können Sie selbst dann auf die Konsole des verwalteten Servers zugreifen,

wenn Sie keinen Netzwerkzugriff auf die Serverschnittstellen haben. Sie können auf dem verwalteten Server auch verschiedene Verwaltungsfunktionen ausführen, wie z. B. den Neustart des Computers und die Verwendung von iDRAC6-Einrichtungen. Um auf Netzwerk- und Anwendungsdienste zuzugreifen, die auf dem verwalteten Server gehostet werden, könnten Sie jedoch eventuell eine zusätzliche NIC im verwalteten Server benötigen.

Konfigurieren eines unterstützten Webbrowsers

Die folgenden Abschnitte enthalten Anleitungen zum Konfigurieren der unterstützten Webbrowser zur Verwendung mit der iDRAC6-Webschnittstelle.

Webbrowser öffnen

Die iDRAC6-Webschnittstelle wurde zur Ansicht in einem unterstützten Webbrowser mit einer Mindestbildschirmauflösung von 800 Pixel x 600 Pixel entwickelt. Stellen Sie sicher, dass die Auflösung mindestens 800 x 600 Pixel beträgt, und/oder passen Sie die erforderliche Größe an Ihren Browser an, damit die Schnittstelle betrachtet und auf alle Funktionen zugegriffen werden kann.

ANMERKUNG: In einigen Situationen, meistens während der ersten Sitzung nach einer Firmwareaktualisierung, kann Benutzern von Internet Explorer eventuell die Meldung **Mit Fehlern abgeschlossen** in der Statusleiste des Browsers zusammen mit einer teilweise erstellten Seite im Hauptfenster des Browsers angezeigt werden. Dieser Fehler kann auch bei Konnektivitätsproblemen auftreten. Es handelt sich dabei um ein bekanntes Problem bei Internet Explorer. Schließen Sie den Browser und starten Sie ihn erneut.

Webbrowser zur Verbindung mit der Webschnittstelle konfigurieren

Wenn Sie von einer Management Station aus, die über einen Proxyserver mit dem Internet verbunden ist, eine Verbindung zur iDRAC6-Webschnittstelle herstellen, muss der Webbrowser so konfiguriert werden, dass er von diesem Server aus auf das Internet zugreifen kann.

Führen Sie folgende Schritte zum Konfigurieren des Internet Explorer-Webbrowsers zum Zugriff auf einen Proxyserver aus:

1. Öffnen Sie ein Webbrowser-Fenster.
2. Klicken Sie auf **Extras** und dann auf **Internetoptionen**.

   Das Fenster **Internetoptionen** wird angezeigt.
3. Wählen Sie **Extras→ Internetoptionen→ Sicherheit→ Lokales Intranet**.
4. Klicken Sie auf **Stufe anpassen**.
5. Wählen Sie aus dem Drop-Down-Menü **Mittel-Niedrig** aus, und klicken Sie auf **Zurücksetzen**. Klicken Sie zum Bestätigen auf **OK**. Sie müssen das Dialogfeld zum Festlegen der **benutzerdefinierten Stufe** erneut öffnen, indem Sie auf die entsprechende Schaltfläche klicken.
6. Blättern Sie zum Abschnitt mit der Bezeichnung ActiveX-Steuerelemente und -Plug-ins herunter und prüfen Sie die einzelnen Einstellungen, da in den verschiedenen Versionen von Internet Explorer auf der Stufe **Mittel-Niedrig** unterschiedliche Einstellungen vorgenommen werden können:

   - Automatische Eingabeaufforderung für ActiveX-Steuerelemente: Aktivieren
   - Binär- und Skript-Verhalten: Aktivieren
   - Signierte ActiveX-Steuerelemente herunterladen: Bestätigen
   - ActiveX-Steuerelemente initialisieren und ausführen, die nicht als sicher gekennzeichnet sind: Bestätigen
   - ActiveX-Steuerelemente und Plug-ins ausführen: Aktivieren
   - ActiveX-Steuerelemente ausführen, die für Skripting sicher sind: Aktivieren

   Im Abschnitt **Download**:

   - Automatische Eingabeaufforderung für Datei-Downloads: Aktivieren
   - Datei-Download: Aktivieren
   - Schriftart-Download: Aktivieren

   Im Abschnitt **Verschiedenes**:

   - META-AKTUALISIERUNG zulassen: Aktivieren
   - Skripting von Web-Browser-Steuerung für Internet Explorer zulassen: Aktivieren

- Skript-initiierte Fenster ohne Größen- bzw. Positionsbeschränkungen zulassen: Aktivieren
- Keine Eingabeaufforderungen für die Client-Zertifikatsauswahl anzeigen, wenn keine Zertifikate vorliegen, oder wenn nur ein einziges Zertfikat vorhanden ist: Aktivieren
- Programme und Dateien in einem IFRAME starten: Aktivieren
- Dateien nach Inhalt, nicht nach Dateierweiterung öffnen: Aktivieren
- Softwarekanal-Berechtigungen: Niedrige Sicherheitsstufe
- Daten nicht verschlüsselter Formulare senden: Aktivieren
- Pop-up-Blocker verwenden: Deaktivieren

Im Abschnitt **Skripting**:

- Aktives Skripting: Aktivieren
- Zugriff auf Zwischenablage zulassen: Aktivieren
- Scripting von Java-Applets: Aktivieren

7 Wählen Sie **Extras→ Internetoptionen→ Erweitert**.

8 Stellen Sie sicher, dass die folgenden Elemente markiert oder nicht markiert sind:

Im Abschnitt **Browsen**:

- URLs immer als UTF-8 senden: markiert
- Skriptdebugging deaktivieren (Internet Explorer): markiert
- Skriptdebugging deaktivieren (Andere): markiert
- Zu jedem Skript-Fehler eine Benachrichtigung anzeigen: nicht markiert
- Aktivieren von Installation nach Bedarf (Andere): markiert
- Seitenübergänge aktivieren: markiert
- Browser-Erweiterungen von Drittanbietern aktivieren: markiert
- Verknüpfungen im gleichen Fenster öffnen: nicht markiert

Im Abschnitt **HTTP 1.1-Einstellungen**:

- HTTP 1.1 verwenden: markiert
- HTTP 1.1 über Proxy-Verbindungen verwenden: markiert

Im Abschnitt **Java (Sun)**:

- JRE 1.6.x_yz verwenden: markiert (optional; Version kann unterschiedlich sein)

Im Abschnitt **Multimedia**:

- Automatische Bildgrößenanpassung aktivieren: markiert
- Animationen auf Webseiten abspielen: markiert
- Videos auf Webseiten abspielen: markiert
- Bilder anzeigen: markiert

Im Abschnitt **Sicherheit**:

- Auf gesperrte Zertifikate von Herausgebern überprüfen: nicht markiert
- Signaturen von heruntergeladenen Programmen überprüfen: nicht markiert
- Signaturen von heruntergeladenen Programmen überprüfen: markiert
- SSL 2.0 verwenden: nicht markiert
- SSL 3.0 verwenden: markiert
- TLS 1.0 verwenden: markiert
- Zu ungültigen Standortzertifikaten Warnungen ausgeben: markiert
- Beim Wechsel zwischen sicherem und nicht sicherem Modus warnen: markiert
- Warnung ausgeben, wenn Einreichung des Formulars umgeleitet wird: markiert

ANMERKUNG: Möchten Sie eine der oben aufgeführten Einstellungen ändern, sollten Sie sich zuvor über die entsprechenden Auswirkungen informieren. Wenn Sie z. B. wählen, Popups zu blockieren, funktionieren gewisse Bereiche der iDRAC6-Webschnittstelle nicht richtig.

9 Klicken Sie auf **Anwenden** und dann auf **OK**.

10 Klicken Sie auf die Registerkarte **Verbindungen**.

11 Klicken Sie unter **LAN-Einstellungen (Lokales Netzwerk)** auf **LAN-Einstellungen**.

12 Ist das Kästchen **Proxyserver verwenden** markiert, wählen Sie **Proxyserver für lokale Adressen umgehen** aus.

13 Klicken Sie zweimal auf **OK**.

14 Schließen Sie den Browser und starten Sie ihn anschließend neu. So stellen Sie sicher, dass alle Änderungen wirksam werden.

iDRAC6 zur Liste vertrauenswürdiger Domänen hinzufügen

Wenn Sie über den Webbrowser auf die iDRAC6-Webschnittstelle zugreifen, können Sie dazu aufgefordert werden, die iDRAC6-IP-Adresse der Liste vertrauenswürdiger Domänen hinzuzufügen, wenn die IP-Adresse auf der Liste fehlt. Klicken Sie nach Ausführen dieses Vorgangs auf **Aktualisieren**, oder starten Sie den Webbrowser neu, um eine Verbindung zur iDRAC6-Webschnittstelle herzustellen.

Bei einigen Betriebssystemen kann es vorkommen, dass Internet Explorer 8 Sie nicht dazu auffordert, eine iDRAC6-IP-Adresse zur Liste vertrauenswürdiger Domänen hinzuzufügen, obwohl sich die IP-Adresse nicht in der Liste befindet.

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. Dies ist das erwartete Verhalten zur Sicherheitsgewährleistung.

Um bei Internet Explorer 8 die iDRAC6-IP-Adresse zur Liste der vertrauenswürdigen Domänen hinzuzufügen, gehen Sie folgendermaßen vor:

1. Wählen Sie **Extras→ Internetoptionen→ Sicherheit→ Vertrauenswürdige Sites→ Sites** aus.
2. Geben Sie die IP-Adresse des iDRAC6 in das Feld **Diese Website zur Zone hinzufügen** ein.
3. Klicken Sie auf **Add** (Hinzufügen).
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Close** (Schließen).
6. Klicken Sie auf **OK** und aktualisieren Sie dann den Browser.

Wenn Sie die virtuelle Konsole zum ersten Mal über Internet Explorer 8 mit Active-X-Plugin starten, kann die Nachricht „`Zertifikatsfehler: Navigation blockiert`“ angezeigt werden.

1. Klicken Sie auf **Weiter zu dieser Website**.
2. Klicken Sie auf **Installieren**, um Active-X-Steuerelemente im Fenster **Sicherheitswarnung** zu installieren.

   Die Virtuelle Konsole-Sitzung wird gestartet.

Lokalisierte Versionen der Webschnittstelle anzeigen

Die iDRAC6-Webschnittstelle wird in den folgenden Betriebssystemsprachen 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 spezifischen Sprachvarianten, die unterstützt werden. Die Verwendung der Schnittstelle mit anderen Dialekten oder Sprachen wird nicht unterstützt und kann eventuell nicht wie vorgesehen funktionieren. Bei einigen unterstützten Sprachen kann es erforderlich sein, das Browserfenster auf eine Breite von 1024 Pixel einzustellen, um alle Funktionen anzuzeigen.

Die iDRAC6-Webschnittstelle wurde für den Einsatz mit den jeweiligen Tastaturbelegungen für die oben aufgeführten Sprachvarianten entwickelt. Einige Funktionen der iDRAC6-Webschnittstelle, wie z. B. Virtuelle Konsole, können zusätzliche Schritte für den Zugriff auf bestimmte Funktionen/Buchstaben erfordern. Weitere Einzelheiten, wie lokalisierte Tastaturen in diesen Situationen verwendet werden, finden Sie unter „Verwendung des Video Viewer“ auf Seite 242. Die Verwendung anderer Tastaturen wird nicht unterstützt und könnte 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 iDRAC6-Webschnittstelle anzeigen.

Gebietsschema in Linux einstellen

Für die korrekte Anzeige des Virtuelle Konsole-Viewers ist ein UTF-8-Zeichensatz erforderlich. Wird die Anzeige nicht richtig dargestellt, überprüfen Sie das Gebietsschema, und setzen Sie ggf. den Zeichensatz zurück.

Um den Zeichensatz auf einem Linux-Client mit einer GUI in vereinfachtem Chinesisch einzustellen:

1. Öffnen Sie ein Terminal.
2. Geben Sie `locale` (Sprachumgebung) ein und drücken Sie die Eingabetaste. Es wird eine Ausgabe ähnlich der folgenden Ausgabe angezeigt:

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3. Schließen die Werte `zh_CN.UTF-8` ein, sind keine Änderungen erforderlich. Enthalten die Werte nicht `zh_CN.UTF-8`, fahren Sie mit Schritt 4 fort.
4. Bearbeiten Sie die Datei **/etc/sysconfig/i18n** mit einem Texteditor.
5. Wenden Sie in der Datei folgende Änderungen an:

   Aktueller Eintrag:

```
LANG="zh_CN.GB18030"
SUPPORTED="zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

   Aktualisierter Eintrag:

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-
8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

6. Melden Sie sich beim Betriebssystem ab und dann wieder an.

Wechseln Sie in eine andere Anzeigesprache, müssen Sie sicherstellen, dass die oben dargestellte Korrektur noch wirksam ist. Ist dies nicht der Fall, wiederholen Sie das Verfahren.

Whitelist-Funktion in Firefox deaktivieren

Firefox verfügt über eine „Whitelist"-Sicherheitsfunktion, die eine Benutzerberechtigung zum Installieren von Plugins für jede Site erfordert, die ein Plugin hostet. Ist die Whitelist-Funktion aktiviert, ist die Installation eines Virtuelle Konsole-Viewers für jeden besuchten iDRAC6 erforderlich, obwohl die Viewer-Versionen identisch sind.

Führen Sie zum Deaktivieren der Whitelist-Funktion und zum Vermeiden unnötiger Plugin-Installationen folgende Schritte aus:

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 **Einstellungσname** den Eintrag **xpinstall.enabled** ausfindig.

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

iDRAC6-Software auf der Management Station installieren

Ihr System enthält die DVD *Dell Systems Management Tools and Documentation*. Diese DVD beinhaltet die folgenden Komponenten:

- DVD-Stammverzeichnis - Enthält das Dell Systems Build und das Update-Dienstprogramm, das Informationen zur Server-Einrichtung und Systeminstallation bereitstellt
- SYSMGMT - Enthält die Systemmanagement-Softwareprodukte einschließlich des Dell OpenManage Server Administrators

RACADM auf einer Management Station installieren und deinstallieren

Zur Verwendung der Remote-RACADM-Funktionen installieren Sie RACADM auf einer Management Station. Im *Dell OpenManage Management Station Software-Installationshandbuch* unter **dell.com/support/manuals** finden Sie Informationen zur Installation von DRAC-Hilfsprogrammen auf einer Management Station, auf der ein Microsoft Windows-Betriebssystem ausgeführt wird.

RACADM unter Linux installieren und deinstallieren

1. Melden Sie sich als root an dem System an, auf dem Sie die Management Station-Komponenten installieren möchten.
2. Falls erforderlich, stellen Sie die DVD *Dell Systems Management Tools and Documentation* unter Verwendung des folgenden Befehls oder eines ähnlichen Befehls bereit:

   ```
   mount /media/cdrom
   ```

3. Wechseln Sie zum Verzeichnis **/linux/rac** und führen Sie den folgenden Befehl aus:

   ```
   rpm -ivh *.rpm
   ```

Um Hilfe zum RACADM-Befehl zu erhalten, geben Sie nach der Eingabe der vorherigen Befehle **racadm help** ein.

Um RACADM zu deinstallieren, öffnen Sie eine Eingabeaufforderung, und geben Sie Folgendes ein:

```
rpm -e <racadm-Paketname>
```

, wobei *<racadm_Paketname>* das RPM-Paket ist, das zur Installation der iDRAC6-Software verwendet wurde.

Wenn der RPM-Paketname z. B. **srvadmin-racadm5** lautet, geben Sie Folgendes ein:

```
rpm -e srvadmin-racadm5
```

Installation einer Java-Laufzeitumgebung (JRE)

ANMERKUNG: Wenn Sie Internet Explorer verwenden, ist für den Konsolen-Viewer bereits eine ActiveX-Steuerung bereitgestellt. Sie können den Java-Virtuelle Konsole-Viewer auch mit Firefox verwenden, wenn Sie eine JRE installieren und den Virtuelle Konsole-Viewer in der iDRAC6-Webschnittstelle konfigurieren, bevor Sie den Viewer starten. Weitere Informationen finden Sie unter „Konfigurieren der virtuellen Konsole und der virtuellen Datenträger auf der iDRAC6-Webschnittstelle“ auf Seite 236.

Bevor Sie den Viewer starten, können Sie stattdessen wählen, den Java-Viewer zu verwenden.

Wenn Sie den Firefox-Browser verwenden, müssen Sie eine JRE (oder ein Java Development Kit [JDK]) installieren, um die Virtuelle Konsole-Funktion verwenden zu können. Der Konsolen-Viewer ist eine Java-Anwendung, die von der iDRAC6-Webschnittstelle auf die Management Station heruntergeladen und dann mit Java Web Start auf der Management Station gestartet wird.

Wechseln Sie zu **www.java.com**, um eine JRE oder ein JDK zu installieren. Version 1.6 (Java 6.0) oder höher wird empfohlen.

Das Java Web Start-Programm wird automatisch mit der Java Laufzeitumgebung (JRE) oder dem Java Entwicklungssatz (JDK) installiert. Die Datei **jviewer.jnlp** wird auf den Desktop heruntergeladen und ein Dialogfeld weist an, welche Maßnahme getroffen werden soll. Es könnte notwendig sein, den Erweiterungstyp **.jnlp** mit der Java Web Start-Anwendung im Browser zu verknüpfen. Klicken Sie andernfalls auf **Öffnen mit** und wählen Sie dann die Anwendung javaws aus, die sich im Unterverzeichnis bin des JRE-Installationsverzeichnisses befindet.

ANMERKUNG: Wenn der Dateityp **.jnlp** nach der Installation der JRE oder des JDK nicht mit Java Web Start verknüpft ist, können Sie die Zuordnung manuell einstellen. Klicken Sie in Windows (**javaws.exe**) auf **Start**→ **Systemsteuerung**→ **Darstellung und Designs**→ **Ordneroptionen**. Markieren Sie auf der Registerkarte **Dateitypen** unter **Registrierte Dateitypen** die Erweiterung **.jnlp** und klicken Sie dann auf **Ändern**. Bei Linux (**javaws**) starten Sie Firefox und klicken auf **Bearbeiten**→ **Einstellungen**→ **Downloads** und dann auf **Maßnahmen ansehen und bearbeiten**.

Sobald Sie entweder die JRE oder das JDK installiert haben, fügen Sie bei Linux am Anfang Ihres System-PATH einen Pfad zum Java-Verzeichnis bin hinzu. Wenn Java beispielsweise in /usr/java installiert ist, fügen Sie die folgende Zeile zu Ihrem lokalen Profil .bashrc oder /etc/ hinzu:

```
PATH=/usr/java/bin:$PATH; export PATH
```

ANMERKUNG: In den Dateien können sich eventuell schon PATH-Modifizierungszeilen befinden. Stellen Sie sicher, dass die von Ihnen eingegebenen Pfadinformationen keine Konflikte erzeugen.

Telnet- oder SSH-Clients installieren

Standardmäßig ist der iDRAC6-Telnet-Dienst deaktiviert und der SSH-Dienst aktiviert. Da es sich bei Telnet um ein ungesichertes Protokoll handelt, darf es nur verwendet werden, wenn Sie keinen SSH-Client installieren können oder wenn Ihre Netzwerkverbindung auf andere Weise gesichert ist.

ANMERKUNG: iDRAC6 unterstützt bis zu vier Telnet-Sitzungen und vier SSH-Sitzungen gleichzeitig.

Telnet mit iDRAC6

Der Telnet-Client ist bei Windows- und Linux-Betriebssystemen enthalten und kann von einer Befehlsshell aus ausgeführt werden. Sie können auch einen handelsüblichen oder kostenlos erhältlichen Telnet-Client installieren, der mehr Bedienungsfunktionen als die mit dem Betriebssystem mitgelieferte Standardversion bietet.

Die Rücktaste für Telnet-Sitzungen 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 Microsoft Telnet-Clients für die Verwendung der <Rücktaste> zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie ein Eingabeaufforderungsfenster (falls erforderlich).
2. Wenn Sie keine Telnet-Sitzung ausführen, geben Sie Folgendes ein:

   ```
   telnet
   ```

   Wenn sich eine Telnet-Sitzung in Ausführung befindet, drücken Sie <Strg><]>.
3. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   set bsasdel
   ```

   Die folgende Meldung wird angezeigt:

   ```
   Rücktaste wird als Löschen gesendet.
   ```

Um eine Linux-Telnet-Sitzung zur Verwendung der <Rücktaste> zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie ein Shell, und geben Sie Folgendes ein:

   ```
   stty erase ^h
   ```

2. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   telnet
   ```

SSH mit iDRAC6

Secure Shell (SSH) ist eine Befehlszeilenverbindung mit denselben Leistungsfähigkeiten wie eine Telnet-Sitzung, jedoch mit Sitzungsverhandlungs- und Verschlüsselungsfähigkeiten zum Erhöhen der Sicherheit. iDRAC6 unterstützt SSH Version 2 mit Kennwortauthentifizierung. SSH ist auf dem iDRAC6 standardmäßig aktiviert.

Sie können auf einer Management Station kostenlose Programme wie PuTTY oder OpenSSH verwenden, um eine Verbindung zum iDRAC6 eines verwalteten Servers herzustellen. Wenn während des Anmeldeverfahrens ein Fehler auftritt, gibt der **SSH**-Client eine Fehlermeldung aus. Der Meldungstext ist vom Client abhängig und wird nicht vom iDRAC6 gesteuert.

ANMERKUNG: `OpenSSH` sollte unter Windows von einem VT100 oder ANSI-Terminalemulator ausgeführt werden. Das Ausführen von `OpenSSH` mit der Windows-Eingabeaufforderung ergibt nicht die volle Funktionalität (einige Tasten reagieren nicht und es werden keine Grafiken angezeigt).

iDRAC6 unterstützt bis zu vier Telnet-Sitzungen und vier SSH-Sitzungen gleichzeitig. Nur eine der acht potentiellen Sitzungen kann jedoch das SM-CLP benutzen. Dies bedeutet, dass der iDRAC6 nur jeweils eine SM-CLP-Sitzung auf einmal unterstützt. Die Sitzungszeitüberschreitung wird über die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert, deren Beschreibung im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist, enthalten ist.

Die iDRAC6-SSH-Umsetzung unterstützt mehrfache Verschlüsselungs-Schemata, wie in Tabelle 3-1 dargestellt.

ANMERKUNG: SSHv1 wird nicht unterstützt.

Tabelle 3-1. Verschlüsselungs-Schemata

Schematyp	Schema
Asymmetrische Verschlüsselung	Diffie-Hellman DSA/DSS 512-1024 (zufällige) Bits nach NIST-Spezifizierung
Symmetrische Verschlüsselung	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Meldungsintegrität	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentifizierung	• Kennwort

TFTP-Server installieren

Das Dateiübertragungsprotokoll TFTP ist eine vereinfachte Form des FTP-Protokolls. Es wird mit den SM-CLP- und RACADM-Befehlszeilenschnittstellen zum Übertragen von Dateien zum und vom iDRAC verwendet.

ANMERKUNG: Wenn Sie nur die iDRAC6-Webschnittstelle zum Übertragen von SSL-Zertifikaten und zum Hochladen neuer iDRAC6-Firmware verwenden, ist kein TFTP-Server erforderlich.

Sie brauchen nur dann Dateien zum oder vom iDRAC6 zu kopieren, wenn Sie iDRAC6-Firmware aktualisieren oder Zertifikate auf den iDRAC6 installieren. Wenn Sie beim Ausführen dieser Aufgaben RACADM auswählen, muss ein TFTP-Server auf einem Computer ausgeführt werden, auf den der iDRAC6 über eine IP-Adresse oder einen DNS-Namen zugreifen kann.

Sie können über den Befehl `netstat -a` unter Windows oder Linux feststellen, ob die Überwachung durch einen TFTP-Server bereits stattfindet. Port 69 ist der Standard-TFTP-Port. Wenn kein Server ausgeführt wird, haben Sie die folgenden Möglichkeiten:

- Suchen Sie im Netzwerk, in dem ein TFTP-Dienst ausgeführt wird, einen anderen Computer.
- Unter Linux installieren Sie mit Ihrer Distribution einen TFTP-Server.
- Wenn Sie Windows verwenden, installieren Sie einen handelsüblichen oder kostenlosen TFTP-Server.

Installation des Dell OpenManage IT Assistant

Das System enthält das Dell OpenManage-Softwarepaket zur Systemverwaltung. Dieses Softwarepaket schließt die folgenden Komponenten ein, ist jedoch nicht auf sie beschränkt:

- DVD *Dell Systems Management Tools and Documentation*
- Support-Website und Infodateien von Dell – Suchen Sie in den Infodateien und auf der Dell Support-Website unter **dell.com/support/manuals** nach aktuellen Informationen zu Ihren Dell-Produkten.

Informationen zur Installation des IT Assistant finden Sie im *Dell OpenManage IT Assistant-Benutzerhandbuch* unter **dell.com/support/manuals**.

Dell-Verwaltungskonsole installieren

Die Dell-Verwaltungskonsole (DMC) ist die One-to-Many-Systemverwaltungsanwendung der neuen Generation mit ähnlicher Funktionalität wie Dell OpenManage IT Assistant. Sie stellt Funktionen zu erweiterter Ermittlung, Bestandsaufnahme, Überwachung und Berichterstattung zur Verfügung. Es handelt sich hierbei um eine webbasierte GUI, die auf einer Management Station in einer Netzwerkumgebung installiert wird.

Sie können die DMC über die *Dell Management Console*-DVD installieren oder von der Dell Website unter **www.dell.com/openmanage** herunterladen und installieren.

Anleitungen zum Installieren dieser Software finden Sie im *Benutzerhandbuch zur Dell-Verwaltungskonsole*, das unter **dell.com/support/manuals** zur Verfügung steht.

4

Verwalteten Server konfigurieren

In diesem Abschnitt werden die Tasks für die Einstellung des verwalteten Servers zum Erweitern der Remote-Verwaltungsmöglichkeiten beschrieben. Diese Tasks beinhalten die Installation der Software Dell Open Manage Server Administrator und die Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz.

Softwareinstallation auf dem verwalteten Server

Die Verwaltungssoftware von Dell schließt die folgenden Funktionen ein:

- RACADM-CLI – Ermöglicht die Konfiguration und Verwaltung des iDRAC6. Ein leistungsfähiges Tool für Scripting-Konfiguration und Verwaltungs-Tasks.
- Server Administrator – muss die iDRAC6-Bildschirmfunktion Letzter Absturz verwenden.
- Server Administrator Instrumentation Service - gewährt Zugriff auf detaillierte Fehler- und Leistungsinformationen, die von standardisierten Systemverwaltungsagenten gesammelt werden, und ermöglicht die Remote-Verwaltung der überwachten Systeme, einschließlich Herunterfahren, Start und Sicherheit.
- Server Administration Storage Management Service - enthält Speicherverwaltungsinformationen in einer integrierten graphischen Ansicht.
- Server Administrator-Protokolle - protokolliert die Befehle, die von dem oder an das System ausgegeben wurden, sowie überwachte Hardwareereignisse, POST-Ereignisse und Systemwarnungen. Sie können die Protokolle auf der Homepage anzeigen, drucken oder als Berichte speichern und sie als E-Mail an einen festgelegten Service-Kontakt senden.

Verwenden Sie zum Installieren des Dell OpenManage Server Administrator die DVD *Dell Systems Management Tools and Documentation*.Anleitungen zur Installation dieser Software finden Sie im *Dell OpenManage Server Administrator-Installationshandbuch* unter **support.dell.com/manuals**. Auf der Seite **Manuals** klicken Sie auf **Software→ Systems Management**. Klicken Sie auf den entsprechenden Produktlink auf der rechten Seite, um auf die Dokumente zuzugreifen.

Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz

Das iDRAC6 kann den Bildschirm Letzter Absturz erfassen, damit Sie ihn in der Webschnittstelle anzeigen und die Ursache des Absturzes des verwalteten Systems feststellen und beheben können.

ANMERKUNG: Sie können die Aufnahme des letzten Absturzbildschirms nur dann anzeigen, wenn der verwaltete Server auf einem Windows-Betriebssystem ausgeführt wird.

Führen Sie folgende Schritte aus, um die Funktion Bildschirm Letzter Absturz zu aktivieren.

1. Installieren Sie die Software des verwalteten Servers. Weitere Informationen finden Sie im *Dell OpenManage Server Administrator-Installationshandbuch* und im *Dell OpenManage Management Station Software-Installationshandbuch*. Diese Dokumente sind auf der **Dell** Support-Website unter support.dell.com/manuals verfügbar.
2. Stellen Sie sicher, dass die Option **Automatischer Neustart** in den **Windows-Start- und Wiederherstellungseinstellungen** deaktiviert ist. Siehe „Die Windows-Option „Automatischer Neustart“ deaktivieren“ auf Seite 87.
3. Aktivieren Sie den **Bildschirm Letzter Absturz** (standardmäßig deaktiviert) in der iDRAC6-Webschnittstelle.

   Klicken Sie zum Aktivieren des **Bildschirms Letzter Absturz** in der iDRAC6-Webschnittstelle auf **System→ iDRAC-Einstellungen→ Ρεγιστερ Netzwerk/Sicherheit → Dienste**, und aktivieren Sie anschließend das Kontrollkästchen **Aktiviert** unter der Überschrift **Automatisierter Systeme-Wiederherstellungsagent**.

   Öffnen Sie zum Aktivieren des Bildschirms Letzter Absturz unter Verwendung des lokalen RACADM eine Eingabeaufforderung auf dem verwalteten System, und geben Sie den folgenden Befehl ein:

   ```
   racadm config -g cfgRacTuning -o
   cfgRacTuneAsrEnable 1
   ```
4. Aktivieren Sie in der Server Administrator-Webschnittstelle den Zeitgeber für die **Autom. Wiederherstellung**, und legen Sie als Maßnahme **Reset**, **Ausschalten** oder **Aus- und Einschalten** ein.

Informationen zur Konfiguration des Zeitgebers für **Autom. Wiederherstellung** finden Sie im *Dell OpenManage Server Administrator-Benutzerhandbuch*. Um sicherzustellen, dass der Bildschirm Letzter Absturz erfasst werden kann, muss der Zeitgeber für die **automatische Wiederherstellung** auf 60 Sekunden eingestellt werden. Die Standardeinstellung ist 480 Sekunden.

Wird der verwaltete Server ausgeschaltet und ist als Maßnahme für die **Automatische Wiederherstellung** die Option **Herunterfahren** oder **Aus- und Einschalten** gewählt, ist der Bildschirm Letzter Absturz nicht verfügbar.

Die Windows-Option „Automatischer Neustart" deaktivieren

Um sicherzugehen, dass iDRAC6 den Bildschirm des letzten Absturzes erfassen kann, deaktivieren Sie die Option **Autom. Neustart** auf den verwalteten Servern, die Windows Server oder Windows Vista bedienen.

1. Öffnen Sie die Windows-**Systemsteuerung** und doppelklicken Sie auf das **System**-Symbol.
2. Klicken Sie auf die Registerkarte **Advanced** (Erweitert).
3. Klicken Sie unter **Autostart und Wiederherstellung** auf **Einstellungen**.
4. Wählen Sie das Kontrollkästchen **Automatischer Neustart** ab.
5. Klicken Sie zweimal auf **OK**.

5

iDRAC6 Enterprise mithilfe der Webschnittstelle konfigurieren

Der iDRAC6 beinhaltet eine Webschnittstelle, über die Sie die iDRAC6-Eigenschaften und Benutzer konfigurieren, Remote-Verwaltungs-Tasks ausführen und Fehler und Probleme auf einem (verwalteten) Remote-System feststellen und beheben können. Die Webschnittstelle wird normalerweise für alltägliche Systemverwaltungs-Tasks verwendet. Dieses Kapitel beschreibt, wie allgemeine Systemverwaltungsaufgaben über die iDRAC6-Webschnittstelle ausgeführt werden, und es enthält Links zu zugehörigen Informationen.

Die meisten Konfigurations-Tasks, für die Sie die Webschnittstelle verwenden, können auch mit lokalen oder mit Remote-RACADM-Befehlen oder mit SM-CLP-Befehlen ausgeführt werden.

Befehle des lokalen RACADM werden vom verwalteten Server aus ausgeführt. Remote-RACADM ist ein Client-Dienstprogramm, das auf einer Management Station ausgeführt wird, und die bandexterne Schnittstelle zum Kommunizieren mit dem verwalteten Server verwendet. Dieses Dienstprogramm wird mit der Option **–r** zum Ausführen von Befehlen über ein Netzwerk verwendet. Weitere Informationen zu RACADM finden Sie unter „RACADM-Befehlszeilenschnittstelle verwenden“ auf Seite 295.

SM-CLP-Befehle werden in einer Shell ausgeführt, auf die über eine Telnet- oder SSH-Verbindung im Remote-Verfahren zugegriffen werden kann. Weitere Informationen zu SM-CLP finden Sie unter „iDRAC6-Enterprise verwenden SM-CLP-Befehlszeilenschnittstelle“ auf Seite 339.

Zugriff auf die Webschnittstelle

Führen Sie zum Zugriff auf die iDRAC6-Webschnittstelle folgende Schritte aus:

1. Öffnen Sie einen unterstützten Webbrowser.
2. Geben Sie in das Feld **Adresse** `https://<iDRAC6-IP-Adresse>` ein und drücken Sie die Eingabetaste.

   Wenn die Standard-HTTPS-Anschlussnummer (Anschluss 443) geändert wurde, geben Sie Folgendes ein:

   `https://<iDRAC6-IP-Adresse>:<Anschlussnummer>`

   wobei *iDRAC-IP-Adresse* die IP-Adresse für den iDRAC6 und *Anschlussnummer* die HTTPS-Anschlussnummer ist.

   Das Fenster für die iDRAC6-**Anmeldung** wird angezeigt.

Anmeldung

Sie können sich entweder als iDRAC6-Benutzer, Microsoft Active Directory-Benutzer oder als LDAP-Benutzer anmelden. Der Standardbenutzername und das Standardkennwort lauten **root** bzw. **calvin**.

Damit Sie sich am iDRAC6 anmelden können, muss Ihnen der Administrator zuerst die Berechtigung zur **Anmeldung bei iDRAC** gewähren.

Um sich anzumelden, führen Sie die folgenden Schritte aus.

1. Geben Sie eine der folgenden Eingaben in das Feld **Benutzername** ein:
   - Ihren iDRAC6-Benutzernamen.

     ANMERKUNG: Bei der Eingabe des Benutzernamens für lokale Benutzer wird zwischen *Groß-* und *Kleinschreibung* unterschieden. Beispiele sind root, it_user, IT_user oder john_doe.

   - Ihren Active Directory (AD)-Benutzernamen. Der AD-Domänenname kann ebenfalls im Drop-Down-Menü ausgewählt werden.

     Sie können die folgenden Formen als Active Directory-Namen verwenden: <*Domäne*>\<*Benutzername*>, <*Domäne*>/<*Benutzername*> oder <*Benutzer*>@<*Domäne*>. Es wird hier nicht zwischen Groß- und Kleinschreibung unterschieden. Beispiele sind `dell.com\john_doe` oder `JOHN_DOE@DELL.COM`. Sie können aber auch die Domäne in das Feld **Domäne** eingeben.

   - Den LDAP-Benutzernamen (ohne Domänennamen).

2 Geben Sie in das Feld **Kennwort** entweder Ihr iDRAC6-Benutzerkennwort, Ihr Active Directory-Benutzerkennwort oder Ihr LDAP-Kennwort ein. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

3 Klicken Sie auf **OK** oder drücken Sie die Taste <Eingabe>.

Abmeldung

1 Klicken Sie in der oberen rechten Ecke des Hauptfensters auf **Abmelden**, um die Sitzung zu schließen.

2 Schließen Sie das Browser-Fenster.

ANMERKUNG: Die Schaltfläche **Abmelden** wird erst eingeblendet, wenn Sie sich anmelden.

ANMERKUNG: Wenn Sie den Browser schließen, ohne sich ordnungsgemäß abzumelden, kann dies dazu führen, dass die Sitzung so lange aktiv bleibt, bis eine Sitzungszeitüberschreitung eintritt. Es wird empfohlen, zum Beenden einer Sitzung auf die Schaltfläche **Abmelden** zu klicken.

ANMERKUNG: Wenn Sie die iDRAC6-Webschnittstelle in Internet Explorer mit der Schließen-Schaltfläche („x") in der oberen rechten Ecke des Fensters schließen, kann dies zu einem Anwendungsfehler führen. Um dieses Problem zu lösen, laden Sie von der Microsoft Support-Website unter **support.microsoft.com** die neueste kumulative Sicherheitsaktualisierung für Internet Explorer herunter.

VORSICHTSHINWEIS: Wenn Sie mehrere Web-GUI-Sitzungen entweder mit <Strg+T> oder <Strg+N> geöffnet haben, um von derselben Management Station aus auf denselben iDRAC6 zuzugreifen, und sich dann von einer der Sitzungen abmelden, werden sämtliche Web-GUI-Sitzungen beendet.

Mehrere Browser-Registerkarten und -Fenster verwenden

Beim Öffnen neuer Register und Fenster verhalten sich verschiedene Versionen von Webbrowsern unterschiedlich. Internet Explorer (IE) 7 und IE 8 bieten die Option, sowohl Register als auch Fenster zu öffnen. Jedes Register übernimmt die Merkmale des zuletzt geöffneten Registers. Drücken Sie <Strg-T>, um ein neues Register zu öffnen, und <Strg-N>, um ein neues Browser-Fenster in der aktiven Sitzung zu öffnen. Die automatische Anmeldung erfolgt nur über <Strg-N>. Wenn Sie ein neues Register öffnen, müssen Sie sich erneut anmelden. Durch das Schließen eines beliebigen Registers laufen alle Register der iDRAC6-Webschnittstelle ab. Wenn sich z. B. ein Benutzer in einem Register mit Hauptbenutzerberechtigungen anmeldet und dann in einem anderen als Administrator, erhalten beide geöffneten Register Administratorberechtigungen.

Das Verhalten der Register in Firefox 3 ist identisch mit dem Registerverhalten in IE 7 und IE 8; d. h. neue Register leiten neue Sitzungen ein. Das Fenster-Verhalten in Firefox ist jedoch anders. Firefox-Fenster werden mit denselben Berechtigungen betrieben wie das Fenster, das als letztes geöffnet wurde. Beispiel: Wenn ein Firefox-Fenster mit einem angemeldeten Hauptbenutzer und ein anderes Fenster mit Administratorrechten geöffnet ist, haben **beide** Benutzer Administratorrechte.

Tabelle 5-1. Benutzerrechte-Verhalten in unterstützten Browsern

Browser	Registerverhalten	Fensterverhalten
Microsoft IE7 und IE8	Von letzter geöffneter Sitzung	Neue Sitzung
Firefox 3	Von letzter geöffneter Sitzung	Von letzter geöffneter Sitzung

iDRAC6-NIC konfigurieren

Für diesen Abschnitt wird angenommen, dass der iDRAC6 bereits konfiguriert wurde und über das Netzwerk auf ihn zugegriffen werden kann. Hilfe bei der ersten iDRAC6-Netzwerkkonfiguration finden Sie unter „iDRAC6-Netzwerkbetrieb konfigurieren“ auf Seite 37.

Netzwerk-, IPMI- und VLAN-Einstellungen konfigurieren

ANMERKUNG: Zur Ausführung der nachfolgenden Schritte müssen Sie die Berechtigung **iDRAC6 konfigurieren** besitzen.

ANMERKUNG: Für die meisten DHCP-Server ist ein Server zum Speichern eines Client-Bezeichner-Tokens in der Reservierungstabelle erforderlich. Der Client (z. B. iDRAC6) muss dieses Token während der DHCP-Verhandlung zur Verfügung stellen. iDRAC6 liefert die Option der Client-Identifikation unter Verwendung einer Ein-Byte-Schnittstellennummer (0), gefolgt von einer Sechs-Byte-MAC-Adresse.

1. Klicken Sie auf **System→ iDRAC-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit**.

   Der Bildschirm **Netzwerk** wird angezeigt.
3. Konfigurieren Sie die Netzwerk-, IPMI- und VLAN-Einstellungen je nach Bedarf. Beschreibungen der Optionen für die **Netzwerk-**, **IPMI-** und **VLAN-Einstellungen** finden Sie unter Tabelle 5-2, Tabelle 5-3 und Tabelle 5-4.

4 Klicken Sie auf **Anwenden**.

5 Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche.

Tabelle 5-2. Netzwerkeinstellungen

Einstellung	Beschreibung
Einstellungen der Netzwerkschnittstellenkarte	
MAC-Adresse	Zeigt die MAC-Adresse (Media Access Control) an, die die einzelnen Knoten in einem Netzwerk eindeutig identifiziert. Die MAC-Adresse kann nicht geändert werden.
NIC aktivieren	Wenn markiert, weist dies darauf hin, dass die NIC aktiviert ist und die verbleibenden Steuerungen dieser Gruppe aktiviert werden. Wenn eine NIC deaktiviert ist, wird die Datenübertragung zum und vom iDRAC6 über das Netzwerk blockiert. Die Standardeinstellung lautet **Nicht markiert**.
Allgemeine Einstellungen	
iDRAC6 auf DNS registrieren	Registriert den iDRAC6-Namen auf dem DNS-Server. Die Standardeinstellung lautet **Nicht markiert**.
DNS-iDRAC6 Name	Zeigt den iDRAC6-Namen an. Der Standardname lautet idrac-*service_tag*, wobei *service_tag* die Service-Tag-Nummer des Dell-Servers darstellt. Beispiel: iDRAC-HM8912S.
DHCP für den DNS-Domänennamen verwenden	**Markiert**: Abruf des DNS-Domänennamens vom DHCP-Server aktivieren. **Nicht markiert**: Abruf des DNS-Domänennamens vom DHCP-Server deaktivieren.
DNS-Domänenname	Der Standard-**DNS-Domänenname** ist leer. Wenn das Kontrollkästchen **DHCP für den DNS-Domänennamen verwenden** ausgewählt ist, ist diese Option grau unterlegt, und das Feld kann nicht geändert werden.
IPv4-Einstellungen	
Enabled (Aktiviert)	Aktiviert (**Markiert**) oder deaktiviert (**Nicht markiert**) die IPv4-Protokollunterstützung. Die Option **NIC aktivieren** muss zum Aktivieren dieser Einstellung markiert werden.
DHCP aktivieren	Wenn **Markiert**, erhält Server Administrator die IP-Adresse für die iDRAC6-NIC vom DHCP-Server. Deaktiviert auch die Felder **IP-Adresse**, **Subnetzmaske** und **Gateway**.

Tabelle 5-2. Netzwerkeinstellungen *(fortgesetzt)*

Einstellung	Beschreibung
IP-Adresse	Ermöglicht, eine statische IP-Adresse für den iDRAC6-NIC einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, heben Sie die Markierung der Option **DHCP aktivieren** auf.
Subnetzmaske	Ermöglicht, eine Subnetzmaske für den iDRAC6-NIC einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, heben Sie die Markierung der Option **DHCP aktivieren** auf.
Gateway	Ermöglicht, einen statischen IPv4-Gateway für den iDRAC6-NIC einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, heben Sie die Markierung der Option **DHCP aktivieren** auf.
DHCP zum Abrufen von DNS-Serveradressen verwenden	Wählen Sie die Option **DHCP aktivieren** zum Abrufen von DNS-Server-Adressen aus, indem Sie das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** auswählen. Wenn Sie DHCP nicht zum Abrufen der DNS-Server-Adressen verwenden, geben Sie die IP-Adressen in die Felder **Bevorzugter DNS-Server** und **Alternativer DNS-Server** ein.
Bevorzugter DNS-Server	Ermöglicht, eine statische IP-Adresse für den bevorzugten DNS-Server einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, muss zuerst die Auswahl der Option **DHCP zum Abrufen von DNS-Serveradressen verwenden** aufgehoben werden.
Alternativer DNS-Server	Verwendet die sekundäre DNS-Server-IP-Adresse nur, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden nicht ausgewählt** ist. Geben Sie eine IP-Adresse mit 0.0.0.0 ein, wenn kein alternativer DNS-Server vorhanden ist.
IPv6-Einstellungen:	
Enabled (Aktiviert)	Wenn das Kontrollkästchen **Markiert** ist, ist IPv6 aktiviert. Wenn das Kontrollkästchen **Nicht markiert** ist, ist IPv6 deaktiviert. Die Standardeinstellung lautet **Nicht markiert**.
Automatische Konfiguration aktivieren	Durch die Auswahl dieser Option kann der iDRAC6 die IPv6-Adresse für die iDRAC6-NIC vom Server des dynamischen Host-Konfigurationsprotokolls (DHCPv6) abrufen. Wenn **Automatische Konfiguration aktivieren** aktiviert wird, werden auch die statischen Werte für **IPv6-Adresse**, **Präfixlänge** und **Gateway** deaktiviert und gelöscht.

Tabelle 5-2. Netzwerkeinstellungen *(fortgesetzt)*

Einstellung	Beschreibung
IPv6-Adresse	Konfiguriert die IPv6-Adresse für die iDRAC6-NIC. Zum Ändern dieser Einstellung müssen Sie zuerst **Automatische Konfiguration aktivieren** deaktivieren, indem Sie die Auswahl des entsprechenden Kontrollkästchens aufheben. **ANMERKUNG:** Nur zwei IPv6-Adressen (Link-Local-Adresse und globale Adresse) werden angezeigt, wenn beim Netzwerk-Setup IPv6-DHCP konfiguriert ist und alle 16 IPv6-Adressen angezeigt werden, wenn Sie den Netzwerk-Router so konfiguriert haben, dass er Router-Advertisement-Meldungen aussendet. **ANMERKUNG:** In iDRAC6 ist es nicht möglich, die Einstellungen zu speichern, wenn Sie eine IPv6-Adresse eingeben, die sich aus mehr als acht Gruppen zusammensetzt.
Präfixlänge	Konfiguriert die Präfixlänge der IPv6-Adresse. Dieser kann ein Wert im Bereich von 1 bis 128 sein. Zum Ändern dieser Einstellung müssen Sie zuerst **Automatische Konfiguration aktivieren** deaktivieren, indem Sie die Auswahl des entsprechenden Kontrollkästchens aufheben.
Gateway	Konfiguriert das statische IPv6-Gateway für die iDRAC6-NIC. Zum Ändern dieser Einstellung müssen Sie zuerst **Automatische Konfiguration aktivieren** deaktivieren, indem Sie die Auswahl des entsprechenden Kontrollkästchens aufheben.
DHCPv6 zum Abrufen von DNS-Serveradressen verwenden	Aktivieren Sie DHCP zum Abrufen von IPv6-DNS-Serveradressen, indem Sie das Kontrollkästchen **DHCPv6 zum Abrufen von DNS-Serveradressen verwenden** auswählen. Wenn Sie nicht DHCP zum Abrufen der DNS-Server-Adressen verwenden, geben Sie die IP-Adressen in die Felder **Bevorzugter DNS-Server** und **Alternativer DNS-Server** ein. Der Standardwert lautet **Nicht markiert**. **ANMERKUNG:** Wenn das Kontrollkästchen **DHCPv6 zum Abrufen von DNS-Serveradressen verwenden** markiert ist, können IP-Adressen nicht in die Felder **Bevorzugter DNS-Server** und **Alternativer DNS-Server** eingegeben werden.
Bevorzugter DNS-Server	Konfiguriert die statische IPv6-Adresse für den bevorzugten DNS-Server. Heben Sie zum Ändern dieser Einstellung die Auswahl von **DHCP zum Abrufen von DNS-Serveradressen verwenden** auf.

Tabelle 5-2. Netzwerkeinstellungen *(fortgesetzt)*

Einstellung	Beschreibung
Alternativer DNS-Server	Konfiguriert die statische IPv6-Adresse für den alternativen DNS-Server. Heben Sie zum Ändern dieser Einstellung die Auswahl von **DHCP zum Abrufen von DNS-Serveradressen verwenden** auf.

Tabelle 5-3. IPMI-Einstellungen

Einstellung	Beschreibung
IPMI-über-LAN aktivieren	Wenn markiert, weist dies darauf hin, dass der IPMI-LAN-Kanal aktiviert ist. Die Standardeinstellung lautet **Nicht markiert**.
Beschränkung der Kanalberechtigungsebene	Konfiguriert die höchste Berechtigungsebene für den Benutzer, die auf dem LAN-Kanal akzeptiert werden kann. Wählen Sie eine der folgenden Optionen aus: **Administrator, Operator** oder **Benutzer**. Die Standardeinstellung ist **Administrator**.
Encryption Key (Verschlüsselungsschlüssel)	Konfiguriert den Verschlüsselungsschlüssel. Der Verschlüsselungsschlüssel muss aus einer geraden Anzahl von maximal 40 hexadezimalen Zeichen ohne Leerzeichen bestehen. Der standardmäßige IPMI-Verschlüsselungsschlüssel besteht ausschließlich aus Nullen.

Tabelle 5-4. VLAN-Einstellungen

Schaltfläche	Beschreibung
VLAN-ID aktivieren	**Ja** – Aktiviert. **Nein** – Deaktiviert. Wenn aktiviert, wird nur abgestimmter VLAN-ID-Datenverkehr (virtuelles LAN) akzeptiert. **ANMERKUNG:** Die VLAN-Einstellungen können nur über die CMC-Webschnittstelle konfiguriert werden. iDRAC6 zeigt nur den aktuellen Aktivierungsstatus an; die Einstellungen auf diesem Bildschirm können nicht modifiziert werden.
VLAN ID	VLAN-ID-Feld von 802.1g-Feldern. Zeigt einen Wert von 1 bis 4094 (außer 4001 bis 4020) an.
Priorität	Prioritätsfeld von 802.1g-Feldern. Dies wird zum Identifizieren der Priorität der VLAN-ID verwendet und zeigt einen Wert von 0 bis 7 als VLAN-Priorität an.

Tabelle 5-5. Schaltflächen der Seite Netzwerkkonfiguration

Schaltfläche	Beschreibung
Erweiterte Einstellungen	Zeigt den Bildschirm **Netzwerksicherheit** an und ermöglicht, die Attribute für den IP-Bereich und die IP-Blockierung einzugeben.
Anwenden	Speichert alle neuen Einstellungen, die Sie auf der Seite Netzwerkkonfiguration vorgenommen haben. **ANMERKUNG:** Wenn Sie Änderungen an den Einstellungen der NIC-IP-Adresse vornehmen, werden alle Benutzersitzungen geschlossen, und Benutzer müssen unter Verwendung der aktualisierten IP-Adresseneinstellungen eine neue Verbindung zur iDRAC6-Webschnittstelle herstellen. Alle anderen Änderungen erfordern, dass die NIC zurückgesetzt wird, was eine kurzzeitige Unterbrechung der Verbindungen verursachen kann.

IP-Filterung und IP-Blockierung konfigurieren

ANMERKUNG: Zur Ausführung der nachfolgenden Schritte müssen Sie die Berechtigung **iDRAC6 konfigurieren** besitzen.

1. Klicken Sie auf **System→ iDRAC-Einstellungen**.
2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit**.

   Der Bildschirm **Netzwerk** wird angezeigt.
3. Klicken Sie auf **Erweiterte Einstellungen**.

   Der Bildschirm **Netzwerksicherheit** wird angezeigt.
4. Konfigurieren Sie die IP-Filterungs- und IP-Blockierungseinstellungen wie erforderlich. Sie finden unter Tabelle 5-6 Beschreibungen der Einstellungen zur IP-Filterung und IP-Blockierung.
5. Auf **Anwenden klicken**, um die Einstellungen zu speichern.

Tabelle 5-6. Einstellungen zu IP-Filterung und -Blockierung

Einstellungen	Beschreibung
IP-Bereich aktiviert	Aktiviert die Funktion zum Prüfen des IP-Bereichs, mit der eine Reihe von IP-Adressen definiert wird, die auf den iDRAC6 zugreifen können. Die Standardeinstellung ist **Deaktiviert**.
IP-Bereichs-Adresse	Bestimmt die akzeptable IP-Subnetzadresse. Die Standardeinstellung ist **192.168.1.0**.
IP-Bereichs-Subnetzmaske	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Subnetzmaske muss in Form einer Netzmaske sein, wobei die bedeutenderen Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu nur Nullen (0) in den niederwertigeren Bits. Der Standardwert ist **255.255.255.0**.
IP-Blockierung aktiviert	Aktiviert die IP-Adressen-Blockierungsfunktion, mit der während einer festgelegten Zeitspanne die Anzahl von Anmeldungsfehlversuchen einer spezifischen IP-Adresse eingeschränkt wird. Die Standardeinstellung ist **Deaktiviert**.
IP-Blockierung, Zählung von Fehlversuchen	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche von dieser Adresse zurückgewiesen werden. Die Standardeinstellung ist **10**.
IP-Blockierung, Fenster der Fehlversuche	Bestimmt die Zeitspanne in Sekunden, während der ?die gezählten IP-Blockierungsfehlversuche auftreten müssen, um die IP-Blockierungs-Penalty-Zeit auszulösen. Die Standardeinstellung ist **3600**.
IP-Blockierung, Strafzeit	Der Zeitraum in Sekunden, während dessen Anmeldeversuche von einer IP-Adresse auf Grund übermäßiger Fehler abgewiesen werden. Die Standardeinstellung ist **3600**.

Plattformereignisse konfigurieren

Die Plattformereigniskonfiguration enthält einen Mechanismus zur Konfiguration des iDRAC6, damit auf bestimmte Ereignismeldungen hin ausgewählte Maßnahmen getroffen werden können. Die Maßnahmen schließen ein: Keine Maßnahme, System neu starten, System aus- und einschalten, System ausschalten und Warnung erstellen (Plattformereignis-Trap [PET] und/oder E-Mail).

Die filterbaren Plattformereignisse sind unter Tabelle 5-7 aufgeführt.

Tabelle 5-7. Filterbare Plattformereignisse

Stichwortverzeichnis	Plattformereignis
1	Assertionsfilter Batteriewarnung
2	Assertionsfilter Batterie kritisch
3	Assertionsfilter Spannung kritisch
4	Assertionsfilter Temperaturwarnung
5	Assertionsfilter Temperatur kritisch
6	Assertionsfilter Prozessor kritisch
7	Assertionsfilter Prozessor nicht vorhanden/kritisch
8	Assertionsfilter Ereignisprotokoll kritisch
9	Assertionsfilter Watchdog kritisch
10	Assertionsfilter wechselbarer Flash-Datenträger – Warnung
11	Assertionsfilter wechselbarer Flash-Datenträger nicht vorhanden – Zur Information
12	Assertionsfilter wechselbarer Flash-Datenträger – Kritisch
13	Filter Redundanz verloren
14	Assertionsfilter Sicherheitsschlüsselverwaltung kritisch

Wenn ein Plattformereignis auftritt (z. B. eine *Batteriesondenwarnung*), wird ein Systemereignis erstellt und im Systemereignisprotokoll (SEL) eingetragen. Wenn dieses Ereignis mit einem Plattformereignisfilter (PEF) übereinstimmt, der aktiviert ist, und der Filter so konfiguriert ist, dass er eine Warnung erstellt (PET oder E-Mail), wird eine PET- oder E-Mail-Warnung an ein oder mehrere konfigurierte Ziele gesendet.

Wenn derselbe Plattformereignisfilter auch zur Ausführung einer Maßnahme (z. B. ein Systemneustart) konfiguriert ist, wird die Maßnahme ausgeführt.

Plattformereignisfilter (PEF) konfigurieren

ANMERKUNG: Konfigurieren Sie zunächst die Plattformereignisfilter, bevor Sie die Plattformereignis-Traps oder E-Mail-Warnungseinstellungen konfigurieren.

1. Melden Sie sich an der iDRAC6-Webschnittstelle an.
2. Klicken Sie auf **System** und dann auf das Register **Warnungsverwaltung**.

   Der Bildschirm **Plattformereignisse** wird angezeigt.
3. Aktivieren Sie das Kontrollkästchen **Plattformereignisfilter-Warnungen**. Sie müssen diese Option für jede Plattformwarnung wählen, die an eine gültige Adresse gesendet werden soll.
4. Wählen Sie eine der folgenden Aktionen, die Sie jeweils für ein Ereignis aktivieren wollen:
   - Neustart des Systems - Tritt ein Ereignis auf, startet das System neu (Warmstart).
   - Ein- und wieder Ausschalten des Systems - Tritt ein Ereignis auf, schaltet das System ab, trennt die Stromversorgung und startet dann neu (Kaltstart).
   - Ausschalten des Systems - Tritt ein Ereignis auf, schaltet das System ab und trennt die Stromversorgung.
   - Keine Aktion - Tritt ein Ereignis auf, wird keine Aktion durchgeführt. Dies ist die Standardeinstellung für ein Ereignis.
5. Wählen Sie die Option **Warnung erstellen** neben allen Ereignissen aus, für die eine Warnung erstellt werden soll.

ANMERKUNG: Die Warnungserstellung kann für alle Ereignisse aktiviert oder deaktiviert werden, indem Sie das Kontrollkästchen neben der Spaltenüberschrift **Warnung erstellen** markieren oder dessen Markierung aufheben.

6. Klicken Sie auf **Anwenden**.

Plattformereignis-Traps (PET) konfigurieren

ANMERKUNG: Sie müssen über die Berechtigung **iDRAC konfigurieren** verfügen, um SNMP-Warnungen hinzuzufügen oder zu aktivieren/deaktivieren. Die folgenden Optionen stehen nur dann zur Verfügung, wenn Sie die Berechtigung **iDRAC konfigurieren** besitzen.

1 Melden Sie sich an der iDRAC6-Webschnittstelle an.

2 Vergewissern Sie sich, dass Sie die unter „Plattformereignisfilter (PEF) konfigurieren“ auf Seite 100beschriebenen Verfahren ausgeführt haben.

3 Klicken Sie auf **System** und dann auf die Registerkarte **Warnungsverwaltung**.

Der Bildschirm **Plattformereignisse** wird angezeigt.

4 Klicken Sie auf **Trap-Einstellungen**.

Der Bildschirm **Trap-Einstellungen** wird eingeblendet.

5 Konfigurieren Sie die PET-Ziel-IP-Adresse:

a Klicken Sie auf das Kontrollkästchen **Aktiviert** neben der **Zielnummer**, die Sie aktivieren möchten.

b Geben Sie in das entsprechende Feld für die IPv4- oder IPv6-**Ziel-IP-Adresse** eine IP-Adresse ein.

c Klicken Sie auf **Anwenden**.

ANMERKUNG: Konfigurieren Sie den Wert **Community-Zeichenkette**, um erfolgreich einen Trap zu senden. Der Wert **Community-Zeichenkette** weist auf die Community-Zeichenkette hin, die für ein SNMP-Warnungs-Trap (einfaches Netzwerkverwaltungsprotokoll) verwendet werden soll, das vom iDRAC6 gesendet wird. SNMP-Warnungs-Traps werden vom iDRAC6 übertragen, wenn ein Plattformereignis auftritt. Die Standardeinstellung für die **Community-Zeichenkette** ist **Öffentlich**.

d Um die konfigurierte Warnung zu testen, klicken Sie auf **Senden**.

e Um eine weitere Ziel-IP-Adresse hinzuzufügen, wiederholen Sie die SchritteSchritt a bis Schritt d. Sie können bis zu vier IPv4- und vier IPv6-Zieladressen angeben.

Konfiguration von E-Mail-Warnungen

1 Melden Sie sich an der iDRAC6-Webschnittstelle an.

2 Vergewissern Sie sich, dass Sie die unter „Plattformereignisfilter (PEF) konfigurieren“ auf Seite 100beschriebenen Verfahren ausgeführt haben.

3 Klicken Sie auf **System** und dann auf das Register **Warnungsverwaltung**.

Der Bildschirm **Plattformereignisse** wird angezeigt.

4 Klicken Sie auf **E-Mail-Warnungseinstellungen**.

Der Bildschirm **E-Mail-Warnungseinstellungen** wird angezeigt.

5 Konfigurieren Sie das E-Mail-Warnungsziel.

a Klicken Sie auf das Kontrollkästchen **Aktiviert** für die erste undefinierte E-Mail-Warnung.

b Geben Sie eine gültige E-Mail-Adresse in das Feld **Ziel-E-Mail-Adresse** ein.

c Klicken Sie auf **Anwenden**.

ANMERKUNG: Zum erfolgreichen Senden einer Test-E-Mail muss der SMTP- (E-Mail-) Server im Abschnitt **SMTP- (E-Mail-) Server-Adresseneinstellungen** auf dem Bildschirm **E-Mail-Warnungseinstellungen** konfiguriert werden. Geben Sie einen SMTP-Server in das dafür vorgesehene Feld ein, entweder im punktseparierten Format (z. B. 192.168.1.1) oder als DNS-Namen. Die IP-Adresse des SMTP-Servers sendet bei Eintreten eines Plattformereignisses E-Mail-Warnungen an iDRAC.

d Geben Sie in das Feld **Quell-E-Mail-Name ändern** den Ausgangspunkt der E-Mail-Warnung an oder lassen Sie das Feld leer, um den Standard-E-Mail-Absender zu verwenden. Die Standardeinstellung ist blade_slot@iDRAC6 IP-Adresse.

- Wenn das Feld **Quell-E-Mail-Name ändern** leer gelassen wird, der iDRAC6-Hostname konfiguriert und der DNS-Domänenname aktiv ist, lautet die Quell-E-Mail-Adresse <iDRAC6-Hostname>@<DNS-Domänenname>.
- Wenn das Feld leer gelassen wird, der iDRAC6-Hostname nicht eingetragen und der DNS-Domänenname aktiv ist, lautet die Quell-E-Mail-Adresse:<iDRAC6 Slot*x*>@<DNS-Domänenname>.
- Wenn das Feld leer gelassen wird und der iDRAC6-Hostname und der DNS-Domänenname nicht eingetragen sind, lautet die Quell-E-Mail-Adresse:<iDRAC6 Slot*x*>@<<iDRAC6 IP-Adresse>.
- Wenn im Feld „eine Zeichenkette ohne @“ eingetragen und der DNS-Domänenname aktiv ist, lautet die Quell-E-Mail-Adresse: <eine Zeichenkette ohne @>@<DNS-Domänenname>.
- Wenn im Feld „eine Zeichenkette ohne @“ eingetragen und der DNS-Domänenname nicht eingetragen ist, lautet die Quell-E-Mail-Adresse: <eine Zeichenkette ohne @>@<iDRAC6 IP-Adresse>.
- Wenn im Feld „eine Zeichenkette mit @“ eingetragen und der DNS-Domänenname aktiv ist, lautet die Quell-E-Mail-Adresse: <eine Zeichenkette mit @>@<DNS-Domänenname>.

- Wenn im Feld „eine Zeichenkette mit @“ eingetragen und der DNS-Domänenname nicht eingetragen ist, lautet die Quell-E-Mail-Adresse: <eine Zeichenkette mit @>@<iDRAC6 IP-Adresse>.

e Klicken Sie auf **Senden**, um die konfigurierte E-Mail-Warnung zu testen (falls gewünscht).

f Um ein weiteres E-Mail-Warnungsziel hinzuzufügen, wiederholen Sie die Schritte **Schritt a** bis **Schritt e**. Sie können bis zu vier E-Mail-Warnungsziele angeben.

IPMIüber LAN konfigurieren

1 Melden Sie sich an der iDRAC6-Webschnittstelle an.

2 Konfigurieren Sie IPMI über LAN.

a Klicken Sie auf **System→ iDRAC-Einstellungen** und dann auf das Register **Netzwerk/Sicherheit**.

Der Bildschirm **Netzwerk** wird angezeigt.

b Klicken Sie auf **IPMI-Einstellungen**.

c Klicken Sie auf das Kontrollkästchen **IPMI-über-LAN aktivieren**.

d Aktualisieren Sie, falls erforderlich, die **Beschränkung der Kanalberechtigungsebene**:

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.

Klicken Sie unter **IPMI-Einstellungen** auf das Drop-Down-Menü **Beschränkung der Kanalberechtigungsebene**, wählen Sie **Administrator**, **Operator** oder **Benutzer** aus, und klicken Sie auf **Anwenden**.

e Stellen Sie den IPMI-LAN-Kanalverschlüsselungsschlüssel ein, falls erforderlich.

ANMERKUNG: iDRAC6-IPMI unterstützt das RMCP+-Protokoll.

Geben Sie unter **IPMI-Einstellungen** im Feld **Verschlüsselungsschlüssel** den Verschlüsselungsschlüssel ein.

f Klicken Sie auf **Anwenden**.

3 IPMI Seriell über LAN (SOL) konfigurieren:

a Klicken Sie auf **System→ iDRAC-Einstellungen** und dann auf das Register **Netzwerk/Sicherheit**.

Der Bildschirm **Netzwerk** wird angezeigt.

b Klicken Sie auf das Register **Seriell über LAN**.

c Wählen Sie **Seriell über LAN aktivieren** aus.

d Aktualisieren Sie die IPMI-SOL-**Baudrate**, falls erforderlich, indem Sie aus dem **Baudraten**-Drop-Down-Menü eine Datengeschwindigkeit auswählen.

ANMERKUNG: Wenn die serielle Konsole über das LAN umgeleitet werden soll, ist sicherzustellen, dass die SOL-**Baudrate** mit der Baudrate des verwalteten Servers identisch ist.

e Klicken Sie auf **Anwenden**.

f Konfigurieren Sie auf der Seite **Erweiterte Einstellungen** je nach Bedarf die IP-Filterungs- und IP-Blockierungseinstellungen.

iDRAC6-Benutzer hinzufügen und konfigurieren

Um das System mit dem iDRAC6 zu verwalten und die Systemsicherheit zu erhalten, erstellen Sie eindeutige Benutzer mit spezifischen Verwaltungsberechtigungen (oder *rollenbasierter Autorität*).

Um iDRAC6-Benutzer hinzuzufügen und zu konfigurieren, führen Sie folgende Schritte aus:

ANMERKUNG: Zum Ausführen der nachfolgenden Schritte müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

1 Klicken Sie auf **System→ iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Benutzer**.

Der Bildschirm **Benutzer** zeigt für die einzelnen Benutzer Benutzer-ID, Zustand, Benutzername, IPMI-LAN-Berechtigungen, iDRAC6-Berechtigungen sowie Seriell über LAN-Fähigkeit an.

ANMERKUNG: Benutzer-1 ist für den anonymen IPMI-Benutzer reserviert und kann nicht konfiguriert werden.

2 In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.

3 Auf der Seite **Benutzer-Hauptmenü** (siehe Tabelle 5-8, Tabelle 5-9 und Tabelle 5-10) können Sie einen Benutzer konfigurieren, einen öffentlichen SSH-Schlüssel hochladen oder einen angegebenen oder alle SSH-Schlüssel anzeigen oder löschen.

Authentifizierung mit öffentlichem Schlüssel über SSH.

iDRAC6 unterstützt die Authentifizierung mit öffentlichem Schlüssel (PKA) über SSH. Diese Authentifizierungsmethode verbessert die SSH-Skripting-Automatisierung, da keine Benutzer-ID/kein Kennwort eingebettet ist bzw. keine Eingabeaufforderung erfolgt.

Bevor Sie beginnen

Sie können bis zu 4 öffentliche Schlüssel *pro Benutzer* konfigurieren, die über eine SSH-Schnittstelle verwendet werden können. Stellen Sie sicher, dass Sie vor dem Hinzufügen oder Löschen öffentlicher Schlüssel unbedingt den Anzeigebefehl verwenden, um zu sehen, welche Schlüssel bereits eingerichtet sind, sodass kein Schlüssel versehentlich überschrieben oder gelöscht wird. Wenn die PKA über SSH richtig eingestellt und verwendet wird, müssen Sie für die Anmeldung bei iDRAC 6 kein Kennwort eingeben. Das kann sehr nützlich sein für automatisierte Skripts zur Durchführung verschiedener Funktionen.

Beachten Sie vor dem Einrichten dieser Funktionen Folgendes:

- Sie können diese Funktion mit RACADM und auch über die GUI verwalten.
- Beim Hinzufügen neuer öffentlicher Schlüssel müssen Sie sicherstellen, dass bestehende Schlüssel nicht bereits den Index belegen, zu dem der neue Schlüssel hinzugefügt werden soll. Der iDRAC6 führt vor dem Hinzufügen eines Schlüssels keine Prüfungen durch, um sicherzustellen, dass keine vorherigen Schlüssel gelöscht werden. Sobald ein neuer Schlüssel hinzugefügt wurde, tritt er automatisch in Kraft, solange die SSH-Schnittstelle aktiviert ist.

Generieren öffentlicher Schlüssel für Windows

Vor dem Hinzufügen eines Kontos ist ein öffentlicher Schlüssel von dem System erforderlich, das über SSH auf den iDRAC6 zugreift. Es gibt zwei Möglichkeiten, das öffentliche/private Schlüsselpaar zu generieren: mit der *Schlüsselgeneratoranwendung PuTTY* für Clients unter Windows bzw. mit *ssh-keygen* CLI für Clients unter Linux. Das *ssh-keygen* CLI-Dienstprogramm ist in allen Standardinstallationen enthalten.

Dieser Abschnitt enthält einfache Anweisungen zum Generieren eines öffentlichen/privaten Schlüsselpaars für beide Anwendungen. Weitere Informationen über erweiterte Funktionen dieser Hilfsprogramme finden Sie in der Anwendungshilfe.

So verwenden Sie den *PuTTY-Schlüsselgenerator* für Windows-Clients zum Erstellen des Grundschlüssels:

1. Starten Sie die Anwendung und wählen Sie entweder SSH-2 RSA oder SSH-2 DSA als Typ des zu generierenden Schlüssels aus. SSH-1 wird nicht unterstützt.
2. Geben Sie die Anzahl Bits für den Schlüssel ein. RSA und DSA sind die einzigen unterstützten Schlüsselerstellungsalgorithmen. Die Anzahl muss für RSA zwischen 768 und 4096 Bits liegen und für DSA 1024 Bits betragen.
3. Klicken Sie auf **Generieren** und bewegen Sie die Maus gemäß Anleitung im Fenster. Nachdem der Schlüssel erstellt wurde, können Sie das Schlüsselanmerkungsfeld ändern. Sie können auch einen Kennsatz eingeben, um den Schüssel sicher zu machen. Stellen Sie sicher, dass Sie den privaten Schüssel speichern.
4. Sie können den öffentlichen Schlüssel mit der Option **Öffentlichen Schlüssel speichern** in einer Datei speichern, um ihn später hochzuladen. Alle hochgeladenen Schlüssel müssen im RFC 4716- oder openSSH-Format sein. Ist dies nicht der Fall, müssen Sie die Schlüssel in diese Formate umwandeln.

Generieren öffentlicher Schlüssel für Linux

Die Anwendung *ssh-keygen* für Linux-Clients ist ein Befehlszeilendienstprogramm ohne grafische Benutzeroberfläche.

Öffnen Sie ein Terminalfenster und geben bei der Shell-Eingabeaufforderung Folgendes ein:

```
ssh-keygen –t rsa –b 1024 –C testing
```

ANMERKUNG: Bei den Optionen wird zwischen Groß- und Kleinschreibung unterschieden.

wobei

-t entweder *dsa* oder *rsa* sein kann.

–b die Bit-Verschlüsselungsgröße zwischen 768 und 4096 angibt.

–C das Ändern der Anmerkung des öffentlichen Schlüssels ermöglicht und optional ist.

Laden Sie nach Ausführung des Befehls den öffentlichen Schlüssel hoch.

ANMERKUNG: Schlüssel, die mit ssh-keygen auf der Linux Management Station erstellt werden, sind nicht im RFC4716- sondern im openSSH-Format. Die öffentlichen Schlüssel im openSSH-Format können auf den iDRAC6 hochgeladen werden. Der Algorithmus für öffentliche Schlüssel des iDRAC6 bestätigt Schlüssel im openSSH- und im RFC4716-Format, wandelt RFC4716-Schlüssel intern in das openSSH-Format um und speichert die Schlüssel dann intern.

ANMERKUNG: iDRAC6 unterstützt nicht die ssh-agent-Weiterleitung von Schlüsseln.

Anmeldung mit Authentifizierung mit öffentlichem Schlüssel

Nachdem die öffentlichen Schlüssel hochgeladen wurden, können Sie sich über SSH beim iDRAC6 anmelden, ohne ein Kennwort einzugeben. Sie können auch einen einzelnen RACADM-Befehl als Befehlszeilenargument an die SSH-Anwendung senden. Die Befehlszeilenoptionen verhalten sich wie Remote-RACADM, da die Sitzung endet, wenn der Befehl abgeschlossen ist.

Zum Beispiel:

Anmeldung:

```
SSH-Benutzername@<Domäne>
```

oder

```
SSH-Benutzername@<IP-Adresse>
```

wobei „IP_Adresse“ die IP-Adresse des iDRAC6 ist.

Senden von RACADM-Befehlen:

```
SSH-Benutzername@<Domäne> racadm getversion
```

```
SSH-Benutzername@<Domäne> racadm getsel
```

Unter „SSH-Schlüssel mit RACADM hochladen, anzeigen oder löschen“ auf Seite 303 finden Sie Informationen zum Hochladen, Anzeigen und Löschen von SSH-Schlüsseln mit RACADM.

Tabelle 5-8. SSH-Schlüsselkonfigurationen

Option	Beschreibung
SSH-Schlüssel hochladen	Ermöglicht lokalen Benutzern, eine öffentliche SSH-Schlüsseldatei hochzuladen. Beim Hochladen eines Schlüssels wird der Inhalt der Schlüsseldatei auf der Seite **Benutzerkonfiguration** in einem schreibgeschützten Textfeld angezeigt.
SSH-Schlüssel anzeigen/entfernen	Ermöglicht lokalen Benutzern, einen angegebenen SSH-Schlüssel oder alle SSH-Schlüssel anzuzeigen oder zu löschen.

Über die Seite **SSH-Schlüssel hochladen** können Sie einen öffentlichen SSH-Schlüssel hochladen. Beim Hochladen eines Schlüssels wird der Inhalt der Schlüsseldatei auf der Seite **SSH-Schlüssel anzeigen/entfernen** in einem schreibgeschützten Textfeld angezeigt.

VORSICHTSHINWEIS: 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. Weitere Informationen finden Sie unterTabelle 5-13.

Tabelle 5-9. SSH-Schlüssel hochladen

Option	Beschreibung
Datei/Text	Wählen Sie die Option **Datei** aus und geben Sie den Pfad zum Speicherort des Schlüssels ein. Sie können auch die Option **Text** auswählen und den Inhalt der Schlüsseldatei in das Feld einfügen. Sie können einen oder mehrere neue Schlüssel hochladen oder vorhandene Schlüssel überschreiben. Um eine Schlüsseldatei hochzuladen, klicken Sie auf **Durchsuchen**, wählen die Datei aus und klicken dann auf die Schaltfläche **Anwenden**. **ANMERKUNG:** Die Option zum Einfügen von Schlüsseltext wird für öffentliche Schlüssel im openSSH-Format unterstützt. Für Schlüssel im RFC4716-Format wird die Texteinfügeoption nicht unterstützt.
Durchsuchen	Klicken Sie auf diese Schaltfläche, um den vollständigen Pfad und den Dateinamen des Schlüssels ausfindig zu machen.

Die Seite **SSH-Schlüssel anzeigen/entfernen** ermöglicht Ihnen, öffentliche SSH-Schlüssel eines Benutzers anzuzeigen oder zu entfernen.

Tabelle 5-10. SSH-Schlüssel anzeigen/entfernen

Option	Beschreibung
Entfernen	Der hochgeladene Schlüssel wird im Feld angezeigt. Wählen Sie die Option **Entfernen** aus und klicken Sie auf **Anwenden,** um den vorhandenen Schlüssel zu löschen.

1 Wenn Sie **Benutzer konfigurieren** auswählen und auf **Weiter** klicken, wird die Seite Benutzerkonfiguration angezeigt.

2 Konfigurieren Sie die Eigenschaften und Berechtigungen des jeweiligen Benutzers auf der Seite **Benutzerkonfiguration**.

Tabelle 5-11 beschreibt die **allgemeinen** Einstellungen zur Konfiguration eines Benutzernamens und -kennworts für iDRAC6.

Tabelle 5-12 beschreibt die **IPMI-LAN-Berechtigungen** zum Konfigurieren der LAN-Berechtigungen des Benutzers.

Tabelle 5-13 beschreibt die **Benutzergruppen**-Berechtigungen für die Einstellungen der **IPMI-LAN-Berechtigungen** und der iDRAC6-**Benutzerberechtigungen**.

Tabelle 5-14 beschreibt **iDRAC6-Gruppenberechtigungen**. Wenn Sie eine **iDRAC6-Benutzerberechtigung** zum **Administrator**, **Hauptbenutzer** oder **Gastbenutzer** hinzufügen, ändert sich die iDRAC6-**Gruppe** zur **benutzerdefinierten** Gruppe.

3 Wenn Sie fertig sind, klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Tabelle 5-11. Allgemeine Eigenschaften

Eigenschaft	Beschreibung
Benutzer-ID	Enthält eine von 16 voreingestellten Benutzer-ID-Nummern. Dieses Feld darf nicht bearbeitet werden.
Benutzer aktivieren	Wenn **Markiert**, weist dies darauf hin, dass der Benutzerzugriff auf den iDRAC6 aktiviert ist. Wenn das Feld **Nicht markiert** ist, ist der Benutzerzugriff deaktiviert.
Benutzername	Gibt einen iDRAC6-Benutzernamen von bis zu 16 Zeichen an. Jeder Benutzer muss einen eindeutigen Benutzernamen besitzen. • 0-9 • A-Z • a-z • Sonderzeichen: + % = , - {] § ! (? ; _ } I #) * : $ [| **ANMERKUNG:** Wenn der Benutzername geändert wird, erscheint der neue Name erst bei der nächsten Benutzeranmeldung in der Benutzeroberfläche.

Tabelle 5-11. Allgemeine Eigenschaften *(fortgesetzt)*

Eigenschaft	Beschreibung
Kennwort ändern	Aktiviert die Felder **Neues Kennwort** und **Neues Kennwort bestätigen**. Wenn diese Option nicht markiert ist, kann das Kennwort des Benutzers nicht geändert werden.
Neues Kennwort	Aktiviert die Bearbeitung des Kennworts des iDRAC6-Benutzers. Geben Sie ein **Kennwort** mit bis zu 20 Zeichen ein. Die Zeichen werden nicht angezeigt. • 0-9 • A-Z • a-z • Sonderzeichen: + % = , - {] . ! (? ; _ } I | #) * : $ [/ @
Neues Kennwort bestätigen	Geben Sie das iDRAC6-Benutzerkennwort erneut ein, um es zu bestätigen.

ANMERKUNG: iDRAC6 ermöglicht die Erstellung von Benutzernamen mit den in Tabelle 5-12 beschriebenen unterstützten Zeichen. Einige wenige Begrenzungszeichen werden jedoch nicht in allen Schnittstellen unterstützt, wie z. B. in RACADM. Verzeichnisdienste verfügen ebenfalls über bestimmte Einschränkungen in Bezug auf das Benutzernamenformat.

Tabelle 5-12. IPMI-LAN-Berechtigung

Eigenschaft	Beschreibung
Maximale LAN-Benutzerberechtigung gewährt	Legt die maximale Berechtigung des Benutzers auf dem IPMI-LAN-Kanal auf eine der folgenden Benutzergruppen fest: **Keine**, **Administrator**, **Operator** oder **Benutzer**.
Seriell über LAN aktivieren	Ermöglicht dem Benutzer, IPMI seriell über LAN zu verwenden. Wenn **Markiert**, ist diese Berechtigung aktiviert.

Tabelle 5-13. Andere Berechtigung

Eigenschaft	Beschreibung
iDRAC6-Gruppe	Legt die maximale iDRAC6-Benutzerberechtigung als eine der Folgenden fest: **Administrator**, **Hauptbenutzer**, **Gastbenutzer**, **Benutzerdefiniert** oder **Keine**. Siehe Tabelle 5-14 zu **iDRAC6-Gruppen**-Berechtigungen.
Anmeldung am iDRAC6	Ermöglicht dem Benutzer, sich am iDRAC6 anzumelden.
iDRAC6 konfigurieren	Ermöglicht dem Benutzer, den iDRAC6 zu konfigurieren.
Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern den Zugriff auf das System zu erlauben. **VORSICHTSHINWEIS: 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.**
Protokolle löschen	Ermöglicht dem Benutzer, die iDRAC6-Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer, RACADM-Befehle auszuführen.
Auf die virtuelle Konsole zugreifen	Ermöglicht dem Benutzer, die virtuelle Konsole auszuführen. **VORSICHTSHINWEIS: Diese Berechtigung ist im Normalfall für Benutzer reserviert, die Mitglieder der Administrator- oder Hauptbenutzergruppe auf iDRAC sind. Benutzer mit der Berechtigung zum Zugriff auf die virtuelle Konsole sind nicht nur in der Lage, die virtuelle Konsole zu benutzen, sondern können auch in der iDRAC6-Webschnittstelle die Aktivitäten jeder Person einsehen, die die virtuelle Konsole verwendet. Weisen Sie diese Berechtigung daher mit Bedacht zu.**

Tabelle 5-13. Andere Berechtigung *(fortgesetzt)*

Eigenschaft	Beschreibung
Zugriff auf virtuelle Datenträger	Ermöglicht dem Benutzer, virtuelle Datenträger auszuführen und zu verwenden.
Testwarnungen	Ermöglicht dem Benutzer, Testwarnungen (E-Mail und PET) an alle derzeit konfigurierten Warnungsempfänger zu senden.
Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Tabelle 5-14. iDRAC6-Gruppen-Berechtigungen

User Group (Benutzergruppe)	Gewährte Berechtigungen
Administrator	Am iDRAC6 anmelden, iDRAC6 konfigurieren, Benutzer konfigurieren, Protokolle löschen, Serversteuerungsbefehle ausführen, Zugriff auf die virtuelle Konsole, Zugriff auf virtuelle Datenträger, Testwarnungen, Diagnosebefehle ausführen
Hauptbenutzer	Am iDRAC6 anmelden, Protokolle löschen, Serversteuerungsbefehle ausführen, Zugriff auf die virtuelle Konsole, Zugriff auf virtuelle Datenträger, Testwarnungen
Gastbenutzer	Anmeldung am iDRAC6
Custom (Benutzerdefiniert)	Wählt eine beliebige Kombination der folgenden Berechtigungen aus: Am iDRAC6 anmelden, iDRAC6 konfigurieren, Benutzer konfigurieren, Protokolle löschen, Serversteuerungsbefehle ausführen, Zugriff auf die virtuelle Konsole, Zugriff auf virtuelle Datenträger, Testwarnungen, Diagnosebefehle ausführen
NONE	Keine zugewiesenen Berechtigungen

iDRAC6-Datenübertragung mit SSL und digitalen Zertifikaten sichern

Dieser Abschnitt enthält Informationen über die folgenden Datensicherheitsfunktionen, die in Ihrem iDRAC6 integriert sind:

- Secure Sockets Layer (SSL)
- Zertifikatsignierungsanforderung (CSR)
- Zugriff auf das SSL-Hauptmenü
- Neues CSR erstellen
- Serverzertifikat hochladen
- Serverzertifikat anzeigen

Secure Sockets Layer (SSL)

Der iDRAC6 beinhaltet einen Webserver, der zur Verwendung des standardisierten SSL-Sicherheitsprotokolls konfiguriert wurde, um verschlüsselte Daten über ein Netzwerk zu übertragen. SSL baut auf öffentlicher und privater Verschlüsselungstechnologie auf und ist eine allgemein akzeptierte Technologie, die authentifizierte und verschlüsselte Kommunikationen zwischen Clients und Servern bietet, um unbefugtes Abhören auf dem Netzwerk zu verhindern.

Ein SSL-aktiviertes System kann die folgenden Aufgaben ausführen:

- Sich an einem SSL-aktivierten Client authentifizieren
- Dem Client erlauben, sich am Server zu authentifizieren
- Beiden Systemen gestatten, eine verschlüsselte Verbindung herzustellen

Das Verschlüsselungsverfahren bietet eine hohe Stufe von Datenschutz. Der iDRAC6 verwendet den SSL 128-Bit-Verschlüsselungsstandard, die sicherste Form der Verschlüsselung, die für Webbrowser in Nordamerika allgemein verfügbar ist.

Der iDRAC6-Web Server enthält standardmäßig ein selbstsigniertes Dell-SSL-Digitalzertifikat (Server-ID). Um für Internetübertragungen eine hohe Sicherheitsstufe zu gewährleisten, ersetzen Sie das Web Server-SSL-Zertifikat durch ein Zertifikat, das von einer bekannten Zertifizierungsstelle (CA) signiert wurde. Eine Zertifizierungsstelle ist ein Unternehmen, das in der IT-Industrie dafür anerkannt ist, hohe Ansprüche bezüglich der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger

Sicherheitskriterien zu erfüllen. Beispiele für CAs umfassen Thawte und VeriSign. Um das Verfahren zum Erhalt eines signierten Zertifikats einzuleiten, können Sie die iDRAC6-Webschnittstelle zum Erstellen einer Zertifikatsignierungsanforderung (CSR) mit den Informationen Ihres Unternehmens verwenden. Sie können die erstellte CSR dann an eine Zertifizierungsstelle wie VeriSign oder Thawte senden.

Zertifikatsignierungsanforderung (CSR)

Eine CSR ist eine digitale Anforderung eines sicheren Serverzertifikats von einer Zertifizierungsstelle (CA). Sichere 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, verifiziert und bestätigt sie die darin enthaltenen Informationen. Wenn der Bewerber die Sicherheitsstandards der Zertifizierungsstelle erfüllt, gibt diese ein digital signiertes Zertifikat aus, das diesen Bewerber im Hinblick auf Transaktionen über Netzwerke und über das Internet eindeutig identifiziert.

Nachdem die CA die CSR genehmigt und das Zertifikat gesendet hat, muss das Zertifikat auf die iDRAC6-Firmware hochgeladen werden. Die auf der iDRAC6-Firmware gespeicherten CSR-Informationen müssen mit den Informationen übereinstimmen, die im Zertifikat enthalten sind, d. h. das Zertifikat muss als Reaktion auf die CSR erstellt worden sein, die vom iDRAC6 ausgegeben wurde.

Zugriff auf das SSL-Hauptmenü

1. Klicken Sie auf **System→ iDRAC-Einstellungen→** Register **Netzwerk/Sicherheit**.
2. Klicken Sie auf **SSL**, um den Bildschirm **SSL** zu öffnen.

Tabelle 5-15 beschreibt die Optionen, die zum Erstellen einer CSR verfügbar sind.

Tabelle 5-15. SSL-Hauptmenüoptionen

Feld	Beschreibung
Eine neue Zertifikatsignierungsanforderung erstellen (CSR)	Wählen Sie die Option aus und klicken Sie auf **Weiter**, um die Seite **Zertifikatsignierungsanforderung (CSR) erstellen** zu öffnen. Weitere Informationen finden Sie unter „Neue Zertifikatsignierungsanforderung erstellen“ auf Seite 115. **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 iDRAC6 nicht das Zertifikat.
Serverzertifikat hochladen	Wählen Sie die Option aus und klicken Sie auf **Weiter**, um die Seite **Zertifikat hochladen** zu öffnen und das Zertifikat hochzuladen, das Ihnen die Zertifizierungsstelle zugesandt hat. Weitere Informationen finden Sie unter „Serverzertifikat hochladen“ auf Seite 117. **ANMERKUNG:** iDRAC6 akzeptiert lediglich X509-v3-Base-64-kodierte Zertifikate. DER-kodierte Zertifikate werden nicht angenommen.
Serverzertifikat anzeigen	Wählen Sie die Option aus, und klicken Sie auf **Weiter**, um den Bildschirm **Serverzertifikat anzeigen** zu öffnen und ein vorhandenes Serverzertifikat anzuzeigen. Weitere Informationen finden Sie unter „Serverzertifikat anzeigen“ auf Seite 117.

Neue Zertifikatsignierungsanforderung 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 iDRAC6 nicht das Zertifikat.

1 Wählen Sie auf dem **SSL**-Bildschirm die Option **Neue Zertifikatsignierungsanforderung (CSR) erstellen** aus und klicken Sie auf **Weiter**.

2 Geben Sie auf der Seite **Zertifikatsignierungsanforderung (CSR) erstellen** jeweils einen Wert für die einzelnen CSR-Attribute ein.

Tabelle 5-16 beschreibt die Optionen der Seite **Zertifikatsignierungsanforderung (CSR) erstellen**.

3 Klicken Sie auf **Erstellen**, um die CSR zu erstellen.

4 Klicken Sie auf **Herunterladen**, um die CSR-Datei auf Ihre Remote-Management Station zu speichern.

Tabelle 5-16. Optionen der Seite Zertifikatsignierungsanforderung (CSR) erstellen

Feld	Beschreibung
Allgemeiner Name	Der genaue Name, der zertifiziert werden soll (normalerweise der Web Server-Domänenname, z. B. **xyzcompany.com**). Alle Zeichen außer '$' werden unterstützt.
Name der Organisation	Der mit dieser Organisation assoziierte Name (zum Beispiel, XYZ Corporation). Alle Zeichen außer '$' werden unterstützt.
Organisationseinheit	Der einer Organisationseinheit, z. B. eine IT-Abteilung zugeordnete Name. Alle Zeichen außer '$' werden unterstützt.
Ort	Die Stadt oder ein anderer Standort des Unternehmens, das zertifiziert wird (z. B. München). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie kein Unterstreichungszeichen oder andere Zeichen, um Wörter zu trennen.
Zustandsname	Das Bundesland oder der Kanton, in dem sich das Unternehmen, das sich für eine Zertifizierung bewirbt, befindet (z. B. Bayern). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie keine Abkürzungen.
Landescode	Der Name des Landes, in dem sich das Unternehmen befindet, das sich um eine Zertifizierung bewirbt.
E-Mail	Die mit der CSR verbundene E-Mail-Adresse. Geben Sie die E-Mail-Adresse der Firma oder eine beliebige mit der CSR in Zusammenhang stehende E-Mail-Adresse ein. Dieses Feld ist optional.
Schlüsselgröße	Die Größe des zu erzeugenden CSR-Schlüssels (Zertifikatsignierungsanforderung). Die Größe kann 1024 KB oder 2048 KB betragen.

Serverzertifikat hochladen

1 Auf dem **SSL**-Bildschirm wählen Sie **Serverzertifikat hochladen** aus und klicken Sie auf **Weiter**.

Der Bildschirm **Zertifikat hochladen** wird angezeigt.

2 Klicken Sie im Feld **Dateipfad** auf **Durchsuchen**, um zur Zertifikatsdatei der Management Station zu wechseln und diese anzugeben.

ANMERKUNG: Der Wert Dateipfad zeigt den Dateipfad des Zertifikats an, das Sie hochladen möchten, einschließlich dem vollständigen Pfad, dem vollständigen Dateinamen und der Dateierweiterung.

3 Klicken Sie auf **Anwenden**, um das Zertifikat in die iDRAC6-Firmware hochzuladen.

Serverzertifikat anzeigen

1 Wählen Sie auf dem **SSL**-Bildschirm **Serverzertifikat anzeigen** aus, und klicken Sie auf **Weiter**.

Tabelle 5-17 erläutert die Felder und zugehörigen Beschreibungen, die im Fenster **Serverzertifikat anzeigen** aufgeführt werden.

Tabelle 5-17. Informationen zum Serverzertifikat anzeigen

Feld	Beschreibung
Seriennummer	Seriennummer des Zertifikats
Informationen des Antragstellers	Vom Antragsteller eingegebene Zertifikatsattribute
Ausstellerinformationen	Vom Aussteller zurückgegebene Zertifikatsattribute
Gültig von	Ausgabedatum des Zertifikats
Gültig bis	Ablaufdatum des Zertifikats

Microsoft Active Directory-Zertifikate konfigurieren und verwalten

ANMERKUNG: Sie müssen über die Berechtigung **iDRAC konfigurieren** verfügen, um Active Directory konfigurieren und ein Active Directory-Zertifikat hochladen, herunterladen und anzeigen zu können.

ANMERKUNG: Weitere Informationen zur Active Directory-Konfiguration und dazu, wie Active Directory mit dem Standardschema oder einem erweiterten Schema konfiguriert wird, finden Sie unter „Verwendung des iDRAC6-Verzeichnisdiensts“ auf Seite 135.

Um auf den Zusammenfassungsbildschirm von **Microsoft Active Directory** zuzugreifen, klicken Sie auf **System→ iDRAC-Einstellungen→** Register **Netzwerk/Sicherheit→ Verzeichnisdienst→ Microsoft Active Directory**.

Tabelle 5-18 führt die Zusammenfassungsoptionen für das **Active Directory** auf. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche.

Tabelle 5-18. Optionen des Active Directory

Feld	Beschreibung
Allgemeine Einstellungen	Zeigt häufig konfigurierte Einstellungen für das Active Directory an.
Active Directory-CA-Zertifikat	Zeigt das Zertifikat der Zertifizierungsstelle an, die alle SSL-Serverzertifikate des Domänen-Controllers unterzeichnet.
Einstellungen zum Standardschema/Einstellungen zum erweiterten Schema	Abhängig von der aktuellen Active Directory-Konfiguration werden Einstellungen zum erweiterten Schema oder Einstellungen zum Standardschema angezeigt.
Active Directory konfigurieren	Klicken Sie auf diese Option, um Schritt 1 von 4 in den Active Directory-Einstellungen zu konfigurieren. Auf der Seite **Schritt 1 von 4 Active Directory** können Sie ein Active Directory-Zertifizierungsstellenzertifikat auf den iDRAC6 hochladen, das aktuelle Active Directory-Zertifizierungsstellenzertifikat anzeigen, das auf den iDRAC6 hochgeladen wurde, oder die Zertifikatsvalidierung aktivieren.

Tabelle 5-18. Optionen des Active Directory *(fortgesetzt)*

Feld	Beschreibung
Einstellungen testen	Klicken Sie auf diese Option, um die Konfiguration von Active Directory mit den von Ihnen festgelegten Einstellungen zu testen.
Kerberos-Keytab-Hochladen	Klicken Sie auf diese Option, um den Kerberos-Keytab auf den iDRAC6 hochzuladen. Informationen zum Erstellen einer Keytab-Datei finden Sie unter „Konfiguration von iDRAC6 für Einmaliges Anmelden und Smart-Card-Anmeldung“ auf Seite 183.

Active Directory konfigurieren (Standardschema und erweitertes Schema)

1. Klicken Sie auf dem Zusammenfassungsbildschirm von **Active Directory** auf **Active Directory konfigurieren**.
2. Auf dem Bildschirm **Schritt 1 von 4 Active Directory** können Sie entweder die Zertifikatsvalidierung aktivieren, das Active Directory-Zertifizierungsstellenzertifikat zum iDRAC6 hochladen oder das aktuelle Active Directory-Zertifizierungsstellenzertifikat anzeigen.

   Tabelle 5-19 beschreibt die Einstellungen und Auswahlen für die einzelnen Schritte im Verfahren zu **Active Directory-Konfiguration und -Verwaltung**. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche.

Tabelle 5-19. Einstellungen der Seite Active Directory-Konfiguration

Einstellung	Beschreibung
Schritt 1 von 4 Active Directory Konfiguration und Verwaltung	
Zertifikatsvalidierung aktiviert	Gibt an, ob die Zertifikatsvalidierung aktiviert oder deaktiviert ist. Falls **Markiert**, ist die Zertifikatsvalidierung aktiviert. iDRAC6 verwendet beim Herstellen einer Verbindung zum Active Directory LDAP über Secure Socket Layer (SSL). Standardmäßig bietet der iDRAC6 hohe Sicherheit, indem er das auf den iDRAC6 geladene Zertifizierungsstellenzertifikat verwendet, um während des SSL-Handshake das SSL-Serverzertifikat des Domänen-Controllers zu überprüfen. Zertifikatsvalidierung kann zu Testzwecken deaktiviert werden.

Tabelle 5-19. Einstellungen der Seite Active Directory-Konfiguration *(fortgesetzt)*

Einstellung	Beschreibung
Active Directory-CA-Zertifikat hochladen	Klicken Sie zum Hochladen eines Active Directory-Zertifizierungsstellenzertifikats auf **Durchsuchen**, wählen Sie die Datei aus und klicken Sie auf **Hochladen**. Stellen Sie sicher, dass die SSL-Zertifikate des Domänen-Controllers von derselben Zertifizierungsstelle signiert wurden und dass dieses Zertifikat auf der Management Station verfügbar ist, die auf den iDRAC6 zugreift. Der Wert **Dateipfad** zeigt den relativen Dateipfad des Zertifikats an, das Sie hochladen. Wenn Sie sich entscheiden, nicht zum Zertifikat zu browsen, geben Sie den Dateipfad ein, der den vollständigen Pfad sowie den gesamten Dateinamen und die Dateierweiterung enthält.
Aktuelles Active Directory-Zertifizierungsstellenzertifikat	Zeigt das Active Directory-Zertifizierungsstellenzertifikat an, das zum iDRAC6 hochgeladen wurde.
Schritt 2 von 4 Active Directory Konfiguration und Verwaltung	
Active Directory aktiviert	Wählen Sie diese Option aus, wenn Sie Active Directory aktivieren möchten.
Smart-Card-Anmeldung aktivieren	Wählen Sie diese Option aus, um die Smart-Card-Anmeldung zu aktivieren. Sie werden bei allen nachfolgenden Anmeldungsversuchen über die GUI zu einer Smart-Card-Anmeldung aufgefordert. **ANMERKUNG:** Die Smart-Card-basierte Zweifaktor-Authentifizierung (TFA) und das einmalige Anmelden werden nur auf Microsoft Windows-Betriebssystemen mit Internet Explorer unterstützt. Außerdem unterstützen Terminaldienste (Remote-Desktop) unter Windows XP den Smart-Card-Betrieb nicht. Windows Vista unterstützt diese Verwendungsart jedoch.

Tabelle 5-19. Einstellungen der Seite Active Directory-Konfiguration *(fortgesetzt)*

Einstellung	Beschreibung
Einmaliges Anmelden aktivieren	Wählen Sie diese Option aus, wenn Sie sich am iDRAC6 anmelden möchten, ohne Ihre Authentifizierungs-Benutzeranmeldeinformationen für die Domäne, z. B. Benutzername und Kennwort, einzugeben. Wenn Sie Einmaliges Anmelden (SSO) aktivieren und sich dann abmelden, können Sie sich unter Verwendung von SSO wieder anmelden. Wenn Sie unter Verwendung von SSO bereits angemeldet sind und sich dann abmelden, oder wenn SSO fehlschlägt, wird die normale Webseite angezeigt. **ANMERKUNG:** Die Aktivierung der Smart–Card-Anmeldung oder der einfachen Anmeldung bewirkt nicht, dass bandexterne Befehlszeilenschnittstellen einschließlich SSH, Telnet, Remote-RACADM und IPMI über LAN deaktiviert werden. **ANMERKUNG:** In dieser Version wird die Funktion der Smart Card-basierten Zweifaktor-Authentifizierung (TFA) nicht unterstützt, wenn Active Directory für das erweiterte Schema konfiguriert ist. Die Funktion der einfachen Anmeldung (SSO) wird sowohl für das Standardschema als auch für das erweiterte Schema unterstützt.
Benutzerdomänenname	Geben Sie die Einträge der Benutzerdomänennamen ein. Wenn konfiguriert, wird auf der Anmeldeseite eine Liste der Benutzerdomänennamen als Drop-Down-Menü angezeigt. Wenn nicht konfiguriert, können sich Active Directory-Benutzer weiterhin anmelden, indem Sie den Benutzernamen im Format Benutzername@Domänenname oder Domänenname\Benutzername eingeben. **Hinzufügen**: Fügt der Liste einen neuen Benutzerdomänennamen hinzu. **Bearbeiten**: Modifiziert einen vorhandenen Benutzerdomänennamen. **Löschen**: Löscht einen Benutzerdomänennamen aus der Liste.
Zeitüberschreitung	Geben Sie die maximale Wartezeit für den Abschluss von Active Directory-Abfragen in Sekunden ein.

Tabelle 5-19. Einstellungen der Seite Active Directory-Konfiguration *(fortgesetzt)*

Einstellung	Beschreibung
Domänen-Controller mit DNS suchen	Wählen Sie die Option **Domänen-Controller mit DNS suchen** aus, um die Active Directory-Domänen-Controller über eine DNS-Suche zu ermitteln. Wenn diese Option ausgewählt ist, werden die Serveradressen 1-3 der Domänen-Controller ignoriert. Wählen Sie **Benutzerdomäne der Anmeldung** aus, um die DNS-Suche mit dem Domänennamen des Anmeldebenutzers durchzuführen. Wählen Sie ansonsten **Domäne angeben** aus und geben Sie den Domänennamen ein, der für die DNS-Suche verwendet werden soll. iDRAC6 versucht so lange, nacheinander mit jeder der Adressen eine Verbindung herzustellen (zu den ersten 4 Adressen, die nach der DNS-Anfrage zurückgegeben wurden), bis eine Verbindung hergestellt werden konnte. Wenn **Erweitertes Schema** ausgewählt ist, repräsentieren die Adressen die Domänen-Controller, auf denen sich das iDRAC6-Geräteobjekt und die Zuordnungsobjekte befinden. Wenn das **Standardschema** ausgewählt ist, repräsentieren die Adressen die Domänen-Controller, auf denen sich die Benutzerkonten und Rollengruppen befinden.
Domänen-Controller-Adressen angeben	Wählen Sie die Option **Domänen-Controller-Adressen angeben** aus, um iDRAC6 die Verwendung der Active Directory Domänen-Controller-Serveradressen zu ermöglichen. Wenn diese Option ausgewählt ist, wird keine DNS-Suche durchgeführt. Geben Sie die IP-Adresse oder den vollständigen qualifizierten Domänennamen (FQDN) des Domänen-Controllers ein. Wenn die Option **Domänen-Controller-Adressen angeben** ausgewählt ist, muss mindestens eine der drei Adressen konfiguriert sein. iDRAC6 versucht, nacheinander mit jeder der konfigurierten Adressen eine Verbindung aufzubauen, bis eine Verbindung hergestellt ist. Wenn das **Standardschema** ausgewählt ist, sind dies die Adressen der Domänen-Controller, auf denen sich die Benutzerkonten und Rollengruppen befinden. Wenn **Erweitertes Schema** ausgewählt ist, sind dies die Adressen der Domänen-Controller, auf denen sich das iDRAC6-Geräteobjekt und die Zuordnungsobjekte befinden.

Tabelle 5-19. Einstellungen der Seite Active Directory-Konfiguration *(fortgesetzt)*

Einstellung	Beschreibung
Schritt 3 von 4 Active Directory Konfiguration und Verwaltung	
Auswahl von „Erweitertes Schema“	Wählen Sie diese Option aus, wenn Sie das erweiterte Schema mit Active Directory aktivieren möchten. Klicken Sie auf **Weiter**, um die Seite **Schritt 4 von 4 Active Directory-Konfiguration und -Verwaltung** anzuzeigen. **iDRAC6-Name**: Gibt den Namen an, der iDRAC6 in Active Directory eindeutig identifiziert. Dieser Wert ist standardmäßig NULL. **iDRAC-Domänenname**: Der DNS-Name (Zeichenkette) der Domäne, in der sich das Active Directory-iDRAC-Objekt befindet. Dieser Wert ist standardmäßig NULL. Diese Einstellungen werden nur angezeigt, wenn der iDRAC6 für die Verwendung mit einem erweiterten Active Directory-Schema konfiguriert wurde.

Tabelle 5-19. Einstellungen der Seite Active Directory-Konfiguration *(fortgesetzt)*

Einstellung	Beschreibung
Auswahl von „Standardschema“	Wählen Sie diese Option aus, wenn Sie das Standardschema mit Active Directory verwenden möchten. Klicken Sie auf **Weiter**, um die Seite **Schritt 4a von 4 Active Directory** anzuzeigen. Wählen Sie die Option **Lookup des Global Catalog-Servers mit DNS** aus und geben Sie den **Root-Domänennamen** ein, der für eine DNS-Anfrage zum Abrufen der Server des Globalen Katalogs des Active Directory verwendet werden soll. Wenn diese Option ausgewählt ist, werden die **Serveradressen 1-3 der globalen Katalogserver** ignoriert. iDRAC6 versucht, sich nacheinander mit jeder der Adressen zu verbinden (die ersten vier Adressen, die bei der DNS-Suche ermittelt wurden), bis ein Verbindungsversuch erfolgreich ist. Ein globaler Katalogserver ist nur für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen auf verschiedenen Domänen befinden. Wählen Sie die Option **Globale Katalog-Serveradressen angeben** aus und geben Sie die IP-Adressen oder den FQDN eines oder mehrerer globaler Katalogserver ein. Wenn diese Option ausgewählt ist, wird keine DNS-Suche durchgeführt. Mindestens eine der drei Adressen muss konfiguriert sein. iDRAC6 versucht, nacheinander mit jeder der konfigurierten Adressen eine Verbindung aufzubauen, bis eine Verbindung hergestellt ist. Ein Server des Globalen Katalogs ist nur dann für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen auf verschiedenen Domänen befinden. **Rollengruppen**: Gibt die Liste der dem iDRAC6 zugeordneten Rollengruppen an. **Gruppenname**: Gibt den Namen an, der die Rollengruppe im Active Directory identifiziert, die dem iDRAC6 zugeordnet ist. **Gruppendomäne**: Gibt den Typ der Gruppendomäne an, in der sich die Rollengruppe befindet. **Rollengruppen-Berechtigungen**: Gibt die Klasse der Gruppenberechtigung an. (siehe Tabelle 5-20). Diese Einstellungen werden nur angezeigt, wenn der iDRAC6 für die Verwendung mit einem Active Directory-Standardschema konfiguriert wurde.

Tabelle 5-20. Rollengruppenberechtigungen

Einstellung	Beschreibung
Zugriffsstufe der Rollengruppe	Legt die maximale iDRAC6-Benutzerberechtigung als eine der Folgenden fest: **Administrator**, **Hauptbenutzer**, **Gastbenutzer**, **Keine** oder **Benutzerdefiniert**. Siehe Tabelle 5-21 zu **Rollengruppen**-Berechtigungen.
Anmeldung am iDRAC6	Erlaubt der Gruppe den Anmeldezugriff auf den iDRAC6.
iDRAC6 konfigurieren	Gibt der Gruppe die Berechtigung, den iDRAC6 zu konfigurieren.
Benutzer konfigurieren	Gibt der Gruppe die Berechtigung, Benutzer zu konfigurieren.
Protokolle löschen	Erlaubt der Gruppenberechtigung, Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Erlaubt der Gruppenberechtigung, Serversteuerungsbefehle auszuführen.
Auf die virtuelle Konsole zugreifen	Erlaubt der Gruppe, auf die virtuelle Konsole zuzugreifen.
Zugriff auf virtuelle Datenträger	Erlaubt der Gruppe, auf virtuelle Datenträger zuzugreifen.
Testwarnungen	Erlaubt der Gruppe, einem bestimmten Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnosebefehle ausführen	Erlaubt der Gruppenberechtigung, Diagnosebefehle auszuführen.

Tabelle 5-21. Rollengruppenberechtigungen

Eigenschaft	Beschreibung
Administrator	Am iDRAC6 anmelden, iDRAC6 konfigurieren, Benutzer konfigurieren, Protokolle löschen, Serversteuerungsbefehle ausführen, Zugriff auf die virtuelle Konsole, Zugriff auf virtuelle Datenträger, Testwarnungen, Diagnosebefehle ausführen
Hauptbenutzer	Am iDRAC6 anmelden, Protokolle löschen, Serversteuerungsbefehle ausführen, Zugriff auf die virtuelle Konsole, Zugriff auf virtuelle Datenträger, Testwarnungen
Gastbenutzer	Anmeldung am iDRAC6
Custom (Benutzerdefiniert)	Wählt eine beliebige Kombination der folgenden Berechtigungen aus: Am iDRAC6 anmelden, iDRAC6 konfigurieren, Benutzer konfigurieren, Protokolle löschen, Serversteuerungsbefehle ausführen, Zugriff auf die virtuelle Konsole, Zugriff auf virtuelle Datenträger, Testwarnungen, Diagnosebefehle ausführen
NONE	Keine zugewiesenen Berechtigungen

Active Directory-CA-Zertifikat anzeigen

Klicken Sie auf dem Zusammenfassungsbildschirm von **Active Directory** auf **Active Directory konfigurieren**. Der Abschnitt **Aktuelles Active Directory-Zertifizierungsstellenzertifikat** wird eingeblendet. Siehe Tabelle 5-22.

Tabelle 5-22. Informationen zum Active Directory-CA-Zertifikat

Feld	Beschreibung
Seriennummer	Seriennummer des Zertifikats
Informationen des Antragstellers	Vom Bewerber eingegebene Zertifikatsattribute
Ausstellerinformationen	Vom Aussteller zurückgegebene Zertifikatsattribute.
Gültig von	Datum der Zertifikatsausstellung.
Gültig bis	Verfalldatum des Zertifikats.

Lokalen Konfigurationszugriff aktivieren oder deaktivieren

ANMERKUNG: Die Standardeinstellung für lokalen Konfigurationszugriff ist Aktiviert.

Lokalen Konfigurationszugriff aktivieren

1. Klicken Sie auf **System**→ **iDRAC-Einstellungen**→ **Netzwerk/Sicherheit**→ **Dienste**.
2. Klicken Sie unter **Lokale Konfiguration** zur **Aufhebung der Markierung** auf **Lokale BENUTZER-Konfigurationsaktualisierungen von iDRAC6 deaktivieren**, um den Zugriff zu aktivieren.
3. Klicken Sie auf **Anwenden**.

Lokalen Konfigurationszugriff deaktivieren

1. Klicken Sie auf **System**→ **iDRAC-Einstellungen**→ **Netzwerk/Sicherheit**→ **Dienste**.
2. Klicken Sie unter **Lokale Konfiguration** zum Markieren von **Lokale BENUTZER-Konfigurationsaktualisierungen von iDRAC6 deaktivieren**, um den Zugriff zu deaktivieren.
3. Klicken Sie auf **Anwenden**.

iDRAC6-Dienste konfigurieren

ANMERKUNG: Sie müssen die Berechtigung **iDRAC6 konfigurieren** besitzen, um diese Einstellungen zu ändern.

ANMERKUNG: Wenn Sie Änderungen auf Dienste anwenden, werden diese sofort wirksam. Bestehende Verbindungen können ohne vorherige Warnung abgebrochen werden.

ANMERKUNG: Bei dem von Microsoft Windows bereitgestellten Telnet-Client liegt ein bekanntes Problem vor. Verwenden Sie einen anderen Telnet-Client, wie z. B. HyperTerminal oder PuTTY.

1. Klicken Sie auf **System**→ **iDRAC-Einstellungen**→ Register **Netzwerk/ Sicherheit**.
2. Klicken Sie auf **Dienste**, um die Seite Konfiguration von **Diensten** zu öffnen.

3 Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Web Server — siehe Tabelle 5-23 für Web Server-Einstellungen
   - SSH — siehe Tabelle 5-24 für Informationen zu SSH-Einstellungen
   - Telnet — unter Tabelle 5-25 finden Sie Informationen zu Telnet-Einstellungen.
   - SNMP-Agent — siehe Tabelle 5-26 zu SNMP-Agent-Einstellungen
   - Automatisierter Systemwiederherstellungsagent – siehe Tabelle 5-27 für die Einstellungen des automatisierten Systemwiederherstellungsagenten
4 Klicken Sie auf **Anwenden**.

Tabelle 5-23. Web Server-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert den iDRAC6-Web Server. Wenn **Markiert**, weist dies darauf hin, dass der Web Server aktiviert ist. Der Standardwert lautet **Markiert**.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger Web Server-Sitzungen, die für dieses System zulässig sind. Dieses Feld kann nicht bearbeitet werden. Es können vier Web Server-Sitzungen gleichzeitig ausgeführt werden.
Aktive Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich **Max**. **Sitzungen**. Dieses Feld kann nicht bearbeitet werden.
Zeitüberschreitung	Die Zeit in Sekunden, für die eine Verbindung ungenutzt bleiben kann. Die Sitzung wird abgebrochen, wenn der Zeitüberschreitungswert erreicht wird. Änderungen an der Einstellung zur Zeitüberschreitung werden sofort wirksam und führen zu einem Reset des Web Servers. Der Zeitüberschreitungsbereich beträgt 60 bis 10800 Sekunden. Die Standardeinstellung ist **1800** Sekunden.
HTTP-Schnittstellennummer	Der Anschluss, an dem der iDRAC6 abhört, ob eine Browser-Verbindung besteht. Die Standardeinstellung ist **80.**
HTTPS-Schnittstellennummer	Der Anschluss, an dem der iDRAC6 abhört, ob eine sichere Browser-Verbindung besteht. Die Standardeinstellung ist **443.**

Tabelle 5-24. SSH-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert SSH. Wenn **Markiert**, weist das Kontrollkästchen darauf hin, dass SSH aktiviert ist.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger SSH-Sitzungen, die für dieses System zulässig sind. Es können vier SSH-Sitzungen gleichzeitig unterstützt werden. Sie können dieses Feld nicht bearbeiten.
Aktive Sitzungen	Die Anzahl der aktuellen Sitzungen auf dem System. Sie können dieses Feld nicht bearbeiten.
Zeitüberschreitung	Die Leerlaufzeitüberschreitung der Secure Shell in Sekunden. Der Zeitüberschreitungsbereich beträgt 60 bis 10800 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitüberschreitungsfunktion zu deaktivieren. Die Standardeinstellung ist **1800.**
Port Number (Schnittstellennummer)	Der Anschluss, an dem der iDRAC6 abhört, ob eine SSH-Verbindung besteht. Die Standardeinstellung ist **22.**

Tabelle 5-25. Telnet-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert Telnet. Wenn **Markiert**, ist Telnet aktiviert. Der Standardwert lautet **Nicht markiert**.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger Telnet-Sitzungen, die für dieses System zulässig sind. Es können vier Telnet-Sitzungen gleichzeitig unterstützt werden. Sie können dieses Feld nicht bearbeiten.
Aktive Sitzungen	Die Anzahl der aktuellen Telnet-Sitzungen auf dem System. Sie können dieses Feld nicht bearbeiten.
Zeitüberschreitung	Die Inaktivitätszeitüberschreitung von Telnet, in Sekunden. Der Zeitüberschreitungsbereich beträgt 60 bis 10800 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitüberschreitungsfunktion zu deaktivieren. Die Standardeinstellung ist **1800.**
Port Number (Schnittstellennummer)	Der Anschluss, an dem der iDRAC6 überwacht, ob eine Telnet-Verbindung besteht. Die Standardeinstellung ist **23.**

Tabelle 5-26. SNMP-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert/deaktiviert SNMP. Wenn markiert, ist SNMP aktiviert.
SNMP-Community-Name	Geben Sie den SNMP-Community-Namen ein. Die Standardeinstellung ist **öffentlich**.

Tabelle 5-27. Automatisierter Systemwiederherstellungs-Agent

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert den automatisierten Systemwiederherstellungs-Agenten.

iDRAC6-Firmware aktualisieren

ANMERKUNG: Sollte die iDRAC6-Firmware beschädigt worden sein, was bei Unterbrechung des Aktualisierungsprozesses der iDRAC6-Firmware passieren kann, können Sie den iDRAC6 unter Verwendung des CMC wiederherstellen. Anleitungen hierzu finden Sie im *CMC Firmware-Benutzerhandbuch*.

ANMERKUNG: Die Firmware-Aktualisierung behält standardmäßig die aktuellen iDRAC6-Einstellungen bei. Während des Aktualisierungsprozesses haben Sie die Option, die iDRAC6-Konfigurationen auf den Herstellerstandard zurückzusetzen. Wenn Sie die Konfiguration auf die Werkseinstellungen einstellen, wird der Zugriff auf das externe Netzwerk nach Abschluss der Aktualisierung deaktiviert. Das Netzwerk muss unter Verwendung des iDRAC6-Konfigurationsdienstprogramms oder der CMC-Webschnittstelle aktiviert und konfiguriert werden.

1 Starten Sie die iDRAC6-Webschnittstelle.

2 Klicken Sie auf **System→ iDRAC-Einstellungen→** Register **Aktualisierung**.

Die Seite **Firmwaraktualisierung** wird angezeigt.

ANMERKUNG: Damit die Firmware aktualisiert werden kann, muss der iDRAC6 in den Aktualisierungsmodus versetzt werden. Sobald sich der iDRAC6 in diesem Modus befindet, wird er automatisch zurückgesetzt, selbst wenn Sie den Aktualisierungsvorgang abbrechen.

3 Klicken Sie im Abschnitt **Hochladen** auf **Durchsuchen** und wählen Sie das Firmware-Image.

Der standardmäßige Firmware-Imagename lautet **firmimg.imc**.

4 Klicken Sie auf **Hochladen**. Die Datei wird auf den iDRAC6 hochgeladen. This may take several minutes to complete.

5 Auf der Seite **Hochladen (Schritt 2 von 3)** können Sie die Ergebnisse der Validierung einsehen, die auf der hochgeladenen Imagedatei ausgeführt wurde.

- Wenn die Imagedatei erfolgreich hochgeladen wurde und alle Überprüfungsvorgänge erfolgreich durchlaufen sind, wird eine Meldung ausgegeben, die besagt, dass das Firmware-Image überprüft wurde.
- Wenn das Image nicht erfolgreich hochgeladen wurde oder die Überprüfungsvorgänge nicht bestanden hat, setzen Sie den iDRAC6 zurück, schließen Sie die aktuelle Sitzung und versuchen Sie die Aktualisierung erneut.

ANMERKUNG: Wenn Sie das Kontrollkästchen **Konfiguration beibehalten** nach Abschluss der Firmwareaktualisierung deaktivieren, wird iDRAC6 auf die Standardkonfiguration zurückgesetzt. Das LAN ist in den Standardeinstellungen deaktiviert. Sie werden nicht in der Lage sein, sich an der iDRAC6-Webschnittstelle anzumelden. Sie müssen die LAN-Einstellungen unter Verwendung der CMC-Webschnittstelle oder unter Verwendung des iDRAC6-Konfigurationsdienstprogramms während des BIOS-POST neu konfigurieren.

6 Standardmäßig ist das Kontrollkästchen **Konfiguration beibehalten** markiert, um die aktuellen Einstellungen auf dem iDRAC6 nach einer Erweiterung beizubehalten. Wenn die Einstellungen nicht beibehalten werden sollen, entfernen Sie die Markierung im Kontrollkästchen **Konfiguration beibehalten**.

7 Klicken Sie auf **Aktualisierung starten**, um den Aktualisierungsvorgang zu starten. Unterbrechen Sie den Aktualisierungsvorgang nicht.

8 Im Fenster **Hochladen (Schritt 3 von 3)** können Sie den Status des Upgrades einsehen. Der Fortschritt des in Prozent gemessenen Firmware-Upgrade-Vorgangs wird in der Spalte **Fortschritt** angezeigt.

9 Sobald das Firmware-Update vollständig ist, wird das Fenster **Hochladen (Schritt 3 von 3)** mit dem Ergebnis neu angezeigt, und iDRAC6 wird automatisch zurückgesetzt. Um weiterhin über die Webschnittstelle auf den iDRAC6 zuzugreifen, schließen Sie das aktuelle Browserfenster und stellen Sie in einem neuen Browserfenster eine neue Verbindung zum iDRAC6 her.

iDRAC6-Firmware mithilfe des CMC aktualisieren

Normalerweise wird die iDRAC6-Firmware unter Verwendung von iDRAC6-Dienstprogrammen wie der iDRAC6-Webschnittstelle oder der betriebssystemspezifischen Update Packages aktualisiert, die von **support.dell.com** heruntergeladen werden können.

Zur Aktualisierung der iDRAC6-Firmware können Sie die CMC-Webschnittstelle oder RACADM verwenden. Diese Funktion ist verfügbar, wenn sich die iDRAC6-Firmware im Normalmodus befindet, aber auch wenn sie beschädigt ist.

ANMERKUNG: Anleitungen zur Verwendung der CMC-Webschnittstelle finden Sie im *Chassis Management Controller Firmware-Benutzerhandbuch*.

Zur Aktualisierung der iDRAC6-Firmware führen Sie folgende Schritte aus:

1 Laden Sie die neueste iDRAC6-Firmware von **support.dell.com** auf Ihre Management Station herunter.

2 Melden Sie sich bei der CMC-Webschnittstelle an.

3 Klicken Sie auf **Gehäuseübersicht** in der Systemstruktur.

4 Klicken Sie auf die Registerkarte **Aktualisieren**. Der Bildschirm **Firmwareaktualisierung** wird angezeigt.

5 Wählen Sie im Abschnitt **iDRAC6 Enterprise Firmware**→ Spalte **Ziele aktualisieren** die zu aktualisierenden iDRAC6s aus.

6 Klicken Sie auf **iDRAC6 Enterprise-Aktualisierung anwenden**.

7 Klicken Sie auf **Durchsuchen**, und suchen Sie nach dem von Ihnen heruntergeladenen iDRAC-Firmware-Image. Klicken Sie dann auf **Öffnen**.

8 Klicken Sie auf **Firmware-Aktualisierung beginnen**.

Nachdem die Firmware-Imagedatei auf den CMC hochgeladen wurde, aktualisiert sich der iDRAC6 eigenständig mit dem Image.

ANMERKUNG: Bei der iDRAC-Aktualisierung über die CMC-Webschnittstelle wird die Konfiguration immer beibehalten.

Zurücksetzen der iDRAC6-Firmware

iDRAC6 verfügt über die Möglichkeit, zwei Firmware-Images gleichzeitig beizubehalten. Sie können wählen, von dem Firmware-Image Ihrer Wahl aus zu starten (oder darauf zurückzusetzen).

1. Öffnen Sie die iDRAC6-Webschnittstelle und melden Sie sich am Remote-System an.
2. Klicken Sie auf **System→ iDRAC-Einstellungen→** Register **Aktualisierung**.
3. Klicken Sie auf **Rollback**. Die aktuelle Firmware-Version und die Rollback-Firmware-Version werden auf der Seite **Rollback (Schritt 2 von 3)** angezeigt.
4. Klicken Sie auf **Weiter**, um das Rollback-Verfahren für die Firmware zu starten.

   Auf der Seite **Rollback (Schritt 3 von 3)** können Sie den Status des Rollback-Vorgangs einsehen. Nach erfolgreichem Abschluss zeigt er an, dass das Verfahren erfolgreich abgeschlossen wurde.

   Wenn das Firmware-Rollback erfolgreich abgeschlossen ist, wird der iDRAC6 automatisch zurückgesetzt. Um weiterhin über die Webschnittstelle mit dem iDRAC6 zu arbeiten, schließen Sie den aktuellen Browser und stellen Sie unter Verwendung eines neuen Browserfensters eine neue Verbindung zum iDRAC6 her. Wenn ein Fehler auftritt, wird eine entsprechende Fehlermeldung eingeblendet.

   ANMERKUNG: Die Funktion **Konfiguration beibehalten** kann nicht genutzt werden, wenn Sie für iDRAC6-Firmware ein Rollback von Version 2.2 zu Version 2.1 durchführen möchten.

6

Verwendung des iDRAC6-Verzeichnisdiensts

Ein Verzeichnisdienst unterhält eine allgemeine Datenbank zum Speichern von Informationen über Benutzer, Computer, Drucker usw. auf einem Netzwerk. Wenn Ihre Firma die Microsoft Active Directory- oder LDAP Directory Service-Software verwendet, kann die Software so konfiguriert werden, dass sie Zugriff auf iDRAC6 bietet. Sie können dann bestehenden Benutzern im Verzeichnisdienst iDRAC6-Benutzerberechtigungen erteilen und diese steuern.

Verwendung des iDRAC6 mit Microsoft Active Directory

ANMERKUNG: Die Verwendung der Active Directory-Software zum Erkennen von iDRAC6 Benutzern wird von den Betriebssystemen Microsoft Windows 2000, Windows Server 2003 und Windows Server 2008 unterstützt.

Sie können die Benutzerauthentifizierung über Microsoft Active Directory konfigurieren, um sich am iDRAC6 anzumelden. Sie können auch eine rollenbasierte Berechtigung bereitstellen, die einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren. Weitere Informationen stehen in den nachfolgenden Abschnitten zur Verfügung.

Tabelle 6-1 zeigt die iDRAC6 Active Directory-Benutzerberechtigungen.

Tabelle 6-1. iDRAC6-Benutzerberechtigungen

Berechtigung	Beschreibung
Anmeldung am iDRAC6	Ermöglicht dem Benutzer, sich am iDRAC6 anzumelden.
iDRAC6 konfigurieren	Ermöglicht dem Benutzer, den iDRAC6 zu konfigurieren.
Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern zu erlauben, auf das System zuzugreifen
Protokolle löschen	Ermöglicht dem Benutzer, iDRAC6-Protokolle zu löschen
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer, RACADM-Befehle auszuführen

Tabelle 6-1. iDRAC6-Benutzerberechtigungen *(fortgesetzt)*

Berechtigung	Beschreibung
Auf die virtuelle Konsole zugreifen	Ermöglicht dem Benutzer, die virtuelle Konsole auszuführen
Zugriff auf virtuelle Datenträger	Ermöglicht dem Benutzer, virtuelle Datenträger auszuführen und zu verwenden
Testwarnungen	Ermöglicht dem Benutzer, einem bestimmten Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen

Sie haben verschiedene Möglichkeiten, um sich über das Active Directory im iDRAC6 anzumelden:

- Webschnittstelle
- Lokaler RACADM
- SSH- oder Telnet-Konsole für SM-CLP-CLI

Die Anmeldungssyntax ist für alle drei Methoden gleich:

`<Benutzername@Domäne>`

oder

`<Domäne>\<Benutzername>` oder `<Domäne>/<Benutzername>`

wobei `Benutzername` eine ASCII-Zeichenkette mit 1-256 Zeichen ist.

Leerzeichen und Sonderzeichen (wie \,/ oder @) dürfen nicht im Benutzernamen oder Domänennamen verwendet werden.

ANMERKUNG: NetBIOS-Domänennamen, wie z. B. *Americas* können nicht verwendet werden, da diese Namen nicht aufgelöst werden können.

Wenn Sie sich über die Webschnittstelle anmelden und konfigurierte Benutzerdomänen haben, führt der Anmeldebildschirm der Webschnittstelle im Pulldown-Menü sämtliche Benutzerdomänen zur Auswahl auf. Wenn Sie eine Benutzerdomäne aus dem Pulldown-Menü wählen, sollten Sie nur den Benutzernamen eingeben. Wenn Sie **Diesen iDRAC** wählen, können Sie sich nach wie vor als Active Directory-Benutzer anmelden, wenn Sie die unter „Verwendung des iDRAC6 mit Microsoft Active Directory“ auf Seite 135 beschriebene Anmeldesyntax verwenden.

Voraussetzungen zur Aktivierung der Active Directory-Authentifizierung des iDRAC6

Um die Active Directory-Authentifizierungsfunktion auf dem iDRAC6 verwenden zu können, müssen Sie bereits eine Active Directory-Infrastrukur bereitgestellt haben. Die Microsoft-Website enthält Informationen zum Einrichten einer Active Directory-Infrastruktur, falls diese noch nicht vorhanden sein sollte.

iDRAC6 verwendet die standardmäßige PKI-Methode (Public Key Infrastructure, Infrastruktur des öffentlichen Schlüssels), um eine sichere Authentifizierung in das Active Directory durchzuführen. Sie benötigen daher auch eine integrierte PKI für die Active Directory-Infrastruktur.

Weitere Informationen zum PKI-Setup finden Sie auf der Microsoft-Website.

Um eine korrekte Authentifizierung zu allen Domänen-Controllern vornehmen zu können, müssen Sie auch die SSL-Verschlüsselung auf sämtlichen Domänen-Controllern aktivieren, zu denen iDRAC6 eine Verbindung herstellt. Nähere Informationen finden Sie unter „SSL auf einem Domänen-Controller aktivieren“ auf Seite 137.

SSL auf einem Domänen-Controller aktivieren

Wenn Benutzer durch das iDRAC6 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 iDRAC6 geladen wird. Damit also die iDRAC6-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 *automatisch* einem SSL-Zertifikat zuzuweisen, müssen Sie die folgenden Schritte ausführen, um SSL auf den einzelnen Domänen-Controllern zu aktivieren.

1. Aktivieren Sie SSL auf jedem einzelnen Domänen-Controller, indem Sie das SSL-Zertifikat für jeden Controller installieren.
   a. Klicken Sie auf **Start→ Verwaltung→ Domänensicherheitsregeln**.

b Erweitern Sie den Ordner **Richtlinien öffentlicher Schlüssel,** klicken Sie mit der rechten Maustaste auf **Automatische Zertifikatanforderungs-Einstellungen** und klicken Sie auf **Automatische Zertifikatanforderung**.

c Klicken Sie im **Setup-Assistent der automatischen Zertifikatanforderung** auf **Weiter** und wählen Sie **Domänen-Controller** aus.

d Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Das CA-Stammzertifikat des Domänen-Controllers zu iDRAC6 exportieren

ANMERKUNG: Wenn Ihr System Windows 2000 ausführt, können die folgenden Schritte abweichen.

ANMERKUNG: Wenn Sie mit einem unabhängigen CA arbeiten, können die folgenden Schritte abweichen.

1. Machen Sie den Domänen-Controller ausfindig, der den Microsoft Enterprise-CA-Dienst ausführt.
2. Klicken Sie auf **Start→Run** (Ausführen).
3. Geben Sie im Feld **Ausführen** den Befehl `mmc` ein, und klicken Sie auf **OK**.
4. Klicken Sie im Fenster **Konsole 1** (MMC) auf **Datei** (oder auf **Konsole** bei 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**-Konto und klicken Sie auf **Weiter**.
8. Wählen Sie **Lokaler Computer** und klicken Sie auf **Fertig stellen**.
9. Klicken Sie auf **OK**.
10. Erweitern Sie im Fenster **Konsole 1** den Ordner **Zertifikate**, erweitern Sie den Ordner **Persönlich** und klicken Sie auf den Ordner **Zertifikate**.
11. Suchen Sie das Stammzertifizierungsstellenzertifikat und klicken Sie mit der rechten Maustaste darauf, wählen Sie **Alle Aufgaben** aus und klicken Sie auf **Exportieren**.
12. Klicken Sie im **Zertifikate exportieren-Assistenten** auf **Weiter** und wählen Sie **Privaten Schlüssel nicht exportieren** aus.
13. Klicken Sie auf **Weiter** und wählen Sie **Base-64-kodiert X.509 (.cer)** als Format.

14 Klicken Sie auf **Weiter**, um das Zertifikat in einem Verzeichnis auf dem System zu speichern.

15 Laden Sie das unter Schritt 14 gespeicherte Zertifikat auf das iDRAC6.

Informationen zum Hochladen des Zertifikats unter Verwendung von RACADM finden Sie unter „Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM“ auf Seite 169.

Informationen zum Hochladen des Zertifikats über die Webschnittstelle finden Sie unter „Active Directory mit Standardschema unter Verwendung der iDRAC6-Webschnittstelle konfigurieren“ auf Seite 164.

SSL-Zertifikat der iDRAC6-Firmware importieren

ANMERKUNG: Wenn der Active Directory-Server so eingestellt ist, dass der Client während der Initialisierungsphase einer SSL-Sitzung authentifiziert wird, muss das iDRAC6-Serverzertifikat auch 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 iDRAC6-Firmware von einer bekannten 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.

Das iDRAC6-SSL-Zertifikat ist identisch mit dem Zertifikat, das für den iDRAC6-Web Server verwendet wird. Alle iDRAC6-Controller werden mit einem selbstsignierten Standard-Zertifikat versandt.

So importieren Sie das SSL-Zertifikat der iDRAC6-Firmware in alle Listen vertrauenswürdiger Zertifikate der Domänen-Controller:

1 Zum Herunterladen des iDRAC6-SSL-Zertifikats führen Sie den folgenden RACADM-Befehl aus:

```
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** und klicken Sie auf **Importieren**.

4 Klicken Sie auf **Weiter** und suchen Sie die SSL-Zertifikatdatei.

5 Installieren Sie das iDRAC6-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 dann auf **OK**.

Unterstützte Active Directory-Authentifizierungsmechanismen

Es gibt zwei Möglichkeiten, mit Active Directory den Benutzerzugang zum iDRAC6 zu definieren: Sie können die Lösung *Erweitertes Schema* nutzen, die von Dell so eingerichtet wurde, dass Dell-spezifische Active Directory-Objekte hinzugefügt werden können. Oder Sie können die Lösung *Standardschema* nutzen, die nur Active Directory-Gruppenobjekte verwendet. In den folgenden Abschnitten finden Sie weitere Informationen zu diesen Lösungen.

Wenn Sie den Zugang zum iDRAC6 mit Active Directory konfigurieren, müssen Sie entweder die Lösung „Erweitertes Schema“ oder „Standardschema“ wählen.

Die Vorteile bei der Verwendung des erweiterten Schemas sind:

- Alle Zugriffssteuerungsobjekte werden im Active Directory verwahrt.
- Bei der Konfiguration des Benutzerzugangs auf verschiedenen iDRAC6-Karten mit unterschiedlichen Ebenen der Benutzerberechtigung besteht maximale Flexibilität.

Der Vorteil der Standardschema-Lösung ist, dass keine Erweiterung des Schemas notwendig ist, da alle erforderlichen Objektklassen in der Microsoft-Standardkonfiguration des Active Directory-Schemas enthalten sind.

Übersicht des Active Directory mit erweitertem Schema

Für die Verwendung des erweiterten Schemas ist die Erweiterung des Active Directory-Schemas notwendig (Erläuterung im folgenden Abschnitt).

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. Firmen können die Active Directory-Datenbank erweitern, indem sie ihre eigenen einzigartigen Attribute und Klassen hinzufügen, um umgebungsspezifische Anforderungen zu erfüllen. 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.

- Die Dell Dateierweiterung lautet: `dell`
- Die Dell Basis-OID lautet: `1.2.840.113556.1.8000.1280`
- Der RAC-LinkID-Bereich ist: `12070 bis 12079`

Übersicht über die iDRAC6-Schemaerweiterungen

Um in der Vielzahl von Kundenumgebungen die größte Flexibilität zu bieten, stellt Dell eine Gruppe von Objekten bereit, die, abhängig von den gewünschten Ergebnissen, vom Benutzer konfiguriert werden können. Dell hat das Schema um Zuordnungs-, Geräte- und Berechtigungseigenschaften erweitert. Die Zuordnungseigenschaft wird zur Verknüpfung der Benutzer oder Gruppen mit einem spezifischen Satz Berechtigungen an einem oder mehreren iDRAC6-Geräten verwendet. Dieses Modell ist unkompliziert und gibt dem Administrator höchste Flexibilität bei der Verwaltung von verschiedenen Benutzergruppen, iDRAC6-Berechtigungen und iDRAC6-Geräten im Netzwerk.

Active Directory - Objektübersicht

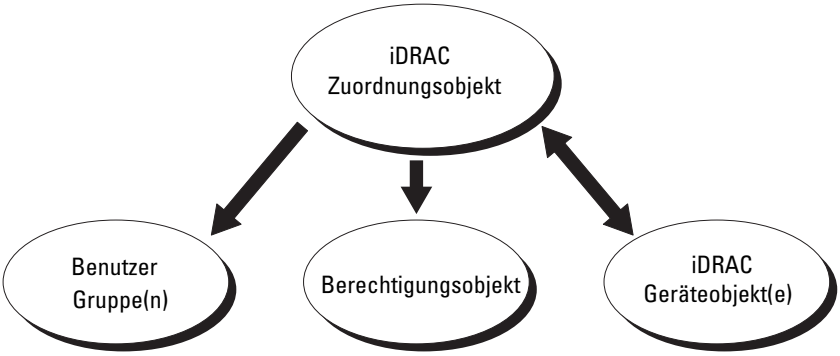
Für jedes iDRAC6 des Netzwerkes, das Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein iDRAC6-Geräteobjekt erstellen. Sie können verschiedene Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt mit beliebig vielen Benutzern, Benutzergruppen oder iDRAC6-Geräteobjekten verbunden werden kann. Die Benutzer und iDRAC6-Benutzergruppen können Mitglieder jeder Domäne im Unternehmen sein.

Jedes Zuordnungsobjekt darf jedoch nur mit einem Berechtigungsobjekt verbunden werden bzw. kann Benutzer, Benutzergruppen oder iDRAC6-Geräteobjekte nur mit einem Berechtigungsobjekt verbinden. Dies ermöglicht dem Administrator, die Berechtigungen jedes Benutzers über spezielle iDRAC6-Geräte zu steuern.

Das iDRAC6-Geräteobjekt ist die Verknüpfung zur iDRAC6-Firmware für die Abfrage des Active Directory auf Authentifizierung und Autorisierung. Wenn dem Netzwerk ein iDRAC6 hinzugefügt wird, muss der Administrator den iDRAC6 und sein Geräteobjekt mit seinem Active Directory-Namen so konfigurieren, dass Benutzer mit Active Directory Authentifizierungen und Autorisierungen ausführen können. Der Administrator muss außerdem mindestens einem Zuordnungsobjekt den iDRAC6 hinzufügen, damit Benutzer Authentifizierungen vornehmen können.

Abbildung 6-1 zeigt, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für die gesamte Authentifizierung und Autorisierung erforderlich ist.

Abbildung 6-1. Typisches Setup für Active Directory-Objekte



Sie können je nach Bedarf eine beliebige Anzahl von Zuordnungsobjekten erstellen. Es ist jedoch erforderlich, dass Sie mindestens ein Zuordnungsobjekt erstellen, und Sie müssen ein iDRAC6-Geräteobjekt für jedes iDRAC6 auf dem Netzwerk haben, das zum Zweck der Authentifizierung und Autorisierung mit dem iDRAC6 mit dem Active Directory integriert werden soll.

Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer bzw. Gruppen sowie iDRAC6-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die *Benutzer*, die *Berechtigungen* auf iDRAC6-Geräten haben.

Über die Dell-Erweiterung zum ADUC MMC Snap-In können nur Berechtigungsobjekte und iDRAC6-Objekte derselben Domäne mit dem Verbindungsobjekt verbunden werden. Mit der Dell-Erweiterung können keine Gruppen oder iDRAC6-Objekte aus anderen Domänen als Product-Member des Verbindungsobjekts 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.

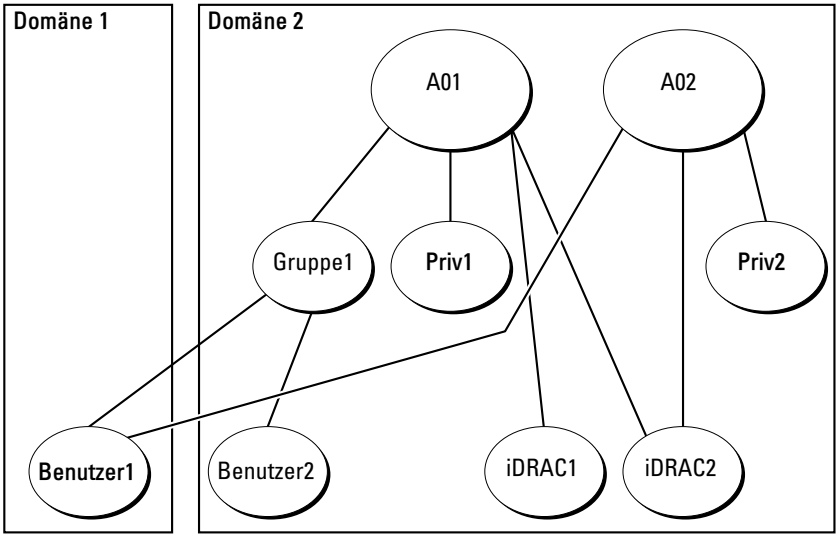
Benutzer, Benutzergruppen oder verschachtelte Benutzergruppen jeglicher Domäne können dem Verbindungsobjekt hinzugefügt werden. Lösungen mit erweitertem Schema unterstützen jede Art von Benutzergruppe sowie jede Benutzergruppe, die über mehrere Domänen verschachtelt und von Microsoft Active Directory 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.

Abbildung 6-2 bietet ein Beispiel des Ansammelns von Berechtigungen unter Verwendung des erweiterten Schemas.

Abbildung 6-2. Ansammeln von Berechtigungen für einen Benutzer



Die Abbildung stellt zwei Zuordnungsobjekte dar – A01 und A02. Benutzer1 ist über beide Verbindungsobjekte mit iDRAC2 verbunden. Benutzer1 verfügt daher über die Berechtigungen, die sich aus der Kombination der Berechtigungen für die Objekte Priv1 und Priv2 auf iDRAC2 ergeben.

Angenommen, Priv1 hat folgende Berechtigungen: Anmeldung, virtuelle Datenträger, Protokolle löschen; und Priv2 hat folgende Berechtigungen: iDRAC-Anmeldung, iDRAC konfigurieren, Testwarnungen. Benutzer1 hat dementsprechend Zugriff auf die Berechtigungen von Priv1 und Priv2: iDRAC-Login, virtuelle Datenträger, Protokolle löschen, iDRAC-Konfiguration und Testwarnungen.

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 dieser Konfiguration 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.

Konfiguration des erweiterten Schemas für den Zugriff auf den iDRAC6

Vor der Nutzung von Active Directory für den Zugang zum iDRAC6 müssen die Active Directory-Software und der iDRAC6 mit folgenden Schritten konfiguriert werden:

1. Erweitern Sie das Active Directory-Schema (siehe „Erweitern des Active Directory-Schemas“ auf Seite 146).
2. Erweitern Sie das Snap-In von Active Directory-Benutzern und -Computern (siehe „Dell-Erweiterung zum Active Directory-Benutzer und -Computer-Snap-In installieren“ auf Seite 152).
3. Fügen Sie iDRAC6-Benutzer und deren Berechtigungen zum Active Directory hinzu (siehe „iDRAC6-Benutzer und -Berechtigungen zum Active Directory hinzufügen“ auf Seite 153).
4. Konfigurieren Sie die iDRAC6-Active Directory-Eigenschaften entweder über die iDRAC6-Webschnittstelle oder über RACADM (siehe „Active Directory mit erweitertem Schema unter Verwendung der iDRAC6-Webschnittstelle konfigurieren“ auf Seite 156 oder „Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM“ auf Seite 159).

Erweitern des Active Directory-Schemas

Wichtig: Die Schema-Erweiterung für dieses Produkt unterscheidet sich von den Vorgänger-Generationen der Dell Remote Management-Produkte. Sie müssen das neue Schema erweitern und das neue **Active Directory-Benutzer und Computer Microsoft Management Console (MMC) Snap-In** in ihrem Verzeichnis installieren. Das alte Schema kann bei diesem Produkt nicht verwendet werden.

ANMERKUNG: Eine Erweiterung des neuen Schemas oder die Installation einer Erweiterung auf das Active Directory Benutzer und Computer-Snap-In ändert nichts an den Vorgängerversionen des Produktes.

Die Erweiterung und das MMC Snap-In für Active Directory Users and Computers sind auf der DVD *Dell Systems Management Tools and Documentation* erhältlich. Informationen zur Installation finden Sie unter „Dell-Erweiterung zum Active Directory-Benutzer und -Computer-Snap-In installieren“ auf Seite 152. Weitere Details zum Erweitern des Schemas für iDRAC6 und zum Installieren des Benutzer- und Computer-MMC-Snap-In von Active Directory finden Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*, das unter **support.dell.com/manuals** zur Verfügung steht.

ANMERKUNG: Beim Erstellen von iDRAC6-Zuordnungsobjekten oder iDRAC6-Geräteobjekten müssen Sie **Dell Remote Management Object Advanced** auswählen.

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 Schema-Admin-Berechtigungen auf dem Schema Master-FSMO-Rollenbesitzer (Flexible Single Master Operation) der Domänenstruktur besitzen.

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**
- *<DVD-Laufwerk>*:*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**. Zur Verwendung des Dell Schema Extender für Erweiterungen des Active Directory-Schemas siehe „Dell Schema Extender verwenden“ auf Seite 147.

Sie können Schema Extender oder die LDIF-Dateien an einem beliebigen Standort kopieren und ausführen.

Dell Schema Extender verwenden

VORSICHTSHINWEIS: Das Dell Schema Extender-Dienstprogramm verwendet die Datei SchemaExtenderOem.ini. Um sicherzustellen, dass das Dell Schema Extender-Dienstprogramm ordnungsgemäß funktioniert, darf der Name dieser Datei nicht geändert werden.

1. Klicken Sie auf dem **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-Administratorberechtigungen ein.
4. Klicken Sie auf **Weiter,** um Dell Schema Extender auszuführen.
5. Klicken Sie auf **Fertig stellen**.

   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 folgende Elemente vorhanden sind:

   - Klassen (siehe Tabelle 6-2 bis Tabelle 6-7)
   - Attribute (Tabelle 6-8)

   Näheres zur Benutzung der Verwaltungskonsole (MMC) und des Active Directory-Schema-Snap-In finden Sie in der Microsoft-Dokumentation.

Tabelle 6-2. 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 6-3. dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Beschreibung	Stellt das Dell iDRAC6-Gerät dar. iDRAC6 wird wie delliDRACDevice in Active Directory konfiguriert. Mit dieser Konfiguration kann der iDRAC6 CMC Lightweight Directory Access Protocol (LDAP)-Abfragen an das Active Directory senden.
Klassentyp	Strukturklasse
SuperClasses	dellProduct
Attribute	**dellSchemaVersion** **dellRacType**

Tabelle 6-4. delliDRACAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Beschreibung	Repräsentiert das Dell-Zuordnungsobjekt. Das Zuordungsobjekt ist die Verbindung zwischen Benutzern und Geräten.
Klassentyp	Strukturklasse
SuperClasses	Gruppe
Attribute	**dellProductMembers** **dellPrivilegeMember**

Tabelle 6-5. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Beschreibung	Legt die Berechtigungen für iDRAC6 fest (Autorisierungsrechte)
Klassentyp	Erweiterungsklasse
SuperClasses	NONE
Attribute	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Tabelle 6-6. 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 6-7. 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 6-8. 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 Liste der dellRacDevice- und DelliDRACDevice-Geräteobjekte, die dieser Rolle angehören. Dieses Attribut ist die Vorwärtsverbindung zur dellAssociationMembers-Rückwärtsverbindung. 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
delIsLogClearAdmin 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

Tabelle 6-8. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden *(fortgesetzt)*

Attributname/Beschreibung	Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
dellIsServerResetUser	1.2.840.113556.1.8000.1280.1.1.2.7	TRUE
TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat.	Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsConsoleRedirectUser	1.2.840.113556.1.8000.1280.1.1.2.8	TRUE
TRUE, wenn der Benutzer über Virtuelle-Konsole-Rechte auf dem Gerät verfügt.	Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsVirtualMediaUser	1.2.840.113556.1.8000.1280.1.1.2.9	TRUE
TRUE, wenn der Benutzer Rechte für den virtuellen Datenträger auf dem Gerät hat.	Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsTestAlertUser	1.2.840.113556.1.8000.1280.1.1.2.10	TRUE
TRUE, wenn der Benutzer Testwarnungsbenutzerrechte auf dem Gerät hat.	Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsDebugCommandAdmin	1.2.840.113556.1.8000.1280.1.1.2.11	TRUE
TRUE, wenn der Benutzer Debug-Befehls-Administrator-Rechte auf dem Gerät hat.	Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellSchemaVersion	1.2.840.113556.1.8000.1280.1.1.2.12	TRUE
Die aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren.	Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
dellRacType	1.2.840.113556.1.8000.1280.1.1.2.13	TRUE
Dieses Attribut ist der aktuelle RAC-Typ für das dellRacDevice-Objekt und der Rückwärtslink zum dellAssociationObjectMembers-Vorwärtslink.	Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	

Tabelle 6-8. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden *(fortgesetzt)*

Attributname/Beschreibung	Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
dellAssociationMembers	1.2.840.113556.1.8000.1280.1.1.2.14	FALSE
Liste der dellAssociationObjectMembers, die diesem Produkt angehören. Dieses Attribut ist der Rückwärtslink zum Attribut dellProductMembers. Link-ID: 12071	Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	

Dell-Erweiterung zum Active Directory-Benutzer und -Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch die Active Directory-Benutzer und das Computer-Snap-In erweitern, sodass der Administrator iDRAC6-Geräte, Benutzer und Benutzergruppen, iDRAC6-Zuordnungen und iDRAC6-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.

Administratorpaket installieren

Sie müssen das Administratorpaket auf jedem System installieren, das die Active Directory-iDRAC6-Objekte verwaltet. Wenn Sie das Administratorpaket nicht installieren, kann das Dell iDRAC6-Objekt nicht im Container angezeigt werden.

Weitere Informationen finden Sie unter „Öffnen des Active Directory-Benutzer- und -Computer-Snap-In“ auf Seite 153.

Öffnen des Active Directory-Benutzer- und -Computer-Snap-In

So öffnen Sie das Active Directory-Benutzer- und -Computer-Snap-In:

1. Wenn Sie auf dem Domänen-Controller angemeldet sind, klicken Sie auf **Start Admin-Hilfsprogramme→ Active Directory-Benutzer und -Computer**.

   Wenn Sie nicht auf dem Domänen-Controller angemeldet sind, muss das entsprechende Microsoft-Administratorpaket auf dem lokalen System installiert sein. Zum Installieren dieses Administratorpakets klicken Sie auf **Start→ Ausführen**, geben Sie `MMC` ein und drücken Sie anschließend die **Eingabetaste**.

   Die MMC wird angezeigt.

2. Klicken Sie im Fenster **Konsole 1** auf **Datei** (oder auf **Konsole** bei Systemen, auf denen Windows 2000 ausgeführt wird).
3. Klicken Sie auf **Add/Remove Snap-in** (Snap-In hinzufügen/entfernen).
4. Wählen Sie das **Active Directory-Benutzer- und -Computer-Snap-In** aus und klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **Cose** (Schließen) und anschließend auf **OK**.

iDRAC6-Benutzer und -Berechtigungen zum Active Directory hinzufügen

Mit dem Dell-erweiterten Active Directory-Benutzer und -Computer-Snap-In können Sie iDRAC6-Benutzer und -Berechtigungen hinzuzufügen, indem Sie iDRAC6-, Zuordnungs- und Berechtigungsobjekte erstellen. Um die einzelnen Objekttypen hinzuzufügen, führen Sie folgende Verfahren durch:

- Ein iDRAC6-Geräteobjekt erstellen
- Erstellen eines Berechtigungsobjekts
- Erstellen eines Zuordnungsobjekts
- Einem Zuordnungsobjekt Objekte hinzufügen

Ein iDRAC6-Geräteobjekt erstellen

1. Klicken Sie im Fenster **Console Root** (MCC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu→ Dell Remote Management Object Advanced**.

   Das Fenster **New Object** (Neues Objekt) wird angezeigt.
3. Geben Sie einen Namen für das neue Objekt ein. Der Name muss mit dem iDRAC6-Namen identisch sein, den Sie in Schritt A von „Active Directory mit erweitertem Schema unter Verwendung der iDRAC6-Webschnittstelle konfigurieren“ auf Seite 156 eingeben.
4. Wählen Sie **iDRAC-Geräteobjekt**.
5. Klicken Sie auf **OK**.

Erstellen von Berechtigungsobjekten

ANMERKUNG: Ein Berechtigungsobjekt muss in derselben Domäne wie das zugehörige Zuordnungsobjekt erstellt werden.

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu→ Dell Remote Management Object Advanced**.

   Das Fenster **New Object** (Neues Objekt) wird angezeigt.
3. Geben Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Berechtigungsobjekt** aus.
5. Klicken Sie auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf das Berechtigungsobjekt, das Sie erstellt haben, und wählen Sie **Eigenschaften** aus.
7. Klicken Sie auf die Registerkarte **Remote Management-Berechtigungen** und wählen Sie die von Ihnen vorgesehenen Berechtigungen für den Benutzer oder die Gruppe aus (sieheTabelle 5-13).

Erstellen von Zuordnungsobjekten

ANMERKUNG: Das iDRAC6-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**.

Hierdurch wird das Fenster **Neues Objekt** geöffnet.

3 Geben Sie einen Namen für das neue Objekt ein.

4 Wählen Sie **Zuordnungsobjekt**.

5 Wählen Sie den Wirkungsbereich für das **Zuordnungsobjekt**.

6 Klicken Sie auf **OK**.

7 Geben Sie den authentifizierten Benutzern Zugriffsberechtigungen für den Zugriff auf die angelegten Zuordnungsobjekte. Führen Sie dazu folgende Schritte durch:

   a Wechseln Sie zu **Verwaltung→ ADSI bearbeiten**. Das Fenster **ADSI bearbeiten** wird angezeigt.

   b Wechseln Sie im rechten Bereich zum angelegten Zuordnungsobjekt, klicken Sie auf die rechte Maustaste und wählen Sie **Eigenschaften**.

   c Klicken Sie in der Registerkarte **Sicherheit** auf **Hinzufügen**.

   d Geben Sie `Authentifizierte Benutzer` ein, klicken Sie auf **Namen überprüfen** und klicken Sie auf **OK**. Die **authentifizierten Benutzer** werden der Liste der **Gruppen- und Benutzernamen** hinzugefügt.

   e Klicken Sie auf **OK**.

Hinzufügen von Objekten zu einem Zuordnungsobjekt

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und iDRAC6-Geräte oder iDRAC6-Gerätegruppen zuordnen.

Sie können Benutzergruppen und iDRAC6-Geräte hinzufügen. Die Verfahren zum Erstellen von Dell-bezogenen Gruppen und nicht-Dell-bezogenen Gruppen sind identisch.

Benutzer oder Benutzergruppen hinzufügen

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

1. Wählen Sie das Register **Berechtigungsobjekt** und klicken Sie auf **Hinzufügen.**
2. Geben Sie den Namen des Berechtigungsobjekts ein und klicken Sie auf **OK**.

Klicken Sie auf die Registerkarte **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, die die Berechtigungen des Benutzers bzw. der Benutzergruppe bei Authentifizierung eines iDRAC6-Geräts definiert. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

Hinzufügen von iDRAC6-Geräten oder iDRAC6-Gerätegruppen

Um iDRAC6-Geräte oder iDRAC6-Gerätegruppen hinzuzufügen:

1. Wählen Sie die Registerkarte **Produkte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie die Namen der iDRAC6-Geräte oder iDRAC6-Gerätegruppen ein und klicken Sie auf **OK**.
3. Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.

Wählen Sie die Registerkarte **Produkte** und fügen Sie ein iDRAC6-Gerät hinzu, das mit dem Netzwerk verbunden und für die gewählten Benutzer oder Benutzergruppen verfügbar ist. Einem Zuordnungsobjekt können mehrere iDRAC6-Geräte hinzugefügt werden.

Active Directory mit erweitertem Schema unter Verwendung der iDRAC6-Webschnittstelle konfigurieren

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der iDRAC6-Webschnittstelle an.
3. Wählen Sie in der Systemstruktur **System→ iDRAC-Einstellungen→** Register **Netzwerk/Sicherheit→ Verzeichnisdienst→ Microsoft Active Directory** aus.

   Der **Active Directory-**Zusammenfassungsbildschirm wird angezeigt.
4. Klicken Sie am Ende der Bildschirmanzeige auf **Active Directory konfigurieren**.

   Der Bildschirm **Schritt 1 von 4 Active Directory** wird angezeigt.

5 Um das SSL-Zertifikat Ihres Active Directory-Servers zu überprüfen, wählen Sie das Kontrollkästchen für **Zertifikatsvalidierung aktiviert** unter **Zertifikateinstellungen** aus.

Wenn Sie das SSL-Zertifikat Ihres Active Directory-Servers nicht überprüfen möchten, fahren Sie mit Schritt 7 fort.

6 Unter **Active Directory CA-Zertifikat laden** geben Sie den Dateipfad des Zertifikats ein oder durchsuchen Sie das Verzeichnis nach der Datei und klicken Sie anschließend auf **Laden**.

ANMERKUNG: Sie müssen den vollständigen Dateipfad eingeben, der den gesamten Pfad und den vollständigen Dateinamen mit Dateierweiterung enthält.

Die Informationen zum Active Directory CA-Zertifikat, das Sie hochgeladen haben, werden im Abschnitt **Aktuelles Active Directory CA-Zertifikat** angezeigt.

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

Der Bildschirm **Schritt 2 von 4 Active Directory Konfiguration und Verwaltung** wird eingeblendet.

8 Wählen Sie das Kontrollkästchen **Active Directory aktiviert** aus.

ANMERKUNG: In dieser Version wird die Funktion der Smart Card-basierten Zweifaktor-Authentifizierung (TFA) nicht unterstützt, wenn Active Directory für das erweiterte Schema konfiguriert ist. Die Funktion der einfachen Anmeldung (SSO) wird sowohl für das Standardschema als auch für das erweiterte Schema unterstützt.

9 Klicken Sie auf **Hinzufügen**, um den **Benutzerdomänennamen** einzugeben. Sie geben den Domänennamen in das Textfeld ein und klicken dann auf **OK**. Dieser Schritt ist optional. Wenn Sie eine Liste von Benutzerdomänen konfigurieren, wird diese Liste auf dem Anmeldebildschirm der Webschnittstelle verfügbar sein. Sie können eine Auswahl treffen und brauchen anschließend nur noch den Benutzernamen einzugeben.

10 Geben Sie im Feld **Timeout** in Sekunden ein, wie lange das iDRAC6-Programm auf eine Antwort des Active Directory warten soll.

11 Wählen Sie die Option **Domänen-Controller mit DNS suchen** aus, um die Active Directory-Domänen-Controller über eine DNS-Suche zu ermitteln. Ist dies bereits konfiguriert, werden die **Domänen-Controller-Serveradressen 1-3** ignoriert. Wählen Sie **Benutzerdomäne der Anmeldung** aus, um die DNS-Suche mit dem Domänennamen des Anmeldebenutzers durchzuführen. Wählen Sie ansonsten **Eine Domäne angeben** aus und geben Sie den Domänennamen für die DNS-Suche ein. iDRAC6 versucht so lange, nacheinander mit jeder der Adressen eine Verbindung herzustellen (zu den ersten 4 Adressen, die nach der DNS-Anfrage zurückgegeben wurden), bis eine Verbindung hergestellt werden konnte. Wenn **Erweitertes Schema** ausgewählt ist, repräsentieren die Adressen die Domänen-Controller, auf denen sich das iDRAC6-Geräteobjekt und die Zuordnungsobjekte befinden.

Wenn das **Standardschema** ausgewählt ist, repräsentieren die Adressen die Domänen-Controller, auf denen sich die Benutzerkonten und Rollengruppen befinden.

ANMERKUNG: iDRAC6 greift nicht auf die angegebenen Domänencontroller zurück, wenn eine DNS-Suche fehlschlägt oder die durch die Suche ermittelten Server nicht funktionieren.

12 Wählen Sie die Option **Domänen-Controller-Adressen angeben** aus, um iDRAC6 die Verwendung der Active Directory Domänen-Controller-Serveradressen zu ermöglichen. DNS-Suche wird nicht durchgeführt. Geben Sie die IP-Adresse oder den FQDN des Domänen-Controllers an. Wenn die Option **Domänen-Controller-Adressen angeben** ausgewählt ist, muss mindestens eine der drei Adressen konfiguriert sein. iDRAC6 versucht, nacheinander mit jeder der konfigurierten Adressen eine Verbindung aufzubauen, bis eine Verbindung hergestellt ist. Wenn **Erweitertes Schema** ausgewählt ist, sind dies die Adressen der Domänen-Controller, auf denen sich das iDRAC6-Geräteobjekt und die Zuordnungsobjekte befinden.

ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie in diesem Feld angeben, muss mit dem Feld **Server** oder **Alternativer Servername** im Zertifikat Ihres Domänen-Controllers übereinstimmen, wenn Sie die Zertifikatsvalidierung aktiviert haben.

13 Klicken Sie auf **Weiter**.

Der Bildschirm **Schritt 3 von 4 Active Directory Konfiguration und Verwaltung** wird eingeblendet.

14 Wählen Sie unter **Schemaauswahl** das Kontrollkästchen **Erweitertes Schema** aus.

15 Klicken Sie auf **Weiter**.

Der Bildschirm **Schritt 4 von 4 Active Directory** wird angezeigt.

16 Geben Sie unter **Erweitertes Schema Einstellungen** den **iDRAC6-Namen** und den **iDRAC6-Domänennamen** ein, um das iDRAC6-Geräteobjekt und seine Speicherstelle im Active Directory zu konfigurieren.

17 Klicken Sie auf **Beenden**, um Ihre Änderungen zu speichern, und anschließend auf **Fertig**.

Die Hauptzusammenfassungsseite für **Active Directory Konfiguration und Verwaltung** wird angezeigt. Als nächstes müssen Sie die Active Directory-Einstellungen überprüfen, die Sie soeben konfiguriert haben.

18 Klicken Sie am Ende der Bildschirmanzeige auf **Einstellungen überprüfen**.

Der Bildschirm **Active Directory-Einstellungen überprüfen** wird angezeigt.

19 Geben Sie Ihren iDRAC6-Benutzernamen und Ihr Kennwort ein und klicken Sie auf **Überprüfung starten**.

Die Überprüfungsergebnisse und das Überprüfungsprotokoll werden angezeigt. Weitere Informationen finden Sie unter „Einstellungen testen“ auf Seite 172.

ANMERKUNG: Um die Anmeldung beim Active Directory zu unterstützen, müssen Sie einen DNS-Server korrekt im iDRAC6-Programm konfiguriert haben. Wechseln Sie in den Bildschirm **Netzwerk** (klicken Sie dazu auf **System→ iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Netzwerk**), um die DNS-Server manuell zu konfigurieren, oder verwenden Sie DHCP, um DNS-Server abzurufen.

Die Active Directory-Konfiguration mit erweitertem Schema ist damit abgeschlossen.

Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM

Verwenden Sie die folgenden Befehle zum Konfigurieren der Active Directory-Funktion von iDRAC6 mit erweitertem Schema über das RACADM-Befehlszeilendienstprogramm (CLI) statt der Webschnittstelle.

1 Öffnen Sie eine Eingabeaufforderung und geben Sie die folgenden RACADM-Befehle ein:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 1

racadm config -g cfgActiveDirectory -o
cfgADRacName <allgemeiner RAC-Name>

racadm config -g cfgActiveDirectory -o
cfgADRacDomain <vollständig qualifizierter
rac-Domänenname>

racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <vollständig qualifizierter
Domänenname oder IP-Adresse des Domänen-Controllers>

racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <vollständig qualifizierter
Domänenname oder IP-Adresse des Domänen-Controllers>

racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <vollständig qualifizierter
Domänenname oder IP-Adresse des Domänen-Controllers>
```

ANMERKUNG: Sie müssen mindestens eine der drei Adressen konfigurieren. iDRAC6 versucht, nacheinander mit jeder der konfigurierten Adressen eine Verbindung aufzubauen, bis eine Verbindung hergestellt ist. Mit erweitertem Schema sind dies der FQDN oder die IP-Adresse des Domänen-Controllers, auf dem sich das iDRAC6-Gerät befindet. Global Catalog Server werden im Modus „Erweitertes Schema" nicht verwendet.

Wenn Sie für den SSL-Handshake die Zertifikatsvalidierung deaktivieren möchten, geben Sie den folgenden RACADM-Befehl ein:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

In diesem Fall brauchen Sie kein CA-Zertifikat zu laden.

Wenn Sie die Zertifikatsvalidierung auch beim SSL-Handshake durchführen möchten, geben Sie den folgenden RACADM-Befehl ein:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 1
```

In diesem Fall müssen Sie mit dem folgenden RACADM-Befehl ein CA-Zertifikat laden:

```
racadm sslcertupload -t 0x2 -f <ADS root CA
Certificate>
```

Die Verwendung des folgenden RACADM-Befehls kann optional sein. Weitere Informationen hierzu finden Sie unter „SSL-Zertifikat der iDRAC6-Firmware importieren“ auf Seite 139.

```
racadm sslcertdownload -t 0x1 -f <RAC SSL
Certificate>
```

2 Wenn DHCP auf dem iDRAC6 aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgenden RACADM-Befehl ein:

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 1
```

3 Wenn DHCP auf dem iDRAC6 deaktiviert ist oder Sie ihre DNS IP-Adresse manuell eingeben möchten, arbeiten Sie mit den folgenden RACADM-Befehlen:

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1
<primary DNS IP Adresse>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2
<secondary DNS IP Adresse>
```

4 Möchten Sie eine Liste mit Benutzerdomänen konfigurieren, sodass für die Anmeldung an der iDRAC6-Webschnittstelle nur der Benutzername eingegeben werden muss, verwenden Sie dazu den folgenden Befehl:

```
racadm config -g cfgUserDomain -o
cfgUserDomainName <fully qualified Domain namr or
IP Adresse of the domain controller> -i <index>
```

Sie können bis zu 40 Benutzerdomänen mit Indexzahlen zwischen 1 und 40 konfigurieren.

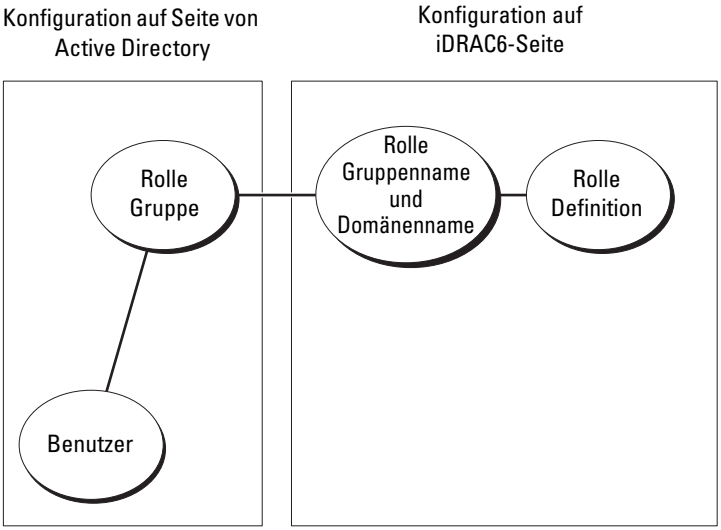
Details zu Benutzerdomänen finden Sie unter „Verwendung des iDRAC6 mit Microsoft Active Directory“ auf Seite 135.

5 Drücken Sie die **Eingabetaste**, um die Konfiguration des Active Directory mit erweitertem Schema abzuschließen.

Übersicht des Standardschema-Active Directory

Wie in Abbildung 6-3 dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration unter Active Directory und unter iDRAC6.

Abbildung 6-3. Konfiguration des iDRAC6 mit Microsoft Active Directory und Standardschema



Auf der Seite des Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der Zugang zum iDRAC6 hat, wird Mitglied der Rollengruppe. Um diesem Benutzer Zugriff auf eine spezifische iDRAC6-Karte zu gewähren, müssen der Rollengruppenname und sein Domänenname auf der spezifischen iDRAC6-Karte konfiguriert werden. Im Unterschied zur Lösung des erweiterten Schemas, ist die Rolle und die Berechtigungsebene auf jeder iDRAC6-Karte und nicht im Active Directory definiert. Es können bis zu fünf Rollengruppen in jedem iDRAC6 konfiguriert und definiert werden. Tabelle 6-9 zeigt die Standard-Rollengruppen-Berechtigungen.

Tabelle 6-9. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppen	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
Rollengruppe 1	NONE	**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	NONE	**Anmelden am iDRAC, iDRAC konfigurieren, Serversteuerungsbefehle ausführen**, Zugriff auf **virtuelle Konsole, Zugriff auf virtuellen Datenträger, Testwarnungen, Diagnosebefehle ausführen**	0x000000f9
Rollengruppe 3	NONE	**Am iDRAC anmelden**	0x00000001
Rollengruppe 4	NONE	Keine zugewiesenen Berechtigungen	0x00000000
Rollengruppe 5	NONE	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bitmasken-Werte werden nur verwendet, wenn das Standardschema mit dem RACADM eingerichtet wird.

Einfache Domänen (Single Domains) und mehrfache Domänen (Multiple Domains)

Wenn sich alle Anmeldebenutzer und Rollengruppen sowie die verschachtelten Benutzergruppen in derselben Domäne befinden, müssen lediglich die Adressen der Domänen-Controller auf dem iDRAC6 konfiguriert werden. In diesem Muster einer einfachen Domäne wird jede Art von Gruppe unterstützt.

Wenn die Anmeldebenutzer und Rollengruppen oder eine verschachtelte Benutzergruppe mehreren Domänen angehören, müssen Global Catalog Server-Adressen auf dem iDRAC6 konfiguriert werden. In diesem Muster einer mehrfachen Domäne müssen alle Rollengruppen und, wenn vorhanden, alle verschachtelten Benutzergruppen einer Universal Group angehören.

Konfiguration des Standardschemas von Active Directory für den Zugriff auf den iDRAC6

Active Directory muss mit den folgenden Schritten konfiguriert werden, um Active Directory-Benutzern den Zugriff auf den iDRAC6 zu ermöglichen:

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 bestehende Gruppe aus. Fügen Sie den Active Directory-Benutzer als ein Mitglied der Active Directory-Gruppe hinzu, um auf den iDRAC6 zuzugreifen.
3. Konfigurieren Sie den Namen der Gruppe und den Domänennamen auf iDRAC6 durch Verwendung der Webschnittstelle oder durch RACADM (siehe „Active Directory mit Standardschema unter Verwendung der iDRAC6-Webschnittstelle konfigurieren“ auf Seite 164 oder „Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM“ auf Seite 169).

Active Directory mit Standardschema unter Verwendung der iDRAC6-Webschnittstelle konfigurieren

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der iDRAC6-Webschnittstelle an.
3. Wählen Sie in der Systemstruktur **System→ iDRAC-Einstellungen→** Register **Netzwerk/Sicherheit→ Verzeichnisdienst→ Microsoft Active Directory** aus.

   Die **Active Directory-**Zusammenfassungsseite wird angezeigt.
4. Klicken Sie am Ende der Bildschirmanzeige auf **Active Directory konfigurieren**.

   Der Bildschirm **Schritt 1 von 4 Active Directory** wird angezeigt.

5 Wählen Sie unter **Zertifikateinstellungen** die Option **Zertifikatsvalidierung aktiviert** aus.

6 Unter **Active Directory CA-Zertifikat laden** geben Sie den Dateipfad des Zertifikats ein oder durchsuchen Sie das Verzeichnis nach der Datei und klicken Sie anschließend auf **Laden**.

ANMERKUNG: Sie müssen den vollständigen Dateipfad eingeben, der den gesamten Pfad und den vollen Dateinamen mit Dateierweiterung enthält.

Die Informationen zum Active Directory CA-Zertifikat, das Sie hochgeladen haben, werden im Abschnitt **Aktuelles Active Directory CA-Zertifikat** angezeigt.

7 Klicken Sie auf **Weiter**.

Der Bildschirm **Schritt 2 von 4 Active Directory Konfiguration und Verwaltung** wird eingeblendet.

8 Wählen Sie das Kontrollkästchen für **Active Directory aktiviert** aus.

9 Wählen Sie **Smart Card-Anmeldung aktivieren** aus, um die Smart Card-Anmeldung zu aktivieren. Sie werden bei allen nachfolgenden Anmeldungsversuchen über die GUI zu einer Smart Card-Anmeldung aufgefordert. Diese Eingabe ist optional.

10 Wählen Sie **Einmaliges Anmelden aktivieren** aus, wenn Sie sich bei iDRAC6 anmelden möchten, ohne Ihre Benutzerauthentifizierungs-Anmeldeinformationen für die Domäne, wie Benutzername und Kennwort, einzugeben.

11 Klicken Sie auf **Hinzufügen**, um den **Benutzerdomänennamen** einzugeben. Sie geben den Domänennamen in das Textfeld ein und klicken dann auf **OK**. Dieser Schritt ist optional. Wenn Sie eine Liste von Benutzerdomänen konfigurieren, wird diese Liste auf dem Anmeldebildschirm der Webschnittstelle verfügbar sein. Sie können eine Auswahl treffen und brauchen anschließend nur noch den Benutzernamen einzugeben.

12 Geben Sie im Feld **Timeout** in Sekunden ein, wie lange das iDRAC6-Programm auf eine Antwort des Active Directory warten soll.

13 Wählen Sie die Option **Domänen-Controller mit DNS suchen** aus, um die Active Directory-Domänen-Controller über eine DNS-Suche zu ermitteln. Ist dies bereits konfiguriert, werden die **Domänen-Controller-Serveradressen 1-3** ignoriert. Wählen Sie **Benutzerdomäne der Anmeldung** aus, um die DNS-Suche mit dem Domänennamen des Anmeldebenutzers durchzuführen. Wählen Sie ansonsten **Eine Domäne angeben** aus und geben Sie den Domänennamen für die DNS-Suche ein. iDRAC6 versucht so lange, nacheinander mit jeder der Adressen eine Verbindung herzustellen (zu den ersten 4 Adressen, die nach der DNS-Anfrage zurückgegeben wurden), bis eine Verbindung hergestellt werden konnte. Wenn das **Standardschema** ausgewählt ist, repräsentieren die Adressen die Domänen-Controller, auf denen sich die Benutzerkonten und Rollengruppen befinden.

14 Wählen Sie die Option **Domänen-Controller-Adressen angeben** aus, um iDRAC6 die Verwendung der Active Directory Domänen-Controller-Serveradressen zu ermöglichen. DNS-Suche wird nicht durchgeführt. Geben Sie die IP-Adresse oder den FQDN des Domänen-Controllers an. Wenn die Option **Domänen-Controller-Adressen angeben** ausgewählt ist, muss mindestens eine der drei Adressen konfiguriert sein. iDRAC6 versucht, nacheinander mit jeder der konfigurierten Adressen eine Verbindung aufzubauen, bis eine Verbindung hergestellt ist.

Wenn das **Standardschema** ausgewählt ist, sind dies die Adressen der Domänen-Controller, auf denen sich die Benutzerkonten und Rollengruppen befinden.

ANMERKUNG: iDRAC6 greift nicht auf die angegebenen Domänencontroller zurück, wenn eine DNS-Suche fehlschlägt oder die durch die Suche ermittelten Server nicht funktionieren.

15 Klicken Sie auf **Weiter**.

Der Bildschirm **Schritt 3 von 4 Active Directory Konfiguration und Verwaltung** wird eingeblendet.

16 Wählen Sie unter **Schemaauswahl** das Kontrollkästchen **Standardschema** aus.

17 Klicken Sie auf **Weiter**.

Der Bildschirm **Schritt 4a von 4 Active Directory** wird angezeigt.

18 Wählen Sie unter **Standardschema-Einstellungen** die Option **Globale Katalogserver mit DNS suchen** aus und geben Sie den **Root-Domänennamen** ein, der für die DNS-Suche zur Ermittlung von globalen Katalogservern in Active Directory verwendet werden soll. Ist dies bereits konfiguriert, werden die Adressen 1-3 der globalen Katalogserver ignoriert. iDRAC6 versucht, sich nacheinander mit jeder der Adressen zu verbinden (die ersten vier Adressen, die bei der DNS-Suche ermittelt wurden), bis ein Verbindungsversuch erfolgreich ist. Ein globaler Katalogserver ist nur für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen auf verschiedenen Domänen befinden.

ANMERKUNG: iDRAC6 greift nicht auf die angegebenen globalen Katalogserver zurück, wenn eine DNS-Suche fehlschlägt oder die durch die Suche ermittelten Server nicht funktionieren.

19 Wählen Sie die Option **Globale Katalogserveradressen angeben** aus und geben Sie die IP-Adresse oder den voll qualifizierten Domänennamen (FQDM) der globalen Katalogserver ein. DNS-Suche wird nicht durchgeführt. Mindestens eine der drei Adressen muss konfiguriert werden. iDRAC6 versucht, nacheinander mit jeder der konfigurierten Adressen eine Verbindung aufzubauen, bis eine Verbindung hergestellt ist.

ANMERKUNG: Der globale Katalogserver ist nur für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen in verschiedenen Domänen befinden. Bei einer mehrfachen Domäne wie dieser kann nur die Universalgruppe verwendet werden. Wenn Sie zum Konfigurieren von Active Directory die iDRAC6-Web-GUI verwenden, müssen Sie selbst dann eine globale Adresse eingeben, wenn sich der Benutzer und die Gruppe in derselben Domäne befinden.

20 Klicken Sie auf die Schaltfläche einer **Rollengruppe**, um diese hinzuzufügen

Der Bildschirm **Schritt 4b von 4 Rollengruppe konfigurieren** wird angezeigt.

21 Geben Sie den **Gruppennamen** ein. Der Gruppenname identifiziert die Rollengruppe in dem Active Directory, das dem iDRAC zugeordnet ist.

22 Geben Sie den **Gruppendomäne** ein. Die **Gruppendomäne** ist der vollständig qualifizierte root-Domänenname der Gesamtstruktur.

23 Richten Sie auf der Seite **Rollengruppenberechtigungen** die Gruppenberechtigungen ein. Unter Tabelle 5-13 erhalten Sie Informationen zu Rollengruppenberechtigungen.

ANMERKUNG: Wenn Sie eine Berechtigung modifizieren, wird die vorhandene Rollengruppenberechtigung (Administrator, Hauptbenutzer oder Gastbenutzer) auf Grundlage der modifizierten Berechtigungen entweder zur benutzerdefinierten Gruppe oder zur entsprechenden Rollengruppenberechtigung verändert.

24 Klicken Sie auf **OK**, um die Einstellungen der Rollengruppe zu speichern.

Ein Warnhinweis wird angezeigt und zeigt an, dass die Einstellungen geändert wurden. Klicken Sie auf **OK**, um zum Bildschirm **Schritt 4a von 4 Active Directory Konfiguration und Verwaltung** zurückzukehren.

25 Um eine weitere Rollengruppe hinzuzufügen, wiederholen Sie Schritt 20 bis Schritt 24.

26 Klicken Sie auf **Beenden** und anschließend auf **Fertig**.

Der Hauptzusammenfassungsbildschirm für **Active Directory Konfiguration und Verwaltung** wird angezeigt. Überprüfen Sie die Active Directory-Einstellungen, die Sie soeben konfiguriert haben.

27 Klicken Sie am Ende der Bildschirmanzeige auf **Einstellungen überprüfen**.

Der Bildschirm **Active Directory-Einstellungen überprüfen** wird angezeigt.

28 Geben Sie Ihren iDRAC6-Benutzernamen und Ihr Kennwort ein und klicken Sie auf **Überprüfung starten**.

Die Überprüfungsergebnisse und das Überprüfungsprotokoll werden angezeigt. Weitere Informationen finden Sie unter „Einstellungen testen“ auf Seite 172.

ANMERKUNG: Um die Anmeldung beim Active Directory zu unterstützen, müssen Sie einen DNS-Server korrekt im iDRAC6-Programm konfiguriert haben. Wechseln Sie in den Bildschirm **Netzwerk** (klicken Sie dazu auf **System→ iDRAC-Einstellungen** und dann auf **Netzwerk/Sicherheit→** Register **Netzwerk**), um manuell DNS-Server zu konfigurieren, oder verwenden Sie DHCP, um DNS-Server abzurufen.

Die Konfiguration des Active Directory mit Standardschema ist nun abgeschlossen.

Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM

Verwenden Sie die folgenden Befehle zum Konfigurieren der Active Directory-Funktion von iDRAC6 mit Standardschema unter Verwendung der RACADM-CLI statt der Webschnittstelle.

1 Öffnen Sie eine Eingabeaufforderung und geben Sie die folgenden RACADM-Befehle ein:

```
racadm config -g cfgActiveDirectory -o
cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 2

racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupName <common name of the role
group>

racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupDomain <fully qualified damain
name>

racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupPrivilege <Bit Mask Value for
specific Role group permissions>
```

ANMERKUNG: Informationen zu Bitmaskenwerten für spezifische Rollengruppenberechtigungen finden Sie unter Tabelle 6-9.

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <fully qualified domain
name or IP address of the domain controller>

racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <fully qualified domain
name or IP address of the domain controller>

racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <fully qualified domain
name or IP address of the domain controller>
```

ANMERKUNG: Geben Sie unbedingt den FQDN des Domänen-Controllers ein, *nicht* den FQDN der Domäne selbst. Geben Sie z. B. `servername.dell.com` ein und nicht `dell.com`.

ANMERKUNG: Mindestens eine der 3 Adressen muss konfiguriert werden. iDRAC6 versucht, nacheinander mit jeder der konfigurierten Adressen eine Verbindung aufzubauen, bis eine Verbindung hergestellt ist. Im Standardschema sind dies die Adressen der Domänen-Controller, auf denen sich die Benutzerkonten und die Rollengruppen befinden.

```
racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog1 <fully qualified domain name or IP
address of the domain controller>
```

```
rracadm config -g cfgActiveDirectory -o cfgGlobal
Catalog2 <fully qualified domain name or IP
address of the domain controller>
```

```
racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog3 <fully qualified domain name or IP
address of the domain controller>
```

ANMERKUNG: Im Standardschema ist der Global Catalog Server nur erforderlich, wenn die Benutzerkonten und Rollengruppen in verschiedenen Domänen liegen. Bei einer mehrfachen Domäne wie dieser kann nur die Universalgruppe verwendet werden.

ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie in diesem Feld angeben, muss mit dem Feld **Server** oder **Alternativer Servername** im Zertifikat Ihres Domänen-Controllers übereinstimmen, wenn Sie die Zertifikatsvalidierung aktiviert haben.

Wenn Sie für den SSL-Handshake die Zertifikatsvalidierung deaktivieren möchten, geben Sie den folgenden RACADM-Befehl ein:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

In diesem Fall brauchen Sie kein CA-Zertifikat zu laden.

Wenn Sie die Zertifikatsvalidierung auch beim SSL-Handshake durchführen möchten, geben Sie den folgenden RACADM-Befehl ein:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 1
```

In diesem Fall müssen Sie mit dem folgenden RACADM-Befehl auch das CA-Zertifikat hochladen:

```
racadm sslcertupload -t 0x2 -f <ADS root CA
certificate>
```

Die Verwendung des folgenden RACADM-Befehls kann optional sein. Weitere Informationen hierzu finden Sie unter „SSL-Zertifikat der iDRAC6-Firmware importieren“ auf Seite 139.

```
racadm sslcertdownload -t 0x1 -f <RAC SSL
certificate>
```

2 Wenn DHCP auf dem iDRAC6 aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgenden RACADM-Befehl ein:

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 1
```

3 Wenn DHCP auf dem iDRAC6 deaktiviert ist oder Sie ihre DNS IP-Adresse manuell eingeben möchten, geben Sie die folgenden RACADM-Befehle ein:

```
racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1
<primary DNS IP address>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2
<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, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgUserDomain -o
cfgUserDomainName <fully qualified domain name or
IP Address of the domain controller> -i <index>
```

Sie können bis zu 40 Benutzerdomänen mit Indexzahlen zwischen 1 and 40 erstellen.

Mehr Informationen zu Benutzerdomänen finden Sie unter „Verwendung des iDRAC6 mit Microsoft Active Directory“ auf Seite 135.

Einstellungen testen

Wenn Sie überprüfen möchten, ob eine Konfiguration korrekt funktioniert oder ob eine Problemanalyse der fehlgeschlagenen Anmeldung am Active Directory erforderlich ist, können Sie Ihre Einstellungen über die iDRAC6-Webschnittstelle prüfen.

Nach dem Konfigurieren von Einstellungen in der iDRAC6-Webschnittstelle klicken Sie am Ende der Bildschirmanzeige auf **Einstellungen überprüfen**. Sie müssen nun einen Überprüfungs-Benutzernamen (z. B. **benutzername@domäne.com**) und ein Kennwort eingeben, um die Überprüfung durchzuführen. Abhängig von den Einstellungen kann es einige Zeit dauern, bis alle Schritte der Überprüfung durchgeführt sind und die Ergebnisse der einzelnen Schritte angezeigt werden können. Am Ende der Bildschirmanzeige der einzelnen Ergebnisse wird ein ausführliches Protokoll der Überprüfung angezeigt.

Überprüfen Sie gegebenenfalls die einzelnen Fehlermeldungen und mögliche Lösungen im Testprotokoll. Informationen zu den am häufigsten auftretenden Fehlern finden Sie unter „Häufig gestellte Fragen“ auf Seite 177.

Wenn Sie Ihre Einstellungen ändern müssen, wählen Sie die Registerkarte **Active Directory** und ändern Sie die Konfiguration Schritt für Schritt.

iDRAC6 mit dem LDAP-Verzeichnisdienst verwenden

iDRAC6 bietet eine generische Lösung zur Unterstützung der LDAP-basierten (Lightweight Directory Access Protocol) Authentifizierung. Für diese Funktion ist keine Schemaerweiterung Ihrer Verzeichnisdienste erforderlich.

Um die iDRAC6 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 iDRAC6 konfiguriert werden.

Anmeldesyntax (Verzeichnis-Benutzer im Vergleich zum lokalen Benutzer)

Im Gegensatz zur Syntax bei Active Directory werden keine Sonderzeichen („@“, „\“ und „/“) verwendet, um einen LDAP-Benutzer von einem lokalen Nutzer zu unterscheiden. Der Anmeldebenutzer muss den Benutzernamen ohne den Domänennamen eingeben. iDRAC6 übernimmt den Benutzernamen so, wie er ist, ohne ihn in Benutzernamen und Benutzerdomäne zu unterteilen.

Wenn generisches LDAP aktiviert ist, versucht iDRAC6 zunächst, den Benutzer als Verzeichnis-Benutzer anzumelden. Schlägt dies fehl, wird die Suche nach lokalen Benutzern aktiviert.

ANMERKUNG: Es tritt keine Funktionsänderung der Active Directory-Anmeldesyntax auf. Wenn generisches LDAP aktiviert ist, zeigt die GUI-Anmeldungsseite nur **Dieser iDRAC** im Dropdown-Menü an.

ANMERKUNG: Bei diesem Release werden nur Verzeichnisdienste auf Basis von openLDAP, openDS, Novell eDir und Fedora unterstützt. Der Benutzername darf die Zeichen „<“ und „>“ nicht enthalten.

Konfiguration des generischen LDAP-Verzeichnisdienstes mit der iDRAC6-Webschnittstelle

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
3. Klicken Sie auf **System→ iDRAC-Einstellungen→** Register **Netzwerk/Sicherheit→ Verzeichnisdienst→ Allgemeiner LDAP-Verzeichnisdienst**.
4. Die Seite **Generisches LDAP - Konfiguration und Verwaltung** zeigt die aktuellen Einstellungen für den iDRAC6 und das generische LDAP an. Scrollen Sie auf der Seite **Generisches LDAP - Konfiguration und Verwaltung** nach unten und klicken Sie auf **Generisches LDAP konfigurieren**.

   Die Seite **Schritt 1 von 3 Generisches LDAP- Konfiguration und Verwaltung** wird angezeigt. Konfigurieren Sie auf dieser Seite das digitale Zertifikat, das Sie zum Aufbau von SSL-Verbindungen bei der Kommunikation mit einem generischen LDAP-Server verwendet haben. Bei diesen Kommunikationen wird LDAP über SSL (LDAPS) verwendet. Wenn Sie Zertifikatsvalidierung aktivieren, laden Sie das Zertifikat der Zertifikatsstelle (CA) hoch, die das vom LDAP-Server für den Aufbau von SSL-Verbindungen verwendete Zertifikat ausgestellt hat. Dieses CA-Zertifikat wird verwendet, um die Authentizität des vom LDAP-Server verwendeten Zertifikats bei der Einleitung von SSL zu bestätigen.

ANMERKUNG: Bei dieser Version wird eine LDAP-Bindung, die nicht auf einem SSL-Anschluss basiert, nicht unterstützt. Nur LDAP über SSL wird unterstützt.

5 Markieren Sie unter **Zertifikatseinstellungen** die Option **Zertifikatsvalidierung aktivieren**, um die Zertifikatsvalidierung zu aktivieren. Wenn diese Option aktiviert ist, verwendet iDRAC6 das CA-Zertifikat, um das LDAP-Serverzertifikat während des Secure Socket Layer (SSL)-Handshake zu validieren; ist sie deaktiviert, überspringt iDRAC6 die Zertifikatsvalidierung beim SSL-Handshake. Sie können die Zertifikatsvalidierung während eines Tests deaktivieren oder wenn sich Ihr Systemadministrator dafür entscheidet, den Domänen-Controllern im Sicherheitsbereich zu vertrauen, ohne ihre SSL-Zertifikate zu validieren.

VORSICHTSHINWEIS: Stellen Sie sicher, dass bei der Zertifikatserstellung CN = open LDAP FQDN (z. B. CN= openldap.lab) im Betreff-Feld des LADP-Serverzertifikats eingestellt ist. Damit die Zertifikatsvalidierung funktioniert, sollte das CN-Feld des Serverzertifikats so eingestellt sein, dass es dem Adressfeld des LDAP-Servers von iDRAC6 entspricht.

6 Geben Sie unter **Verzeichnisdienst-CA-Zertifikat laden** den Dateipfad des Zertifikats ein oder durchsuchen Sie das Verzeichnis, um die Zertifikatsdatei zu finden.

ANMERKUNG: Sie müssen den vollständigen Dateipfad eintippen, der den vollständigen Pfad und den kompletten Dateinamen und die Dateierweiterung umfasst.

7 Klicken Sie auf **Hochladen.**

Das Zertifikat der Stamm-CA, das sämtliche Security Socket Layer (SSL)-Serverzertifikate des Domänen-Controllers signiert, wird hochgeladen.

8 Klicken Sie auf **Weiter**, um auf die Seite **Schritt 2 von 3 Generisches LDAP - Konfiguration und Verwaltung** zu gelangen. Auf dieser Seite können Sie Informationen über die Speicherorte generischer LDAP-Server und Benutzerkonten konfigurieren.

ANMERKUNG: Bei dieser Version werden die Funktionen Smart Card-basierte Zweifaktor-Authentifizierung (TFA) und Einmaliges Anmelden (SSO) für den generischen LDAP-Verzeichnisdienst nicht unterstützt.

9 Wählen Sie **Generisches LDAP aktivieren** aus.

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.

10 Wählen Sie die Option **Distinguished Name zur Gruppenmitgliedschaft-Suche verwenden** aus, um den abgegrenzten Namen (DN, Distinguished Name) als Gruppenmitglieder zu verwenden. iDRAC6 vergleicht die aus dem Verzeichnis abgerufenen Benutzer-DN mit den Mitgliedern der Gruppe. Ist diese Option nicht markiert, wird der vom Anmeldebenutzer angegebene Benutzername zum Vergleich mit den Gruppenmitgliedern verwendet.

11 Geben Sie in das Feld **LDAP-Serveradresse** den FQDN oder die IP-Adresse des LDAP-Servers ein. Um mehrere redundante LDAP-Server anzugeben, die der gleichen Domäne dienen, legen Sie eine Liste aller Server an (durch Kommata getrennt). iDRAC6 versucht, sich nacheinander mit jedem Server zu verbinden, bis ein Verbindungsversuch erfolgreich ist.

12 Geben Sie den Anschluss, der für LDAP über SSL verwendet wird, in das Feld **LDAP-Serveranschluss** ein. Die Standardeinstellung ist 636.

13 Geben Sie in das Feld **Bindungs-DN** den DN eines Benutzers ein, der bei der Suche nach dem DN des Anmeldebenutzers zur Bindung an den Server verwendet wird. Wird hier nichts angegeben, wird eine anonyme Bindung verwendet.

14 Geben Sie das **Bindungskennwort** ein, das zusammen mit dem **Bindungs-DN** verwendet werden soll. Dies ist erforderlich, wenn keine anonyme Bindung zugelassen ist.

15 Geben Sie in das Feld **Basis-DN zur Suche** den DN des Verzeichnisasts ein, bei dem alle Suchen starten sollen.

16 Geben Sie in das Feld **Attribut der Benutzeranmeldung** das Benutzerattribut ein, nach dem gesucht werden soll. Die Standardeinstellung ist UID. Es wird empfohlen, hier ein innerhalb des Basis-DN eindeutiges Attribut zu wählen, da sonst ein Suchfilter konfiguriert werden muss, um den Anmeldebenutzer eindeutig sicherzustellen. Wenn der Benutzer-DN durch die Suchkombination von Attribut und Suchfilter nicht eindeutig identifiziert werden kann, schlägt die Anmeldung fehl.

17 Geben Sie im Feld **Attribut der Gruppenmitgliedschaft** an, welches LDAP-Attribut für die Überprüfung der Gruppenmitgliedschaft verwendet werden soll. Dies sollte ein Attribut der Gruppenklasse sein. Wird hier nichts angegeben, verwendet iDRAC6 die Attribute *member* und *uniquemember*.

18 Geben Sie in das Feld **Suchfilter** einen gültigen LDAP-Suchfilter ein. Verwenden Sie den Filter, wenn das Benutzerattribut den Anmeldebenutzer mit dem ausgewählten Basis-DN nicht eindeutig identifizieren kann. Wird hier nichts angegeben, wird der Standardwert *objectClass*=* zugrunde gelegt, mit dem nach allen Objekten in der Baumstruktur gesucht wird. Dieser zusätzliche, vom Benutzer konfigurierte Suchfilter kann nur für die Benutzer-DN-Suche und nicht für die Gruppenmitgliedschaft-Suche verwendet werden.

19 Klicken Sie auf **Weiter**, um auf die Seite **Schritt 3a von 3 Generisches LDAP - Konfiguration und Verwaltung** zu gelangen. Auf dieser Seite können Sie die Berechtigungsgruppen für Benutzerbefugnisse konfigurieren. Wenn generisches LDAP aktiviert ist, werden eine oder mehrere Rollengruppen verwendet, um die Befugnisrichtlinien für iDRAC6-Benutzer festzulegen.

20 Klicken Sie unter **Rollengruppen** auf eine **Rollengruppe**.

Die Seite **Schritt 3b von 3 Generisches LDAP - Konfiguration und Verwaltung** wird angezeigt. Auf dieser Seite können Sie jede zur Kontrolle der Benutzerbefugnisse verwendete Rollengruppe konfigurieren.

21 Geben Sie den **Gruppen-Distinguished Name (DN)** ein, der die mit iDRAC6 verbundene Rollengruppe im generischen LDAP-Verzeichnisdienst identifiziert.

22 Geben Sie im Abschnitt **Rollengruppe-Berechtigungen** die zur Gruppe gehörenden Berechtigungen an, indem Sie die **Rollengruppe-Berechtigungsebene** auswählen. Wenn Sie zum Beispiel **Administrator** auswählen, werden alle Berechtigungen für diese Berechtigungsebene ausgewählt.

23 Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern.

Der iDRAC6-Webserver führt Sie automatisch zur Seite **Schritt 3a von 3 Generisches LDAP - Konfiguration und Verwaltung** zurück, wo Ihre Rollengruppen-Einstellungen angezeigt werden.

24 Konfigurieren Sie bei Bedarf weitere Rollengruppen.

25 Klicken Sie auf **Fertigstellen,** um zur Zusammenfassungsseite **Generisches LDAP - Konfiguration und Verwaltung** zurückzukehren.

26 Klicken Sie auf **Einstellungen überprüfen,** um die Einstellungen für das generische LDAP zu überprüfen.

27 Geben Sie den Benutzernamen und das Kennwort eines Verzeichnisbenutzers ein, der zur Überprüfung der LDAP-Einstellungen ausgewählt wurde. Das Format hängt davon ab, welches *Attribut der Benutzeranmeldung* verwendet wird, und der eingegebene Benutzername muss dem Wert des gewählten Attributs entsprechen.

ANMERKUNG: Wenn die LDAP-Einstellungen überprüft werden und dabei „Zertifikatsüberprüfung aktiviert" ausgewählt ist, erfordert iDRAC6, 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 iDRAC6 nicht mit dem LDAP-Server kommunizieren kann.

Die Testergebnisse und das Testprotokoll werden angezeigt. Sie haben die Konfiguration des **Generischen LDAP-Verzeichnisdienstes** abgeschlossen.

Häufig gestellte Fragen

Probleme bei der Anmeldung im Active Directory

Mithilfe der Active Directory Einmaliges Anmelden dauert es fast vier Minuten, um sich am iDRAC6 anzumelden.

Das normale Active Directory Einmalige Anmelden dauert für gewöhnlich weniger als zehn Sekunden; es kann jedoch fast vier Minuten dauern, um sich mit dem Active Directory Einmaliges Anmelden am iDRAC6 anzumelden, wenn Sie auf der **Netzwerk**-Seite des iDRAC6 den **bevorzugten DNS-Server** und den **alternativen DNS-Server** angegeben haben und der bevorzugte DNS-Server ausgefallen ist. DNS-Zeitüberschreitungen sind zu erwarten, wenn ein DNS-Server ausgeschaltet ist. iDRAC6 meldet Sie unter Verwendung des alternativen DNS-Servers an.

Ich habe das Active Directory für eine im Windows Server 2008 Active Directory vorhandene Domäne konfiguriert und diese Konfigurationen vorgenommen. 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. Wenn ich jetzt versuche, mich unter Verwendung des Benutzers, der sich in der untergeordneten Domäne befindet, am iDRAC6 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 und diese zum Filtern von Gruppenrichtlinieneinstellungen verwenden.

Die Active Directory-Anmeldung ist gescheitert. Wie gehe ich vor?

iDRAC6 enthält in der Webschnittstelle ein Diagnoseprogramm.

1. Melden Sie sich über die Webschnittstelle als lokaler Benutzer mit Administratorrechten an.
2. Wählen Sie in der Systemstruktur **System→ iDRAC-Einstellungen→** Register **Netzwerk/Sicherheit → Verzeichnisdienst→ Microsoft Active Directory** aus.

   Der **Active Directory-**Zusammenfassungsbildschirm wird angezeigt.
3. Klicken Sie am Ende der Bildschirmanzeige auf **Einstellungen überprüfen**.

   Der Bildschirm **Active Directory-Einstellungen überprüfen** wird angezeigt.
4. Geben Sie einen Test-Benutzernamen und ein Kennwort ein und klicken Sie auf **Überprüfung starten**.

   iDRAC6 führt die Überprüfungen Schritt für Schritt durch und zeigt das Ergebnis für jeden Schritt an. iDRAC6 erstellt auch einen detaillierten Testbericht, anhand dessen Sie die verschiedensten Probleme lösen können.

Wenn die Probleme weiter bestehen, konfigurieren Sie Ihre Active Directory-Einstellungen, ändern Sie Ihre Benutzerkonfiguration und führen Sie den Test erneut durch, bis der Testbenutzer den Authentifizierungsschritt durchführen kann.

Ich habe die Überprüfung des Zertifikats deaktiviert, meine Active Directory-Anmeldung ist aber trotzdem gescheitert. Ich habe die Diagnosen von der GUI aus durchgeführt, und die Testergebnisse zeigen die folgende Fehlermeldung: Wo liegt das Problem, und wie kann ich es beheben?

```
FEHLER: Keine Verbindung zum LDAP-Server möglich,
Fehler:14090086: SSL-Routinen:
SSL3_GET_SERVER_CERTIFICATE: Zertifikatprüfung
fehlgeschlagen: Bitte überprüfen Sie, ob das
korrekte CA-Zertifikat auf den iDRAC hochgeladen
wurde. Kontrollieren Sie bitte auch, dass die
Gültigkeit des iDRAC die der Zertifikate nicht
überschreitet und die Adresse des im iDRAC
konfigurierten Domänen-Controllers mit dem
Directory-Server-Zertifikat übereinstimmt.
```

Wenn die Funktion zur Überprüfung des Zertifikats aktiviert ist, nutzt iDRAC6 bei bestehender SSL-Verbindung mit dem Server das verfügbare CA-Zertifikat zur Überprüfung des Active Directory Server-Zertifikats.
Die häufigsten Gründe für das Scheitern der Zertifizierung sind:

- Das Gültigkeitsdatum des iDRAC6 liegt nicht innerhalb des Gültigkeitszeitraums des Serverzertifikats oder des Zertifizierungsstellenzertifikats. Überprüfen Sie die iDRAC6-Zeit und den Gültigkeitszeitraum Ihres Zertifikats.
- Die im iDRAC6 konfigurierten Adressen der Domänen-Controller stimmen nicht mit dem Servernamen oder dem alternativen Servernamen im Verzeichnis überein.
  - Wenn Sie eine IP-Adresse nutzen, siehe „Ich verwende eine IP-Adresse als Adresse des Domänen-Controllers und erhalte keine Zertifikatsvalidierung. Worin besteht das Problem genau?“ auf Seite 181.
  - Wenn Sie einen FQDN nutzen, müssen Sie sicherstellen, dass Sie den FQDN des Domänen-Controllers nutzen, nicht den der Domäne selbst. Verwenden Sie z. B.: `Servername.beispiel.com` und *nicht* `beispiel.com`.

Was muss ich überprüfen, wenn ich mich nicht über Active Directory bei iDRAC6 anmelden kann?

Stellen Sie zunächst mithilfe der Funktion „Einstellungen überprüfen“ fest, wo das Problem liegt. Anleitungen hierzu finden Sie unter „Die Active Directory-Anmeldung ist gescheitert. Wie gehe ich vor?“ auf Seite 178

Dann lösen Sie das Problem anhand der vorgegebenen Schritte. Weitere Informationen finden Sie unter „Einstellungen testen“ auf Seite 172.

Die häufigsten Fragen werden in diesem Abschnitt beantwortet. Grundsätzlich sollte jedoch Folgendes überprüft werden:

1. Stellen Sie sicher, dass Sie während einer Anmeldung den korrekten Benutzerdomänennamen statt des NetBIOS-Namens verwenden.
2. Wenn Sie ein lokales iDRAC6-Benutzerkonto haben, melden Sie sich mit Ihren lokalen Anmeldeinformationen beim iDRAC6 an.
   a. Stellen Sie sicher, dass das Kontrollkästchen **Active Directory aktiviert** auf der Seite **Schritt 2 von 4 Active Directory Konfiguration und Verwaltung** markiert ist.
   b. Wenn die Zertifikatsvalidierung aktiviert ist, stellen Sie sicher, dass Sie das richtige Stamm-Zertifizierungsstellenzertifikat des Active Directory auf iDRAC6 hochgeladen haben. Das Zertifikat wird im **aktuellen** Feld des **Active Directory-Zertifizierungsstellenzertifikats** angezeigt. Stellen Sie sicher, dass sich die iDRAC6-Zeit innerhalb des Gültigkeitszeitraums des Zertifizierungsstellenzertifikats befindet.
   c. Wenn Sie das erweiterte Schema verwenden, ist sicherzustellen, dass der **iDRAC6-Name** und der **iDRAC6-Domänenname** mit der Active Directory-Umgebungskonfiguration übereinstimmen.

      Wenn Sie das Standardschema verwenden, stellen Sie sicher, dass der **Gruppenname** und die **Gruppendomäne** mit der Active Directory-Konfiguration übereinstimmen.
   d. Navigieren Sie zum Bildschirm **Netzwerk**. Wählen Sie **System→ iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Netzwerk** aus. Stellen Sie sicher, dass die DNS-Einstellungen korrekt sind.
   e. Überprüfen Sie die Domänen-Controller SSL-Zertifikate, um sicherzustellen, dass sich die iDRAC6-Zeit innerhalb des Gültigkeitszeitraums des Zertifikats befindet.

Überprüfen des Active Directory-Zertifikats

Ich verwende eine IP-Adresse als Adresse des Domänen-Controllers und erhalte keine Zertifikatsvalidierung. Worin besteht das Problem genau?

Prüfen Sie das Feld Servername oder alternativer Servername Ihres Domänen-Controller-Zertifikats. Gewöhnlich verwendet Active Directory den Hostnamen und nicht die IP-Adresse des Domänen-Controllers im Feld Servername oder alternativer Servername des Domänen-Controller-Zertifikats.

Das Problem kann folgendermaßen behoben werden:

- Konfigurieren Sie den Hostnamen (FQDN) des Domänen-Controllers als *Adresse(n) des Domänen-Controllers* auf dem iDRAC6, damit er mit dem Servernamen oder alternativen Servernamen des Server-Zertifikats übereinstimmt.
- Erstellen Sie das Server-Zertifikat erneut, um eine IP-Adresse im Feld Servername oder alternativer Servername zu verwenden, die mit der auf iDRAC6 konfigurierten IP-Adresse übereinstimmt.
- Deaktivieren Sie die Überprüfung des Zertifikats, wenn Sie dem Domänen-Controller beim SSL-Handshake ohne diese Überprüfung vertrauen.

Warum ist in der Standardkonfiguration des iDRAC6 die Überprüfung des Zertifikats aktiviert?

iDRAC6 setzt eine hohe Sicherheit durch, um die Identität des Domänen-Controllers, mit dem iDRAC6 eine Verbindung herstellt, sicherzustellen. Ohne Überprüfung des Zertifikats könnte 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 das GUI oder CLI deaktivieren.

Erweitertes Schema und Standardschema

Ich verwende das erweiterte Schema in einer Umgebung mit mehrfacher Domäne. Wie kann ich die Adresse(n) des Domänen-Controllers konfigurieren?

Verwenden Sie den Hostnamen (FQDN) oder die IP-Adresse des Domänen-Controllers bzw. der Domänen-Controller, die die Domäne bedienen, in der sich das iDRAC6-Objekt befindet.

Muss ich (eine) Global Catalog-Adresse(n) konfigurieren?

Wenn Sie im erweiterten Schema arbeiten, können Sie keine Global Catalog-Adressen konfigurieren, da diese im erweiterten Schema nicht verwendet werden.

Wenn Sie im Standardschema arbeiten und Benutzer und Rollengruppen verschiedenen Domänen angehören, müssen Sie (eine) Global Catalog Adresse(n) konfigurieren. In diesem Fall können Sie nur die Universalgruppe benutzen.

Wenn Sie im Standardschema arbeiten und alle Benutzer und alle Rollengruppen der selben Domäne angehören, brauchen Sie keine Global Catalog Adresse(n) zu konfigurieren.

Wie funktioniert die Abfrage im Standardschema?

iDRAC6 stellt zuerst eine Verbindung zu der/den konfigurierten Domänen-Controller-Adresse(n) her. Wenn die Benutzer und Rollengruppen dieser Domäne angehören, werden die Berechtigungen 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.

Verschiedenes

Verwendet iDRAC6 immer LDAP über SSL?

Ja Der gesamte Transfer erfolgt über den geschützten Anschluss 636 und/oder 3269.

Unter *Einstellungen überprüfen* führt iDRAC6 einen LDAP CONNECT durch, um das Problem herauszustellen; er führt jedoch keinen LDAP BIND auf einer ungesicherten Verbindung aus.

Unterstützt iDRAC6 den NetBIOS-Namen?

Nicht in dieser Version.

7

Konfiguration von iDRAC6 für Einmaliges Anmelden und Smart-Card-Anmeldung

Dieser Abschnitt enthält Informationen zum Konfigurieren von iDRAC6 für die Smart Card-Anmeldung von lokalen Benutzern und Active Directory-Benutzern sowie für die einfache Anmeldung (Single Sign-On, SSO) von Active Directory-Benutzern.

iDRAC6 unterstützt die Kerberos-basierte Active Directory-Authentifizierung zur Unterstützung der Active Directory Smart-Card-Anmeldungen und Einmaligen Anmeldungen (SSO).

Informationen zur Kerberos-Authentifizierung

Kerberos ist ein Netzwerk-Authentifizierungsprotokoll, das Systemen ermöglicht, auf sichere Weise über ein ungesichertes Netzwerk zu kommunizieren. Dazu wird den Systemen erlaubt, ihre Authentizität zu beweisen. Um den höheren Authentifizierungsstandards gerecht zu werden, unterstützt iDRAC6 jetzt Kerberos-basierte Active Directory-Authentifizierung zur Unterstützung von Active Directory Smart-Card- und Einmaliger Anmeldung (SSO).

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista und Windows Server 2008 verwenden Kerberos standardmäßig als Authentifizierungsmethode.

Der iDRAC6 verwendet Kerberos, um zwei Typen von Authentifizierungsmechanismen zu unterstützen: Einmalige Anmeldung über Active Directory und Active Directory Smart-Card-Anmeldung. Bei der einmaligen Anmeldung verwendet der iDRAC6 die Anmeldeinformationen des Benutzers, die im Betriebssystem zwischengespeichert werden, nachdem sich der Benutzer mit einem gültigen Active Directory-Konto angemeldet hat.

Bei der Active Directory-Smart Card-Anmeldung verwendet iDRAC6 Smart Card-basierte Zweifaktor-Authentifizierung (TFA) als Anmeldeinformationen, um eine Active Directory-Anmeldung zu ermöglichen.

Die Kerberos-Authentifizierung an iDRAC6 schlägt fehl, wenn die iDRAC6-Zeit von der Zeit des Domänen-Controllers abweicht. Es ist ein maximaler Unterschied von 5 Minuten zulässig. Um erfolgreiche Authentifizierung zu ermöglichen, synchronisieren Sie die Serverzeit mit der Zeit des Domänen-Controllers und setzen Sie dann den iDRAC6 zurück **(reset)**.

Sie können auch den folgenden RACADM-Zeitzonenabweichungsbefehl verwenden, um die Zeit zu synchronisieren:

```
racadm config -g cfgRacTuning -o
cfgRacTuneTimeZoneOffset <Abweichungswert>
```

Voraussetzungen für die Active Directory-SSO- und -Smart Card-Authentifizierung

Sowohl für die Active Directory-SSO- als auch die Active Directory-Smart Card-Authentifizierung sind folgende Maßnahmen Voraussetzung:

- Konfigurieren Sie den iDRAC6 für die Active Directory-Anmeldung. Weitere Informationen finden Sie unter„Verwendung des iDRAC6-Verzeichnisdiensts“ auf Seite 135.
- Registrieren Sie den iDRAC6 als Computer in der Active Directory-Root-Domäne.
  - **a** Klicken Sie auf **System→ iDRAC-Einstellungen→ Netzwerk/Sicherheit→** Unterregister **Netzwerk**.
  - **b** Geben Sie eine gültige IP-Adresse für **Bevorzugter/Alternativer DNS-Server** an. Dieser Wert ist die IP-Adresse des DNS, der Teil der Root-Domäne ist, die die Active Directory-Konten der Benutzer authentifiziert.
  - **c** Wählen Sie **iDRAC6 auf DNS registrieren** aus.
  - **d** Geben Sie einen gültigen **DNS-Domänennamen an**.
  - **e** Stellen Sie sicher, dass die Netzwerk-DNS-Konfiguration mit den Active Directory-DNS-Informationen übereinstimmt.

    Weitere Informationen finden Sie in der iDRAC6-Onlinehilfe.

- Zur Unterstützung der zwei neuen Authentifizierungsmechanismustypen unterstützt iDRAC6 die Konfiguration zur Selbstaktivierung als Kerberos-Dienst in einem Windows-Kerberos-Netzwerk. Die Kerberos-Konfiguration am iDRAC6 umfasst dieselben Schritte wie die Konfiguration eines Kerberos-Dienstes als Sicherheitsprinzipal in Windows Server Active Directory auf einem Nicht-Windows-Server.

  Mit dem Microsoft-Hilfsprogramm **ktpass** (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.

  Die vom Dienstprogramm ktpass abgerufene Keytab wird dem iDRAC6 als Datei-Hochladen zur Verfügung gestellt und als Kerberos-Dienst im Netzwerk aktiviert.

  Da es sich beim iDRAC6 um ein Gerät mit einem Nicht-Windows-Betriebssystem handelt, führen Sie das Dienstprogramm **ktpass** (Teil von Microsoft Windows) auf dem Domänen-Controller (Active Directory-Server) aus, auf dem Sie den iDRAC6 einem Benutzerkonto in Active Directory zuordnen möchten.

  Beispiel: Verwenden Sie den folgenden **ktpass**-Befehl, um die Kerberos-Keytab-Datei zu erstellen:

  ```
  C:\> ktpass.exe -princ
  HTTP/idracname.domainname.com@DOMAINNAME.COM -
  mapuser DOMAINNAME\username -mapOp set -crypto
  DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass
  <Kennwort> +DesOnly -out c:\krbkeytab
  ```

  ANMERKUNG: Wenn beim iDRAC6-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, kann sie nicht korrekt konfiguriert werden.

Nachdem der oben aufgeführte Befehl erfolgreich ausgeführt wurde, führen Sie bitte den folgenden Befehl aus:

```
C:\>setspn -a HTTP/idracname.domainname.com
username
```

Der Verschlüsselungstyp, den iDRAC6 für die Kerberos-Authentifizierung verwendet, lautet DES-CBC-MD5. Der Prinzipaltyp lautet KRB5_NT_PRINCIPAL. Die Eigenschaften des Benutzerkontos, dem der Dienstprinzipalname zugeordnet ist, muss die Eigenschaft DES-Verschlüsselungstypen für dieses Konto verwenden aktiviert haben.

ANMERKUNG: Sie müssen 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.

ANMERKUNG: Es wird empfohlen, das neueste **ktpass**-Dienstprogramm zum Erstellen der Keytab-Datei zu verwenden. Verwenden Sie außerdem beim Erstellen der Keytab-Datei *Kleinbuchstaben* für den **idracname** und den **Dienstprinzipalnamen**.

Dieses Verfahren erstellt eine Keytab-Datei, die Sie auf den iDRAC6 hochladen müssen.

ANMERKUNG: Das Keytab enthält einen Verschlüsselungsschlüssel und muss an einem sicheren Ort aufbewahrt werden.

Weitere Informationen zum Dienstprogramm **ktpass** finden Sie auf der Microsoft-Website unter: **http://technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

- Die iDRAC6-Zeit muss mit dem Active Directory-Domänen-Controller synchronisiert sein.

Browser-Einstellungen zum Aktivieren der Active Directory-SSO

So konfigurieren Sie die Browser-Einstellungen für Internet Explorer:

1. Öffnen Sie den Internet-Explorer.
2. Wählen Sie **Extras→ Internetoptionen→ Sicherheit→ Lokales Intranet** aus.
3. Klicken Sie auf **Sites**.

4 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.
5 Klicken Sie auf **Advanced** (Erweitert).
6 Fügen Sie alle betreffenden Domänennamen ein, die für iDRAC-Instanzen, die Teil der SSO-Konfiguration sind, verwendet werden (z. B. myhost.example.com.)
7 Klicken Sie auf **Cose** (Schließen) und anschließend auf **OK**.
8 Klicken Sie auf **OK**.

So konfigurieren Sie die Browser-Einstellungen für Firefox:

1 Öffnen Sie den Webbrowser Firefox.
2 Geben Sie in die Adresszeile `about:config` ein.
3 Geben Sie unter **Filter** `network.negotiate` ein.
4 Fügen Sie den iDRAC-Namen zu network.negotiate-auth.trusted-uris (kommaseparierte Liste verwenden) hinzu.
5 Fügen Sie den iDRAC-Namen zu network.negotiate-auth.delegation-uris (kommaseparierte Liste verwenden) hinzu.

Verwenden des Active Directory SSO

Sie können iDRAC6 aktivieren, um mithilfe von Kerberos, einem Netzwerk-Authentifizierungsprotokoll, die einmalige Anmeldung zu aktivieren. Weitere Informationen zum Einrichten des iDRAC6 zur Verwendung der einmaligen Anmeldung über Active Directory finden Sie unter „Voraussetzungen für die Active Directory-SSO- und -Smart Card-Authentifizierung“ auf Seite 184.

iDRAC6 für die Verwendung von SSO konfigurieren

1 Vergewissern Sie sich, dass Sie Folgendes durchgeführt haben:
   a Anlegen des Geräteobjekts, des Berechtigungsobjekts und des Zuordnungsobjekts im Active Directory-Server.

b Einstellung von Zugangsberechtigungen für das angelegte Berechtigungsobjekt. Es wird empfohlen, keine Administratorberechtigungen zu vergeben, da hiermit einige Sicherheitsprüfungen umgangen werden könnten.

c Ordnen Sie das Geräteobjekt und das Berechtigungsobjekt mit dem Zuordnungsobjekt zu.

d Fügen Sie dem Geräteobjekt den vorherigen SSO-Benutzer (anmeldender Benutzer) zu.

e Vergeben Sie die Zugangsberechtigung zum Zugriff auf das angelegte Zuordnungsobjekt an *authentifizierte Benutzer.*

Informationen zum Durchführen dieser Schritte finden Sie unter „iDRAC6-Benutzer und -Berechtigungen zum Active Directory hinzufügen“ auf Seite 153.

2 Öffnen Sie einen unterstützten Webbrowser.

3 Melden Sie sich an der iDRAC6-Webschnittstelle an.

4 Wählen Sie in der Systemstruktur **System→ iDRAC-Einstellungen→** Register **Netzwerk/Sicherheit → Netzwerk** aus. Überprüfen Sie auf der Seite **Netzwerk**, ob der **DNS-iDRAC6-Name** korrekt ist und mit dem für den vollständigen qualifizierten Domänennamen von iDRAC6 verwendeten Namen übereinstimmt.

5 Wählen Sie in der Systemstruktur **System→ iDRAC-Einstellungen→** Register **Netzwerk/Sicherheit→ Verzeichnisdienst→ Microsoft Active Directory** aus.

Der **Active Directory-**Zusammenfassungsbildschirm wird angezeigt.

6 Klicken Sie am Ende der Bildschirmanzeige auf **Active Directory konfigurieren**.

Der Bildschirm **Active Directory Konfiguration und Verwaltung, Schritt 1 von 4** wird angezeigt.

7 Um das SSL-Zertifikat des Active Directory-Servers zu überprüfen, aktivieren Sie das Kontrollkästchen **Zertifikatsvalidierung aktivieren** unter **Zertifikatseinstellungen.**

Wenn Sie das SSL-Zertifikat Ihres Active Directory-Servers nicht überprüfen möchten, tun Sie nichts und wechseln Sie direkt zu Schritt 9.

8 Unter **Active Directory CA-Zertifikat laden** geben Sie den Dateipfad des Zertifikats ein oder durchsuchen Sie das Verzeichnis nach der Datei und klicken Sie anschließend auf **Laden**.

ANMERKUNG: Sie müssen den vollständigen Dateipfad eingeben, der den gesamten Pfad und den vollen Dateinamen mit Dateierweiterung enthält.

Die Informationen zum Active Directory CA-Zertifikat, das Sie hochgeladen haben, werden im Abschnitt **Aktuelles Active Directory CA-Zertifikat** angezeigt.

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

Der Bildschirm **Active Directory Konfiguration und Verwaltung, Schritt 2 von 4** wird angezeigt.

10 Aktivieren Sie das Kontrollkästchen **Active Directory** aktivieren.

11 Mit der Option **Einmalige Anmeldung aktivieren** können Sie sich direkt nach der Anmeldung an der Workstation am iDRAC6 anmelden, ohne die Benutzerauthentifizierungs-Anmeldeinformationen für die Domäne (wie Benutzername und Kennwort) eingeben zu müssen.

Zum Anmelden am iDRAC6 mit dieser Funktion sollten Sie sich bereits mit einem gültigen Active Directory-Benutzerkonto am System angemeldet haben. Außerdem sollten Sie bereits das Benutzerkonto konfiguriert haben, mit dem Sie sich unter Verwendung der Active Directory-Anmeldeinformationen beim iDRAC6 anmelden möchten. Der iDRAC6 verwendet die zwischengespeicherten Active Directory-Anmeldeinformationen, um Sie anzumelden.

Führen Sie zum Aktivieren der einmaligen Anmeldung über die CLI diesen RACADM-Befehl aus:

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

12 Fügen Sie **Benutzerdomänenname** hinzu und geben Sie die IP-Adresse der Serveradresse des Domänen-Controllers ein. Wählen Sie entweder **Domänen-Controller mit DNS suchen** oder **Domänen-Controller-Adressen angeben** aus. Wählen Sie **Next** (Weiter) aus. Der Bildschirm **Active Directory Konfiguration und Verwaltung, Schritt 3 von 4** wird angezeigt.

13 Wählen Sie die Option **Standardschema** oder **Erweitertes Schema** und klicken Sie auf **Weiter**.

Wenn Sie **Standardschema** gewählt haben, fahren Sie mit Schritt 13 fort. Wenn Sie **Erweitertes Schema** gewählt haben, fahren Sie mit Schritt 14 fort.

14 Für Standardschema:

a Geben Sie auf der Seite **Schritt 4a von 4** Active Directory die IP-Adresse des **globalen Katalogservers** ein oder wählen Sie die Option **globale Katalogserver mit DNS suchen** aus und geben Sie den **Root-Domänennamen** ein, der für die DNS-Suche nach den globalen Katalogservern in Active Directory verwendet werden soll.

b Klicken Sie auf eine beliebige Rollengruppe und fügen Sie die Informationen der Rollengruppe hinzu, zu der Ihr Active Directory-Benutzer gehört. Das Fenster **Active Directory Schritt 4b von 4** wird angezeigt.

c Geben Sie den Rollengruppennamen, die Gruppendomäne, die Rollengruppen-Berechtigungsebenen sowie die erforderlichen Berechtigungen ein und klicken Sie auf **Fertig stellen**. Die Nachricht „Konfiguration erfolgreich abgeschlossen“ wird angezeigt. Klicken Sie auf **OK**. Das Fenster **Schritt 4a von 4** zeigt den angelegten Rollengruppennamen, die Gruppendomäne und die Gruppenberechtigungsebene an.

d Klicken Sie auf **Fertig stellen**. Die Erfolgsmeldung wird angezeigt.

15 Geben Sie für das erweiterte Schema im Fenster **Active Directory Schritt 4 von 4** den **iDRAC6-Namen** und den **iDRAC6-Domänennamen** an und klicken Sie auf **Fertig stellen**. Die Erfolgsmeldung wird angezeigt.

Unter Verwendung der SSO am iDRAC6 anmelden

1 Melden Sie sich unter Verwendung Ihres gültigen Active Directory-Netzwerkkontos an der Management Station an.

2 Melden Sie sich unter Verwendung des vollständig qualifizierten Domänennamens von iDRAC6 an der iDRAC6-Webseite an.

http://idracname.domain.com.

Der iDRAC6 meldet Sie an und verwendet dabei die Anmeldeinformationen, die im Betriebssystem zwischengespeichert wurden, als Sie sich unter Verwendung Ihres gültigen Active Directory-Netzwerkkontos angemeldet haben.

Smart Card-Authentifizierung konfigurieren

iDRAC6 unterstützt die Zweifaktor-Authentifizierung (TFA) durch Aktivieren der **Smart-Card-Anmeldung**.

Für herkömmliche Authentifizierungsschemata werden der Benutzername und das Kennwort zum Authentifizieren von Benutzern verwendet. Diese Option bietet minimale Sicherheit.

TFA bietet jedoch eine höhere Sicherheitsstufe, da die Benutzer zwei Authentifizierungsfaktoren angeben müssen („was sie haben" und „was sie wissen"). „Was sie haben" ist die Smart Card, das physische Gerät, und „was sie wissen" ist ein Geheimcode, z. B. ein Kennwort oder eine PIN.

Für die Zweifaktor-Authentifizierung ist es erforderlich, dass Benutzer ihre Identität durch die Angabe *beider* Faktoren bestätigen.

Smart Card-Anmeldung am iDRAC6 konfigurieren

So aktivieren Sie die iDRAC6-Smart-Card-Anmeldung über die Webschnittstelle:

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der iDRAC6-Webschnittstelle an.
3. Gehen Sie zum Bildschirm **Schritt 1 von 4 Active Directory Konfiguration und Verwaltung**.
4. Um das SSL-Zertifikat des Active Directory-Servers zu überprüfen, markieren Sie das Kontrollkästchen für **Zertifikatsvalidierung aktiviert** unter **Zertifikat-Einstellungen**. Wenn Sie das SSL-Zertifikat Ihres Active Directory-Servers nicht überprüfen möchten, springen Sie direkt zu Schritt 6.
5. Unter **Active Directory CA-Zertifikat laden** geben Sie den Dateipfad des Zertifikats ein oder durchsuchen Sie das Verzeichnis nach der Datei und klicken Sie anschließend auf **Laden**. Sie müssen den vollständigen Dateipfad eingeben, der den gesamten Pfad und den vollen Dateinamen mit Dateierweiterung enthält. Die Informationen zum Active Directory CA-Zertifikat, das Sie hochgeladen haben, werden im Abschnitt **Aktuelles Active Directory CA-Zertifikat** angezeigt.
6. Klicken Sie auf Weiter. Der Bildschirm **Schritt 2 von 4 Active Directory Konfiguration und Verwaltung** wird eingeblendet.

7. Wählen Sie das Kontrollkästchen **Active Directory aktiviert** aus.
8. Wählen Sie **Smart–Card–Anmeldung aktivieren** aus, um die Smart–Card-Anmeldung zu aktivieren. Sie werden bei allen nachfolgenden Anmeldungsversuchen über die GUI zu einer Smart-Card-Anmeldung aufgefordert.
9. Fügen Sie **Benutzerdomänenname** hinzu und geben Sie die IP-Adresse der Serveradresse des Domänen-Controllers ein. Wählen Sie **Next** (Weiter) aus.
10. Wählen Sie **Einstellungen zum Standardschema** auf der Seite **Schritt 3 von 4 Active Directory Konfiguration und Verwaltung** aus. Wählen Sie **Next** (Weiter) aus.
11. Geben Sie auf der Seite **Schritt 4a von 4 Active Directory** die IP-Adresse des **Global Catalog-Servers** ein. Fügen Sie Informationen über die Rollengruppen hinzu, bei der der gültige Active Directory-Benutzer Mitglied ist, indem Sie eine der Rollengruppen auswählen (Seite **Schritt 4b von 4 Rollengruppe konfigurieren**). Geben Sie den **Gruppennamen**, die **Gruppendomäne** und die **Rollengruppenberechtigungen** ein. Wählen Sie **OK** aus und dann **Fertig stellen**. Nachdem Sie **Fertig** ausgewählt haben, scrollen Sie auf der **Active Directory**-Zusammenfassungsseite wieder nach unten und wählen Sie **Kerberos-Keytab-Hochladen** aus.
12. Laden Sie eine gültige Kerberos-Keytab-Datei hoch. Stellen Sie sicher, dass die Zeit des Active Directory-Servers und die des iDRAC6 synchronisiert sind. Überprüfen Sie, dass sowohl die Zeit als auch die Zeitzonen korrekt sind, bevor Sie die Keytab-Datei hochladen. Weitere Informationen zum Erstellen einer Keytab-Datei finden Sie unter „Konfiguration von iDRAC6 für Einmaliges Anmelden und Smart-Card-Anmeldung“ auf Seite 183.

Heben Sie die Markierung der Option **Smart–Card–Anmeldung aktivieren** auf, um die Funktion der TFA-Smart-Card-Anmeldung zu deaktivieren. Wenn Sie sich das nächste Mal an der iDRAC6-GUI anmelden, werden Sie zur Eingabe eines Microsoft Active Directory- oder eines lokalen Benutzernamens und Kennworts für die Anmeldung aufgefordert, was als Standard-Anmeldeaufforderung der Webschnittstelle ausgegeben wird.

Unter Verwendung der Active Directory Smart-Card-Authentifizierung am iDRAC6 anmelden

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

1. Melden Sie sich über https am iDRAC6 an.

   `https://<IP-Adresse>`

   Wurde die Standard-HTTPS-Portnummer (443) geändert, geben Sie Folgendes ein:

   `https://<IP-Adresse>:<Anschlussnummer>`

   wobei *IP-Adresse* die IP-Adresse des iDRAC6 und *Anschlussnummer* die Nummer des HTTPS-Anschlusses ist.

   Die iDRAC6-Anmeldungsseite wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

2. Legen Sie die Smart Card ein.

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

   Sie werden über Ihre in Active Directory festgelegten Anmeldeinformationen am iDRAC6 angemeldet.

   ANMERKUNG: Die Smart Card muss nicht im Lesegerät verbleiben, damit Sie angemeldet bleiben.

Häufig gestellte Fragen zur SSO

Die SSO-Anmeldung schlägt bei Windows 7 und Windows Server 2008 R2 fehl.

Sie müssen die Verschlüsselungstypen DES_CBC_CRC und DES_CBC_MD5 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 starten Sie **gpedit**. Das Fenster **Lokaler Gruppenregeln-Editor** wird angezeigt.

3 Wechseln Sie zu **Lokale Computereinstellungen→ Windows-Einstellungen→ Sicherheitseinstellungen→ Lokale Regeln→ 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, und klicken Sie auf **OK**.

Fehler bei der Smart-Card-Anmeldung am iDRAC6 beheben

Wenden Sie die folgenden Tipps an, die beim Debuggen einer Smart Card, auf die nicht zugegriffen werden kann, behilflich sein können.

Bei Verwendung der Active Directory Smart-Card-Anmeldung dauert es fast vier Minuten, um sich am iDRAC6 anzumelden.

Die normale Active Directory Smart-Card-Anmeldung dauert für gewöhnlich weniger als zehn Sekunden, doch es kann fast vier Minuten dauern, um sich unter Verwendung der Active Directory Smart-Card-Anmeldung am iDRAC6 anzumelden, wenn Sie auf der **Netzwerk**-Seite des iDRAC6 den **bevorzugten DNS-Server** und den **alternativen DNS-Server** angegeben haben und der bevorzugte DNS-Server ausgefallen ist. DNS-Zeitüberschreitungen sind zu erwarten, wenn ein DNS-Server ausgeschaltet ist. iDRAC6 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.

Tipp: 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.

Anmeldung am iDRAC6 als Active Directory-Benutzer nicht möglich.

- Wenn Sie sich nicht als Active Directory-Benutzer am iDRAC6 anmelden können, versuchen Sie sich anzumelden, ohne die Smart-Card-Anmeldung zu aktivieren. Sie können die Smart-Card-Anmeldung über RACADM mit dem folgenden Befehl deaktivieren:

  ```
  racadm config -g cfgSmartCard -o
  cfgSmartCardLogonEnable 0
  ```

- Bei 64–Bit-Windows-Plattformen wird das iDRAC6-Authentifizierungs-Plug-In nicht korrekt installiert, wenn eine 64-Bit-Version des „Microsoft Visual C++ 2005 Redistributable Package" eingesetzt wird. Damit das Plug-In korrekt installiert und ausgeführt werden kann, muss die 32-Bit-Version des „Microsoft Visual C++ 2005 Redistributable Package" eingesetzt werden.
- Wenn die Fehlermeldung „`Not able to load the Smart Card Plug-in. Please check your IE settings or you may have insufficient privileges to use the Smart Card Plug-in`", („Smart-Card-Plug-In konnte nicht geladen werden. Überprüfen Sie bitte Ihre IE-Einstellungen, da Ihnen sonst ungenügende Berechtigungen zur Verwendung des Smart-Card-Plug-In zur Verfügung stehen könnten") eingeblendet wird, installieren Sie bitte das „Microsoft Visual C++ 2005 Redistributable Package". Die Datei steht auf der Microsoft-Website unter **www.microsoft.com** zur Verfügung. Zwei verteilte Versionen des C++ Redistributable Package wurden überprüft; diese ermöglichen, dass das Dell Smart Card-Plug-In geladen wird:

Tabelle 7-1. Verteilte Versionen des C++ Redistributable Package

Dateiname des Redistributable Package	Version	Freigabedatum	Größe	Beschreibung
vcredist_x86.exe	6.0.2900.2180	21. März 2006	2,56 MB	MS Redistributable 2005
vcredist_x86.exe	9.0.21022.8	7. November 2007	1,73 MB	MS Redistributable 2008

- Damit die Kerberos-Authentifizierung korrekt funktioniert, ist sicherzustellen, dass die iDRAC6-Zeit und die Domänen-Controller-Zeit beim Domänen-Controller-Server nicht mehr als 5 Minuten voneinander abweichen. Sie können die **iDRAC6-Zeit** unter **System→ iDRAC-Einstellungen→ Eigenschaften** auf der Seite **Remote-Zugriffsinformationen** nachprüfen; die Domänen-Controller-Zeit überprüfen Sie, indem Sie mit der rechten Maustaste auf die Uhrzeit in der rechten unteren Ecke des Bildschirms klicken. Der Zeitzonen-Unterschied wird in der Popup-Anzeige dargestellt. Für US Central Standard Time (CST) ist dies –6. Verwenden Sie den folgenden Befehl für den RACADM-Zeitzonen-Offset, um die iDRAC6-Zeit zu synchronisieren (durch Remote- oder Telnet/SSH-RACADM): `racadm config -g cfgRacTuning –o cfgRacTuneTimeZoneOffset <Offset-Wert in Minuten>`. Wenn die Systemzeit z. B. GMT-6 (US CST) ist und die Uhrzeit 14:00 Uhr, stellen Sie die iDRAC6-Zeit auf die GMT-Zeit von 18:00 Uhr, wozu Sie in den oben aufgeführten Befehl für den Offset „360“ eingeben müssen. Sie können auch `cfgRacTuneDaylightoffset` verwenden, um die Sommerzeitdifferenz zu berücksichtigen. Hierdurch können Sie vermeiden, jedes Jahr zu diesen beiden Anlässen die Zeit umzustellen, wenn die Zeitumstellung vorgenommen wird, oder berücksichtigen Sie sie im Offset des oben aufgeführten Beispiels einfach, indem Sie „300“ wählen.

8

Anzeige von Konfiguration und Zustand des verwalteten Servers

System Summary (Systemübersicht)

Die Seite **Systemzusammenfassung** ermöglicht Ihnen, den Systemzustand und andere grundlegende iDRAC6-Informationen auf einen Blick zu prüfen und bietet Links zum Zugriff auf die Systemzustand- und Informationsseiten. Außerdem können Sie über diese Seite allgemeine Aufgaben schnell starten und aktuelle protokollierte Ereignisse im Systemereignisprotokoll (SEL) anzeigen.

Um auf die Seite **Systemzusammenfassung** zuzugreifen, klicken Sie auf **System**→ Registerkarte **Eigenschaften**→ **Systemzusammenfassung**. In der *iDRAC6-Online-Hilfe* finden Sie detaillierte Informationen zu jedem Abschnitt der Seite **Systemzusammenfassung**.

Systemdetails

Die Seite **Systemdetails** enthält Informationen über die folgenden Systemkomponenten:

- Hauptsystemgehäuse
- Integrierter Dell Remote Access Controller 6 – Enterprise

Hauptsystemgehäuse

Systeminformationen

Dieser Abschnitt der iDRAC6-Webschnittstelle enthält die folgenden grundlegenden Informationen zum verwalteten Server:

- Beschreibung – Die Modellnummer oder der Name des verwalteten Servers.
- BIOS-Version – Die BIOS-Versionsnummer des verwalteten Servers.
- Service-Tag-Nummer – Service-Tag-Nummer des Servers.

- Express-Servicecode – Die Servicecodenummer des Systems. Sie entspricht der dezimal-numerischen Darstellung der Service-Tag-Nummer.
- Hostname – Der mit dem verwalteten Server verbundene DNS-Hostname.
- Betriebssystemname – Der Name des auf dem verwalteten Server installierten Betriebssystems.

  ANMERKUNG: Das Feld **BS-Name** ist nur dann ausgefüllt, wenn Dell OpenManage Server Administrator auf dem verwalteten System installiert ist. Eine Ausnahme hierzu stellen VMware-Betriebssystemnamen dar, die selbst dann angezeigt werden, wenn Server Administrator nicht auf dem verwalteten System installiert ist. Bei bestimmten Betriebssystemen kann es nach dem Serverstart einige Minuten dauern, bis der Betriebssystemname in iDRAC aktualisiert wird.
- Systemrevision – Die Geräte-Revisionsnummer.
- Lifecycle Controller-Firmware – Die Firmwareversion von Lifecycle Controller.

E/A-Mezzanine-Karte

In diesem Abschnitt der iDRAC6-Webschnittstelle erhalten Sie die folgenden Informationen über die E/A-Mezzanine-Karten, die auf dem verwalteten Server installiert sind:

- Verbindung – Führt die auf dem verwalteten Server installierte(n) E/A-Mezzaninkarte(n) auf. Die Liste zeigt auch die E/A-Mezzanine-Karten für Plattformen an, die Erweiterungskarten unterstützen.
- Vorhandenseinsstatus – zeigt an, of die Mezzanine-Karte vorhanden ist, oder ob es sich um eine Erweiterung des Steckplatzes der Mezzanine-Karte einer anderen Struktur handelt.
- Kartentyp – Der physische Typ der installierten Mezzanine-Karte/-Verbindung.
- Modellname – Modellnummer, Typ oder Beschreibung der installierten Mezzanine-Karte(n).

Integrierte Speicherkarte

Dieser Abschnitt der iDRAC6-Webschnittstelle enthält Informationen über die integrierte Speicher-Controller-Karte, die auf dem verwalteten Server installiert ist:

- Kartentyp – Zeigt den Modellnamen der installierten Speicherkarte an, z. B. SAS6/iR.

Integrierte Netzwerkkarte

Dieser Abschnitt der iDRAC6-Webschnittstelle bietet Informationen über die integrierte Netzwerkkarte, die auf dem verwalteten Server installiert ist. Er wird nur für geeignete Plattformen angezeigt.

- Kartentyp – Zeigt den Kartentyp der auf der Platine installierten integrierten Netzwerkkarte an, z. B. Gigabit Ethernet.
- Modellname – Zeigt den Modellnamen der integrierten Netzwerkkarte an.

Weitere Informationen über integrierte Netzwerkkarten finden Sie im *Hardware-Benutzerhandbuch*, verfügbar auf der Dell Support-Website unter **support.dell.com/manuals**.

Automatische Wiederherstellung

In diesem Abschnitt der iDRAC6-Webschnittstelle wird der aktuelle Betriebsmodus der Funktion Automatische Wiederherstellung auf dem verwalteten Server, wie zuvor von Open Manage Server Administrator eingestellt, beschrieben:

- Wiederherstellungsmaßnahme – Die Maßnahme wird durchgeführt, wenn ein Systemfehler oder *Hängen des Systems* erkannt wird. Verfügbare Maßnahmen sind **Keine Maßnahme**, **Hardware-Reset**, **Herunterfahren** oder **Aus- und Einschalten**.
- Anfänglicher Countdown – Der Zeitumfang (in Sekunden), bis der iDRAC6 eine Wiederherstellungsmaßnahme durchführt, nachdem ein Hängen des Systems erkannt wurde.
- Derzeitiger Countdown – Der aktuelle Wert (in Sekunden) des Countdown-Zeitgebers.

Integrierter Dell Remote Access Controller 6 – Enterprise

iDRAC6-Informationen

Dieser Abschnitt der iDRAC6-Webschnittstelle enthält folgende Informationen über den iDRAC6 selbst:

- Datum/Uhrzeit – Zeigt das aktuelle Datum und die aktuelle Uhrzeit (seit der letzten Aktualisierung der Seite) des iDRAC6 an.
- Firmware-Version – Zeigt die aktuelle Version der auf dem verwalteten Server installierten iDRAC6-Firmware an.

- CPLD-Version – Zeigt die CPLD (Complex Programmable Logic Device)-Version an.
- Erweiterte CPLD-Version – Zeigt die CPLD-Version der erweiterten Platine an.
- Firmware aktualisiert – Zeigt das Datum und die Uhrzeit der letzten erfolgreichen Aktualisierung der iDRAC6-Firmware an.
- MAC-Adresse – Zeigt die MAC-Adresse an, die dem LOM-Netzwerkschnittstellen-Controller (LAN auf der Hauptplatine) des iDRAC6 zugeordnet ist.

IPv4-Einstellungen

- Aktiviert – Zeigt an, ob die IPv4-Protokollunterstützung aktiviert oder deaktiviert ist

  ANMERKUNG: Die IPv4-Protokolloption ist standardmäßig aktiviert.
- DHCP Aktiviert – Ist aktiviert, wenn der iDRAC6 zum Abrufen der IP-Adresse und zugehöriger Informationen von einem DHCP-Server eingestellt ist.
- IP-Adresse – Zeigt die dem iDRAC6 (und nicht dem verwalteten Server) zugeordnete IP-Adresse an.
- Subnetzmaske – Zeigt die für den iDRAC6 konfigurierte TCP/IP-Subnetzmaske an.
- Gateway – Zeigt die IP-Adresse des für den iDRAC6 konfigurierten Netzwerk-Gateways an.
- DHCP zum Abrufen von DNS-Serveradressen verwenden – Zeigt an, ob DHCP zum Abrufen von DNS-Serveradressen verwendet wird.
- Bevorzugter DNS-Server – Zeigt den derzeit aktiven primären DNS-Server an.
- Alternativer DNS-Server – Zeigt die alternative DNS-Serveradresse an.

IPv6-Einstellungen:

- Aktiviert – Zeigt an, ob die IPv6-Protokollunterstützung aktiviert oder deaktiviert ist.
- Automatische Konfiguration aktiviert – Zeigt an, ob die automatische Konfiguration aktiviert oder deaktiviert ist.

- Link Lokale Adresse – Zeigt die lokale IPv6-Link-Adresse des iDRAC6-NIC an.
- IPv6 Adresse 1-16 – Zeigt bis zu 16 IPv6-Adressen (IPv6-Adresse 1 bis IPv6-Adresse 16) für iDRAC6 NIC an.
- Gateway – Zeigt die IP-Adresse des für den iDRAC6 konfigurierten Netzwerk-Gateways an.
- DHCPv6 zum Abrufen von DNS-Serveradressen verwenden – Zeigt an, ob DHCP zum Abrufen von DNS-Serveradressen verwendet wird.
- Bevorzugter DNS-Server – Zeigt den derzeit aktiven primären DNS-Server an.
- Alternativer DNS-Server – Zeigt die alternative DNS-Serveradresse an.

ANMERKUNG: Diese Informationen sind außerdem verfügbar unter **System→ iDRAC-Einstellungen→ Eigenschaften→ Remote-Zugriffsinformationen**.

Integrierte NIC-MAC-Adressen

- NIC 1 – Zeigt die MAC (Media Access Control)-Adressen des eingebetteten Netzwerkschnittstellen-Controllers (NIC) 1 an.

  MAC-Adressen identifizieren jeden Knoten der Media Access Control-Schicht eindeutig.

  Der iSCSI (Internet Small Computer System Interface)-NIC ist ein Netzwerkschnittstellen-Controller, dessen iSCSI-Stack auf dem Host-Computer ausgeführt wird.

  Ethernet-NICs unterstützen den verkabelten Ethernet-Standard und werden in den Systembus des Servers eingesetzt.
- NIC 2 – Zeigt die MAC-Adresse(n) des eingebetteten NIC 2 an, über den sie im Netzwerk eindeutig identifiziert werden.
- NIC 3 – Zeigt die MAC-Adresse(n) des eingebetteten NIC 3 an, über den sie im Netzwerk eindeutig identifiziert werden. Die MAC-Adressen des eingebetteten NIC 3 können unter Umständen nicht auf allen Systemen angezeigt werden.
- NIC 4 – Zeigt die MAC-Adresse(n) des eingebetteten NIC 4 an, über den sie im Netzwerk eindeutig identifiziert werden. Die MAC-Adressen des eingebetteten NIC 4 können unter Umständen nicht auf allen Systemen angezeigt werden.

Bei den eingebetteten NIC-MAC-Adressen, die über den racadm-Befehl `getSysInfo` ausgegeben werden, und der MAC-Adresse, die unter **System→ Eigenschaften→ Systemdetails** angezeigt wird, handelt es sich um die Server-zugewiesenen MAC-Adressen. Wenn es sich um remote verwaltete oder Gehäuse-zugewiesene MAC-Adressen handelt, werden die aktiven MAC-Adressen unter **System→ Eigenschaften→ WWN/MAC** angezeigt.

WWN/MAC

Klicken Sie auf **System→** Register **Eigenschaften→ WWN/MAC**, damit die aktuelle Konfiguration der installierten E/A-Mezzanine-Karten und ihrer zugeordneten Netzwerkstrukturen angezeigt werden. Sie können auch die remote zugewiesenen MAC-Adressen anzeigen. Wenn die Funktion FlexAddress im CMC aktiviert ist, ersetzen die global zugewiesenen (Gehäuse-zugewiesenen) permanent gültigen MAC-Adressen die fest verdrahteten Werte der einzelnen LOMs.

Server-Funktionszustand

Klicken Sie auf **System→ Register Eigenschaften→ Systemzusammenfassung**. Im Abschnitt **Server-Funktionszustand** können Sie durch Klicken auf die verschiedenen Links wichtige Informationen zum Funktionszustand von iDRAC6 und zu den von iDRAC6 überwachten Komponenten anzeigen. In der Spalte **Zustand** ist der Zustand jeder Komponente aufgeführt. Eine Liste von Zustandssymbolen und deren Bedeutung finden Sie unter Tabelle 19-3. Klicken Sie auf den Komponentennamen in der Spalte **Komponente**, um weitere Informationen über die jeweilige Komponente zu erfahren.

ANMERKUNG: Sie können Komponenteninformationen ebenso erhalten, indem Sie im linken Fensterbereich auf den Komponentennamen klicken. Komponenten bleiben im linken Fensterbereich unabhängig vom ausgewählten Register/Bildschirm sichtbar.

Die im Abschnitt **Server-Funktionszustand** verfügbaren Komponenten-Links werden in den folgenden Abschnitten ausführlich beschrieben.

iDRAC6

Auf dem Bildschirm **Remote-Zugriffsinformationen** finden Sie eine Liste wichtiger Details zum iDRAC6, wie z. B. den Namen, die Firmware-Revision, aktualisierte Firmware, die iDRAC6-Zeit, die IPMI-Version, die CPLD-Version, den Servertyp sowie Netzwerkparameter. Weitere Einzelheiten finden Sie auf den jeweiligen Registerkarten am oberen Rand der Bildschirmanzeige.

In **iDRAC-Zeit** wird entweder die BIOS-Zeit oder die CMC-Zeit angezeigt. Bei einem Neustart des Systems sendet das BIOS die Zeit an iDRAC. Wird das Hostsystem beim Starten von iDRAC eingeschaltet, erhält iDRAC die Zeit vom BIOS. Wird das Hostsystem nicht beim Starten von iDRAC eingeschaltet, erhält iDRAC die Zeit vom CMC. Das BIOS ist also die bevorzugte Quelle, allerdings muss der Hostserver eingeschaltet sein, damit die BIOS-Zeit übernommen werden kann.

Der Firmware-Zeitstempel entspricht stets dem letzten Zeitstempel, den iDRAC vor der Firmware-Aktualisierung aufwies. Dies kann entweder die BIOS-Zeit sein, wenn das System vor der Firmware-Aktualisierung gestartet oder neu gestartet wurde, oder aber die CMC-Zeit.

CMC

Der CMC-Bildschirm zeigt den Funktionszustand, die Firmware-Revision und die IP-Adressen des Chassis Management Controller an. Außerdem kann durch Klicken auf die Schaltfläche **CMC-Webschnittstelle starten** die CMC-Webschnittstelle gestartet werden. Weitere Informationen stehen im *Benutzerhandbuch zur Dell Chassis Management Controller-Firmware* zur Verfügung.

ANMERKUNG: Durch das Starten der CMC-Web-GUI über den iDRAC6 wird die Suche mit demselben IP-Adressenformat weitergeleitet. Wenn Sie z. B. eine iDRAC6-Web-GUI mit einem IPv6-Adressenformat öffnen, wird auch die CMC-Webseite mit einer gültigen IPv6-Adresse geöffnet.

Batterien

Der Bildschirm **Batterien** zeigt den Status der Systemplatinen-Knopfzellenbatterie an, die die Echtzeituhr (RTC) und den Datenspeicher für die CMOS-Konfiguration auf dem verwalteten System mit Strom versorgt.

Temperatures (Temperaturen)

Der Bildschirm **Temperaturen** zeigt den Status und die Messwerte der Umgebungstemperatursonde auf der Platine an. Minimale und maximale Temperaturschwellenwerte für die Zustände *Warnung* oder *Fehler* werden zusammen mit dem aktuellen Funktionszustand der Sonde angezeigt.

ANMERKUNG: Temperaturschwellenwerte für die Zustände *Warnung* und *Fehler* und/oder der Funktionszustand der Sonde können abhängig vom Servermodell eventuell nicht angezeigt werden.

Spannungen

Der Bildschirm **Spannungssonden** zeigt den Status und Messwert der Spannungssonden an und liefert Informationen, wie z. B. zum Status der Spannungsschiene auf der Platine und zu den CPU-Kernsensoren.

Stromüberwachung

Auf dem Bildschirm **Stromüberwachung** erhalten Sie die folgenden Informationen zur Überwachungs- und Stromstatistik:

- Stromüberwachung – Zeigt die Menge an Strom (eine Minute durchschnittlicher Stromwert, gemessen in AC-Watt) an, der gemäß Stromüberwachungsbericht der Systemplatine vom Server verbraucht wird.
- Stromstärke – Zeigt den gegenwärtigen Verbrauch (Wechselstrom in Ampere) der aktiven Netzteileinheit an.
- Stromverfolgungsstatistik – Zeigt Informationen über die Menge des vom System verbrauchten Stroms an, seit der Messwert das letzte Mal zurückgesetzt wurde.
- Spitzenwert-Statistik – Zeigt Informationen über den Spitzenwert des vom System verbrauchten Stroms an, seit der Messwert das letzte Mal zurückgesetzt wurde.
- Stromverbrauch – Zeigt den durchschnittlichen, minimalen und maximalen Stromverbrauch, sowie die Zeit des maximalen und minimalen Stromverbrauchs des Systems (vorangehende(r) Minute, Stunde, Tag und Woche) an.
- Diagramm anzeigen – Zeigt eine grafische Darstellung des Stromverbrauchs während 1 Stunde, 24 Stunden, 3 Tagen und 1 Woche an.

ANMERKUNG: Strom und Stromstärke werden in Wechselstrom gemessen.

CPU

Der **CPU**-Bildschirm berichtet den Funktionszustand der einzelnen CPUs auf dem verwalteten Server. Dieser Funktionszustand wird aus zahlreichen individuellen Wärme-, Strom- und Funktionstests zusammengesetzt.

POST

Die Seite **POST-Code** zeigt den letzten POST-Code des Systems (hexadezimal) an, bevor das Betriebssystem des verwalteten Servers gestartet wurde.

Sonstige Zustände

Die Seite **Sonstige Zustände** gewährt Zugriff auf die folgenden Systemprotokolle:

- System-Ereignisprotokoll – Zeigt systemkritische Ereignisse an, die auf dem verwalteten System auftreten.
- POST-Code – Zeigt den letzten POST-Code des Systems (hexadezimal) an, bevor das Betriebssystem des verwalteten Servers gestartet wurde.
- Bildschirm Letzter Absturz – Zeigt den Bildschirm und die Uhrzeit des letzten Absturzes an.
- Start-Capture – Gibt die letzten drei Startbildschirme wieder.

ANMERKUNG: Diese Informationen stehen auch unter **System**→ Register **Protokolle**→ **Systemereignisprotokoll** zur Verfügung.

Systembestand

Auf der Seite **Systembestand** werden die auf dem verwalteten System installierten Hardware- und Firmware-Komponenten angezeigt.

Klicken Sie zum Aufrufen der Systembestandsseite auf **System**→ **Eigenschaften**→ **Systembestand**.

Im Abschnitt **Hardware-Bestandsliste** werden Informationen zu den verschiedenen Komponenten angezeigt, z. B. zum iDRAC, zum installierten RAID-Controller, zu den installierten CPUs, DIMMs, HDDs und Host-NICs (integrierte und eingebettete), zur installierten Videokarte und ggf. zur installierten SD-Karte.

Im Abschnitt **Firmware-Bestandsliste** werden Versionsinformationen zu den Firmware-Komponenten angezeigt, z. B. zum BIOS, zu Lifecycle Controller (USC) und zur iDRAC-Firmware.

In jedem Feld können maximal 48 Zeichen angezeigt werden. Bei mehr als 48 Zeichen wird die Zeichenfolge abgeschnitten.

Weitere Informationen finden Sie in der *iDRAC6-Online-Hilfe*.

Gehen Sie folgendermaßen vor, um sicherzustellen, dass die Systembestandserfassung funktioniert:

1. Das System muss für die Erfassung der Systembestandsdaten konfiguriert sein. Verwenden Sie dazu das iDRAC-Options-ROM-Dienstprogramm während des Systemstarts (Strg-E). Aktivieren Sie im Menü **Systemdienste** die Option **Systembestand bei Neustart erfassen (CSIOR)**.
2. Nach dem Aktivieren der CSIOR-Option bootet das Hostsystem neu und startet. Gegen Ende des BIOS-Startvorgangs weist nach einigen Minuten eine Meldung im Ausgabebildschirm darauf hin, dass der Systembestand erfasst wird.
3. Führen Sie nach dem Neustart des Hosts und der Erfassung des Systembestands lediglich einen Neustart des iDRAC durch.
4. Sobald der iDRAC startet, kann auf die Hardware-Bestandsliste zugegriffen werden.

   Nach einem Neustart des iDRAC sind die erforderlichen internen Komponenten für die Bedienung der Anfragen, durch die die Hardware-Bestandliste bereitgestellt wird, nicht sofort verfügbar. Warten Sie daher nach dem Neustart 5 Minuten ab, bevor Sie die Verbindung zum iDRAC zum Anzeigen der Hardware-Bestandsliste herstellen. Dies kann mehrere Minuten nach dem ersten Zurücksetzen des iDRAC sein. Alternativ können Sie anhand der WSMAN-Überprüfung für die Verfügbarkeit von Remote-Diensten auf dem iDRAC feststellen, wann die Hardware-Bestandsliste verfügbar ist. Verwenden Sie zum Aufrufen die GetRSStatus-Methode der DCIM_LCService-Klasse. Weitere Details finden Sie in der Datei „Dell DCIM LC Service MOF“, die unter **www.delltechcenter.com** verfügbar ist. Der Remote-Dienst muss vor der Hardware-Bestandsliste verfügbar sein. Dies gilt unabhängig davon, ob ein Neustart des iDRAC erfolgt ist oder nicht (siehe Schritt 3).

Fehlerbehebung

Auf der Seite „Hardware-Bestandsliste“ wird angezeigt, dass keine Hardware-Bestandsinformationen verfügbar sind.

Stellen Sie sicher, dass die beschriebenen Schritte zur ordnungsgemäßen Aktivierung der Hardware-Bestandserfassung ausgeführt wurden. Insbesondere ist die erforderliche Mindestwartezeit auf dem iDRAC nach einem iDRAC-Neustart einzuhalten, bevor versucht wird, die Bestandsseite aufzurufen. Diese Mindestwartezeit ist bei jedem iDRAC-Neustart (einschließlich Firmware-Aktualisierung) zu berücksichtigen. Führen Sie die WSMAN-Überprüfung für die Verfügbarkeit von Remote-Diensten durch, um festzustellen, wann die Hardware-Bestandsliste verfügbar ist.

In der Hardware-Bestandsliste fehlen einige Hardware-Attributswerte.

Möglicherweise werden einige Werte für bestimmte Hardware-Komponenten nicht ordnungsgemäß befüllt. Die darunter liegenden Elemente, die diese Daten abrufen, weisen sehr wahrscheinlich leere Felder auf. Dies wird in der GUI entsprechend dargestellt. In der iDRAC-GUI werden die erhaltenen Informationen ordnungsgemäß dargestellt. Wenn Daten fehlen, fehlen diese auch in der USC-Hardware-Bestandsliste. Wenn die Hardware-Komponente neu angeschlossen werden kann, schließen Sie sie neu an, und prüfen Sie, ob das Problem behoben wurde. Wenn die Hardware-Komponente ausgetauscht werden kann, tauschen Sie sie aus. Das Problem sollte danach nicht mehr auftreten. Stellen Sie nach dem neuerlichen Anschließen bzw. nach dem Austauschen einer Komponente sicher, dass die CSIOR-Funktion ausgeführt wird, und führen Sie die WSMAN-Überprüfung für die Verfügbarkeit von Remote-Diensten durch, bevor Sie versuchen, die aktualisierte Bestandsliste anzuzeigen.

Die Hardware-Bestandsliste weist mehrheitlich leere Datenfelder auf und es fehlen zahlreiche unterstützte Komponenten.

Dieses Problem tritt in der Regel dann auf, wenn die CSIOR-Funktion nicht aktiviert ist oder wenn Daten einer früheren Erfassung verloren gegangen sind. Um die vollständige Bestandsliste zu erhalten, starten Sie das System, und stellen Sie bei der Einrichtung über Strg-E für Systemdienste sicher, dass die CSIOR-Funktion aktiviert ist. Vergewissern Sie sich, dass vor dem Starten des Hosts die Erfassung des Systembestands im Bildschirm durch eine entsprechende Meldung bestätigt wird (Systembestand wird erfasst...).

Es fehlen Firmware-Bestandsdaten oder die LC-Version auf der Seite „Systemzusammenfassung“ bzw. „Systemdetails“ wird als „Nicht gefunden“ angezeigt.

Versuchen Sie, das Problem durch einen iDRAC-Neustart zu beheben. Möglicherweise müssen Sie außerdem die iDRAC-Firmware aktualisieren, auch wenn es sich dabei um eine Aktualisierung auf die derzeit installierte Firmware handelt.

9

Seriell über LAN konfigurieren und verwenden

Seriell über LAN (SOL) ist eine IPMI-Funktion, mit der textbasierte Konsolendaten eines verwalteten Servers, die üblicherweise über die serielle E/A-Schnittstelle gesendet würden, über das dedizierte Außenband-Ethernet-Verwaltungsnetzwerk des iDRAC6 umgeleitet werden. Die SOL-bandexterne Konsole ermöglicht Systemadministratoren, die textbasierte Konsole des Blade-Servers von einem beliebigen Standort mit Netzwerkzugriff aus im Remote-Zugriff zu verwalten. Vorteile des SOL-Systems:

- Im Remote-Verfahren und ohne Zeitüberschreitung auf Betriebssysteme zugreifen.
- Hostsysteme auf Emergency Management Services (EMS) oder Special Administrator Console (SAC) für Windows oder in einer Linux-Shell diagnostizieren.
- Den Fortschritt eines Blade-Servers während POST anzeigen und das BIOS-Setup-Programm neu konfigurieren (während der Umleitung auf eine serielle Schnittstelle).

Seriell über LAN im BIOS aktivieren

Um einen Server ordnungsgemäß für Seriell über LAN zu konfigurieren, sind die folgenden Konfigurationsschritte erforderlich. Sie werden im Detail beschrieben.

1. Seriell über LAN im BIOS konfigurieren (standardmäßig deaktiviert).
2. iDRAC6 für Seriell über LAN konfigurieren.
3. Wählen Sie eine Methode zum Initialisieren von Seriell über LAN aus (SSH, Telnet, SOL-Proxy oder IPMI-Hilfsprogramm).
4. Betriebssystem für SOL konfigurieren.

Die serielle Kommunikation ist im BIOS standardmäßig **aus**geschaltet. Um die Daten der Hosttextkonsole zu Seriell über LAN umzuleiten, müssen Sie die virtuelle Konsole über COM1 aktivieren.

So ändern Sie die BIOS-Einstellung:

1. Starten Sie den verwalteten Server.
2. Drücken Sie <F2>, um das BIOS-Setup-Dienstprogramm während POST aufzurufen.
3. Scrollen Sie zu Serielle Kommunikation herunter und drücken Sie die Taste <Eingabe>.

   Im Popup-Fenster wird die Liste der seriellen Kommunikation mit den folgenden Optionen angezeigt:

   - Aus
   - Ein ohne virtuelle Konsole
   - Ein mit virtueller Konsole

   Verwenden Sie die Pfeiltasten, um zwischen Optionen hin und her zu navigieren.
4. Stellen Sie sicher, dass **Ein mit virtueller Konsole** aktiviert ist. Stellen Sie sicher, dass die **Adresse der seriellen Schnittstelle** COM1 lautet.
5. Stellen Sie sicher, dass die **Failsafe-Baudrate** mit der SOL-Baudrate identisch ist, die auf iDRAC6 konfiguriert ist. Der Standardwert sowohl für die Einstellung der Failsafe-Baudrate als auch der SOL-Baudrate des iDRAC6 beträgt 115,2 Kbit/s.
6. Stellen Sie sicher, dass **Umleitung nach dem Start** aktiviert ist. Durch diese Option wird die BIOS-SOL-Umleitung über nachfolgende Neustarts aktiviert. Für BIOS gelten die **Remote-Terminaltyp**-Werte VT100/VT220 und ANSI.
7. Speichern Sie die Änderungen und beenden Sie.

   Der verwaltete Server startet neu.

Seriell über LAN in der iDRAC6-Web-GUI konfigurieren

1. Öffnen Sie den Bildschirm **Seriell über LAN-Konfiguration**, indem Sie **System→ iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Seriell über LAN** auswählen.
2. Stellen Sie sicher, dass die Option **Seriell über LAN aktivieren** ausgewählt (aktiviert) ist. Standardmäßig ist sie aktiviert.
3. Wählen Sie im Drop-Down-Menü **Baudrate** die IPMI SOL-Baudrate (Datengeschwindigkeit) aus. Die Optionen lauten 9600 Bit/s, 19,2 Kbit/s, 57,6 Kbit/s und 115,2 Kbit/s. Der Standardwert lautet 115,2 Kbit/s.
4. Wählen Sie im Drop-Down-Menü **Kanalberechtigungsebenenlimit** eine Berechtigungsebene für SOL aus.

ANMERKUNG: Stellen Sie sicher, dass die SOL-Baudrate mit der Failsafe-Baudrate, die im BIOS eingestellt wurde, identisch ist.

5. Auf **Anwenden klicken**, um die Einstellungen zu speichern.
6. Klicken Sie auf **Erweiterte Einstellungen**. Es wird der Bildschirm **Seriell über LAN-Konfiguration Erweiterte Einstellungen** angezeigt, mit dem Sie die SOL-Leistung einstellen können. Siehe Tabelle 9-1.

Tabelle 9-1. Einstellungen der Seite Seriell über LAN - Konfiguration - Erweiterte Einstellungen

Einstellung	Beschreibung
?Intervall der Zeichenakkumulation	Der typische Zeitumfang, den iDRAC6 abwartet, bevor er ein teilweises SOL-Datenpaket sendet. Dieser Parameter wird in Millisekunden angegeben. Für eine optimale Leistung werden 10 Millisekunden empfohlen.
Schwellenwert der gesendeten Zeichen	Gibt die Anzahl von Zeichen pro SOL-Datenpaket an. Sobald die Anzahl der vom iDRAC6 akzeptierten Zeichen gleich dem oder größer als der Schwellenwert der gesendeten Zeichen ist, beginnt der iDRAC6, SOL-Datenpakete zu übertragen, deren Zeichenanzahl gleich dem oder kleiner als der Schwellenwert der gesendeten Zeichen ist. Wenn ein Paket weniger Zeichen enthält als dieser Wert, wird es als teilweises SOL-Datenpaket definiert. Für eine optimale Leistung werden 255 Zeichen empfohlen.

ANMERKUNG: Wenn Sie diese Werte auf niedrigere Werte herabsetzen, kann dies eventuell zu einer Leistungsminderung der SOL-Funktion Virtuelle Konsole führen. Des Weiteren muss die SOL-Sitzung den Empfang einer Bestätigung für jedes Paket abwarten, bevor das nächste Paket gesendet werden kann. Es ergibt sich daraus eine bedeutend herabgesetzte Leistung.

7 Auf **Anwenden klicken**, um die Einstellungen zu speichern.

8 Konfigurieren Sie SSH und Telnet für SOL unter **System→ iDRAC-Einstellungen→** Registerkarte **Netzwerk/Sicherheit→ Dienste**.

ANMERKUNG: Jeder Blade-Server unterstützt nur eine (1) aktive SOL-Sitzung.

ANMERKUNG: Das SSH-Protokoll ist standardmäßig aktiviert. Das Telnet-Protokoll ist standardmäßig deaktiviert.

9 Klicken Sie auf **Dienste**, um den Bildschirm **Dienste** zu öffnen.

ANMERKUNG: Sowohl SSH- als auch Telnet-Programme bieten Zugriff auf ein Remote-System.

10 Klicken Sie je nach Bedarf auf **Aktiviert** – entweder auf **SSH** oder auf **Telnet**.

11 Klicken Sie auf **Anwenden**.

ANMERKUNG: Aufgrund besserer Sicherheits- und Verschlüsselungsmechanismen wird SSH empfohlen.

ANMERKUNG: Die SSH/Telnet-Sitzungsdauer kann unendlich sein, solange der Zeitüberschreitungswert auf 0 eingestellt wird. Der Standard-Zeitüberschreitungswert beträgt 1800 Sekunden.

12 Aktivieren Sie die iDRAC6-bandexterne Schnittstelle (IPMI über LAN), indem Sie **System→ iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Netzwerk** auswählen.

13 Wählen Sie die Option **IPMI über LAN aktivieren** unter **IPMI-Einstellungen** aus.

14 Klicken Sie auf **Anwenden**.

Seriell über LAN (SOL) verwenden

Dieser Abschnitt enthält mehrere Methoden zum Initialisieren einer Seriell über LAN-Sitzung, einschließlich eines Telnet-Programms, eines SSH-Clients, IPMItools und einer SOL Proxy. Der Zweck der Seriell über LAN-Funktion besteht darin, den seriellen Anschluss des verwalteten Servers über iDRAC6 in die Konsole der Management Station umzuleiten.

Modell zum Umleiten von SOL über Telnet oder SSH

Telnet (Anschluss 23)/ SSH (Anschluss 22) Client←→ WAN-Verbindung←→ iDRAC6-Server

Die IPMI-basierte SOL-über-SSH/Telnet-Implementierung macht ein zusätzliches Hilfsprogramm überflüssig, da die Seriell-zu-Netzwerk-Übersetzung innerhalb des iDRAC6 stattfindet. Die verwendete SSH- oder Telnet-Konsole muss in der Lage sein, die Daten zu interpretieren, die von der seriellen Anschluss des verwalteten Servers eingehen und auf diese Daten zu reagieren. Der serielle Anschluss wird normalerweise mit einer Shell verbunden, die ein ANSI- oder VT100/VT220-Terminal emuliert. Die serielle Konsole wird automatisch auf Ihre SSH- oder Telnet-Konsole umgeleitet.

Stellen Sie zum Einleiten einer SOL-Sitzung über SSH/Telnet eine Verbindung zum iDRAC6 her, wodurch Sie zur iDRAC6-Befehlszeilenkonsole gelangen. Geben Sie dann in der $-Eingabeaufforderung `connect` ein.

Informationen zur Verwendung von Telnet- und SSH-Clients bei iDRAC6 finden Sie unter „Telnet- oder SSH-Clients installieren“ auf Seite 80.

Modell für den SOL Proxy

Telnet Client (Anschluss 623) ←→ WAN-Verbindung ←→ SOL Proxy ←→ iDRAC6-Server

Wenn der SOL Proxy mit dem Telnet-Client auf einer Management Station kommuniziert, verwendet er das TCP/IP-Protokoll. Der SOL Proxy kommuniziert jedoch mit dem iDRAC6 des verwalteten Systems über das UDP-basierte RMCP/IPMI/SOL-Protokoll. Wenn Sie daher mit dem iDRAC6 des verwalteten Systems vom SOL Proxy aus über einen WAN-Anschluss kommunizieren, können eventuell Probleme mit der Netzwerkleistung auftreten. Im empfohlenen Verwendungsmodell sollen sich der SOL-Proxy und der iDRAC6-Server auf demselben LAN befinden.

Die Management Station mit dem Telnet-Client kann dann über einen WAN-Anschluss eine Verbindung zum SOL Proxy herstellen. In diesem Verwendungsmodell wird der SOL Proxy wie gewünscht funktionieren.

Modell zum Umleiten von SOL über IMPItool

IPMItool ←→ WAN-Verbindung ←→ iDRAC6-Server

Das IPMI-basierte SOL-Dienstprogramm, IPMItool, verwendet das Protokoll RMCP+, das unter Verwendung von UDP-Datengrammen an Anschluss 623 geliefert wird. iDRAC6 erfordert die Verschlüsselung dieser RMCP+-Verbindung. Der Verschlüsselungsschlüssel (KG-Schlüssel) muss Nullzeichen oder NULL enthalten, was über die iDRAC6-Web-GUI oder im iDRAC6-Konfigurationsdienstprogramm konfiguriert werden kann. Sie haben auch die Möglichkeit, den Verschlüsselungsschlüssel zu löschen, indem Sie die Rücktaste drücken, sodass der iDRAC6 standardmäßig NULL-Zeichen als Verschlüsselungsschlüssel angibt. Der Vorteil der Verwendung von RMCP+ besteht darin, dass Authentifizierung, Datenintegritätsprüfungen und Verschlüsselung sowie die Fähigkeit, verschiedene Arten von Nutzlasten zu tragen, verbessert werden. Weitere Informationen stehen unter „SOL über IPMItool verwenden“ auf Seite 217 oder auf der IPMItool-Webseite zur Verfügung: **http://ipmitool.sourceforge.net/manpage.html**.

Verbindung zur SOL-Sitzung in der iDRAC6-Befehlszeilenkonsole abbrechen

Befehle zum Abbrechen einer SOL-Sitzung sind dienstprogrammorientiert. Sie können das Dienstprogramm nur beenden, wenn eine SOL-Sitzung vollständig beendet ist. Beenden Sie zum Abbrechen einer SOL-Sitzung die SOL-Sitzung über die iDRAC6-Befehlszeilenkonsole.

Wenn Sie bereit sind, die SOL-Umleitung zu beenden, drücken Sie die Eingabetaste, <Esc> und dann <t> (drücken Sie die Tasten nacheinander). Die SOL-Sitzung wird entsprechend geschlossen. Die Escape-Sequenz wird außerdem auf dem Bildschirm angezeigt, sobald die Verbindung zu einer SOL-Sitzung hergestellt ist. Wenn der verwaltete Server ausgeschaltet ist, dauert es etwas länger, um die SOL-Sitzung einzurichten.

ANMERKUNG: Wenn eine SOL-Sitzung im Dienstprogramm nicht erfolgreich vollständig geschlossen wurde, könnten eventuell keine weiteren SOL-Sitzungen zur Verfügung stehen. Sie können dieses Problem beheben, indem Sie die Befehlszeilenkonsole in der Web-GUI unter **System**→ **iDRAC-Einstellungen**→ **Netzwerk/Sicherheit**→ **Sitzungen** beenden.

SOL über PuTTY verwenden

Um auf einer Windows-Management Station SOL von PuTTY aus zu starten, führen Sie folgende Schritte aus:

ANMERKUNG: Falls erforderlich, können Sie die standardmäßige SSH/Telnet-Zeitüberschreitung unter **System**→ **iDRAC-Einstellungen**→ **Netzwerk/Sicherheit**→ **Dienste** ändern.

1. Stellen Sie über den folgenden Befehl in der Eingabeaufforderung eine Verbindung zum iDRAC6 her:

   ```
   putty.exe [-ssh | -telnet] <Anmeldename>@<iDRAC-IP-Adresse> <Anschlussnummer>
   ```

   ANMERKUNG: Die Schnittstellennummer ist optional. Sie ist nur erforderlich, wenn die Schnittstellennummer neu vergeben wird.

2. Geben Sie in der Eingabeaufforderung den folgenden Befehl ein, um SOL zu starten:

   ```
   connect
   ```

   Sie werden nun mit dem seriellen Anschluss des verwalteten Servers verbunden. Sobald eine SOL-Sitzung erfolgreich hergestellt wurde, steht Ihnen die iDRAC6-Befehlszeilenkonsole nicht mehr zur Verfügung. Befolgen Sie die Escape-Sequenz ordnungsgemäß, um die iDRAC6-Befehlszeilenkonsole zu erreichen. Beenden Sie die SOL-Sitzung unter Verwendung der in „Verbindung zur SOL-Sitzung in der iDRAC6-Befehlszeilenkonsole abbrechen“ auf Seite 214 ausführlich beschriebenen Befehlssequenz und starten Sie eine neue.

ANMERKUNG: Wenn unter Windows die Emergency Management System (EMS)-Konsole unmittelbar nach einem Host-Neustart geöffnet wird, kann das Special Admin Console (SAC)-Terminal beschädigt werden. Beenden Sie die SOL-Sitzung gemäß „Verbindung zur SOL-Sitzung in der iDRAC6-Befehlszeilenkonsole abbrechen“ auf Seite 214, schließen Sie das Terminal, öffnen Sie ein anderes Terminal und starten Sie die SOL-Sitzung mit dem gleichen, oben beschriebenen Befehl.

SOL über Telnet mit Linux verwenden

Um auf einer Linux-Management Station SOL von Telnet aus zu starten, führen Sie folgende Schritte aus:

ANMERKUNG: Falls erforderlich, können Sie die standardmäßige Telnet-Zeitüberschreitung unter **System→ iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Dienste** ändern.

1. Starten Sie eine Shell.
2. Bauen Sie über den folgenden Befehl eine Verbindung zum iDRAC6 auf:

   `telnet <iDRAC6-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 in der Eingabeaufforderung den folgenden Befehl ein, um SOL zu starten:

   `connect`
4. Um eine SOL-Sitzung von Telnet mit Linux zu beenden, drücken Sie <Strg>+] (Steuerung gedrückt halten, eckige Klammer rechts drücken und loslassen). Eine Telnet-Eingabeaufforderung wird angezeigt. Geben Sie `quit` ein, um Telnet zu beenden.

SOL über OpenSSH mit Linux verwenden

OpenSSH ist ein Open Source-Dienstprogramm zur Verwendung des SSH-Protokolls. Um auf einer Linux-Management Station SOL von OpenSSH aus zu starten, führen Sie folgende Schritte aus:

ANMERKUNG: Falls erforderlich, können Sie die standardmäßige SSH-Sitzungszeitüberschreitung unter **System→ iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Dienste** ändern.

1. Starten Sie eine Shell.
2. Bauen Sie über den folgenden Befehl eine Verbindung zum iDRAC6 auf:

   `ssh <iDRAC-IP-Adresse> -l <Anmeldename>`
3. Geben Sie in der Eingabeaufforderung den folgenden Befehl ein, um SOL zu starten:

   `connect`

Sie werden nun mit dem seriellen Anschluss des verwalteten Servers verbunden. Sobald eine SOL-Sitzung erfolgreich hergestellt wurde, steht Ihnen die iDRAC6-Befehlszeilenkonsole nicht mehr zur Verfügung. Befolgen Sie die Escape-Sequenz ordnungsgemäß, um die iDRAC6-Befehlszeilenkonsole zu erreichen. Beenden Sie die SOL-Sitzung (Informationen zum Schließen einer aktiven SOL-Sitzung finden Sie unter „Verbindung zur SOL-Sitzung in der iDRAC6-Befehlszeilenkonsole abbrechen“ auf Seite 214).

SOL über IPMItool verwenden

Auf der DVD *Dell Systems Management Tools and Documentation* steht IPMItool zur Verfügung, das auf unterschiedlichen Betriebssystemen installiert werden kann. Einzelheiten zur Installation stehen im *Software-Schnellinstallationshandbuch* zur Verfügung. Sie können SOL mit IPMItool auf einer Management Station starten, indem Sie folgende Schritte ausführen:

ANMERKUNG: Falls erforderlich, können Sie die standardmäßige SOL-Zeitüberschreitung unter **System**→ **iDRAC-Einstellungen**→ **Netzwerk/Sicherheit**→ **Dienste** ändern.

1. Machen Sie die Datei **IPMItool.exe** im entsprechenden Verzeichnis ausfindig.

   Der Standardpfad im 32–Bit-Betriebssystem von Windows lautet **C:\Programme\Dell\SysMgt\bmc** und im 64–Bit-Betriebssystem von Windows **C:\Programme (x86)\Dell\SysMgt\bmc**.

2. Stellen Sie sicher, dass der **Verschlüsselungsschlüssel** unter **System**→ **iDRAC-Einstellungen**→ **Netzwerk/Sicherheit**→ **Netzwerk**→ **IPMI-Einstellungen** ausschließlich aus Nullen besteht.

3. Geben Sie in der Windows-Eingabeaufforderung oder in der Linux-Shell-Eingabeaufforderung den folgenden Befehl ein, um SOL über iDRAC zu starten:

   ```
   ipmitool -H <iDRAC-IP-Adresse> -I lanplus -U
   <Anmeldename> -P <Anmeldekennwort> sol activate
   ```

   Sie werden nun mit dem seriellen Anschluss des verwalteten Servers verbunden.

4 Sie können eine SOL-Sitzung von IPMItool aus beenden, indem Sie <~> und <.> drücken (drücken Sie die Taste mit der Tilde und die Taste mit dem Punkt nacheinander). Versuchen Sie es mehr als einmal, da der iDRAC6 möglicherweise ausgelastet ist und die Schlüssel nicht annehmen kann. Die SOL-Sitzung wird geschlossen.

ANMERKUNG: Wenn ein Benutzer die SOL-Sitzung nicht korrekt beendet, geben Sie den folgenden Befehl ein, um iDRAC neu zu starten. iDRAC6 kann bis zu zwei Minuten in Anspruch nehmen, um den Startvorgang abzuschließen. Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

```
racadm racreset
```

SOL mit SOL Proxy öffnen

Beim Seriell über LAN-Proxy (SOL Proxy) handelt es sich um einen Telnet-Daemon, der eine LAN-basierte Verwaltung von Remote-Systemen unter Verwendung der SOL- (Seriell über LAN) und IPMI-Protokolle ermöglicht. Alle standardmäßigen Telnet-Client-Anwendungen wie HyperTerminal unter Microsoft Windows oder Telnet unter Linux können für den Zugriff auf Daemon-Funktionen verwendet werden. SOL kann entweder im Menümodus oder Befehlsmodus verwendet werden. Das SOL-Protokoll zusammen mit der BIOS-Virtuelle Konsole des Remote-Systems ermöglicht Administratoren, die BIOS-Einstellungen eines verwalteten Systems im Remote-Zugriff über ein LAN anzuzeigen und zu ändern. Auf die serielle Konsole von Linux und Microsofts EMS/SAC-Schnittstellen kann ebenso über ein LAN mit SOL zugegriffen werden.

ANMERKUNG: Alle Versionen der Windows-Betriebssysteme enthalten die Terminalemulationssoftware HyperTerminal. Die integrierte Version enthält jedoch viele der Funktionen, die während des Vorgangs der virtuellen Konsole erforderlich sind, nicht. Sie können stattdessen eine beliebige Terminalemulationssoftware verwenden, die die Emulationsmodi VT100/VT220 oder ANSI unterstützt. Ein Beispiel für einen vollständigen VT100/VT220- oder ANSI-Terminalemulator, der die virtuelle Konsole auf dem System unterstützt, ist Hilgraeves HyperTerminal Private Edition 6.1 oder höher. Außerdem kann die Verwendung des Befehlszeilenfensters zum Ausführen einer seriellen Telnet-Virtuelle Konsole dazu führen, dass fehlerhafte Zeichen angezeigt werden.

ANMERKUNG: Weitere Informationen zur virtuellen Konsole, einschließlich Hardware- und Softwareanforderungen sowie Anleitungen zum Konfigurieren von Host- und Client-Systemen zur Verwendung von virtuellen Konsolen, finden Sie im Benutzerhandbuch zum System.

ANMERKUNG: HyperTerminal- und Telnet-Einstellungen müssen mit den Einstellungen auf dem verwalteten System übereinstimmen. Die Baudraten und Terminalmodi müssen ebenso übereinstimmen.

ANMERKUNG: Der Windows-Befehl `telnet`, der von einer MS-DOS-Eingabeaufforderung ausgeführt wird, unterstützt ANSI-Terminalemulation. Das BIOS muss auf ANSI-Emulation eingestellt sein, um alle Bildschirme richtig anzuzeigen.

Vor der Verwendung des SOL Proxy

Bevor Sie den SOL-Proxy verwenden, lesen Sie bitte im *Benutzerhandbuch zu den Dienstprogrammen des Baseboard-Management-Controllers* nach, wie Sie die Management Stations konfigurieren müssen. Standardmäßig sind die BMC-Verwaltungsdienstprogramme auf Windows-Betriebssystemen im folgenden Verzeichnis installiert:

C:\Programme\Dell\SysMgt\bmc – (32–Bit-Betriebssystem)

C:\Programme (x86)\Dell\SysMgt\bmc – (64–Bit-Betriebssystem)

Das Installationsprogramm kopiert die Dateien an die folgenden Speicherorte auf Linux Enterprise-Betriebssystemen:

/etc/init.d/SOLPROXY.cfg

/etc/SOLPROXY.cfg

/usr/sbin/dsm_bmu_solproxy32d

/usr/sbin/solconfig

/usr/sbin/ipmish

SOL Proxy-Sitzung einleiten

Für Windows 2003:

Um den SOL Proxy-Dienst nach der Installation auf einem Windows-System zu starten, können Sie das System neu starten (nach einem Neustart wird SOL Proxy automatisch gestartet). Sie haben auch die Möglichkeit, den SOL Proxy-Dienst manuell zu starten, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz**, und klicken Sie dann auf **Verwalten**.

   Das Fenster **Computerverwaltung** wird angezeigt.

2. Klicken Sie auf **Dienste und Anwendungen** und dann auf **Dienste**.

   Verfügbare Dienste werden rechts angezeigt.

3. Machen Sie **DSM_BMU_SOLProxy** in der Liste von Diensten ausfindig und klicken Sie mit der rechten Maustaste darauf, um den Dienst zu starten.

Abhängig von der Konsole, die Sie verwenden, müssen unterschiedliche Schritte ausgeführt werden, um auf den SOL Proxy zuzugreifen. Innerhalb dieses Abschnitts wird die Management Station, auf der SOL Proxy ausgeführt wird, als SOL Proxy-Server bezeichnet.

Für Linux:

Der SOL Proxy wird automatisch während des Systemstarts gestartet. Alternativ dazu können Sie in das Verzeichnis **/etc/init.d** wechseln und folgende Befehle für die Verwaltung des SOL Proxy-Dienstes eingeben:

```
solproxy status

dsm_bmu_solproxy32d start

dsm_bmu_solproxy32d stop

solproxy restart
```

Telnet mit SOL Proxy verwenden

Hierbei wird angenommen, dass der SOL Proxy-Dienst auf der Management Station bereits eingerichtet ist und ausgeführt wird.

Für Windows 2003:

1. Öffnen Sie auf der Management Station ein Befehlszeilenfenster.
2. Geben Sie den Befehl `telnet` in die Befehlszeile ein, und geben Sie `localhost` als IP-Adresse an, wenn der SOL Proxy-Server auf demselben System ausgeführt wird, sowie die Anschlussnummer, die Sie in der SOL Proxy-Installation festgelegt haben (Standardwert ist `623`). Zum Beispiel:

   ```
   telnet localhost 623
   ```

Für Linux:

1. Öffnen Sie eine Linux Shell auf der Management Station.
2. Geben Sie den Befehl `telnet` ein, und geben Sie `localhost` als IP-Adresse für den SOL Proxy-Server sowie die Anschlussnummer an, die Sie während der Installation von SOL Proxy festgelegt haben (Standardwert ist `623`). Zum Beispiel:

   ```
   telnet localhost 623
   ```

ANMERKUNG: Wenn der SOL Proxy-Server auf einem anderen System als der Management Station ausgeführt wird, müssen Sie unabhängig davon, ob das Hostbetriebssystem Windows oder Linux ist, statt localhost die IP-Adresse des SOL Proxy-Servers eingeben.

```
telnet <IP-Adresse des SOL Proxy-Servers> 623
```

HyperTerminal mit SOL Proxy verwenden

1. Öffnen Sie die Datei **HyperTerminal.exe** von der Remote-Station aus.
2. Wählen Sie **TCPIP(Winsock)** aus.
3. Geben Sie die Hostadresse `localhost` ein und die Anschlussnummer `623`.

Eine Verbindung zum BMC des Remote Managed System herstellen

Sobald eine SOL Proxy-Sitzung erfolgreich eingerichtet ist, werden Ihnen die folgenden Optionen zur Auswahl geboten:

```
1. Eine Verbindung zum BMC des Remote-Servers
herstellen

2. Seriell über LAN für den Remote-Server
konfigurieren

3. Virtuelle Konsole aktivieren

4. Virtuelle Konsole neu starten und aktivieren

5. Hilfe

6. Beenden
```

ANMERKUNG: Es können mehrere SOL-Sitzungen gleichzeitig aktiv sein, es darf jedoch nur eine Virtuelle Konsole-Sitzung für ein verwaltetes System aktiv sein.

ANMERKUNG: Verwenden Sie zum Beenden einer aktiven SOL-Sitzung die Zeichenfolge <~><.> Mit dieser Sequenz wird SOL beendet, und das Hauptmenü wird wieder angezeigt.

1. Wählen Sie Option 1 im Hauptmenü aus.
2. Geben Sie die iDRAC6-**IP-Adresse** des Remote-verwalteten Systems ein.
3. Geben Sie den iDRAC6-**Benutzernamen** und das iDRAC6-**Kennwort** für das verwaltete System ein. iDRAC6-Benutzername und -Kennwort müssen im nicht-flüchtigen Speicher des iDRAC6 zugewiesen und gespeichert werden.

ANMERKUNG: Es ist immer nur eine SOL-Virtuelle Konsole-Sitzung mit iDRAC6 zulässig.

ANMERKUNG: Falls erforderlich, können Sie die SOL-Sitzungsdauer auf unendlich erweitern, indem Sie den Wert der Telnet-**Zeitüberschreitung** auf der iDRAC6-Web-GUI unter **System**→ **iDRAC-Einstellungen**→ **Netzwerk/Sicherheit**→ **Dienste** auf Null ändern.

4. Geben Sie den IPMI-Verschlüsselungsschlüssel an, wenn er im iDRAC6 konfiguriert wurde.

ANMERKUNG: Sie können den IPMI-Verschlüsselungsschlüssel in der iDRAC6-GUI unter **System**→ **iDRAC-Einstellungen**→ **Netzwerk/Sicherheit**→ **Netzwerk**→ **IPMI-Einstellungen**→ **Verschlüsselungsschlüssel** finden.

ANMERKUNG: Der standardmäßige IPMI-Verschlüsselungsschlüssel besteht ausschließlich aus Nullen. Wenn Sie für die Verschlüsselungsoption die <Eingabetaste> drücken, wird iDRAC6 diesen standardmäßigen Verschlüsselungsschlüssel verwenden.

5. Wählen Sie im Hauptmenü **Seriell über LAN für Remote Server konfigurieren** (Option 2).

   Das SOL-Konfigurationsmenü wird angezeigt. Abhängig vom aktuellen SOL-Status variiert der Inhalt des SOL-Konfigurationsmenüs:

   - Wenn SOL bereits aktiviert ist, werden die aktuellen Einstellungen angezeigt und es stehen drei Möglichkeiten zur Auswahl.

     ```
     1. Seriell über LAN deaktivieren
     2. Seriell über LAN-Einstellungen ändern
     3. Abbrechen
     ```

   - Wenn SOL aktiviert ist, stellen Sie sicher, dass die SOL-Baudrate der des iDRAC6 entspricht und der Benutzer über Administratorberechtigungen verfügt.
   - Wenn SOL gegenwärtig deaktiviert ist, geben Sie `Y` ein, um SOL zu aktivieren, oder `N`, um SOL deaktiviert zu lassen.

6 Wählen Sie im Hauptmenü **Virtuelle Konsole aktivieren** (Option 3).

Die Textkonsole des Remote-verwalteten Systems wird auf die Management Station umgeleitet.

7 Wählen Sie optional im Hauptmenü **Virtuelle Konsole neu starten und aktivieren** (Option 4) aus.

Der Energiezustand des Remote-verwalteten Systems wird bestätigt. Wenn das System eingeschaltet ist, haben Sie die Wahl zwischen einem ordentlichen Herunterfahren und einem erzwungenen Herunterfahren.

Der Energiezustand wird überwacht, bis der Status zu **eingeschaltet** wechselt. Die Virtuelle Konsole wird gestartet und die Textkonsole des Remote-verwalteten Systems wird an die Management Station umgeleitet.

Während das verwaltete System neu gestartet wird, können Sie das BIOS-System-Setup-Programm aufrufen, um BIOS-Einstellungen anzuzeigen oder zu ändern.

8 Wählen Sie im Hauptmenü **Hilfe** (Option 5), um detaillierte Beschreibungen der einzelnen Optionen anzuzeigen.

9 Wählen Sie im Hauptmenü **Beenden** (Option 6), um die Telnet-Sitzung zu beenden und die Verbindung zu SOL Proxy abzubrechen.

ANMERKUNG: Wenn ein Benutzer die SOL-Sitzung nicht korrekt beendet, geben Sie den folgenden Befehl ein, um iDRAC neu zu starten. iDRAC6 benötigt 1-2 Minuten für den Startvorgang. Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

```
racadm racreset
```

Konfiguration des Betriebssystems

Führen Sie zum Konfigurieren generischer Betriebssysteme die für Ihr Betriebssystem relevanten Schritte aus. Diese Konfiguration basiert auf Standardinstallationen von Red Hat Enterprise Linux 5.0, SUSE Linux Enterprise Server 10 SP1 und Windows 2003 Enterprise.

Linux Enterprise-Betriebssystem

1 Bearbeiten Sie die Datei **/etc/inittab**, um die Hardware-Ablaufsteuerung zu aktivieren und Benutzern zu ermöglichen, sich über die SOL-Konsole anzumelden. Fügen Sie die nachstehende Zeile am Ende des Abschnitts `#Run gettys in standard runlevels` hinzu.

```
7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220
```

Beispiel von original**/etc/inittab:**

```
#
# inittab Diese Datei beschreibt, wie das INIT-Verfahren das System
#         auf einer bestimmten Ausführungsstufe einrichten sollte.
#

Diesen Teil der Datei ÜBERSPRINGEN

# gettys in Standard-Ausführungsstufen ausführen
1:2345:respawn:/sbin/migetty tty1
2:2345:respawn:/sbin/migetty tty1
3:2345:respawn:/sbin/migetty tty1
4:2345:respawn:/sbin/migetty tty1
5:2345:respawn:/sbin/migetty tty1
6:2345:respawn:/sbin/migetty tty1

# xdm in Ausführungsstufe 5 ausführen
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Beispiel von modifiziertem **/etc/inittab**:

```
#
# inittab Diese Datei beschreibt, wie das INIT-Verfahren das System
#         auf einer bestimmten Ausführungsstufe einrichten sollte.
#

Diesen Teil der Datei ÜBERSPRINGEN

# gettys in Standard-Ausführungsstufen ausführen
1:2345:respawn:/sbin/migetty tty1
2:2345:respawn:/sbin/migetty tty1
3:2345:respawn:/sbin/migetty tty1
4:2345:respawn:/sbin/migetty tty1
5:2345:respawn:/sbin/migetty tty1
6:2345:respawn:/sbin/migetty tty1
7:2345:respawn:/sbin/agetty -h ttyS0 115200 vt220

# xdm in Ausführungsstufe 5 ausführen
x:5:respawn:/etc/X11/prefdm -nodaemon
```

2. Bearbeiten Sie die Datei /etc/securetty, um Benutzern zu ermöglichen, sich über die SOL-Konsole als Stamm-Benutzer anzumelden. Fügen Sie die folgende Zeile im Anschluss an `console` hinzu:

   `ttyS0`

Beispiel von originalem **/etc/securetty**:

```
Konsole
vc/1
vc/2
vc/3
vc/4
```

```
Rest der Datei ÜBERSPRINGEN
```

Beispiel von modifiziertem **/etc/securetty**:

```
Konsole
ttyS0
vc/1
vc/2
vc/3
vc/4

Rest der Datei ÜBERSPRINGEN
```

3 Bearbeiten Sie die Datei **/boot/grub/grub.conf** oder **/boot/grub/menu.list**, um Startoptionen für SOL hinzuzufügen:

   a Kommentieren Sie in den verschiedenen UNIX-ähnlichen Betriebssystemen die Zeilen der grafischen Anzeige aus:

   - `splashimage=(had0,0)/grub/splash.xpm.gz` in RHEL 5
   - `gfxmenu (hda0,5)/boot/message` in SLES 10

   b Fügen Sie die folgende Zeile vor der ersten Zeile mit der Bezeichnung `title=` … hinzu:

   ```
   # Redirect OS boot via SOL
   ```

   c Hängen Sie den folgenden Eintrag der ersten Zeile mit der Bezeichnung `title=` … an:

   ```
   SOL redirection
   ```

   d Hängen Sie den folgenden Text der Zeile `kernel/`… des ersten `title=` … an:

   ```
   console=tty1 console=ttyS0,115200
   ```

ANMERKUNG: **/boot/grub/grub.conf** in Red Hat Enterprise Linux 5 ist eine symbolische Verknüpfung mit **/boot/grub/menu.list**. Sie können die Einstellungen in beiden ändern.

Beispiel von originalem **/boot/grub/grub.conf** in RHEL 5:

```
# grub.conf erstellt durch anaconda
#
# Beachten Sie, dass grub nicht zurückgegeben werden muss,
nachdem Sie Änderungen an dieser
# Datei vorgenommen haben
# HINWEIS: Sie haben eine /Startpartition. Dies bedeutet, dass
#          alle Kernel- und initrd-Pfade im Verhältnis zu /
           boot/ stehen, z. B.
#          root (hd0,0)
#          kernel /vmlinux-version ro root=/dev/VolGroup00/
           LogVol00
#          initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm/gz
hiddenmenu

title Red Hat Enterprise Linux 5
root (hd0,0)
kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00
rhgb quiet
initrd /initrd-2.6.18-8.el5.img
```

Beispiel von modifiziertem **/boot/grub/grub.conf**:

```
# grub.conf erstellt durch anaconda
#
# Beachten Sie, dass grub nicht zurückgegeben werden muss,
nachdem Sie Änderungen an dieser
# Datei vorgenommen haben
# HINWEIS: Sie haben eine /Startpartition. Dies bedeutet, dass
#          alle Kernel- und initrd-Pfade im Verhältnis zu /
           boot/ stehen, z. B.
#          root (hd0,0)
#          kernel /vmlinux-version ro root=/dev/VolGroup00/
           LogVol00
#          initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
#splashimage=(hd0,0)/grub/splash.xpm/gz
hiddenmenu

# BS-Start über SOL umleiten
title Red Hat Enterprise Linux 5 SOL-Umleitung
root (hd0,0)
kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00
rhgb quiet console=tty1 console=ttyS0,115200
initrd /initrd-2.6.18-8.el5.img
```

Beispiel von originalem **/boot/grub/menu.list** in SLES 10:

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09
UTC 2008

Default 0

Timeout 8

gfxmenu (hd0.5)/boot/message


###Don't change this comment - YaST2 identifier: Original name:
linux###

title SUSE Linux Enterprise Server 10 SP1

root (hd0,5)

kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/
by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent
showopts

initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

Beispiel von modifiziertem **/boot/grub/menu.list** in SLES 10:

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09
UTC 2008

Default 0

Timeout 8

#gfxmenu (hd0.5)/boot/message


###Don't change this comment - YaST2 identifier: Original name:
linux###

title SUSE Linux Enterprise Server 10 SP1 SOL redirection

root (hd0,5)

kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/
by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent
showopts console=tty1 console=ttyS0,115200

initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

Windows 2003 Enterprise

1. Bestimmen Sie die Starteintrags-ID, indem Sie an der Windows-Eingabeaufforderung bootcfg eingeben. Suchen Sie die Starteintrags-ID des Abschnitts mit dem Friendly Name des Betriebssystems **Windows Server 2003 Enterprise**. Drücken Sie die Eingabetaste, um die Startoptionen auf der Management Station anzuzeigen.
2. Aktivieren Sie EMS an einer Windows-Eingabeaufforderung, indem Sie Folgendes eingeben:

   ```
   bootcfg /EMS ON /PORT COM1 /BAUD 115200 /ID
   <Start-ID>
   ```

ANMERKUNG: <Start-ID> ist die Starteintrags-ID aus Schritt 1.

3. Drücken Sie die Eingabetaste, um zu überprüfen, ob die EMS-Konsoleneinstellung wirksam ist.

Beispiel einer originalen `bootcfg` Einstellung:

```
Einstellungen des Boot Loaders
--------------------
Zeitüberschreitung:30
Standardeinstellung:multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

Starteinträge
------------
Starteintrags-ID:    1
Friendly Name des BS: Windows Server 2003, Enterprise
Pfad:                 multi(0)disk(0)rdisk(0)partition(1)\
                      WINDOWS
BS-Ladeoptionen:      /nonexecute=optout /fastdetect /
                      usepmtimer /redirect
```

Beispiel von modifizierter `bootcfg`-Einstellung:

```
Einstellungen des Boot Loaders
--------------------
Zeitüberschreitung:          30
Standardeinstellung:
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
Umleitung:         COM1
Umleitungs-Baudrate:115200


Starteinträge
------------
Starteintrags-ID:    1
Friendly Name des BS: Windows Server 2003, Enterprise
Pfad:                  multi(0)disk(0)rdisk(0)partition(1)\
                       WINDOWS
BS-Ladeoptionen:       /nonexecute=optout /fastdetect /
                       usepmtimer /redirect
```

10

Virtuelle GUI-Konsole verwenden

Dieser Abschnitt enthält Informationen über die Verwendung der iDRAC6-Funktion Virtuelle Konsole.

Übersicht

Die iDRAC6-Funktion Virtuelle Konsole ermöglicht den Remote-Zugriff auf lokale Konsolen im Grafik- oder Textmodus. So können Sie ein System oder mehrere Systeme mit iDRAC6 von einer Stelle aus steuern.

Virtuelle Konsole verwenden

Der Bildschirm **Virtuelle Konsole** ermöglicht die Verwaltung des Remote-Systems unter Verwendung von Tastatur, Video und Maus auf Ihrer lokalen Management Station, um die entsprechenden Geräte auf einem Remote-verwalteten Server zu steuern. Diese Funktion kann in Verbindung mit der Funktion Virtueller Datenträger verwendet werden, um Remote-Software-Installationen auszuführen.

Die folgenden Regeln gelten für die Sitzung einer virtuellen Konsole:

- Auf jedem Blade können maximal zwei gleichzeitige Virtuelle Konsole-Sitzungen unterstützt werden. Beide Sitzungen zeigen gleichzeitig dieselbe Konsole des verwalteten Servers an.
- Die Sitzung einer virtuellen Konsole darf nicht über einen Webbrowser auf dem verwalteten System gestartet werden.
- Die erforderliche verfügbare Netzwerk-Mindestbandbreite beträgt 1 MB/s.

Wenn ein zweiter Benutzer eine Virtuelle Konsole-Sitzung anfordert, wird der erste Benutzer benachrichtigt und erhält die Option, den Zugriff abzulehnen, nur Video 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 kein Zugriff gewährt.

Wenn zwei Sitzungen gleichzeitig aktiv sind, sieht der erste Benutzer eine Meldung in der rechten oberen Ecke des Bildschirms, die anzeigt, 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.

Löschen Sie den Cache des Browsers

Wenn beim Betrieb der virtuellen Konsole Probleme auftreten (Reichweitenfehler, Synchronisationsprobleme usw.), löschen Sie den Cache des Browsers, um alte Versionen des Viewer zu entfernen/zu löschen, die auf dem System gespeichert sein könnten, und versuchen Sie es erneut.

So löschen Sie ältere Versionen von Active-X Viewer für IE7:

1. Schließen Sie den Video Viewer und Internet Explorer.
2. Öffnen Sie dann wieder den Internet Explorer und gehen Sie zu **Internet Explorer→ Extras→ Add-Ons verwalten** und klicken Sie auf **Add-Ons aktivieren/deaktivieren**. Das Fenster **Add-Ons verwalten** wird angezeigt.
3. Wählen Sie im Dropdown-Menü **Anzeigen Von Internet Explorer verwendete Add-Ons** aus.
4. Löschen Sie **DELL IDRAC AVCView**.

So löschen Sie ältere Versionen von Active-X Viewer für IE8:

1. Schließen Sie den Video Viewer und Internet Explorer.
2. Öffnen Sie dann wieder den Internet Explorer und gehen Sie zu **Internet Explorer→ Extras→ Add-Ons verwalten** und klicken Sie auf **Add-Ons aktivieren/deaktivieren**. Das Fenster **Add-Ons verwalten** wird angezeigt.
3. Wählen Sie im Drop-Down-Menü **Anzeigen** die Option **Alle Add-ons** aus.
4. Wählen Sie **DELL IDRAC AVCView**, und klicken Sie dann auf den Link **Weitere Informationen**.
5. Klicken Sie auf **Entfernen** im Fenster **Weitere Informationen**.
6. Schließen Sie die Fenster **Weitere Informationen** und **Add-Ons verwalten**.

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

1. Führen Sie an der Eingabeaufforderung `javaws -viewer` aus.

   Der **Java Cache Viewer** wird angezeigt.
2. Löschen Sie das Objekt mit dem Namen *iDRAC6-Virtuelle Konsole-Client* und *JViewer*.

Sie können in der Eingabeaufforderung auch `javaws -uninstall` ausführen, um alle Anwendungen aus dem Cache zu löschen.

Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

Tabelle 10-1 listet die unterstützten Bildschirmauflösungen und entsprechenden Bildwiederholfrequenzen für die Sitzung einer virtuellen Konsole auf, die auf dem verwalteten Server ausgeführt wird.

Tabelle 10-1. 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

Konfiguration der Management Station

Um die virtuelle Konsole auf der Management Station zu verwenden, führen Sie folgende Anweisungen aus:

1. Installieren und konfigurieren Sie einen unterstützten Internet-Browser. Weitere Informationen erhalten Sie unter „Unterstützte Webbrowser“ auf Seite 27 und „Konfigurieren eines unterstützten Webbrowsers“ auf Seite 70.
2. Wenn Sie Firefox verwenden oder den Java Viewer mit Internet Explorer verwenden möchten, installieren Sie eine Java-Laufzeitumgebung (JRE). Siehe „Installation einer Java-Laufzeitumgebung (JRE)“ auf Seite 79.
3. Es wird empfohlen, die Bildschirmauflösung auf 1280x1024 Pixel einzustellen.

ANMERKUNG: Wenn eine aktive Virtuelle Konsole-Sitzung vorhanden ist und ein Monitor mit niedrigerer Auflösung an die virtuelle Konsole angeschlossen wird, dann wird die Serverkonsolenauflösung bei Auswahl des Servers auf der lokalen Konsole eventuell zurückgesetzt. Wenn der Server ein Linux-Betriebssystem ausführt, kann eine X11-Konsole auf dem lokalen Monitor u. U. nicht angezeigt werden. Durch Drücken auf <Strg><Alt><F1> auf der iDRAC-Virtuellen Konsole wird Linux auf eine Textkonsole geschaltet.

4 Wenn Sie den Internet Explorer zum Starten der Virtuelle Konsole-Sitzung mit Java-Plug-In verwenden, führen Sie folgendes durch:

a Wechseln Sie im Internet Explorer zu **Extras→ Internetoptionen→ Sicherheit→ Vertrauenswürdige Sites→ Benutzerdefiniert**.

ANMERKUNG: Bei Windows 7 64-Bit gehen Sie zu **Extras→ Internetoptionen→ Sicherheit→ Internet→ Benutzer definiert**.

b Wählen Sie im Fenster **Sicherheitseinstellungen** die Option **Deaktiviert** für **Automatische Eingabeaufforderung für Datei-Downloads**.

c **Klicken** Sie zweimal hintereinander auf **OK**.

Konfigurieren der virtuellen Konsole und der virtuellen Datenträger auf der iDRAC6-Webschnittstelle

Um auf der iDRAC6-Webschnittstelle eine virtuelle Konsole zu konfigurieren, führen Sie folgende Schritte aus:

1 Klicken Sie auf **System** und dann auf die Registerkarte **Virtuelle Konsole/Datenträger**.

2 Klicken Sie auf **Konfiguration**, um den Bildschirm **Konfiguration** zu öffnen.

3 Konfigurieren Sie die Eigenschaften der virtuellen Konsole. Tabelle 10-2 beschreibt die Eigenschaften der virtuellen Konsole.

4 Wenn Sie fertig sind, klicken Sie auf **Anwenden**.

Tabelle 10-2. Konfigurationseigenschaften der virtuellen Konsole

Eigenschaft	Beschreibung
Enabled (Aktiviert)	Markieren, um die virtuelle Konsole zu aktivieren oder zu deaktivieren. **Markiert** zeigt an, dass die virtuelle Konsole aktiviert ist. **Nicht markiert** zeigt an, dass die virtuelle Konsole deaktiviert ist. Die Standardeinstellung ist **aktiviert**.

Tabelle 10-2. Konfigurationseigenschaften der virtuellen Konsole *(fortgesetzt)*

Eigenschaft	Beschreibung
Max. Sitzungen	Zeigt die Anzahl der maximal möglichen Virtuelle Konsole-Sitzungen an – **1** oder **2**. Verwenden Sie das Dropdown-Menü, um die maximal zulässigen Virtuelle Konsole-Sitzungen zu ändern. Die Standardeinstellung ist **2**.
Aktive Sitzungen	Zeigt die Anzahl der Sitzungen aktiver Konsolen an. Dieses Feld ist schreibgeschützt.
Tastatur- und Mausanschlussnummer	Die Netzwerkschnittstellennummer, die zur Verbindung mit der Tastatur/Maus-Option der virtuellen Konsole verwendet wird. Dieser Datenverkehr ist immer verschlüsselt. Diese Zahl muss eventuell geändert werden, wenn ein anderes Programm den Standardanschluss verwendet. Die Standardeinstellung ist **5900.**
Videoanschlussnummer	Die Netzwerkanschlussnummer, die zur Verbindung mit dem Bildschirmdienst der virtuellen Konsole verwendet wird. Diese Einstellung muss eventuell geändert werden, wenn ein anderes Programm bereits den Standardanschluss verwendet. Die Standardeinstellung ist **5901.**
Videoverschlüsselung aktiviert	**Markiert** zeigt an, dass die Videoverschlüsselung aktiviert ist. Der zum Videoanschluss übertragene Datenverkehr ist verschlüsselt. **Nicht markiert** zeigt an, dass die Videoverschlüsselung deaktiviert ist. Der zum Videoanschluss übertragene Datenverkehr ist nicht verschlüsselt. Die Standardeinstellung ist **Verschlüsselt**. Ein Deaktivieren der Verschlüsselung kann die Leistung auf langsameren Netzwerken verbessern.

Tabelle 10-2. Konfigurationseigenschaften der virtuellen Konsole *(fortgesetzt)*

Eigenschaft	Beschreibung
Mausmodus	Wählen Sie **Windows**, wenn der verwaltete Server auf einem Windows-Betriebssystem ausführt wird. Wählen Sie **Linux** aus, wenn der verwaltete Server auf Linux ausgeführt wird. Wählen Sie **USC/Diags** aus, wenn der Server weder auf einem Windows- noch auf einem Linux-Betriebssystem ausgeführt wird. **ANMERKUNG:** Sie müssen **USC/Diags** in HyperV, Dell Diagnostics oder USC (Systemdienste) auswählen. Die Standardeinstellung ist **Windows**.
Konsolen-Plug-In-Typ für IE	Wenn der Internet Explorer auf einem Windows-Betriebssystem verwendet wird, können die folgenden Viewer ausgewählt werden: **ActiveX** - Der *ActiveX-Virtuelle Konsole*-Viewer **Java** - *Java-Virtuelle Konsole*-Viewer **ANMERKUNG:** Abhängig von Ihrer Internet Explorer-Version müssen möglicherweise zusätzliche Sicherheitseinschränkungen ausgeschaltet werden (siehe „Virtuellen Datenträger konfigurieren und verwenden“ auf Seite 281). **ANMERKUNG:** Auf dem Client-System muss die Java-Laufzeitumgebung installiert sein, damit der Java-Viewer verwendet werden kann.
Lokales Servervideo aktiviert	**Markiert** zeigt an, dass der Ausgang zum Monitor der virtuellen Konsole während der virtuellen Konsole aktiviert ist. **Nicht markiert** zeigt an, dass die unter Verwendung der **virtuellen Konsole** ausgeführten Tasks auf dem lokalen Monitor des verwalteten Servers nicht sichtbar sind.

ANMERKUNG: Für Informationen zur Verwendung des virtuellen Datenträgers mit virtueller Konsole siehe „Virtuellen Datenträger konfigurieren und verwenden“ auf Seite 281.

Sitzung einer virtuellen Konsole öffnen

Wenn Sie eine Sitzung einer virtuellen Konsole öffnen, startet die Dell Virtual Console Viewer-Anwendung (**iDRACView**), und der Desktop des Remote-Systems wird im Viewer eingeblendet. Mit **iDRACView** können Sie die Maus- und Tastaturfunktionen des Remote-Systems von der lokalen Management Station aus steuern.

ANMERKUNG: Das Starten einer virtuellen Konsole über eine Windows Vista-Management Station kann Neustartmeldungen der virtuellen Konsole verursachen. Sie können dies vermeiden, indem Sie die entsprechenden Zeitüberschreitungswerte an den folgenden Stellen einstellen: **Systemsteuerung→ Stromoptionen→ Stromsparmodus→ Erweiterte Einstellungen→ Festplatte→ Festplatte ausschalten nach <Zeitüberschreitung>** und unter **Systemsteuerung→ Stromoptionen→ Hochleistung→ Erweiterte Einstellungen→ Festplatte→ Festplatte ausschalten nach <Zeitüberschreitung>**.

Führen Sie folgende Schritte aus, um auf der Webschnittstelle eine Sitzung der virtuellen Konsole zu öffnen:

1. Klicken Sie auf **System→** Registerkarte **Virtuelle Konsole/Datenträger→ Virtuelle Konsole und Virtuelle Datenträger**.
2. Verwenden Sie auf der Seite **Virtuelle Konsole und Virtuelle Datenträger** die Informationen unter Tabelle 10-3, um sicherzustellen, dass eine Virtuelle Konsole-Sitzung verfügbar ist.

   Sollten Sie einige der angezeigten Eigenschaftswerte neu konfigurieren wollen, finden Sie entsprechende Informationen unter „Konfigurieren der virtuellen Konsole und der virtuellen Datenträger auf der iDRAC6-Webschnittstelle“ auf Seite 236.

Tabelle 10-3. Virtuelle Konsole-Informationen

Eigenschaft	Beschreibung
Virtuelle Konsole aktiviert	**Ja/Nein**
Videoverschlüsselung aktiviert	**Ja/Nein**
Max. Sitzungen	Zeigt die maximale Anzahl unterstützter Sitzungen der virtuellen Konsole an.
Aktive Sitzungen	Zeigt die aktuelle Anzahl aktiver Sitzungen der virtuellen Konsole an.

Tabelle 10-3. Virtuelle Konsole-Informationen *(fortgesetzt)*

Eigenschaft	Beschreibung
Mausmodus	Zeigt die aktuell geltende Mausbeschleunigung an. Der **Mausmodus** muss auf Grundlage des auf dem verwalteten Server installierten Betriebssystemtyps ausgewählt werden.
Konsolen-Plug-In-Typ	Zeigt den aktuell konfigurierten Plug-In-Typ. **ActiveX** - Ein Active-X-Viewer wird gestartet. Der Active-X-Viewer funktioniert nur im Internet Explorer bei der Ausführung auf einem Windows-Betriebssystem. **Java** - Ein Java-Viewer wird gestartet. Der Java-Viewer kann in jedem Browser, einschließlich Internet Explorer, verwendet werden. Wenn der Client auf einem anderen Betriebssystem als Windows ausgeführt wird, müssen Sie den Java-Viewer verwenden. Wenn Sie mit Internet Explorer im Windows-Betriebssystem auf den iDRAC6 zugreifen, können Sie entweder **Active-X** oder **Java** als Plug-In-Typ auswählen. **ANMERKUNG:** Virtuelle Konsole könnte bei Internet Explorer 8 nicht beim ersten Mal starten, wenn **Java** als Plug-In-Typ ausgewählt ist.
Lokales Servervideo aktiviert	**Ja** zeigt an, dass der Ausgang zum Monitor der virtuellen Konsole während der virtuellen Konsole aktiviert ist. **Nein** zeigt an, dass die unter Verwendung der **virtuellen Konsole** ausgeführten Tasks auf dem lokalen Monitor des verwalteten Servers nicht sichtbar sind.

ANMERKUNG: Informationen zur Verwendung des virtuellen Datenträgers mit der virtuellen Konsole finden Sie unter „Virtuellen Datenträger konfigurieren und verwenden“ auf Seite 281.

3 Wenn eine Sitzung der virtuellen Konsole verfügbar ist, klicken Sie auf **Virtuelle Konsole starten**.

ANMERKUNG: 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 innerhalb von drei Minuten diese Dialogfelder durchlaufen. Ansonsten werden Sie aufgefordert, die Anwendung erneut zu starten.

ANMERKUNG: Wenn in den folgenden Schritten ein oder mehrere Fenster zur Sicherheitswarnung eingeblendet werden, lesen Sie die Informationen im jeweiligen Fenster und klicken Sie auf **Ja**, um fortzufahren.

Die Management Station wird mit dem iDRAC6 verbunden und der Desktop des Remote-Systems wird in **iDRACView** angezeigt.

4 Zwei Mauszeiger erscheinen im Viewer-Fenster: einer für das Remote-System und einer für das lokale System. Die beiden Mauszeiger müssen synchronisiert werden, damit der Remote-Mauszeiger dem lokalen Mauszeiger folgt. Siehe „Synchronisieren der Mauszeiger“ auf Seite 246.

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.

ANMERKUNG: Das Virtuelle Konsole-Bild ist nur verfügbar, wenn Sie Virtuelle Konsole aktiviert haben.

Tabelle 10-4 liefert Informationen über die verfügbaren Optionen.

Tabelle 10-4. Vorschau der virtuellen Konsole – Optionen

Option	Beschreibung
Starten	Klicken Sie auf diese Schaltfläche, um die virtuelle Konsole zu starten. Wenn nur der virtuelle Datenträger aktiviert ist, wird durch das Klicken auf diesen Link der virtuelle Datenträger direkt gestartet. Diese Schaltfläche ist deaktiviert, wenn Sie keine Virtuelle Konsole-Berechtigungen haben oder wenn sowohl die virtuelle Konsole als auch der virtuelle Datenträger deaktiviert sind.
Einstellungen	Klicken Sie auf diese Verknüpfung, um die Konfigurationseinstellungen der virtuellen Konsole auf der Seite **Konfiguration der virtuellen/Konsole/des virtuellen Datenträgers** einzusehen oder zu bearbeiten.
Refresh (Aktualisieren)	Klicken Sie auf diese Schaltfläche, um das angezeigte Abbild der virtuellen Konsole zu aktualisieren.

Verwendung des Video Viewer

Der Video Viewer ist eine Benutzerschnittstelle zwischen der Management Station und dem verwalteten Server, durch die der Desktop des verwalteten Servers sichtbar wird, und über die Maus- und Tastaturfunktionen von der Management Station aus gesteuert werden können. Wenn Sie eine Verbindung zum Remote-System herstellen, wird der Video Viewer in einem separaten Fenster gestartet.

ANMERKUNG: Die Titelleiste der virtuellen Konsole 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 angezeigt. Das Format lautet:

```
<DNS-Name / IPv6-Adresse / IPv4-Adresse>,
<Modell>, <Steckplatznummer>, User:
<Benutzername>, <fps>
```

Der Video Viewer bietet die Möglichkeit verschiedener Steuerungseinstellungen, wie Farbmodus, Maussynchronisation, Snapshots, Tastaturmakros, Energiemaßnahmen und Zugriff auf Virtuelle Datenträger. Klicken Sie auf **Hilfe**, um weitere Informationen über diese Funktionen zu erhalten.

Wenn Sie eine Virtuelle Konsole-Sitzung starten und der Video Viewer angezeigt wird, müssen Sie möglicherweise den Farbmodus einstellen und die Mauszeiger synchronisieren.

Tabelle 10-5 beschreibt die Menüoptionen, die im Viewer zum Gebrauch verfügbar sind.

Tabelle 10-5. Auswahlmöglichkeiten auf der Viewer-Menüleiste

Menüelement	Element	Beschreibung
Grafikkarte	**Pause (Anhalten)**	Hält die Virtuelle Konsole vorübergehend an.
	Wieder aufnehmen	Nimmt die Virtuelle Konsole wieder auf.
	Refresh (Aktualisieren)	Zeichnet die Bildschirmanzeige des Viewers neu.
	Aktuellen Bildschirminhalt erfassen	Erfasst den aktuellen Bildschirminhalt des Remote-Systems als **.bmp**-Datei. Ein Dialogfeld wird angezeigt, in dem Sie die Datei zu einem angegebenen Standort speichern können.
	Vollbildschirm	Um den Video Viewer im Vollbildschirm-Modus anzuzeigen, klicken Sie auf die rechte obere Ecke des Viewer.
	Beenden	Wenn Sie die Konsole nicht mehr verwenden und sich abgemeldet haben (über den Abmeldevorgang des Remote-Systems), wählen Sie im **Video**menü **Beenden** aus, um das Fenster **Video Viewer** zu schließen.
Keyboard (Tastatur)	Rechte Alt-Taste halten	Wählen Sie dieses Element aus, bevor Sie Tasten verwenden, die mit der rechten <Alt>-Taste kombiniert werden sollen.
	Linke Alt-Taste halten	Wählen Sie dieses Element aus, bevor Sie Tasten verwenden, die mit der linken <Alt>-Taste kombiniert werden sollen.
	Linke Windows-Taste	Wählen Sie **Gedrückt halten** aus, bevor Sie Zeichen eingeben, die mit der linken Windows-Taste kombiniert werden sollen. Wählen Sie **Drücken und loslassen** aus, um einen Tastenanschlag der linken Windows-Taste zu senden.
	Rechte Windows-Taste	Wählen Sie **Gedrückt halten** aus, bevor Sie Zeichen eingeben, die mit der rechten Windows-Taste kombiniert werden sollen. Wählen Sie **Drücken und loslassen** aus, um einen Tastenanschlag der rechten Windows-Taste zu senden.

Tabelle 10-5. Auswahlmöglichkeiten auf der Viewer-Menüleiste *(fortgesetzt)*

Menüelement	Element	Beschreibung
	Makros	Wenn Sie ein Makro auswählen oder die für das Makro angegebenen Schnelltaste eingeben, wird die Maßnahme auf dem Remote-System ausgeführt. Der Video Viewer enthält die folgenden Makros: • Alt+Strg+Entf • Alt+Tab • Alt+Esc • Strg+Esc • Alt+Leertaste • Alt+Eingabe • Alt+Bindestrich • Alt+F4 • Druck • Alt+Druck • F1 • Pause (Anhalten) • Alt+M • Alt+D • Alt+Druck+M • Alt+Druck+P
	Tastaturdurchgang	Im Modus Tastaturdurchgang können alle Tastaturfunktionen auf dem Client zum Server umgeleitet werden.
Maus	**Cursor synchronisieren**	Synchronisiert den Cursor, sodass die Maus auf dem Client zu der Maus auf dem Server umgeleitet wird.
	Lokalen Cursor ausblenden	Nur der Cursor der virtuellen Konsole wird angezeigt. Diese Einstellung wird empfohlen, wenn USC in einer virtuellen Konsole ausgeführt wird.

Tabelle 10-5. Auswahlmöglichkeiten auf der Viewer-Menüleiste *(fortgesetzt)*

Menüelement	Element	Beschreibung
Optionen	Farbmodus	Ermöglicht eine Farbtiefe auszuwählen, um die Leistung über das Netzwerk zu verbessern. Wenn Sie z. B. Software von einem virtuellen Datenträger installieren, können Sie die niedrigste Farbtiefe auswählen, damit die virtuelle Konsole weniger Netzwerkbandbreite verwendet und somit mehr Bandbreite verbleibt, um Daten vom Datenträger zu übertragen. Der Farbmodus kann auf 15-Bit Farbe und 7-Bit Farbe eingestellt werden.
Strom	System EINschalten	Schaltet das System ein.
	System AUSschalten	Schaltet das System aus.
	Ordentliches Herunterfahren	Fährt das System herunter.
	System Reset (Softwareneustart)	Startet das System neu, ohne es auszuschalten.
	System aus- und wieder einschalten (Hardwareneustart)	Schaltet das System aus und startet es dann erneut.

Tabelle 10-5. Auswahlmöglichkeiten auf der Viewer-Menüleiste *(fortgesetzt)*

Menüelement	Element	Beschreibung
Datenträger	**Virtueller Datenträger-Assistent**	Das **Datenträger**menü bietet Zugriff auf den Virtueller Datenträger-Assistenten, mit dem Sie zu einem Gerät oder einem Image umleiten können, wie z. B.: • Diskettenlaufwerk • CD • DVD • Image im ISO-Format • USB-Flash-Laufwerk Informationen zur Funktion virtueller Datenträger finden Sie unter „Virtuellen Datenträger konfigurieren und verwenden“ auf Seite 281. Wenn Sie Virtueller Datenträger verwenden, muss das Fenster Virtuelle Konsole aktiv sein.
Hilfe	**Info zu iDRACView**	Zeigt die iDRACView-Version an.

Synchronisieren der Mauszeiger

Wenn Sie sich über die virtuelle Konsole mit einem Remote-Dell PowerEdge-System verbinden, kann es sein, dass die Geschwindigkeit der Mausbeschleunigung auf dem Remote-System eventuell nicht mit dem Mauszeiger auf der Management Station synchron ist, was dazu führt, dass zwei Mauszeiger im Video Viewer-Fenster erscheinen.

Zum Synchronisieren der Mauszeiger klicken Sie auf **Maus→ Cursor synchronisieren** oder drücken Sie <Alt><M>.

Das Menü zum Synchronisieren des Cursors lässt sich umschalten. Stellen Sie sicher, dass sich neben dem Menüelement ein Häkchen befindet, damit die Maussynchronisation aktiv ist.

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 starten. Hilfe bei der Konfiguration steht unter „Konfigurieren der virtuellen Konsole und der virtuellen Datenträger auf der iDRAC6-

Webschnittstelle“ auf Seite 236 zur Verfügung. Die Standardmauseinstellungen des Betriebssystems werden zum Steuern des Mauspfeils auf dem Bildschirm der **virtuellen Konsole** des iDRAC6verwendet.

Wenn auf dem Client-Bildschirm der virtuellen Konsole zwei Mauszeiger angezeigt werden, weist dies darauf hin, dass das Betriebssystem des Servers die Relativposition unterstützt. Dies ist in der Regel bei Linux-Betriebssystemen oder dem Universal Server Configurator (USC) von Dell der Fall. Dabei werden zwei Mauszeiger angezeigt, wenn die Mausbeschleunigungseinstellungen des Servers von denen des Virtuelle Konsole-Clients abweichen. Um dies zu vermeiden können Sie in den Einzel-Cursor-Modus wechseln, indem Sie im Menü „Extras“ des Bildschirms „Virtuelle Konsole“ die Option „Einzel-Cursor“ auswählen, oder versuchen, die Mausbeschleunigungseinstellungen von Server und Client anzugleichen.

ANMERKUNG: Dies gilt nicht für Server, die auf Windows-Betriebssystemen ausgeführt werden, da diese die Absolutposition unterstützen.

Wenn Sie mithilfe der virtuellen iDRAC-Konsole eine Verbindung zu einem verwalteten Server herstellen möchten, auf dem ein Betriebssystem einer aktuellen Linux-Distribution installiert ist, können Probleme mit der Maussynchronisierung auftreten. Mögliche Ursache hierfür ist die Funktion zur vorhersehbaren Zeigerbeschleunigung des GNOME-Desktops. Um eine fehlerfreie Maussynchronisierung in der virtuellen iDRAC-Konsole sicherzustellen, muss diese Funktion deaktiviert sein. Führen Sie im Mausabschnitt der Datei **etc/X11/xorg.conf** Folgendes hinzu, um die vorhersehbare Zeigerbeschleunigung zu deaktivieren:

`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`.

Lokale Konsole deaktivieren oder aktivieren

Sie können den iDRAC6 so konfigurieren, dass Virtuelle Konsole-Verbindungen unter Verwendung der iDRAC6-Webschnittstelle unzulässig sind. Ist die lokale Konsole deaktiviert, wird in der Serverliste (in der lokalen Konsole) ein gelber Statuspunkt angezeigt, um anzugeben, dass die Konsole in iDRAC6 gesperrt ist. Wenn die lokale Konsole aktiviert ist, ist der Statuspunkt grün.

Wenn Sie sicherstellen möchten, dass Sie exklusiven Zugriff auf die Konsole des verwalteten Servers haben, müssen Sie die lokale Konsole deaktivieren *und* die **Max. Sitzungen** auf der **Seite Virtuelle Konsole** auf `1` konfigurieren.

ANMERKUNG: Das Deaktivieren (Ausschalten) des lokalen Videos auf dem Server führt dazu, dass der Monitor, die Tastatur und die Maus, die an die virtuelle Konsole angeschlossen sind, deaktiviert werden.

Wenden Sie zum Deaktivieren oder Aktivieren der lokalen Konsole das folgende Verfahren an:

1. Öffnen Sie auf Ihrer Management Station einen unterstützten Webbrowser, und melden Sie sich am iDRAC6 an. Weitere Informationen finden Sie unter „Zugriff auf die Webschnittstelle“ auf Seite 90.
2. Klicken Sie auf **System**, dann auf die Registerkarte **Virtuelle Konsole/Virtueller Datenträger** und dann auf **Konfiguration**.
3. Wenn Sie das lokale Video auf dem Server deaktivieren (ausschalten) möchten, heben Sie auf dem Bildschirm **Konfiguration** die Markierung von **Lokales Servervideo aktiviert** auf und klicken Sie dann auf **Anwenden**. Standardmäßig ist der Wert auf **Aktiviert (markiert)** eingestellt.
4. Wenn Sie auf dem Server das lokale Video aktivieren (einschalten) möchten, markieren Sie auf dem Bildschirm **Konfiguration** das Kontrollkästchen für **Lokales Servervideo aktiviert** und klicken Sie dann auf **Anwenden**.

Die Seite **Virtuelle Konsole** zeigt den Status des lokalen Servervideos an.

Virtuelle Konsole und virtuellen Datenträger im Remote-Zugriff starten

Sie können Virtuelle Konsole/Virtueller Datenträger durch die Eingabe einer einzelnen URL in einen unterstützten Browser statt über die iDRAC6 Web GUI starten. Abhängig von Ihrer Systemkonfiguration werden Sie entweder durch den manuellen Authentifizierungsprozess (Anmeldeseite) oder automatisch zum Viewer für Virtuelle Konsole/Virtueller Datenträger (iDRACView) geführt.

ANMERKUNG: Internet Explorer unterstützt lokale Anmeldungen, Active Directory (AD)- und Smart Card (SC)-Anmeldungen sowie Einzelanmeldungen (SSO). Firefox unterstützt SSO-, AD- und lokale Anmeldungen.

URL-Format

Wenn Sie den Link **https://<idrac6_ip>/console** in den Browser eingeben, kann je nach Anmeldungskonfiguration eine normale manuelle Anmeldung erforderlich sein. Wenn SSO nicht aktiviert und AD-, SC- oder lokale Anmeldung aktiviert ist, wird die entsprechende Anmeldeseite angezeigt. Wenn die Anmeldung erfolgreich ist, wird die Ansicht Virtuelle Konsole oder Virtueller Datenträger nicht gestartet. Stattdessen werden Sie zur iDRAC6 GUI-Startseite zurückgeführt.

ANMERKUNG: Bei der URL für den Start von iDRACView muss die Groß- und Kleinschreibung beachtet werden; verwenden Sie ausschließlich Kleinbuchstaben.

Allgemeine Fehlerszenarien

Tabelle 10-6 listet allgemeine Fehlerszenarien, die Ursachen für diese Fehler und iDRAC6-Funktionsweisen auf.

Tabelle 10-6. Fehlerszenarien

Fehlerszenarien	Ursache	Funktionsweise
Anmeldung ist fehlgeschlagen	Sie haben entweder einen unzulässigen Benutzernamen oder ein falsches Kennwort eingegeben.	Die gleiche Funktionsweise wie bei der Angabe von *https://<ip>* und fehlgeschlagener Anmeldung.

Tabelle 10-6. Fehlerszenarien *(fortgesetzt)*

Fehlerszenarien	Ursache	Funktionsweise
Unzureichende Berechtigungen	Sie haben keine Berechtigung für die virtuelle Konsole und virtuelle Datenträger.	iDRACView wird nicht gestartet und Sie werden auf die GUI-Seite Konfiguration Virtuelle Konsole/Virtuelle Datenträger zurückgeführt.
Virtuelle Konsole deaktiviert	Die virtuelle Konsole ist auf Ihrem System deaktiviert.	iDRACView wird nicht gestartet und Sie werden auf die GUI-Seite Konfiguration Virtuelle Konsole/Virtuelle Datenträger zurückgeführt.
Unbekannte URL-Parameter festgestellt	Die von Ihnen eingegebene URL enthält undefinierte Parameter.	Die Nachricht „Seite nicht gefunden (404)“ wird angezeigt.

Häufig gestellte Fragen

Tabelle 10-7 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 10-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen

Frage	Antwort
Die virtuelle Konsole meldet sich nicht ab, wenn die bandexterne Web-GUI abgemeldet ist.	Die Sitzungen der virtuellen Konsole und des virtuellen Datenträgers bleiben aktiv, auch wenn die Websitzung abgemeldet ist. Schließen Sie die Viewer-Anwendungen des virtuellen Datenträgers und der virtuellen 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

Tabelle 10-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Warum dauert es 15 Sekunden, um das lokale Video auf dem Server auszuschalten, nachdem eine Aufforderung zum Ausschalten des lokalen Videos erteilt 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 iDRAC6 eine Aufforderung zum **EIN**schalten des lokalen Videos erhält, wird das Video sofort eingeschaltet.
Kann der lokale Benutzer das Video auch ausschalten?	Ja, ein lokaler Benutzer kann die lokale RACADM-CLI verwenden, um das Video auszuschalten.
Kann der lokale Benutzer das Video auch einschalten?	Nein. Wenn die lokale Konsole deaktiviert ist, sind auch die Tastatur und die Maus des lokalen Benutzers deaktiviert und Einstellungsänderungen sind nicht möglich.
Werden beim Ausschalten des lokalen Videos auch die lokale Tastatur und Maus ausgeschaltet?	Ja
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 iDRAC6-Benutzer erforderlich, um das lokale Servervideo ein- oder auszuschalten?	Jeder Benutzer mit iDRAC6-Konfigurationsberechtigungen kann die lokale Konsole ein- oder ausschalten.

Tabelle 10-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Wie kann ich den aktuellen Status des lokalen Servervideos abrufen?	Der Status wird auf dem Bildschirm **Virtuelle Konsole und Virtueller Datenträger** der iDRAC6-Webschnittstelle angezeigt. Der RACADM-CLI-Befehl `racadm getconfig -g cfgRacTuning` zeigt den Status im Objekt **cfgRacTuneLocalServerVideo** an. Dieser racadm-Befehl kann über Telnet/SSH oder über eine Remote-Sitzung auf dem iDRAC6 ausgeführt werden. Der Remote-RACADM-Befehl lautet: `racadm -r <idracip> -u <Benutzer> -p <Kennwort> getconfig -g cfgRacTuning` Der Status wird auch auf der Virtuelle Konsole-OSCAR-Anzeige sichtbar. Wenn die lokale Konsole aktiviert ist, erscheint neben dem Servernamen eine grüne Statusanzeige. Wenn sie deaktiviert ist, weist ein gelber Punkt darauf hin, dass die lokale Konsole vom iDRAC6 gesperrt ist.
Ich kann vom Fenster der virtuellen Konsole aus den unteren Teil des Systembildschirms nicht sehen.	Stellen Sie sicher, dass die Bildschirmauflösung der Management Station auf 1280x1024 eingestellt ist.
Das Konsolenfenster wird nicht richtig dargestellt.	Für den Virtuelle Konsole-Viewer ist auf Linux ein UTF-8-Zeichensatz erforderlich. Überprüfen Sie Ihren lokalen Zeichensatz und setzen Sie diesen zurück, wenn notwendig. Weitere Informationen finden Sie unter „Gebietsschema in Linux einstellen“ auf Seite 75.

Tabelle 10-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Warum wird auf dem verwalteten Server ein leerer Bildschirm eingeblendet, wenn das Windows 2000-Betriebssystem geladen wird?	Der verwaltete Server enthält nicht den richtigen ATI-Videotreiber. Aktualisieren Sie den Videotreiber.
Warum synchronisiert die Maus nicht in DOS, 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 Relativposition für den Mauszeiger verwendet, was die Verzögerung in der Synchronisation verursacht. Der iDRAC6 enthält einen USB-Maustreiber, der eine absolute Position und ein genaueres Verfolgen des Mauszeigers ermöglicht. Selbst wenn der iDRAC6 die absolute USB-Mausposition auf das Dell-BIOS überträgt, setzt die BIOS-Emulation sie auf die relative Position zurück, und das Verhalten bleibt unverändert. Um dieses Problem zu beheben, stellen Sie auf dem **Konfigurations**-Bildschirm den Mausmodus auf **USC/Diags** ein.
Warum synchronisiert sich die Maus bei Verwendung der Linux-Textkonsole nicht (entweder mit Dell Unified Server Configurator (USC), Dell Lifecycle Controller (LC) oder Dell Unified Server Configurator Lifecycle Controller Enabled (USC-LCE)?	Die virtuelle Konsole erfordert den USB-Maustreiber, doch der USB-Maustreiber ist nur unter dem X-Window-Betriebssystem verfügbar.

Tabelle 10-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Ich habe immer noch Probleme mit der Maussynchronisierung.	Stellen Sie sicher, dass vor dem Beginn einer Virtuelle Konsole-Sitzung die richtige Maus für das Betriebssystem ausgewählt ist. Stellen Sie sicher, dass im **Maus**-Menü **Maus synchronisieren** markiert ist. Drücken Sie <Alt><M> oder wählen Sie **Maus→ Maus synchronisieren**, um die Maussynchronisation umzuschalten. Wenn die Synchronisation aktiviert ist, wird neben der Auswahl im **Maus**-Menü ein Häkchen angezeigt.
Warum kann ich keine Tastatur oder Maus verwenden, während ich ein Microsoft-Betriebssystem unter Verwendung einer virtuellen iDRAC6-Konsole im Remote-Zugriff installiere?	Wenn Sie im Remote-Zugriff ein unterstütztes Microsoft-Betriebssystem auf einem System installieren, auf dem die virtuelle Konsole im BIOS aktiviert ist, erhalten Sie eine EMS-Verbindungsmeldung, die verlangt, dass Sie **OK** wählen, bevor Sie fortfahren können. Sie können nicht die Maus verwenden, um **OK** im Remote-Zugriff auszuwählen. Sie müssen entweder auf dem lokalen System **OK** auswählen oder den im Remote-Zugriff verwalteten Server neu starten und neu installieren und dann die virtuelle Konsole im BIOS ausschalten. Diese Nachricht wird durch Microsoft erstellt, um den Benutzer darauf hinzuweisen, dass die virtuelle Konsole aktiviert ist. Um sicherzustellen, dass diese Meldung nicht eingeblendet wird, schalten Sie die virtuelle Konsole im BIOS immer aus, bevor Sie ein Betriebssystem im Remote-Zugriff installieren.

Tabelle 10-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Warum zeigt die Num-Tasten-Anzeige auf meiner Management Station nicht den Status der Num-Taste auf dem Remote-Server an?	Wenn über den iDRAC6 auf die Num-Taste zugegriffen wird, stimmt die Num-Taste auf der Management Station nicht unbedingt mit dem Zustand der Num-Taste auf dem Remote-Server überein. Der Zustand der Num-Taste hängt von der Einstellung auf dem Remote-Server ab, wenn die Remote-Sitzung verbunden wird, unabhängig vom Zustand der Num-Taste auf der Management Station.
Warum werden mehrere Session Viewer-Fenster eingeblendet, wenn ich vom lokalen Host aus eine Sitzung der virtuellen Konsole aufbaue?	Sie konfigurieren eine Sitzung der virtuellen Konsole vom lokalen System aus. Dies wird nicht unterstützt.
Erhalte ich eine Warnungsmeldung, wenn ich eine Sitzung der virtuellen Konsole ausführe und ein lokaler Benutzer auf den verwalteten Server zugreift?	Nein. Wenn ein lokaler Benutzer auf das System zugreift, haben Sie beide Kontrolle über das System.
Welche Bandbreite benötige ich, um eine Sitzung der virtuellen Konsole auszuführen?	Für gute Leistungen wird eine Verbindung von 5 MB/s empfohlen. Eine 1 MB/s-Verbindung ist zum Erzielen der Mindestleistung erforderlich.
Was sind die Mindestsystemanforderungen für meine Management Station zum Ausführen der der virtuellen Konsole?	Die Verwaltungsstation erfordert einen Intel Pentium III 500-MHz-Prozessor mit mindestens 256 MB RAM.
Nach Starten der virtuellen Konsole kann ich die Maus nur auf der virtuellen Konsole und nicht auf meinem lokalen System verwenden. Warum geschieht dies; und was muss ich tun, um die Maus in der virtuellen Konsole und in meinem lokalen System verwenden zu können?	Dies geschieht, wenn der **Mausmodus** auf **USC/Diags** gestellt ist. Drücken Sie die Tastenkombination <Alt><M>, um die Maus in Ihrem lokalen System benutzen zu können. Drücken Sie <Alt><M> erneut, um die Maus in der virtuellen Konsole verwenden zu können.

Tabelle 10-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Beim Starten der GUI und der virtuellen Konsole für iDRAC über die CMC-Webschnittstelle wird die GUI-Sitzungszeit überschritten. Warum?	Beim Starten der virtuellen Konsole für iDRAC über die CMC-Webschnittstelle wird ein Popup-Fenster zum Starten der virtuellen Konsole geöffnet. Dieses Popup-Fenster wird kurz nach dem Öffnen der virtuellen Konsole geschlossen. Werden sowohl die GUI als auch die virtuelle Konsole für ein und dasselbe iDRAC-System einer Management Station gestartet, wird die Sitzungszeit der iDRAC-GUI überschritten, wenn die GUI vor dem Schließen des Popup-Fensters gestartet wird. Wenn die iDRAC-GUI über die CMC-Webschnittstelle bei geschlossener virtueller Konsole und nach dem Schließen des Popup-Fensters gestartet wird, tritt dieses Problem nicht auf.

Tabelle 10-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Die Linux-S-Abf-Taste funktioniert nicht in Internet Explorer. Warum?	Das Verhalten der Linux S-Abf-Taste ändert sich, wenn die virtuelle Konsole über Internet Explorer verwendet wird. Zum Senden der S-Abf-Befehle müssen Sie die Taste **Bildschirm drucken** drücken und wieder loslassen und dabei die Tasten **Strg** und **Alt** gedrückt halten. Gehen Sie wie folgt vor, um die S-Abf-Befehle unter Verwendung von Internet Explorer über iDRAC an einen Remote-Linux-Server zu senden: **1** Aktivieren Sie die magische Tastenfunktion auf dem Remote-Linux-Server. Sie können diese mit dem folgenden Befehl auf dem Linux-Terminal aktivieren: `echo 1 > /proc/sys/kernel/sysrq` **2** Aktivieren Sie den Tastaturdurchgangsmodus von Active X Viewer. **3** Drücken Sie auf **Strg** + **Alt** + **Bildschirm drucken**. **4** Lassen Sie nur die Taste **Bildschirm drucken** wieder los. **5** Drücken Sie auf **Bildschirm drucken** + **Strg** + **Alt**. **ANMERKUNG:** Die S-Abf-Funktion wird derzeit nicht für Internet Explorer und Java unterstützt.

11

Konfiguration der vFlash-SD-Karte und Verwalten der vFlash-Partitionen

Die vFlash-SD-Karte ist eine Secure Digital-Karte, die am optionalen Steckplatz der iDRAC6 Enterprise-Karte in der hinteren Ecke des Systems eingesetzt wird. Sie enthält einen Speicherplatz, der sich wie ein übliches USB Flash Key-Gerät verhält. Sie ist der Speicherort für benutzerdefinierte Partitionen, die so konfiguriert werden können, dass sie dem System gegenüber als USB-Gerät präsentiert werden und auch dazu verwendet werden können, ein startfähiges USB-Gerät zu erstellen. Je nach ausgewähltem Emulationsmodus werden die Partitionen dem System gegenüber als Diskettenlaufwerk, als Festplatte oder als CD/DVD-Laufwerk präsentiert. Alle können als startfähiges Gerät festgelegt werden.

Die vFlash-SD-Karten und standardmäßigen SD-Karten werden unterstützt. Als *vFlash-SD-Karte* wird die Karte bezeichnet, die die neuen verbesserten vFlash-Funktionen unterstützt. Eine *Standard-SD-Karte* ist eine normale, handelsübliche SD-Karte, die nur begrenzte vFlash-Funktionen unterstützt.

Mit einer vFlash-SD-Karte können Sie bis zu 16 Partitionen erstellen. Sie können die Partition mit einem bestimmten Namen kennzeichnen, wenn sie erstellt wird, und eine Reihe von Vorgängen ausführen, um die Partitionen zu verwalten und verwenden. Eine vFlash-SD-Karte kann eine beliebige Größe bis zu 8 GB aufweisen. Jede Partition kann bis zu 4 GB groß sein.

Eine standardmäßige SD-Karte kann von beliebiger Größe sein, unterstützt jedoch nur eine einzige Partition. Die Größe der Partition ist auf 256 MB beschränkt. Die Partition wird standardmäßig mit dem Namen VFLASH gekennzeichnet.

ANMERKUNG: Achten Sie darauf, dass Sie nur eine vFlash-SD-Karte oder eine standardmäßige SD-Karte in den Steckplatz für die iDRAC6 Enterprise-Karte einsetzen. Wenn Sie eine Karte eines anderen Formats einsetzen (z. B. eine Multimediakarte – MMC), wird beim Initialisieren der Karte die folgende Fehlermeldung angezeigt: *An error has occurred while initializing SD card.* (Beim Initialisieren der SD-Karte ist ein Fehler aufgetreten.)

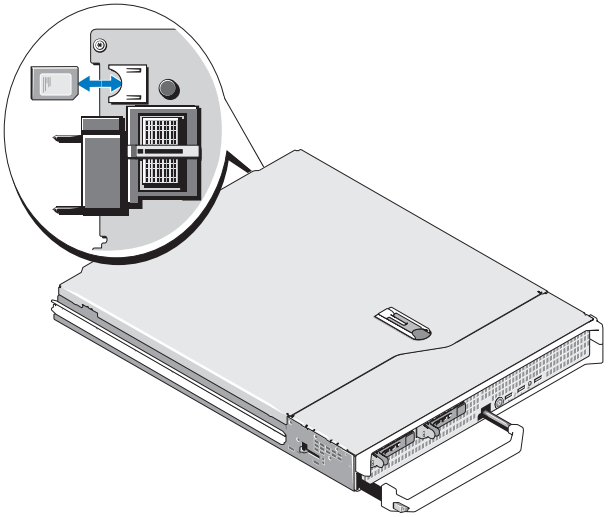
Wenn Sie ein Administrator sind, können Sie alle Vorgänge auf den vFlash-Partitionen ausführen. Wenn Sie kein Administrator sind, müssen Sie über die Berechtigung zum Zugriff auf virtuelle Datenträger verfügen, um die Inhalte für die Partition erstellen, löschen, formatieren, verbinden, abtrennen oder kopieren zu können.

ANMERKUNG: Sie können nur einen einzigen vFlash-Vorgang auf einmal ausführen. Der erste Vorgang muss beendet sein, bevor Sie mit einem weiteren vFlash-Vorgang beginnen. Wenn Sie z. B. einen Vorgang Aus Abbild Anlegen mit RACADM starten, können Sie nicht einen Anlege-, Download- oder Formatierungsvorgang mit RACADM oder der GUI durchführen. Sie müssen bis zum Ende der Operation warten, bevor Sie den nächsten vFlash-Vorgang durchführen können.

Installieren einer vFlash- oder Standard-SD-Karte

1. Entfernen Sie das Blade aus dem Gehäuse.
2. Machen Sie den vFlash-Mediensteckplatz in der hinteren Ecke des Systems ausfindig.

   ANMERKUNG: Für die Installation oder Entnahme der Karte muss das Blade-Cover nicht entfernt werden.



3 Führen Sie das SD-Kartenende mit den Kontakten in den Steckplatz ein, wobei die Etikettseite nach oben weist.

ANMERKUNG: Der Steckplatz ist mit einer Passung versehen, um ein korrektes Einsetzen der Karte sicherzustellen.

4 Drücken Sie die Karte nach innen, um sie im Steckplatz zu sichern.

5 Setzen Sie das Blade wieder in das Gehäuse ein.

Entfernen einer vFlash- oder Standard-SD-Karte

Um die vFlash- oder Standard-SD-Karte zu entfernen, drücken Sie die Karte nach innen, um sie freizugeben, und ziehen Sie dann die Karte aus dem Kartensteckplatz.

vFlash- oder standardmäßige SD-Karte unter Verwendung der iDRAC6-Webschnittstelle konfigurieren

Nachdem Sie die vFlash- oder standardmäßige SD-Karte installiert haben, können Sie ihre Eigenschaften anzeigen, vFlash aktivieren oder deaktivieren und die Karte initialisieren. Die Karte muss zur Durchführung der Partitionsverwaltung aktiviert sein. Wenn die Karte deaktiviert ist, können Sie nur ihre Eigenschaften anzeigen. Durch den Initialisierungsvorgang werden vorhandene Partitionen entfernt und die Karte zurückgesetzt.

ANMERKUNG: Um vFlash aktivieren oder deaktivieren oder die Karte initialisieren zu können, müssen Sie über die Berechtigung zum Konfigurieren von iDRAC verfügen.

Wenn sich im iDRAC6 Enterprise-Kartensteckplatz des Systems keine Karte befindet, wird folgende Fehlermeldung angezeigt.

```
SD-Karte nicht festgestellt. Setzen Sie bitte eine
SD-Karte mit 256 MB oder mehr Speicherplatz ein.
```

So wird die vFlash- oder standardmäßige SD-Karte angezeigt und konfiguriert:

1 Öffnen Sie einen unterstützten Webbrowser und melden Sie sich an der iDRAC6-Webschnittstelle an.

2 Klicken Sie in der Systemstruktur auf **System**.

3 Klicken Sie auf das Register **VFlash**. Die Seite **Eigenschaften der SD-Karte** wird angezeigt.

Tabelle 11-1 führt die Eigenschaften auf, die für die SD-Karte angezeigt werden.

Tabelle 11-1. Eigenschaften der SD-Karte

Attribut	Beschreibung
Name	Zeigt den Namen der in dem iDRAC6 Enterprise-Kartensteckplatz des Servers installierten Karte an. Wenn die Karte die neuen, erweiterten vFlash-Funktionen unterstützt, wird *vFlash SD-Karte* angezeigt. Wenn sie begrenzte vFlash-Funktionen unterstützt, wird *SD-Karte* angezeigt.
Größe	Zeigt die Größe der Karte in Gigabyte (GB) an.
Available Space (Verfügbarer Speicherplatz)	Zeigt den nicht verwendeten Speicherplatz auf der SD-Karte in MB an. Dieser Speicherplatz ist verfügbar, um weitere Partitionen auf der vFlash-SD-Karte zu erstellen. Wenn die eingesetzte SD-Karte nicht initialisiert ist, wird beim verfügbaren Speicherplatz angezeigt, dass die Karte nicht initialisiert wurde.
Schreibgeschützt	Zeigt an, ob die Karte schreibgeschützt ist oder nicht.
Seite „Funktionszustand“	Zeigt den Gesamtzustand der SD-Karte an. Dieser kann lauten: • OK • Warnung • Kritisch Beim Funktionszustand „Warnung“ ist die Karte neu zu initialisieren. Beim Funktionszustand „Kritisch“ ist die Karte neu zu installieren und neu zu initialisieren.
vFlash aktivieren	Markieren Sie das Kontrollkästchen, um auf der Karte vFlash-Partitionsverwaltung auszuführen. Heben Sie die Markierung des Kontrollkästchens auf, um die vFlash-Partitionsverwaltung zu deaktivieren.

4 Klicken Sie auf **Anwenden,** um die vFlash-Partitionsverwaltung auf der Karte zu aktivieren oder zu deaktivieren.

Wenn eine vFlash-Partition verbunden wird, ist es nicht möglich, vFlash zu deaktivieren, und es wird eine Fehlermeldung angezeigt.

ANMERKUNG: Wenn vFlash deaktiviert ist, können Sie nur die Eigenschaften der SD-Karte einsehen, aber keine anderen vFlash-Vorgänge wie das Anlegen von Partitionen (leer und mit Abbilddatei), das Verwalten von Partitionen, das Formatieren von Partitionen und das Herunterladen von Partitionsinhalten durchführen.

5 Klicken Sie auf **Initialisieren**. Sämtliche vorhandenen Partitionen werden entfernt, und die Karte wird zurückgesetzt. Eine Bestätigungsmeldung wird angezeigt.

6 Klicken Sie auf **OK**. Nach Abschluss des Initialisierungsvorgangs wird eine Erfolgsmeldung angezeigt.

ANMERKUNG: **Initialisieren** ist nur verfügbar, wenn Sie die Option **vFlash Aktiviert** wählen.

Wenn eine vFlash-Partition verbunden wird, schlägt der Initialisierungsvorgang fehl, und es wird eine Fehlermeldung angezeigt.

Wenn Sie auf eine beliebige Option auf den vFlash-Seiten klicken, während eine Applikation - wie WSMAN provider, das iDRAC6-Konfigurationsprogramm oder RACADM - vFlash verwendet, oder wenn sie zu einer anderen Seite in der GUI navigieren, kann iDRAC6 die folgende Meldung anzeigen.

```
Die SD-Karte ist vorübergehend nicht verfügbar.
Klicken Sie auf Aktualisieren, um einen neuen Versuch
zu starten.
```

vFlash- oder standardmäßige SD-Karte unter Verwendung von RACADM konfigurieren

Sie können die vFlash- oder standardmäßige SD-Karte unter Verwendung von RACADM-Befehlen über die lokale, Remote- oder Telnet/SSH-Konsole anzeigen und konfigurieren.

ANMERKUNG: Um vFlash aktivieren oder deaktivieren und die Karte initialisieren zu können, müssen Sie über die Berechtigung zum Konfigurieren von iDRAC verfügen.

Eigenschaften der vFlash- oder standardmäßigen SD-Karte anzeigen

Öffnen Sie eine Telnet-/SSH-/serielle Konsole zum Server, melden Sie sich an und geben Sie den folgenden Befehl ein:

```
racadm getconfig -g cfgvFlashSD
```

Die folgenden Nur-Lesen-Eigenschaften werden angezeigt:

- `cfgvFlashSDSize`
- `cfgvFlashSDLicense`
- `cfgvFlashSDAvailableSize`
- `cfgvFlashSDHealth`

vFlash- oder standardmäßige SD-Karte aktivieren oder deaktivieren

Öffnen Sie eine Telnet-/SSH-/serielle Konsole zum Server, melden Sie sich an und geben Sie den folgenden Befehl ein:

- Zum Aktivieren einer vFlash- oder standardmäßigen SD-Karte:

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
  ```

- Zum Deaktivieren einer vFlash- oder standardmäßigen SD-Karte:

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
  ```

ANMERKUNG: Der RACADM-Befehl funktioniert nur, wenn eine vFlash- oder standardmäßige SD-Karte vorhanden ist. Wenn keine Karte vorhanden ist, wird folgende Meldung angezeigt: *FEHLER: SD-Karte nicht vorhanden*.

Initialisieren der vFlash- oder Standard-SD-Karte

Öffnen Sie eine Telnet-/SSH-/serielle Konsole zum Server, melden Sie sich an und geben Sie den folgenden Befehl ein:

```
racadm  vflashsd  initialize
```

Sämtliche vorhandenen Partitionen werden gelöscht, und die Karte wird zurückgesetzt.

Letzten Status der vFlash- oder standardmäßigen SD-Karte abrufen

Öffnen Sie eine telnet-/SSH-/serielle Konsole für den Server, melden Sie sich an und geben Sie den folgenden Befehl ein, um den Status des letzen an die vFlash- oder Standard-SD-Karte gesendeten Befehls zu erhalten:

```
racadm vFlashsd status
```

Zurücksetzen der vFlash- oder Standard-SD-Karte

Öffnen Sie eine Telnet-/SSH-/serielle Konsole für den Server, melden Sie sich an und geben Sie Folgendes ein:

```
racadm vflashsd initialize
```

Weitere Informationen zu `vflashsd`, finden Sie im *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC auf der* Dell Support-Website unter **dell.com/support/manuals**.

ANMERKUNG: Der Befehl `racadm vmkey reset` wird ab Version 1.5 als veraltet eingestuft. Die Funktionalität dieses Befehls wird jetzt durch `vflashsd initialize` abgedeckt. Obgleich die Ausführung des Befehls `vmkey reset` erfolgreich verlaufen wird, wird empfohlen, den Befehl `vflashsd initialize` zu verwenden. Weitere Informationen finden Sie unter„Initialisieren der vFlash- oder Standard-SD-Karte“ auf Seite 264.

vFlash-Partitionen unter Verwendung der iDRAC6-Webschnittstelle verwalten

Sie können folgende Aufgaben ausführen:

- Leere Partition erstellen
- Partition unter Verwendung einer Imagedatei erstellen
- Partition formatieren
- Verfügbare Partitionen anzeigen
- Partition modifizieren
- Partition verbinden/abtrennen
- Vorhandene Partitionen löschen
- Inhalt einer Partition herunterladen
- Zu einer Partition starten

Leere Partition erstellen

Eine leere Partition ist einem leeren USB-Stick ähnlich. Sie können leere Partitionen auf einer vFlash- oder standardmäßigen SD-Karte erstellen. Sie können wählen, ob Sie Partitionen des Typs *Diskette* oder *Festplatte* anlegen wollen. Der Partitionstyp CD wird für das Erstellen leerer Partitionen nicht unterstützt.

ANMERKUNG: Um leere Partitionen erstellen zu können, müssen Sie über die Berechtigung 'Zugriff auf virtuellen Datenträger' verfügen.

Stellen Sie vor dem Anlegen einer leeren Partition Folgendes sicher:

- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Es wird nicht bereits ein Initialisierungsvorgang auf der Karte ausgeführt.

So erstellen Sie eine leere vFlash-Partition:

1. Wählen Sie auf der iDRAC6-Webschnittstelle **System→ vFlash→** Unterregister **Leere Partition erstellen** aus. Die Seite **Leere Partition erstellen** wird angezeigt.
2. Geben Sie die unter Tabelle 11-2 aufgeführten Informationen ein.
3. Klicken Sie auf **Anwenden**. Es wird eine neue Partition erstellt.

ANMERKUNG: Wenn das Anlegen einer Partition läuft, wird der Fortschritt oder Status nicht angezeigt.

Es wird eine Fehlermeldung angezeigt, wenn Folgendes zutrifft:

- Die Karte ist schreibgeschützt.
- Der Kennzeichnungsname stimmt mit der Kennzeichnung einer vorhandenen Partition überein.
- Für die Partitionsgröße wurde ein nicht ganzzahliger Wert eingegeben, der Wert übersteigt den verfügbaren Speicherplatz auf der Karte, oder die geforderte Partitionsgröße ist größer als 4 GB.
- Auf der Karte wird bereits ein Initialisierungsvorgang ausgeführt.

ANMERKUNG: Die neue Partition ist unformatiert (RAW).

Tabelle 11-2. Optionen der Seite 'Leere Partition erstellen'

Feld	Beschreibung
Stichwortverzeichnis	Wählen Sie einen Partitionsindex aus. In der Drop-Down-Liste werden nur ungebrauchte Indizes angezeigt. Standardmäßig wird der niedrigste verfügbare Index ausgewählt. Sie können ihn zu einem beliebigen anderen Indexwert aus der Drop-Down-Liste ändern. **ANMERKUNG:** Für die standardmäßige SD-Karte ist nur Index 1 verfügbar.

Tabelle 11-2. Optionen der Seite 'Leere Partition erstellen'

Feld	Beschreibung
Bezeichnung	Geben Sie eine eindeutige Kennzeichnung für die neue Partition ein. Der Kennzeichnungsname kann aus bis zu sechs alphanumerischen Zeichen bestehen. Er darf keine Leerstellen enthalten. Die Zeichen werden in Großbuchstaben angezeigt. **ANMERKUNG:** Für die Standard-SD-Karte muss die Bezeichnung VFLASH lauten. Wenn nicht, wird eine Fehlermeldung angezeigt.
Emulationstyp	Wählen Sie aus der Drop-Down-Liste den Emulationstyp für die Partition aus. Die verfügbaren Optionen sind **Diskette** und **Festplatte**.
Größe	Geben Sie die Partitionsgröße in Megabytes (MB) an. Die maximale Partitionsgröße ist 4 GB oder weniger oder gleich dem verfügbaren Platz auf der vFlash-SD-Karte. **ANMERKUNG:** Bei der Standard-SD-Karte kann die Partitionsgröße bis zu 256 MB betragen.

Partition unter Verwendung einer Imagedatei erstellen

Sie können eine neue Partition auf der vFlash- oder Standard-SD-Karte mithilfe einer Abbild-Datei anlegen (verfügbar im **.img-** oder **.iso-**Format). Sie können eine Partition des Typs Diskette, Festplatte oder CD anlegen. Die angelegte Partition ist schreibgeschützt.

ANMERKUNG: Um Partitionen erstellen zu können, müssen Sie über die Berechtigung 'Zugriff auf virtuellen Datenträger' verfügen.

Die Größe der neu erstellten Partition ist gleich der Größe der Imagedatei. Die Größe der Imagedatei muss folgende Eigenschaften aufweisen:

- Geringer als der auf der Karte verfügbare Speicherplatz oder gleich diesem Speicherplatz.
- Geringer als oder gleich 4 GB. Die maximale Partitionsgröße beträgt 4 GB.

Bei Verwendung der Webschnittstelle ist die Größe des Images, das auf die vFlash-SD-Karte hochgeladen werden kann, sowohl auf 32-Bit- als auch auf 64-Bit-Browsern (Internet Explorer und FireFox) auf maximal 2 GB beschränkt.

Unter Verwendung der RACADM- und WSMAN-Schnittstelle beträgt die Imagegröße, die auf eine vFlash-SD-Karte hochgeladen werden kann, maximal 4 GB.

Für die Standard-SD-Karte muss die Größe des Abbildes kleiner oder gleich 256 MB sein.

Stellen Sie vor dem Erstellen einer Partition über eine Imagedatei Folgendes sicher:

- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Es wird nicht bereits ein Initialisierungsvorgang auf der Karte ausgeführt.

ANMERKUNG: Stellen Sie beim Erstellen einer Partition über eine Imagedatei sicher, dass der Imagetyp und der Emulationstyp miteinander übereinstimmen. iDRAC emuliert das Gerät anhand des angegebenen Abbild-Typs. Wenn das hochgeladene Image und der Emulationstyp nicht übereinstimmen, können eventuell Probleme auftreten. 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.

So erstellen Sie eine vFlash-Partition unter Verwendung einer Imagedatei:

1. Wechseln Sie in der iDRAC6-Webschnittstelle zu **System**→ Registerkarte **vFlash**→ **Unterregister Aus Abbild anlegen.** Die Seite **Partition aus Abbild-Datei anlegen** wird angezeigt.
2. Geben Sie die unter Tabelle 11-3 aufgeführten Informationen ein.
3. Klicken Sie auf **Anwenden**. Unter Verwendung der Abbild-Datei wird eine neue Partition angelegt.

ANMERKUNG: Wenn das Anlegen einer Partition läuft, wird der Fortschritt oder Status nicht angezeigt.

Es wird eine Fehlermeldung angezeigt, wenn Folgendes zutrifft:

- 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.

Tabelle 11-3. Optionen der Seite 'Partition über Imagedatei erstellen'

Feld	Beschreibung
Stichwortverzeichnis	Wählen Sie einen Partitionsindex aus. In der Drop-Down-Liste werden nur ungebrauchte Indizes angezeigt. Standardmäßig wird der niedrigste verfügbare Index ausgewählt. Sie können ihn zu einem beliebigen anderen Indexwert aus der Drop-Down-Liste ändern. **ANMERKUNG:** Für die standardmäßige SD-Karte ist nur Index 1 verfügbar.
Bezeichnung	Geben Sie eine eindeutige Kennzeichnung für die neue Partition ein. Diese kann aus bis zu sechs alphanumerischen Zeichen bestehen. Der Kennzeichnungsname darf keine Leerstellen enthalten. Die Zeichen werden in Großbuchstaben angezeigt. **ANMERKUNG:** Für die Standard-SD-Karte muss die Bezeichnung VFLASH lauten. Wenn nicht, wird eine Fehlermeldung angezeigt.
Emulationstyp	Wählen Sie aus der Drop-Down-Liste den Emulationstyp für die Partition aus. Die verfügbaren Optionen sind **Diskette**, **Festplatte** und **CDROM**.
Imagespeicherort	Klicken Sie auf **Durchsuchen**, um den Speicherort der Imagedatei festzulegen. Es werden nur die Dateitypen **.img** oder **.iso** 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. Die standardmäßige SD-Karte mit eingeschränkten vFlash-Funktionen unterstützt nur das FAT32-Format.

Sie können nur Festplatten- oder Diskettenpartitionen formatieren. Die Formatierung von CD-Partitionen wird nicht unterstützt. Schreibgeschützte Partitionen können nicht formatiert werden.

ANMERKUNG: Um Partitionen formatieren zu können, müssen Sie über die Berechtigung 'Zugriff auf virtuellen Datenträger' verfügen.

Stellen Sie vor dem Formatieren der Partition Folgendes sicher:

- Die Karte ist aktiviert.
- Die Partition ist nicht verbunden.
- Die Karte ist nicht schreibgeschützt.
- Es wird nicht bereits ein Initialisierungsvorgang auf der Karte ausgeführt.

So formatieren Sie eine vFlash-Partition:

1. Wählen Sie auf der iDRAC6-Webschnittstelle **System→ vFlash→** Unterregister **Formatieren** aus. Die Seite **Formatieren** wird angezeigt.
2. Geben Sie die unter Tabelle 11-4 aufgeführten Informationen ein.
3. Klicken Sie auf **Anwenden**. Es wird eine Warnungsmeldung angezeigt, die darauf hinweist, dass alle Daten auf der Partition gelöscht werden. Klicken Sie auf **OK**. Die gewählte Partition wird mit dem angegebenen Dateisystemtyp formatiert.

   Es wird eine Fehlermeldung angezeigt, wenn Folgendes zutrifft:

   - Die Karte ist schreibgeschützt.
   - Auf der Karte wird bereits ein Initialisierungsvorgang ausgeführt.

Tabelle 11-4. Optionen der Seite 'Partition formatieren'

Feld	Beschreibung
Bezeichnung	Wählen Sie die Partitionskennzeichnung aus, die formatiert werden soll. Standardmäßig wird die erste verfügbare Partition ausgewählt. Alle vorhandenen Partitionen des Typs Diskette oder Festplatte stehen in der Drop-Down-Liste zur Verfügung. Verbundene Partitionen oder schreibgeschützte Partitionen stehen in der Drop-Down-Liste nicht zur Verfügung.
Für die Formatierung zu verwendender Typ	Wählen Sie den Dateisystemtyp aus, auf den die Partition formatiert werden soll. Die verfügbaren Optionen sind EXT2, EXT3, FAT16 und FAT32. Für die Standard-SD-Karte ist nur FAT32 verfügbar.

Verfügbare Partitionen anzeigen

Stellen Sie sicher, dass die vFlash- oder standardmäßige SD-Karte zum Anzeigen der Liste mit verfügbaren Partitionen aktiviert ist.

So zeigen Sie die auf der Karte verfügbaren Partitionen an:

1. Wählen Sie auf der iDRAC6-Webschnittstelle **System→ vFlash→** Unterregister **Verwalten** aus. Die Seite **Partitionen verwalten** listet die verfügbaren Partitionen auf.
2. Für jede Partition können Sie die unter Tabelle 11-5 erwähnten Informationen anzeigen.

Tabelle 11-5. Verfügbare Partitionen anzeigen

Feld	Beschreibung
Stichwortverzeichnis	Partitionen sind von 1 bis 16 indiziert. Der Partitionsindex ist für die jeweilige Partition eindeutig. Sie wird festgelegt, wenn die Partition erstellt wird.
Bezeichnung	Identifiziert die Partition. Sie wird festgelegt, wenn die Partition erstellt wird.
Größe	Größe der Partition in Megabytes (MB).
Schreibgeschützt.	Lese-Schreib-Zugriffszustand der Partition. • Markiert = Nur-Lesen-Partition. • Nicht markiert=Lese-Schreib-Partition **ANMERKUNG:** Bei der standardmäßigen SD-Karte ist die Partition Lesen-Schreiben und diese Spalte wird nicht angezeigt.
Verbunden	Gibt an, ob die Partition für das Betriebssystem als USB-Gerät sichtbar ist. Informationen zum Verbinden oder Abtrennen von Partitionen finden Sie im Abschnitt „Partition verbinden und abtrennen“ auf Seite 272.
Geben Sie Folgendes ein:	Zeigt an, ob der Partitionstyp Diskette, Festplatte oder CD ist.

Partition modifizieren

Stellen Sie sicher, dass die Karte zum Modifizieren der Partition aktiviert ist.

ANMERKUNG: Sie müssen die Berechtigung Zugriff auf virtuelle Datenträger haben, um eine vFlash-Partition ändern zu können.

Sie können eine schreibgeschützte Partition auf Lesen-Schreiben umstellen oder umgekehrt. Führen Sie dazu folgende Schritte durch:

1. Wählen Sie bei der iDRAC6-Webschnittstelle **System→ vFlash→** Unterregister **Verwalten** aus. Die Seite **Partitionen verwalten** wird angezeigt.
2. Aktivieren Sie in der Spalte **Schreibgeschützt** das Kontrollkästchen für die Partition(-en), für die Sie den Schreibschutz setzen wollen, oder deaktivieren Sie das Kontrollkästchen für die Partition(-en), die Sie auf Schreiben/Lesen setzen wollen.

ANMERKUNG: Handelt es sich um eine Partition des Typs CD, ist der Status schreibgeschützt; das Kontrollkästchen ist aktiviert. Sie können den Zustand nicht zu Lesen-Schreiben ändern.
Wenn die Partition verbunden ist, ist das Kontrollkästchen grau unterlegt.
Bei der Standard-SD-Karte ist die Partition nicht schreibgeschützt; die Spalte **Schreibgeschützt** wird nicht angezeigt.

3. Klicken Sie auf **Anwenden**. Auf Grundlage der entsprechenden Auswahl werden die Partitionen zu Nur-Lesen oder Lesen-Schreiben geändert.

Partition verbinden und abtrennen

Sie können eine oder mehrere Partitionen als virtuelle USB-Massenspeichergeräte verbinden, so dass diese für das Betriebssystem und das BIOS als Massenspeichergeräte erkennbar sind. Wenn mehrere Partitionen gleichzeitig verbunden werden, werden sie dem Host-Betriebssystem basierend auf dem Index in aufsteigender Reihenfolge präsentiert.
Das Betriebssystem weist die entsprechenden Laufwerksbuchstaben zu.

Wenn Sie eine Partition abtrennen, wird diese im Host-Betriebssystem nicht mehr als virtuelles USB-Massenspeichergerät betrachtet und aus dem Menü der BIOS-Startreihenfolge entfernt.

Wenn Sie eine Partition verbinden oder abtrennen, wird der USB-Bus des Systems zurückgesetzt. Dies kann alle Applikationen (wie das Betriebssystem) beeinflussen, die vFlash verwenden, und unterbricht sämtliche iDRAC-Virtuelle Datenträger-Sitzungen.

ANMERKUNG: Um eine Partition verbinden oder abtrennen zu können, müssen Sie über die Berechtigung 'Zugriff auf virtuellen Datenträger' verfügen.

Stellen Sie vor dem Verbinden oder Abtrennen einer Partition Folgendes sicher:

- Die Karte ist aktiviert.
- Es wird nicht bereits ein Initialisierungsvorgang auf der Karte ausgeführt.

So werden Partitionen verbunden oder abgetrennt:

1. Wählen Sie bei der iDRAC6-Webschnittstelle **System→ vFlash→** Unterregister **Verwalten** aus. Die Seite **Partitionen verwalten** wird angezeigt.
2. Markieren Sie in der Spalte **Verbunden** das Kontrollkästchen für die Partition(en), die Sie verbinden möchten, oder heben Sie die Markierung des Kontrollkästchens für die Partition(en) auf, die Sie abtrennen möchten.

ANMERKUNG: Die abgetrennten Partitionen werden in der Startsequenz nicht angezeigt.

3. Klicken Sie auf **Anwenden**. Auf Grundlage der entsprechenden Auswahl werden die Partitionen verbunden oder abgetrennt.

Verhalten des Betriebssystems für verbundene Partitionen

Wenn Partitionen verbunden sind und das Host-Betriebssystem Windows ist, werden die Laufwerkbuchstaben, die den verbundenen Partitionen zugewiesen sind, durch das Betriebssystem gesteuert.

Wenn eine Partition schreibgeschützt ist, wird sie vom Host-Betriebssystem als schreibgeschützt dargestellt.

Wenn das Host-Betriebssystem das Dateisystem einer verbundenen Partition nicht unterstützt, kann der Inhalt der Partition nicht über das Host-Betriebssystem gelesen oder modifiziert werden. Beispiel: Der Partitionstyp EXT2 kann nicht über das Windows-Betriebssystem gelesen werden.

Wenn Sie den Kennzeichnungsnamen einer verbundenen Partition über das Host-Betriebssystem ändern, hat dies keine Auswirkung auf den Kennzeichnungsnamen, der von iDRAC für diese Partition gespeichert wurde.

Vorhandene Partitionen löschen

ANMERKUNG: Sie können vorhandene Partitionen für die vFlash- oder standardmäßige SD-Karte löschen.

Stellen Sie vor dem Löschen bestehender Partition(-en) folgendes sicher:

- Die Karte ist nicht schreibgeschützt.
- Die Partition ist nicht verbunden.
- Es wird nicht bereits ein Initialisierungsvorgang auf der Karte ausgeführt.

ANMERKUNG: Sie müssen die Berechtigung Zugriff auf virtuelle Datenträger haben, um eine Partition ändern zu können.

Löschen einer bestehenden Partition:

1. Wählen Sie bei der iDRAC6-Webschnittstelle **System→ vFlash→** Unterregister **Verwalten** aus. Die Seite **Partitionen verwalten** wird angezeigt.
2. Klicken Sie in der Spalte **Löschen** auf das Löschen-Symbol für die Partitionen, die Sie löschen möchten, und klicken Sie auf **Anwenden**. Die Partition(en) ist/sind gelöscht.

Partitionsinhalte herunterladen

Sie können den Inhalt einer vFlash-Partition als Imagedatei im Format **.img** oder **.iso** an einen lokalen oder Remote-Speicherort herunterladen. Der lokale Speicherort befindet sich auf Ihrem Verwaltungssystem dort, von wo aus die iDRAC6-Webschnittstelle betrieben wird. Ein entfernter Speicherort befindet sich auf einem verwalteten System.

ANMERKUNG: Um Partitionen herunterladen zu können, müssen Sie über die Berechtigung 'Zugriff auf virtuellen Datenträger' verfügen.

Stellen Sie vor dem Herunterladen der Inhalte an einen lokalen oder Remote-Speicherort Folgendes sicher:

- Die Karte ist aktiviert.
- Es wird nicht bereits ein Initialisierungsvorgang auf der Karte ausgeführt.
- Wenn eine Lesen-Schreiben-Partition vorliegt, darf diese nicht verbunden sein.

So laden Sie den Inhalt der vFlash-Partition an einen Speicherort auf Ihrem System herunter:

1. Wählen Sie auf der iDRAC6-Webschnittstelle **System→ vFlash→** Unterregister **Herunterladen** aus. Die Seite **Partition herunterladen** wird angezeigt.
2. Wählen Sie aus dem Drop-Down-Menü **Kennzeichnung** eine Partition aus, die Sie herunterladen möchten. Alle vorhandenen Partitionen – außer verbundene Partitionen – werden in der Liste angezeigt. Standardmäßig wird die erste Partition ausgewählt.
3. Klicken Sie auf **Herunterladen**.
4. Legen Sie den Speicherort fest, an dem die Datei gespeichert werden soll.

   Wenn nur der Speicherort des Ordners angegeben wird, wird die Partitionskennzeichnung als Dateiname verwendet, wobei die Erweiterung **.iso** für Partitionen des Typs CD und **.img** für Partitionen des Typs Diskette und Festplatte angehängt wird.
5. Klicken Sie auf **Save** (Speichern). Der Inhalt der ausgewählten Partition wird an den festgelegten Speicherort heruntergeladen.

Zu einer Partition starten

Sie können eine verbundene vFlash-Partition als Startgerät für den nächsten Startvorgang einrichten. Die vFlash-Partition muss ein startfähiges Image (im **IMG**- oder **ISO**-Format) enthalten, das als Startgerät eingerichtet wird. Stellen Sie sicher, dass die Karte zum Einrichten einer Partition als Startgerät und zum Ausführen des Startvorgangs aktiviert ist.

ANMERKUNG: Um eine Partition als Startgerät einrichten zu können, müssen Sie über die Berechtigung 'Zugriff auf virtuellen Datenträger' verfügen.

Sie können den Startvorgang für die vFlash- oder standardmäßige SD-Karte ausführen. Die entsprechenden Schritte sind im Abschnitt „Erstes Startlaufwerk“ auf Seite 49 aufgeführt.

ANMERKUNG: Wenn das System-BIOS vFlash nicht als erstes Startgerät unterstützt, sind die verbundenen vFlash-Partitionen eventuell nicht im Drop-Down-Menü **Erstes Startgerät** aufgeführt. Stellen Sie daher sicher, dass Sie das BIOS auf die neuste Version aktualisieren, die das Einrichten der vFlash-Partition als erstes Startgerät unterstützt. Wenn das BIOS die neuste Version aufweist, wird ein Neustarten des Servers dazu führen, dass das BIOS den iDRAC darüber informiert, dass es vFlash als erstes Startgerät unterstützt. iDRAC führt dann die vFlash-Partition im Drop-Down-Menü **Erstes Startgerät** auf.

vFlash-Partitionen unter Verwendung von RACADM verwalten

Sie können den Unterbefehl `vFlashPartition` dazu verwenden, den Status von Partitionen auf einer bereits initialisierten vFlash- oder standardmäßigen SD-Karte zu erstellen, zu löschen, aufzuführen oder anzuzeigen. Das Format lautet:

```
racadm vflashpartition <erstellen | löschen | Status |
Liste> <Optionen>
```

ANMERKUNG: Um vFlash-Partitionsverwaltung ausführen zu können, müssen Sie über die Berechtigung 'Zugriff auf virtuellen Datenträger' verfügen.

Gültige Optionen:

-i <Index>	Index der Partition, auf die sich dieser Befehl bezieht. <Index> muss eine ganze Zahl von 1 bis 16 sein. **ANMERKUNG:** Bei der standardmäßigen SD-Karte ist der Indexwert auf 1 beschränkt, da nur eine einzige Partition von 256 MB Größe unterstützt wird.

Nur für den Vorgang Anlegen gültige Optionen:

-o <Kennzeichnung>	Kennzeichnung, die angezeigt wird, wenn die Partition auf dem Betriebssystem bereitgestellt wird. <Kennzeichnung> muss eine Zeichenkette von bis zu sechs alphanumerischen Zeichen sein und darf keine Leerstellen enthalten.
-e <Typ>	Emulationstyp für die Partition. <Typ> muss Diskette, CDROM oder Festplatte sein.

-t <Typ> Erstellen Sie eine Partition des Typs <Typ>. <Typ> muss Folgendes sein:

- leer – Erstellen Sie eine leere Partition.
  - -s <Größe> – Partitionsgröße in MB.
  - -f <Typ> – Formattyp der Partition, basierend auf dem Dateisystemtyp. Gültige Optionen sind RAW, FAT16, FAT32, EXT2 oder EXT3.
- image - Anlegen einer Partition mittels einer Abbild-Datei. Die folgenden Optionen sind gültig mit dem Imagetyp:
  - -l <Pfad> – Gibt den Remote-Pfad im Verhältnis zum iDRAC an. Der Pfad kann sich auf einem bereitgestellten oder freigegebenen Laufwerk befinden:
    SMB-Pfad: //<IP oder Domäne>/<Freigabename>/<Pfad_zum_Image>
    NFS-Pfad: <IP-Adresse>:/<Pfad_zum_Image>
  - -u <Benutzer> – Benutzername für den Zugriff auf das Remote-Image.

-p <Kennwort> – Kennwort für den Zugriff auf das Remote-Image.

Nur für die Aktion Status gültige Optionen:

-i Zeigt den Status des Partitionsindex an.

Partition erstellen

- So erstellen Sie eine leere 20-MB-Partition:

  ```
  racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20
  ```

- So erstellen Sie eine Partition unter Verwendung einer Imagedatei auf einem Remote-System:

  ```
  racadm vflashpartition create –i 1 –o drive1 –e HDD –t image –l //myserver/sharedfolder/foo.iso –u root –p mypassword
  ```

ANMERKUNG: Das Erstellen einer Partition unter Verwendung einer Imagedatei wird im lokalen RACADM nicht unterstützt.

Partition löschen

- So löschen Sie eine Partition:

  ```
  racadm vflashpartition delete -i 1
  ```

- Zum Löschen sämtlicher Partitionen ist die vFlash-SD-Karte erneut zu initialisieren. Weitere Informationen finden Sie unter „Initialisieren der vFlash- oder Standard-SD-Karte“ auf Seite 264.

Status einer Partition abrufen

- Zum Abfragen des Status eines Vorgangs auf Partition 1:

  ```
  racadm vflashpartition status -i 1
  ```

- So rufen Sie den Status sämtlicher vorhandener Partitionen ab:

  ```
  racadm vflashpartition status -a
  ```

Partitionsinformationen anzeigen

Zum Auflisten aller bestehenden Partitionen und deren Eigenschaften:

```
racadm vflashpartition list
```

Zu einer Partition starten

- So listen Sie die verfügbaren Geräte in der Startliste auf:

  ```
  racadm  getconfig –g cfgServerInfo –o
  cfgServerFirstBootDevice
  ```

  Bei einer vFlash-SD-Karte werden die Bezeichnungen der verbundenen Partitionen in der Startliste angezeigt. Wenn es sich um eine standardmäßige SD-Karte handelt und die Partition verbunden ist, wird VFLASH in der Startliste angezeigt.

- So richten Sie eine vFlash-Partition als Startgerät ein:

  ```
  racadm  config –g cfgServerInfo –o
  cfgServerFirstBootDevice "<vFlash-
  Partitionsname>"
  ```

wobei <vFlash-Partitionsname> die Bezeichnung für die vFlash-SD-Karte bzw. VFLASH für Standard-SD-Karte ist.

ANMERKUNG: Wenn Sie diesen Befehl ausführen, wird die vFlash-Partitionsbezeichnung automatisch auf „Einmal starten" gesetzt, d. h. **cfgserverBootOnce** wird auf 1 gesetzt. Durch den einmaligen Start wird das Gerät nur einmal zur Partition gestartet und es wird in der Startreihenfolge nicht beständig an erster Stelle behalten.

Partition verbinden oder abtrennen

- So verbinden Sie eine Partition:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAttachState 1
  ```

- So trennen Sie eine Partition ab:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAttachState 0
  ```

Partition modifizieren

- So ändern Sie eine schreibgeschützte Partition zu Lesen-Schreiben:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAccessType 1
  ```

- So ändern Sie eine Lesen-Schreiben-Partition zu Nur-Lesen:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAccessType 0
  ```

Weitere Informationen zu den RACADM-Unterbefehlen und zu Gruppen und Objektdefinitionen der iDRAC6-Eigenschaften-Datenbank finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Häufig gestellte Fragen

Wann ist die vFlash- oder standardmäßige SD-Karte gesperrt?

Der Virtual Flash-Datenträger wird von iDRAC gesperrt, wenn für den ausgeführten Vorgang exklusiver Zugriff auf den Datenträger benötigt wird – beispielsweise während eines Initialisierungsvorgangs.

Beim lokalen RACADM wird bei dem Versuch, eine zuvor erstellte Partition zu löschen, möglicherweise eine Fehlermeldung angezeigt. Warum?

Möglicherweise ist der Partitionserstellungsvorgang noch nicht abgeschlossen. 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.

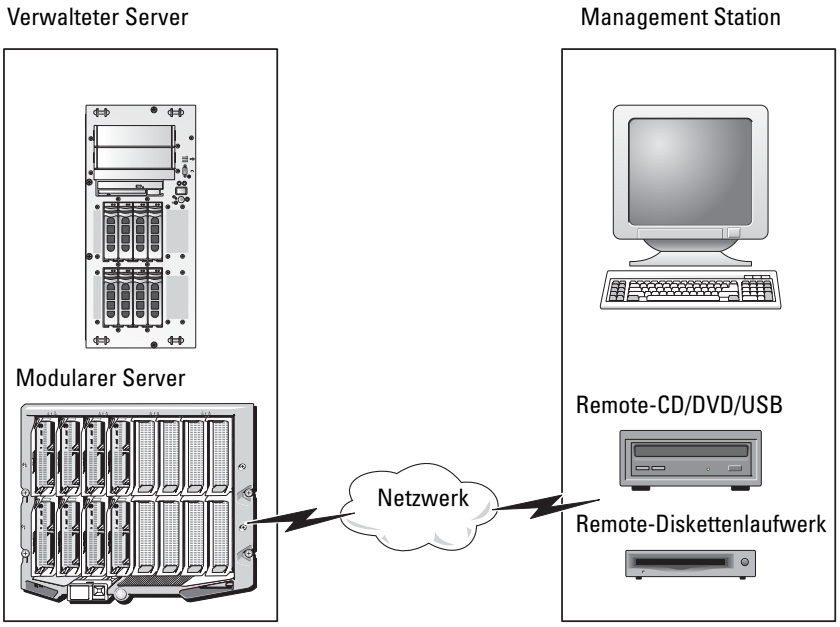
12

Virtuellen Datenträger konfigurieren und verwenden

Übersicht

Die Funktion Virtueller Datenträger, auf die Sie über den Viewer der virtuellen Konsole zugreifen können, gewährt dem verwalteten Server Zugriff auf Datenträger, die mit einem Remote-System im Netzwerk verbunden sind. Abbildung 12-1 zeigt die gesamte Architektur des virtuellen Datenträgers.

Abbildung 12-1. Gesamte Architektur des virtuellen Datenträgers



Mit dem virtuellen Datenträger können Administratoren im Remote-Zugriff verwaltete Server starten, Anwendungen installieren, Treiber aktualisieren oder sogar neue Betriebssysteme von virtuellen CD/DVD- und Diskettenlaufwerken installieren.

ANMERKUNG: Virtuelle Datenträger erfordern eine verfügbare Netzwerkbandbreite von mindestens 128 Kbit/s.

Der virtuelle Datenträger definiert zwei Geräte für das Betriebssystem und das BIOS des verwalteten Servers: ein Diskettenlaufwerk und ein optisches Laufwerk.

Die Management Station stellt den physischen Datenträger oder die Imagedatei über das Netzwerk bereit. Wenn eine Verbindung zum virtuellen Datenträger hergestellt wird, werden alle Zugriffsanforderungen auf virtuelle CD-/Disketten-Laufwerke vom verwalteten Server über das Netzwerk zur Management Station geleitet. Das Verbinden eines virtuellen Datenträgers entspricht dem Einlegen eines Datenträgers in ein physisches Gerät auf dem verwalteten System. Wenn der virtuelle Datenträger den Status „Verbunden/Angeschlossen“ hat, werden virtuelle Geräte auf dem verwalteten System als zwei Laufwerke ohne installierte Datenträger angezeigt.

Tabelle 12-1 listet die unterstützten Laufwerkverbindungen für virtuelle Diskettenlaufwerke und virtuelle optische Laufwerke auf.

ANMERKUNG: Werden virtuelle Datenträger geändert, während sie verbunden sind, kann dies zum Anhalten der System-Startsequenz führen.

Tabelle 12-1. Unterstützte Laufwerkverbindungen

Unterstützte Verbindungen virtueller Diskettenlaufwerke	Unterstützte Verbindungen virtueller optischer Laufwerke
1,44 Zoll Legacy-Diskettenlaufwerk mit 1,44 Zoll-Diskette	CD-ROM, DVD, CDRW, Kombinationslaufwerk mit CD-ROM-Datenträger
USB-Diskettenlaufwerk mit 1,44 Zoll-Diskette	CD-ROM/DVD-Imagedatei im Format ISO9660
1,44 Zoll-Disketten-Image	USB-CD-ROM-Laufwerk mit CD-ROM-Datenträger
USB-Wechselplatte (Mindestgröße 128 MB)	

Windows-basierte Management Station

Um die Funktion des virtuellen Datenträgers auf einer Management Station mit Microsoft Windows-Betriebssystem auszuführen, installieren Sie eine unterstützte Internet Explorer-Version mit dem ActiveX-Steuerelement-Plug-In. Stellen Sie die Browser-Sicherheit auf **Mittelhoch** oder auf eine niedrigere Einstellung ein, damit Internet Explorer signierte ActiveX-Steuerelemente herunterladen und installieren kann.

Abhängig von der Internet Explorer-Version kann eventuell eine benutzerdefinierte Sicherheitseinstellung für ActiveX erforderlich sein:

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf **Extras→ Internetoptionen** und dann auf die Registerkarte **Sicherheit**.
3. Klicken Sie unter **Wählen Sie eine Zone aus, um deren Sicherheitseinstellungen festzulegen**, auf die gewünschte Zone.
4. Klicken Sie dann unter **Sicherheitsstufe dieser Zone** auf **Benutzerdefinierte Stufe**.

   Das Fenster **Sicherheitseinstellungen** wird angezeigt.
5. Stellen Sie unter **ActiveX-Steuerelemente und Plug-Ins** sicher, dass die folgenden Einstellungen auf **Aktivieren** eingestellt sind.
   - Skriptlets zulassen
   - Automatische Eingabeaufforderung für ActiveX-Steuerelemente
   - Signierte ActiveX-Steuerelemente herunterladen
   - Unsignierte ActiveX-Steuerelemente herunterladen
6. Klicken Sie auf **OK**, um die Änderungen zu speichern, und schließen Sie das Fenster **Sicherheitseinstellungen**.
7. Klicken Sie auf **OK**, um das Fenster **Internetoptionen** zu schließen.
8. Starten Sie Internet Explorer neu.

Zum Installieren von ActiveX müssen Sie über Administratorberechtigungen verfügen. Vor der Installation des ActiveX-Steuerelements kann Internet Explorer eventuell eine Sicherheitswarnung anzeigen. Um das Installationsverfahren für das ActiveX-Steuerelement abzuschließen, akzeptieren Sie das ActiveX-Steuerelement, wenn Internet Explorer Sie mit einer Sicherheitswarnung dazu auffordert.

Linux-basierte Management Station

Um die Funktion des virtuellen Datenträgers auf einer Management Station mit Linux-Betriebssystem auszuführen, installieren Sie eine unterstützte Version von Firefox.

Zum Ausführen des Virtuelle Konsole-Plug-In ist eine Java-Laufzeitumgebung (JRE) erforderlich. Sie können eine JRE von **java.sun.com** herunterladen.

Virtuellen Datenträger konfigurieren

1. Melden Sie sich an der iDRAC6-Webschnittstelle an.
2. Klicken Sie auf **System→ Virtuelle Konsole/Virtueller Datenträger→ Konfiguration**.
3. Wählen Sie im Abschnitt Virtueller Datenträger Werte für die Einstellungen aus. Informationen über die Konfigurationswerte des virtuellen Datenträgers finden Sie unter Tabelle 12-2.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

   Ein eingeblendeter Warnungsdialog zeigt die folgende Meldung an: `Sie sind dabei, die Gerätekonfiguration zu ändern. Alle vorhandenen Umleitungssitzungen werden geschlossen. Do you want to continue? (Durch diesen Vorgang werden alle aufgeführten Zähler zurückgesetzt. Möchten Sie fortfahren?)`
5. Klicken Sie auf **OK**, um fortzufahren.

   Ein eingeblendeter Warnungsdialog zeigt die folgende Meldung an: `Die Konfiguration des virtuellen Datenträgers wurde erfolgreich durchgeführt.`

Tabelle 12-2. Konfigurationswerte des virtuellen Datenträgers

Attribut	Wert
Virtuellen Datenträger anschließen	**Anschließen** - Schließt den virtuellen Datenträger umgehend an den Server an. **Trennen** - Trennt den virtuellen Datenträger umgehend vom Server. **Automatisch anschließen** - Schließt den virtuellen Datenträger nur dann am Server an, wenn eine Sitzung des virtuellen Datenträgers gestartet wird.
Maximale Sitzungen	Zeigt die maximale Anzahl zulässiger Virtueller Datenträger-Sitzungen an. Diese beträgt immer 1. **ANMERKUNG:** Es ist nur eine Benutzersitzung für den virtuellen Datenträger zulässig. Es können jedoch mehrere Geräte in einer Sitzung miteinander verbunden sein. Siehe „Virtuellen Datenträger ausführen“ auf Seite 286.
Aktive Sitzungen	Zeigt die Anzahl Virtueller Datenträger-Sitzungen an, die derzeit aktiv sind.
Virtuelle Datenträgerverschlüsselung aktiviert	Aktiviert (markiert) oder deaktiviert (nicht markiert) die Verschlüsselung auf Verbindungen des virtuellen Datenträgers.
Diskettenemulation	Zeigt an, ob der virtuelle Datenträger dem Server als Diskettenlaufwerk oder als USB-Schlüssel angezeigt wird. Wenn **Diskettenemulation** ausgewählt ist, wird das virtuelle Datenträger-Gerät auf dem Server als Diskettengerät angezeigt. Wenn es nicht ausgewählt ist, wird es als USB-Schlüssellaufwerk angezeigt. **ANMERKUNG:** In bestimmten Windows Vista- und Red Hat Enterprise Linux-Umgebungen kann es unter Umständen nicht möglich sein, einen USB mit aktivierter **Diskettenemulation** zu virtualisieren.

Tabelle 12-2. Konfigurationswerte des virtuellen Datenträgers *(fortgesetzt)*

Attribut	Wert
„Einmal Starten“ aktivieren	Aktiviert (markiert) oder deaktiviert (nicht markiert) die Option Einmaliger Start, die nach dem einmaligen Start des Servers die Sitzung des virtuellen Datenträgers automatisch beendet. Verwenden Sie dieses Attribut, um vom virtuellen Datenträger aus zu starten. Beim nächsten Start startet das System vom nächsten Gerät in der Startreihenfolge aus. Diese Option ist nützlich für automatische Bereitstellungen.

Virtuellen Datenträger ausführen

VORSICHTSHINWEIS: Geben Sie keinen racreset-Befehl aus, wenn die Sitzung eines virtuellen Datenträgers ausgeführt wird. Andernfalls könnten unerwünschte Ergebnisse einschließlich Datenverlust auftreten.

ANMERKUNG: Das Virtuelle Konsole-Viewer-Fenster (Anwendung) muss während des Zugriffs auf den virtuellen Datenträger aktiviert bleiben.

1. Öffnen Sie einen unterstützten Internet-Browser auf der Management Station.
2. Melden Sie sich an der iDRAC6-Webschnittstelle an.
3. Klicken Sie auf das Register **Virtuelle Konsole/Virtueller Datenträger**.

   Der Bildschirm **Virtuelle Konsole und Virtueller Datenträger** wird angezeigt.

   Wenn Sie die Werte der angezeigten Attribute ändern möchten, finden Sie entsprechende Informationen unter „Virtuellen Datenträger konfigurieren“ auf Seite 284.

   ANMERKUNG: Die **Disketten-Imagedatei** unter **Diskettenlaufwerk** (falls zutreffend) kann u. U. angezeigt werden, da dieses Gerät als virtuelle Diskette virtualisiert werden kann. Sie können ein optisches Laufwerk und gleichzeitig eine Diskette oder ein einzelnes Laufwerk auswählen.

   ANMERKUNG: Die Laufwerksbuchstaben des virtuellen Geräts auf dem verwalteten Server entsprechen nicht den Buchstaben des physischen 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 beheben, ziehen Sie die Dokumentation zu Ihrem Microsoft-Betriebssystem zurate oder setzen sich mit Ihrem Administrator in Verbindung.

4 Klicken Sie auf **Virtuelle Konsole starten**.

ANMERKUNG: Bei Linux wird die Datei **jviewer.jnlp** auf den Desktop heruntergeladen. In einem Dialogfeld wird gefragt, welche Maßnahme auf die Datei angewendet werden soll. Wählen Sie die Option **Mit Programm öffnen** aus und dann die Anwendung **javaws**, die sich im Unterverzeichnis **bin** des JRE-Installationsverzeichnisses befindet.

Die Anwendung **iDRACView** wird in einem separaten Fenster gestartet.

5 Wählen Sie **Datenträger→ Virtueller Datenträger-Assistent** aus.

Das Fenster **Datenträgerumleitung** wird angezeigt.

6 Prüfen Sie den Abschnitt **Status** unten im Fenster **Datenträgerumleitung**. Wenn eine Datenträgerverbindung besteht, können Sie diese vor dem Verbinden mit einer anderen Datenträgerquelle unterbrechen. Klicken Sie zum Trennen des Datenträgers auf die Schaltfläche **Trennen** neben dem Datenträger im Fenster **Status**.

7 Wählen Sie die Optionsschaltfläche neben den Datenträgertypen aus, zu denen eine Verbindung hergestellt werden soll.

8 Sie können sowohl die Optionsschaltfläche **Disketten-Abbild** als auch eine der Optionsschaltflächen im Abschnitt **CD/DVD-Laufwerk** auswählen.

ANMERKUNG: Wenn der CD/DVD-Datenträger einer Management Station bereits vom iDRAC6-Blade in Anspruch genommen wird, kann derselbe Datenträger umgeleitet und einem anderen iDRAC6-Blade zur Verfügung gestellt werden. Anders ausgedrückt unterstützt iDRAC6 dieselbe Datenträgerumleitung (schreibgeschützt) auf zwei verschiedene iDRAC6-Blades. Mit einem USB-Datenträger sind Sie nicht in der Lage, eine Verbindung zu zwei iDRAC6-Blades herzustellen. iDRAC6 blendet eine entsprechende Warnungsmeldung ein.

Geben Sie zum Anschließen eines Disketten- oder ISO-Abbilds den Pfad zum Speicherort des Abbilds auf Ihrem lokalen Computer ein oder klicken Sie auf die Schaltfläche **Durchsuchen**, um zum Speicherort des Abbilds zu wechseln.

ANMERKUNG: Möglicherweise ist es nicht möglich, Remote-ISO-Abbilder bereitzustellen, wenn Sie das Java-basierte Plug-In des virtuellen Datenträgers verwenden. Linux-Clients lassen beispielsweise nicht zu, dass die Abbilder bereitgestellt werden, da sie das Java-basierte Plug-In verwenden. Um das zu vermeiden, kopieren Sie das ISO-Abbild auf das lokale System, um die Abbilddatei lokal verfügbar zu machen. Das Java-basierte Plug-In des virtuellen Datenträgers gestattet nicht, den Freigabenamen unter Verwendung des Formats **\\computer\share** anzugeben.

9 Klicken Sie neben jedem ausgewählten Datenträgertyp auf die Schaltfläche **Verbinden.**

Die Verbindung zum Datenträger wird hergestellt und das Fenster **Status** aktualisiert.

10 Klicken Sie auf **Schließen**.

ANMERKUNG: Immer wenn eine Sitzung des virtuellen Datenträgers eingeleitet oder ein vFlash angeschlossen wird, wird ein zusätzliches Laufwerk namens „LCDRIVE“ auf dem Host-Betriebssystem und im BIOS angezeigt. Das zusätzliche Laufwerk wird nicht mehr angezeigt, wenn die Verbindung zu vFlash oder zur Sitzung des virtuellen Datenträgers abgebrochen wird.

Verbindung des virtuellen Datenträgers trennen

1 Wählen Sie **Datenträger→ Virtueller Datenträger-Assistent** aus.

Der **Assistent zur Datenträgerumleitung** wird angezeigt.

2 Klicken Sie neben dem Datenträger, dessen Verbindung unterbrochen werden soll, auf **Trennen**.

Die Verbindung zum Datenträger wird getrennt und das Fenster **Status** aktualisiert.

3 Klicken Sie auf **Close** (Schließen).

ANMERKUNG: Wenn Sie **iDRACview** starten und sich dann von der Web-GUI abmelden, wird **iDRACView** nicht beendet und bleibt aktiv.

Starten vom virtuellen Datenträger

Das System-BIOS ermöglicht es, von virtuellen optischen Laufwerken oder virtuellen Diskettenlaufwerken aus zu starten. Öffnen Sie während des POST das BIOS-Setup-Fenster und überprüfen Sie, ob die virtuellen Laufwerke aktiviert und in der richtigen Reihenfolge aufgeführt sind.

Um die BIOS-Einstellung zu ändern, führen Sie die folgenden Schritte aus:

1. Starten Sie den verwalteten Server.
2. Drücken Sie <F2>, um das BIOS-Setup-Fenster aufzurufen.
3. Scrollen Sie zur Startsequenz und drücken Sie die Eingabetaste.

   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. Speichern Sie die Änderungen und beenden Sie.

   Der verwaltete Server startet neu.

   Basierend auf der Startreihenfolge versucht der verwaltete Server, von einem startfähigen Gerät aus 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.

Installation von Betriebssystemen mittels virtuellem Datenträger

In diesem Abschnitt wird eine manuelle, interaktive Methode zum Installieren des Betriebssystems auf der Management Station beschrieben. Das Verfahren kann mehrere Stunden in Anspruch nehmen. Ein geskriptetes Betriebssystem-Installationsverfahren kann unter Verwendung des virtuellen Datenträgers weniger als 15 Minuten in Anspruch nehmen. Weitere Informationen finden Sie unter „Betriebssystem bereitstellen“ auf Seite 359.

1. Überprüfen Sie folgende Punkte:
   - Die Installations-DVD/CD des Betriebssystems ist in das DVD/CD-Laufwerk der Management Station eingelegt.
   - Das lokale DVD/CD-Laufwerk ist ausgewählt.
   - Sie sind mit den virtuellen Laufwerken verbunden.
2. Befolgen Sie die Schritte zum Starten des virtuellen Datenträgers in Abschnitt „Starten vom virtuellen Datenträger“ auf Seite 288 um sicherzustellen, dass das BIOS gemäß Einstellung vom DVD/CD-Laufwerk startet, von dem Sie die Installation vornehmen.
3. Folgen Sie den Bildschirmanleitungen, um die Installation abzuschließen.

Virtuelle Datenträger verwenden, wenn das Betriebssystem des Servers ausgeführt wird

Windows-basierte Systeme

Auf Windows-Systemen werden die Laufwerke der virtuellen Datenträger automatisch geladen, wenn sie angeschlossen und mit einem Laufwerkbuchstaben konfiguriert sind.

Die Verwendung der virtuellen Laufwerke innerhalb von Windows ist der Verwendung der physischen Laufwerke ähnlich. Wenn Sie über den Assistenten des virtuellen Datenträgers eine Verbindung zum Datenträger herstellen, ist der Datenträger am System verfügbar, wenn Sie auf das Laufwerk klicken und dessen Inhalt durchsuchen.

Linux-basierte Systeme

Abhängig von der Software-Konfiguration Ihres Systems können die virtuellen Datenträgerlaufwerke eventuell nicht automatisch geladen werden. Wenn Ihre Laufwerke nicht automatisch geladen werden, laden Sie sie unter Verwendung des Linux-Befehls **mount** manuell.

Häufig gestellte Fragen

Tabelle 12-3 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 12-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen

Frage	Antwort
Manchmal bemerke ich, dass die Client-Verbindung meines virtuellen Datenträgers unterbrochen wird. Warum?	Wenn eine Netzwerk-Zeitüberschreitung eintritt, trennt die iDRAC6-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Wenn die Konfigurationseinstellungen des virtuellen Datenträgers in der iDRAC6-Webschnittstelle oder durch Befehle des lokalen RACADM geändert werden, wird die Verbindung aller verbundener Datenträger bei Übernahme der Konfigurationsänderung unterbrochen. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie den virtuellen Datenträger-Assistenten.

Tabelle 12-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Auf welchem Betriebssystem wird der iDRAC6 unterstützt?	Eine Liste unterstützter Betriebssysteme finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 26.
Welche Webbrowser unterstützen den iDRAC6?	Eine Liste unterstützter Webbrowser finden Sie unter „Unterstützte Webbrowser“ auf Seite 27.
Warum bricht meine Client-Verbindung manchmal ab?	• Es kann sein, dass Ihre Client-Verbindung von Zeit zu Zeit unterbrochen wird, wenn das Netzwerk langsam ist, oder wenn Sie die CD im CD-Laufwerk des Client-Systems wechseln. Beispiel: Wenn Sie die CD im CD-Laufwerk des Client-Systems wechseln, weist die neue CD eventuell eine Autostart-Funktion auf. Wenn dies der Fall ist, kann für die Firmware eine Zeitüberschreitung eintreten und die Verbindung kann unterbrochen werden, wenn es zu lange dauert, bis das Client-System zum Lesen der CD bereit ist. Wenn eine Verbindung verloren geht, können Sie sie über die GUI wieder herstellen und mit dem vorherigen Vorgang fortfahren. • Wenn eine Netzwerk-Zeitüberschreitung eintritt, trennt die iDRAC6-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Es kann auch sein, dass jemand die Konfigurationseinstellungen des virtuellen Datenträgers über die Webschnittstelle oder durch Eingabe von RADACM-Befehlen verändert hat. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie die Funktion Virtueller Datenträger.
Eine Installation des Windows-Betriebssystems scheint zu lange zu dauern. Warum?	Wenn Sie das Windows-Betriebssystem über eine langsame Netzwerkverbindung installieren, kann es sein, dass das Installationsverfahren aufgrund von Netzwerklatenz für den Zugriff auf die iDRAC6-Webschnittstelle mehr Zeit erfordert. Obwohl das Installationsfenster den Installationsfortschritt nicht anzeigt, befindet sich das Installationsverfahren in Ausführung.

Tabelle 12-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Ich sehe den Inhalt eines Diskettenlaufwerks oder eines USB-Speicherschlüssels an. Wenn ich versuche, über das gleiche Laufwerk eine Verbindung zum virtuellen Datenträger herzustellen, erhalte ich eine Verbindungs-Fehlermeldung und werde gebeten, den Vorgang zu wiederholen. 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.
Wie konfiguriere ich mein virtuelles Gerät als startfähiges Gerät?	Greifen Sie auf dem verwalteten Server 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 Geräte-Startreihenfolge nach Bedarf. Um z. B. von einem CD-Laufwerk aus zu starten, konfigurieren Sie das CD-Laufwerk als erstes Laufwerk in der Startreihenfolge.
Von welchen Arten von Datenträgern kann ich starten?	Mit dem iDRAC6 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 Wechselplatte erkannt wird (Mindestgröße 128 MB) • Ein USB-Schlüssel-Image

Tabelle 12-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Wie kann ich meinen USB-Schlüssel startfähig machen?	Suchen Sie unter **support.dell.com** nach dem Dell-Startdienstprogramm, einem Windows-Programm, mit dem Sie den Dell-USB-Schlüssel startfähig machen können. Sie können auch über eine Windows 98-Startdiskette starten und Systemdateien von der Startdiskette auf den USB-Schlüssel kopieren. Geben Sie z. B. bei der DOS-Eingabeaufforderung den folgenden Befehl ein: `sys a: x: /s` wobei *x*: der USB-Schlüssel ist, der startfähig gemacht werden soll.
Welche Dateisystemtypen werden auf meinem virtuellen Diskettenlaufwerk unterstützt?	Ihr virtuelles Diskettenlaufwerk unterstützt FAT16- oder FAT32-Dateisysteme.
Als ich im Remote-Zugriff mithilfe der iDRAC6-Webschnittstelle eine Firmware-Aktualisierung ausgeführt habe, wurden meine virtuellen Laufwerke vom Server entfernt. Warum?	Firmware-Aktualisierungen führen dazu, dass der iDRAC6 zurückgesetzt, die Remote-Verbindung abgebrochen und die virtuellen Laufwerke entladen werden. Die Laufwerke werden wieder angezeigt, wenn der iDRAC6-Reset abgeschlossen ist.

Tabelle 12-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Ich kann meine virtuelle Diskettenkomponente auf einem System, das das Red Hat Enterprise Linux- oder SUSE Linux-Betriebssystem ausführt, nicht finden. Mein virtueller Datenträger ist angeschlossen und ich bin mit meinem Remote-Diskettenlaufwerk verbunden. Was soll ich tun?	Bei einigen Linux-Versionen werden virtuelle Diskettenlaufwerke und virtuelle CD-Laufwerke nicht in gleicher Weise automatisch geladen. Machen Sie zum Laden des virtuellen Diskettenlaufwerks den Geräteknoten ausfindig, den Linux dem virtuellen Diskettenlaufwerk zuweist. Führen Sie die folgenden Schritte durch, um das virtuelle Diskettenlaufwerk ordnungsgemäß ausfindig zu machen und zu laden: **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 Dell-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* ist der in Schritt 4 gefundene Gerätename. `/mnt/floppy` ist der Bereitstellungspunkt.

13

RACADM-Befehlszeilenschnittstelle verwenden

Die RACADM-CLI (Command Line Interface, Befehlszeilenschnittstelle) gewährt Zugriff auf die iDRAC6-Verwaltungsfunktionen auf dem verwalteten Server. RACADM gewährt Zugriff auf die meisten Funktionen der iDRAC6-Webschnittstelle. RACADM kann in Skripts verwendet werden, um die Konfiguration mehrerer Server zu erleichtern, statt die Webschnittstelle zu verwenden, was für die interaktive Verwaltung nützlicher ist.

Die folgenden Schnittstellen sind für RACADM verfügbar:

- Lokaler RACADM
- Remote-RACADM
- Telnet-/SSH-RACADM

Befehle des lokalen RACADM verwenden zum Zugriff auf den iDRAC6 vom verwalteten Server aus keine Netzwerkverbindungen. Dies bedeutet, dass Sie Befehle des lokalen RACADM verwenden können, um den anfänglichen iDRAC6-Netzwerkbetrieb zu konfigurieren. Remote-RACADM ist ein Dienstprogramm auf Client-Seite, das von einer Management Station aus über die bandexterne Netzwerkschnittstelle ausgeführt werden kann. SSH-/Telnet-RACADM wird verwendet, um über eine SSH- oder Telnet-Aufforderung einen Bezug zur RACADM-Befehlsanwendung herzustellen.

Dieser Abschnitt enthält die folgenden Informationen:

- RACADM-Befehle und unterstützte RACADM-Schnittstellen
- Lokales RACADM von einer Befehlszeile aus verwenden
- Remote-RACADM
- SSH-/Telnet-RACADM
- iDRAC6 mithilfe des Befehls **racadm** konfigurieren
- RACADM-Konfigurationsdatei zum Konfigurieren mehrerer iDRAC6s verwenden

VORSICHTSHINWEIS: Die neueste iDRAC6-Firmware unterstützt nur die aktuellste RACADM-Version. Es können Fehler auftreten, wenn Sie eine ältere RACADM-Version zum Abfragen eines iDRAC6 mit der neusten Firmware verwenden. Installieren Sie die RACADM-Version, die mit Ihrer neuesten Dell OpenManage-DVD bereitgestellt wurde.

RACADM-Unterbefehle

Tabelle 13-1 enthält eine Beschreibung der einzelnen RACADM-Unterbefehle, die Sie in RACADM ausführen können. Eine ausführliche Liste der RACADM-Unterbefehle, einschließlich Syntax und gültiger Einträge, finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals**verfügbar ist.

Tabelle 13-1. RACADM-Unterbefehle

Befehl	Beschreibung
arp	Zeigt den Inhalt der ARP-Tabelle an. Es dürfen keine ARP-Tabelleneinträge hinzugefügt oder gelöscht werden.
clearasrscreen	Löscht den Bildschirm Letzter Absturz (ASR).
closessn	Schließt eine Kommunikationssitzung auf dem Gerät.
coredump	Zeigt das letzte Kernspeicherabbild des iDRAC6 an.
coredumpdelete	Löscht das im iDRAC6 gespeicherte Kernspeicherabbild.
clrraclog	Löscht das iDRAC6-Protokoll. Nach dem Löschvorgang wird ein einzelner Eintrag vorgenommen, um den Benutzer und die Uhrzeit, zu der das Protokoll gelöscht wurde, anzuzeigen.
clrsel	Löscht die Einträge des iDRAC-Systemereignisprotokolls.
config	Konfiguriert den iDRAC6.
fwupdate	Aktualisiert die iDRAC6-Firmware.
getconfig	Zeigt die aktuellen iDRAC6-Konfigurationseigenschaften an.
getniccfg	Zeigt die derzeitige IP-Konfiguration für den Controller an.
getraclog	Zeigt das iDRAC6-Protokoll an.
getractime	Zeigt die iDRAC6-Zeit an.
getsel	Zeigt die SEL-Einträge an.

Tabelle 13-1. RACADM-Unterbefehle *(fortgesetzt)*

Befehl	Beschreibung
getssninfo[1]	Zeigt Informationen über aktive Sitzungen an.
getsvctag	Zeigt die Service-Tag-Nummer an.
getsysinfo	Zeigt Informationen zum iDRAC6 und verwalteten Server, einschließlich IP-Konfiguration, Hardwaremodell, Firmware-Versionen und Betriebssysteminformationen, an.
gettracelog	Zeigt das **iDRAC6-Ablaufverfolgungsprotokoll** an. Bei Verwendung mit `-i` zeigt der Befehl die Anzahl von Einträgen im iDRAC6-Ablaufverfolgungsprotokoll an.
Hilfe	Listet iDRAC6-Unterbefehle auf.
Hilfe <Unterbefehl>	Listet die Verwendung für den angegebenen Unterbefehl auf.
ifconfig	Zeigt den Inhalt der Netzwerkschnittstellentabelle an.
krbkeytabupload	Eine Kerberos-Keytab-Datei hochladen.
localConRedirDisable	Führt die Deaktivierung der virtuellen Konsole vom lokalen System aus.
netstat	Zeigt die Routingtabelle und die aktuellen Verbindungen an.
ping	Überprüft, ob die Ziel-IP-Adresse unter Verwendung des Inhalts der aktuellen Routingtabelle vom iDRAC6 aus erreichbar ist. Eine Ziel-IP-Adresse ist erforderlich. Ein ICMP-Echo-Paket wird zur Ziel-IP-Adresse gesendet, basierend auf dem Inhalt der aktuellen Routingtabelle.
ping6	Überprüft, ob die Ziel-IPv6-Adresse unter Verwendung des Inhalts der aktuellen Routingtabelle vom iDRAC6 aus erreichbar ist. Eine Ziel-IPv6-Adresse ist erforderlich. Ein ICMP-Echo-Paket wird, basierend auf dem Inhalt der aktuellen Routingtabelle, zur Ziel-IPv6-Adresse gesendet.
racdump	Zeigt den Status und allgemeine Informationen zum iDRAC6 an.
racreset	Setzt den iDRAC6 zurück.
racresetcfg	Setzt den iDRAC6 auf seine Standardeinstellungen zurück.
remoteimage	Remote-Dateifreigabe

Tabelle 13-1. RACADM-Unterbefehle *(fortgesetzt)*

Befehl	Beschreibung
serveraction	Führt Energieverwaltungsvorgänge auf dem verwalteten Server aus.
setniccfg	Stellt die IP-Konfiguration für den Controller ein.
sshpkauth	Ermöglicht das Hochladen von bis zu vier verschiedenen öffentlichen SSH-Schlüsseln, das Löschen vorhandener Schlüssel und die Anzeige von Schlüsseln, die sich bereits im iDRAC6 befinden.
sslcertdownload	Lädt ein Zertifizierungsstellenzertifikat oder Serverzertifikat von iDRAC herunter.
sslcertupload	Lädt ein Zertifizierungsstellenzertifikat oder Serverzertifikat auf den iDRAC6 hoch.
sslcertview	Zeigt ein Zertifizierungsstellenzertifikat oder Serverzertifikat im iDRAC6 an.
sslcsrgen	Erstellt die SSL-CSR und lädt sie herunter.
testemail	Zwingt den iDRAC6, eine E-Mail über die iDRAC6-NIC zu senden.
testtrap	Zwingt den iDRAC6, eine SNMP-Warnung über die iDRAC6-NIC zu senden.
traceroute	Verfolgt den Netzwerkpfad von Routern, den Pakete verwenden, wenn sie von Ihrem System zu einer Ziel-IPv4-Adresse weitergeleitet werden.
traceroute6	Verfolgt den Netzwerkpfad von Routern, der von Paketen verwendet wird, wenn sie von Ihrem System zu einer Ziel-IPv6-Adresse weitergeleitet werden.
Version	Zeigt Informationen zur iDRAC6-Version an.
vflashsd	Initialisiert den Status der vflash-SD-Karte oder ruft diesen ab.
vflashpartition	Kann den Status von Partitionen auf einer initialisierten vFlash-SD-Karte erstellen, löschen, auflisten oder anzeigen.
vmdisconnect	Schließt alle offenen Verbindungen des virtuellen iDRAC-Datenträgers von Remote-Clients aus.

Tabelle 13-1. RACADM-Unterbefehle *(fortgesetzt)*

Befehl	Beschreibung
vmkey	Setzt die vFlash-Partition auf die Standard-Größeneinstellung von 256 MB und löscht alle Daten von der Partition.

[1] SOL-Sitzungsinformation ist in der Antwort auf den getssninfo-Befehl nicht enthalten.

Lokale RACADM-Befehle verwenden

RACADM-Befehle werden lokal (auf dem verwalteten Server) über eine Befehlseingabeaufforderung oder eine Shell-Eingabeaufforderung ausgeführt.

Melden Sie sich am verwalteten Server an, starten Sie eine Befehls-Shell und geben Sie Befehle des lokalen RACADM in einem der folgenden Formate ein:

- `racadm <Unterbefehl> [parameters]`
- `racadm <getconfig|config> [-g <Gruppe>] [-o <Objekt> <Wert>]`

Ohne Optionen zeigt der Befehl RACADM Informationen zum allgemeinen Gebrauch an. Geben Sie zur Anzeige der Liste der RACADM-Unterbefehle Folgendes ein:

```
racadm help
```

oder

```
racadm getconfig -h
```

Die Liste der Unterbefehle enthält alle RACADM-Befehle, die vom iDRAC6 unterstützt werden.

Um für einen Unterbefehl Hilfe zu erhalten, geben Sie Folgendes ein:

`racadm help <Unterbefehl>`

Der Befehl zeigt die Syntax- und Befehlszeilenoptionen für den Unterbefehl an.

ANMERKUNG: Die Verwendung von Zeichen, außer den nicht-alphanumerischen Zeichen, wie $, % , <, > , | usw., wird für RACADM-Befehlsargumente nicht empfohlen. Die Verwendung solcher anderen Zeichen kann zu einem unerwarteten Verhalten führen.

RACADM-Dienstprogramm zum Konfigurieren des iDRAC6 verwenden

In diesem Abschnitt wird beschrieben, wie RACADM zum Ausführen verschiedener iDRAC6-Konfigurations-Tasks verwendet wird.

Aktuelle iDRAC6-Einstellungen anzeigen

Der RACADM-Unterbefehl **getconfig** ruft aktuelle Konfigurationseinstellungen vom iDRAC6 ab. Die Konfigurationswerte werden in *Gruppen* organisiert, die ein oder mehrere *Objekt(e)* enthalten, wobei die Objekte *Werte* haben.

Eine vollständige Beschreibung der Gruppen und Objekte finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Geben Sie zum Anzeigen einer Liste aller iDRAC6-Gruppen den folgenden Befehl ein:

```
racadm getconfig -h
```

Geben Sie zum Anzeigen der Objekte und Werte für eine bestimmte Gruppe den folgenden Befehl ein:

```
racadm getconfig -g <Gruppe>
```

Beispiel: Um eine Liste aller Gruppenobjekteinstellungen für **cfgLanNetworking** anzuzeigen, geben Sie den folgenden Befehl ein:

```
racadm getconfig -g cfgLanNetworking
```

iDRAC6-Benutzer mit RACADM verwalten

ANMERKUNG: Verwenden Sie den Befehl **racresetcfg** mit Vorsicht, da *alle* Konfigurationsparameter auf die ursprünglichen Standardeinstellungen zurückgesetzt werden. Alle vorherigen Änderungen gehen verloren.

ANMERKUNG: Wenn Sie einen neuen iDRAC6 konfigurieren oder den Befehl **racadm racresetcfg** ausgeführt haben, ist der einzige aktuelle Benutzer **root** mit dem Kennwort **calvin**.

ANMERKUNG: Benutzer können im Laufe der Zeit aktiviert und deaktiviert werden. Infolgedessen kann ein Benutzer auf jedem iDRAC6 eine unterschiedliche Indexnummer besitzen.

ANMERKUNG: Benutzer und Gruppen, die für Active Directory-Umgebungen erstellt wurden, müssen mit der Active Directory-Namenskonvention übereinstimmen.

Sie können in der iDRAC6-Eigenschaftendatenbank bis zu 15 Benutzer konfigurieren. (Ein 16. Benutzer ist für den IPMI-LAN-Benutzer reserviert.) Überprüfen Sie, ob bereits aktuelle Benutzer vorhanden sind, bevor Sie einen iDRAC6-Benutzer manuell aktivieren.

Geben Sie zum Überprüfen, ob ein Benutzer existiert, bei der Eingabeaufforderung den folgenden Befehl ein:

```
racadm getconfig -u <Benutzername>
```

ODER

Geben Sie den folgenden Befehl einmal für jeden Index von 1 bis 16 ein:

```
racadm getconfig -g cfgUserAdmin -i <Index>
```

ANMERKUNG: Sie können auch `racadm getconfig -f <Dateiname>` eingeben und die erstellte Datei <*Dateiname*> anzeigen, die alle Benutzer sowie alle anderen iDRAC6-Konfigurationsparameter einschließt.

Mehrere Parameter und Objekt-IDs werden mit ihren aktuellen Werten angezeigt. Zwei Objekte von Bedeutung sind:

```
# cfgUserAdminIndex=nn

cfgUserAdminUserName=
```

Wenn das Objekt **cfgUserAdminUserName** keinen Wert besitzt, steht diese Indexnummer, die durch das Objekt **cfgUserAdminIndex** angezeigt wird, zur Verfügung. Wenn hinter dem „=“ ein Name steht, ist dieser Index diesem Benutzernamen zugewiesen.

ANMERKUNG: Benutzer und Gruppen, die für Active Directory-Umgebungen erstellt wurden, müssen mit der Active Directory-Namenskonvention übereinstimmen.

iDRAC6-Benutzer hinzufügen

Führen Sie zum Hinzufügen eines neuen Benutzers zum iDRAC6 die folgenden Schritte durch:

1. Legen Sie den Benutzernamen fest.
2. Legen Sie das Kennwort fest.

3 Stellen Sie Anmeldung auf iDRAC6-Benutzerberechtigung ein.

4 Aktivieren Sie den Benutzer.

Beispiel

Das folgende Beispiel beschreibt, wie man dem iDRAC6 einen neuen Benutzer namens „Jan“ mit dem Kennwort „123456“ und Anmeldeberechtigungen hinzufügt.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 2 jan

racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 2 123456

racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i 2 0x00000001

racadm config -g cfgUserAdmin -o cfgUserAdminEnable -
i 2 1
```

Verwenden Sie zum Verifizieren des neuen Benutzers einen der folgenden Befehle:

```
racadm getconfig -u john

racadm getconfig –g cfgUserAdmin –i 2
```

iDRAC6-Benutzer mit Berechtigungen aktivieren

Um einem Benutzer bestimmte administrative (rollenbasierte) Berechtigungen zu erteilen, stellen Sie die Eigenschaft **cfgUserAdminPrivilege** auf eine Bitmaske ein, die aus den unter Tabelle 13-2 gezeigten Werten konstruiert ist:

Tabelle 13-2. Bit-Masken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
Anmeldung am iDRAC6	0x00000001
iDRAC6 konfigurieren	0x00000002
Benutzer konfigurieren	0x00000004
Protokolle löschen	0x00000008
Serversteuerungsbefehle ausführen	0x00000010

Tabelle 13-2. Bit-Masken für Benutzerberechtigungen *(fortgesetzt)*

Benutzerberechtigung	Berechtigungs-Bitmaske
Auf die virtuelle Konsole zugreifen	0x00000020
Zugriff auf virtuelle Datenträger	0x00000040
Testwarnungen	0x00000080
Debug-Befehle ausführen	0x00000100

Um dem Benutzer z. B. die Berechtigungen **iDRAC6 konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen** und **Auf die virtuelle Konsole zugreifen** zu erteilen, fügen Sie die Werte 0x00000002, 0x00000004, 0x00000008 und 0x00000010 hinzu, um die Bitmap 0x0000002E zu konstruieren. Geben Sie dann den folgenden Befehl zum Einstellen der Berechtigung ein:

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i 2 0x0000002E
```

SSH-Schlüssel mit RACADM hochladen, anzeigen oder löschen

Hochladen

Der Modus „Hochladen" ermöglicht Ihnen, eine Schlüsseldatei hochzuladen oder den Schlüsseltext in die Befehlszeile zu kopieren. Sie können einen Schlüssel nicht gleichzeitig hochladen und kopieren.

Von lokalem RACADM:

```
racadm sshpkauth -i <2 to 16> -k <1 to 4> -f
<Dateiname>
```

Vom Telnet/SSH-RACADM:

```
racadm sshpkauth -i <2 bis 16> -k <1 bis 4> -t
<Schlüsseltext>
```

Beispiel:

Laden Sie mit einer Zeichenkette einen gültigen Schlüssel für iDRAC6-Benutzer 2 in den ersten Schlüsselplatz:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

Die PK SSH-Authentifizierungsdatei wurde erfolgreich zum RAC hochgeladen.

VORSICHTSHINWEIS: Die Option „Datei“ wird auf Telnet-/SSH-/seriellen RACADM nicht unterstützt.

Ansicht

Der Modus „Ansicht“ ermöglicht Benutzern, einen vom Benutzer angegebenen Schlüssel oder alle Schlüssel anzuzeigen.

```
racadm sshpkauth -i <2 bis 16> -v -k <1 bis 4>
```

```
racadm sshpkauth -i <2 bis 16> -v -k all
```

Löschen

Der Modus „Löschen“ ermöglicht Benutzern, einen vom Benutzer angegebenen Schlüssel oder alle Schlüssel zu löschen.

```
racadm sshpkauth -i <2 bis 16> -d -k <1 bis 4>
```

```
racadm sshpkauth -i <2 bis 16> -d -k all
```

VORSICHTSHINWEIS: 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.

Informationen zu den Unterbefehlsoptionen finden Sie unter sshpkauth im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

iDRAC6-Benutzer entfernen

Wenn Sie RACADM verwenden, kann der iDRAC-Benutzer nicht gelöscht werden. Der Benutzer kann nur unter Verwendung des **cfgUserAdminEnable**-Objekts deaktiviert werden. Die Befehlssyntax lautet:

```
racadm config –g cfgUserAdmin –o cfgUserAdminEnable –I
<Index>
```

Weitere Informationen zur Verwaltung von Benutzeradministratoren finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Testen von E-Mail-Warnmeldungen

Mit der iDRAC6-E-Mail-Warnungsfunktion können Benutzer E-Mail-Warnungen empfangen, wenn auf dem verwalteten Server ein kritisches Ereignis auftritt. Das folgende Beispiel zeigt, wie man die E-Mail-Warnungsfunktion testet, um sicherzustellen, dass der iDRAC6 ordnungsgemäß E-Mail-Warnungen über das Netzwerk senden kann.

```
racadm testemail -i 2
```

(-i 2 steht für den Indexeintrag Nr. 2 in der Tabelle mit E-Mail-Warnungen)

ANMERKUNG: Stellen Sie sicher, dass die SMTP- und E-Mail-Warnungseinstellungen konfiguriert sind, bevor Sie die E-Mail-Warnungsfunktion testen. Weitere Informationen finden Sie unter „Konfiguration von E-Mail-Warnungen“ auf Seite 101.

iDRAC6-SNMP-Trap-Warnungsfunktion überprüfen

Die iDRAC6-SNMP-Trap-Warnungsfunktion ermöglicht den SNMP-Trap-Abhörkonfigurationen, Traps für Systemereignisse zu empfangen, die auf dem verwalteten Server auftreten.

Das folgende Beispiel zeigt, wie ein Benutzer die SNMP-Trap-Warnungsfunktion testen kann.

```
racadm testtrap -i 2
```

(-i 2 steht für den Indexeintrag Nr. 2 in der Tabelle mit E-Mail-Warnungen)

ANMERKUNG: Stellen Sie vor dem Überprüfen der iDRAC6-SNMP-Trap-Warnungsfunktion sicher, dass die SNMP- und Trap-Einstellungen ordnungsgemäß konfiguriert sind. Diese Einstellungen können anhand der Beschreibungen zu den Unterbefehlen **testtrap** und **testemail** konfiguriert werden. Weitere Informationen finden Sie unter „Plattformereignis-Traps (PET) konfigurieren“ auf Seite 100.

iDRAC6-Netzwerkeigenschaften konfigurieren

Geben Sie Folgendes ein, um eine Liste verfügbarer Netzwerkeigenschaften zu erstellen:

```
racadm getconfig -g cfgLanNetworking
```

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

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

Die Befehle enthalten die gleiche Konfigurationsfunktionalität wie das iDRAC6-Konfigurationsdienstprogramm, wenn Sie dazu aufgefordert werden, <Strg><E> zu drücken. Weitere Informationen zum Konfigurieren von Netzwerkeigenschaften mit dem iDRAC6-Konfigurationsdienstprogramm finden Sie unter „iDRAC6-LAN“ auf Seite 372.

Im folgenden Beispiel wird gezeigt, wie der Befehl zur Konfiguration gewünschter LAN-Netzwerkeigenschaften verwendet werden kann.

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1

racadm config -g cfgLanNetworking -o cfgNicIpAddress
192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask
255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway
192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1
192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2
192.168.0.6

racadm config -g cfgLanNetworking -o
cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName
RAC-EK00002

racadm config -g cfgLanNetworking -o
cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName
MYDOMAIN
```

ANMERKUNG: Wenn **cfgNicEnable** auf **0** gesetzt wird, wird das iDRAC6-LAN selbst dann deaktiviert, wenn DHCP aktiviert ist.

IPMIüber LAN konfigurieren

1 Konfigurieren Sie IPMI über LAN, indem Sie folgenden Befehl eingeben:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 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.

a Aktualisieren Sie die IPMI-Kanalberechtigungen, indem Sie folgenden Befehl eingeben:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit <Stufe>
```

wobei `<Stufe>` eine der Folgenden ist:

- `2` (**Benutzer**)
- `3` (**Operator**)
- `4` (**Administrator**)

Beispiel: Um die IPMI-LAN-Kanalberechtigung auf 2 (Benutzer) einzustellen, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit 2
```

b Stellen Sie, falls erforderlich, den Verschlüsselungsschlüssel des IPMI-LAN-Kanals ein, indem Sie einen Befehl wie den folgenden eingeben:

ANMERKUNG: iDRAC6-IPMI unterstützt das RMCP+-Protokoll. Die IPMI 2.0-Spezifikationen enthalten weitere Informationen.

```
racadm config -g cfgIpmiLan -o
cfgIpmiEncryptionKey <Schlüssel>
```

wobei <*Schlüssel*> ein aus 20 Zeichen bestehender Verschlüsselungsschlüssel in einem gültigen Hexadezimal-Format ist.

2 Konfigurieren Sie IPMI Seriell über LAN (SOL) mit dem folgenden Befehl:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

ANMERKUNG: Die IPMI-SOL-Mindestberechtigungsstufe bestimmt die Mindestberechtigung, die zum Aktivieren von IPMI SOL erforderlich ist. Weitere Informationen enthält die IPMI 2.0-Spezifikation.

a Aktualisieren Sie die IPMI-SOL-Mindestberechtigungsebene mit folgendem Befehl:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege <Stufe>
```

wobei *<Stufe>* eine der folgenden Optionen ist:

- 2 (**Benutzer**)
- 3 (**Operator**)
- 4 (**Administrator**)

Beispiel: Um die IPMI-Berechtigungen für 2 (Benutzer) zu konfigurieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege 2
```

ANMERKUNG: Um die serielle Konsole über LAN umzuleiten, stellen Sie sicher, dass die SOL-Baudrate mit der Baudrate des verwalteten Servers identisch ist.

b Aktualisieren Sie die IPMI-SOL-Baudrate mit folgendem Befehl:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate <Baudrate>
```

wobei *<Baudrate>* 19200, 57600 oder 115200 Bit/s ist.

Zum Beispiel:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate 57600
```

c Aktivieren Sie SOL, indem Sie an der Eingabeaufforderung folgenden Befehl eingeben.

ANMERKUNG: SOL kann für jeden einzelnen Benutzer aktiviert oder deaktiviert werden.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminSolEnable 1 -i <ID>
```

wobei *<ID>* die eindeutige Benutzer-ID ist.

PEF konfigurieren

Sie können die Maßnahme konfigurieren, die iDRAC6 bei den einzelnen Plattformwarnungen ergreifen soll. Tabelle 13-3 führt die möglichen Maßnahmen sowie den Wert auf, mithilfe derer sie in RACADM identifiziert werden können.

Tabelle 13-3. Plattformereignismaßnahme

Aktion	Wert
Keine Maßnahme	0
Stromversorgung aus	1
Neustarten	2
Aus- und Einschalten	3

Konfigurieren Sie PEF-Maßnahmen mit folgendem Befehl:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -
i <Index> <Maßnahmenwert>
```

wobei <*Index*> der PEF-Index (siehe Tabelle 5-7) und <*Maßnahmenwert*> ein Wert von Tabelle 13-3 ist.

Um beispielsweise PEF zum Neustarten des Systems und zum Senden einer IPMI-Warnung zu aktivieren, wenn auf dem Prozessor ein kritisches Ereignis festgestellt wird, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i
9 2
```

PET konfigurieren

1. Aktivieren Sie globale Warnungen mit folgendem Befehl:

   ```
   racadm config -g cfgIpmiLan -o
   cfgIpmiLanAlertEnable 1
   ```

2. Aktivieren Sie PET mit folgendem Befehl:

   ```
   racadm config -g cfgIpmiPet -o
   cfgIpmiPetAlertEnable -i <Index> <0|1>
   ```

   wobei <*Index*> der PET-Zielindex ist und `0` oder `1` PET deaktivieren bzw. PET aktivieren bedeutet.

Beispiel: Um PET mit dem Index 4 zu aktivieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 4 1
```

3 Konfigurieren Sie Ihre PET-Regel mit folgendem Befehl:

```
racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertDestIPAddr -i <Index> <IP-Adresse>
```

wobei <*Index*> der PET-Zielindex und <*IP-Adresse*> die Ziel-IP-Adresse des Systems ist, welches die Plattformereigniswarnungen empfängt.

4 Konfigurieren Sie die Community-Namen-Zeichenkette.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
racadm config -g cfgIpmiLan -o
cfgIpmiPetCommunityName <Name>
```

wobei <*Name*> der PET-Community-Name ist.

Konfiguration von E-Mail-Benachrichtigungen

1 Aktivieren Sie globale Warnungen mit folgendem Befehl:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanAlertEnable 1
```

2 Aktivieren Sie E-Mail-Warnungen mit folgendem Befehl:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i <Index> <0|1>
```

wobei <*Index*> der E-Mail-Zielindex ist und 0 die E-Mail-Warnung deaktiviert oder 1 sie aktiviert. Der E-Mail-Zielindex kann ein Wert von 1 bis 4 sein.

Beispiel: Um E-Mail mit dem Index 4 zu aktivieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i 4 1
```

3 Konfigurieren Sie Ihre E-Mail-Einstellungen mit folgendem Befehl:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertAddress -i 1 <E-Mail-Adresse>
```

wobei 1 der E-Mail-Zielindex und <*E-Mail-Adresse*> die Ziel-E-Mail-Adresse ist, die die Plattformereigniswarnungen empfängt.

4 Geben Sie zum Konfigurieren des SMTP-E–Mail-Servers den folgenden Befehl ein:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSmtpServerIpAddr <SMTP-E-Mail-Server-IP-
Adresse>
```

5 Geben Sie zum Konfigurieren einer benutzerdefinierten Meldung den folgenden Befehl ein:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertCustomMsg -i <Index>
<benutzerdefinierte Meldung>
```

wobei <*Index*> der E-Mail-Zielindex und <b*enutzerdefinierte Meldung*> die benutzerdefinierte Meldung ist.

6 Testen Sie die konfigurierte E-Mail-Warnung, falls gewünscht, mit folgendem Befehl:

```
racadm testemail -i <Index>
```

wobei <*Index*> der zu testende E-Mail-Zielindex ist.

IP-Filterung konfigurieren (IP-Bereich)

Die IP-Adressenfilterung (oder *IP-Bereichsüberprüfung*) gestattet den iDRAC6-Zugriff nur von Clients oder Management Stations aus, deren IP-Adressen innerhalb eines vom Benutzer angegebenen Bereichs liegen. Alle anderen Anmeldeaufforderungen werden abgewiesen.

Die IP-Filterung vergleicht die IP-Adresse einer eingehenden Anmeldung mit dem IP-Adressenbereich, der in den folgenden **cfgRacTuning**-Eigenschaften angegeben ist:

- **cfgRacTuneIpRangeAddr**
- **cfgRacTuneIpRangeMask**

Die Eigenschaft **cfgRacTuneIpRangeMask** wird sowohl auf die eingehende IP-Adresse als auch auf die **cfgRacTuneIpRangeAddr**-Eigenschaften angewendet. Sind die Ergebnisse identisch, wird für die eingehende Anmeldeaufforderung der Zugriff auf den iDRAC6 zugelassen. Anmeldungen von IP-Adressen außerhalb dieses Bereichs erhalten eine Fehlermeldung.

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

```
cfgRacTuneIpRangeMask & (<eingehende IP-Adresse> ^
cfgRacTuneIpRangeAddr)
```

wobei & das binäre UND der Mengen und ^ das binäre ausschließliche ODER ist.

Eine vollständige Beschreibung der cfgRacTuning-Eigenschaften finden Sie unter „cfgRacTuning“ im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Tabelle 13-4. Eigenschaften der IP-Adressenfilterung (IP-Bereich)

Eigenschaft	Beschreibung
cfgRacTuneIpRangeEnable	Aktiviert die IP-Bereichsüberprüfungsfunktion.
cfgRacTuneIpRangeAddr	Bestimmt das akzeptable IP-Adressen-Bitmuster, abhängig von den Einsen (1) in der Subnetzmaske. Diese Eigenschaft wird bitweise mit **cfgRacTuneIpRangeMask** „*geund*et“, um den oberen Teil der zugelassenen IP-Adresse zu bestimmen. Die Anmeldung wird für alle IP-Adressen, die dieses Bitmuster in den oberen Bits aufweisen, zugelassen. Anmeldungen von IP-Adressen außerhalb dieses Bereichs schlagen fehl. Für die Standardwerte der einzelnen Eigenschaften ist für die Anmeldung ein Adressenbereich von 192.168.1.0 bis 192.168.1.255 zulässig.
cfgRacTuneIpRangeMask	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Maske muss in der Form einer Netzmaske sein, wobei die höherwertigen Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu Nullen (0) in den niederwertigen Bits.

Im Folgenden sind Beispiele zur Verwendung des lokalen RACADM zum Einstellen der IP-Filterung aufgeführt.

ANMERKUNG: Unter „RACADM-Befehlszeilenschnittstelle verwenden“ auf Seite 295 finden Sie weitere Informationen zu RACADM- und RACADM-Befehlen.

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

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.255
```

2 Zur Beschränkung von Anmeldungen auf einen kleinen 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, wie unten gezeigt:

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.252
```

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

Richtlinien zu IP-Filtern

Verwenden Sie die folgenden Richtlinien, wenn Sie den IP-Filter aktivieren:

- Stellen Sie sicher, dass **cfgRacTuneIpRangeMask** in Form einer Netzmaske konfiguriert ist, wobei alle höchstwertigen Bits Einsen (1) sind (was das Subnetz in der Maske definiert), mit einem Übergang zu nur Nullen (0) in den niederwertigen Bits.
- Verwenden Sie die Basisadresse des gewünschten Bereichs als Wert von **cfgRacTuneIpRangeAddr**. Der binäre 32 Bit-Wert dieser Adresse muss Nullen in allen niederwertigen Bits haben, wo Nullen in der Maske sind.

IP-Blockierung konfigurieren

Durch IP-Blockierung wird dynamisch festgestellt, wenn von einer bestimmten IP-Adresse aus übermäßige Anmeldefehlversuche auftreten und die Adresse eine bestimmte Zeit lang blockiert bzw. daran gehindert wird, eine Anmeldung am iDRAC6 durchzuführen.

Die Funktionen der IP-Blockierung schließen ein:

- Die Anzahl zulässiger Anmeldefehlschläge (**cfgRacTuneIpBlkFailcount**)
- Die Zeitspanne in Sekunden, während der diese Fehler auftreten müssen (**cfgRacTuneIpBlkFailWindow**)
- Die Zeitdauer in Sekunden, während der die blockierte IP-Adresse daran gehindert wird, eine Sitzung herzustellen, nachdem die zulässige Anzahl von Fehlern überschritten wurde (**cfgRacTuneIpBlkPenaltyTime**)

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 folgende Meldung anzeigen: `ssh exchange identification: Verbindung vom Remote-Host geschlossen`.

Im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist, finden Sie eine vollständige Liste der **cfgRacTune**-Eigenschaften.

Tabelle 13-5 führt die vom Benutzer definierten Parameter auf.

Tabelle 13-5. Anmeldungswiederholungs-Beschränkungseigenschaften (IP-Blockierung)

Eigenschaft	Definition
cfgRacTuneIpBlkEnable	Aktiviert die IP-Blockierungsfunktion. Wenn innerhalb eines bestimmten Zeitraums (**cfgRacTuneIpBlkFailWindow**) aufeinanderfolgende Fehler (**cfgRacTuneIpBlkFailCount**) von einer einzelnen IP-Adresse aus festgestellt werden, werden alle weiteren Versuche, von dieser Adresse aus eine Sitzung herzustellen, während eines bestimmten Zeitraums zurückgewiesen (**cfgRacTuneIpBlkPenaltyTime**).
cfgRacTuneIpBlkFailCount	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche zurückgewiesen werden.
cfgRacTuneIpBlkFailWindow	Die Zeitspanne in Sekunden, während der die fehlgeschlagenen Versuche gezählt werden. Wenn die Fehlversuche diese Grenze überschreiten, werden sie aus dem Zähler gelöscht.
cfgRacTuneIpBlkPenaltyTime	Definiert den Zeitraum in Sekunden, in dem Anmeldeversuche von einer IP-Adresse aus aufgrund übermäßiger Fehler zurückgewiesen werden.

IP-Blockierung aktivieren

Das folgende Beispiel hindert eine Client-IP-Adresse fünf Minuten lang daran, eine Sitzung zu beginnen, wenn dieser Client innerhalb einer Minute fünf fehlerhafte Anmeldeversuche durchführt.

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 300
```

Das folgende Beispiel verhindert mehr als drei Fehlversuche innerhalb einer Minute und verhindert für eine Stunde weitere Anmeldungsversuche.

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkEnable 1

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 3600
```

iDRAC6-Telnet- und SSH-Dienste mittels lokalem RACADM konfigurieren

Die Telnet-/SSH-Konsole kann lokal (auf dem verwalteten Server) unter Verwendung von RACADM-Befehlen konfiguriert werden.

ANMERKUNG: Um die Befehle in diesem Abschnitt ausführen zu können, müssen Sie über die Berechtigung **iDRAC6 konfigurieren** verfügen.

ANMERKUNG: Eine Neukonfiguration von Telnet- oder SSH-Einstellungen im iDRAC6 führt dazu, dass alle aktuellen Sitzungen ohne Warnung beendet werden.

Um Telnet und SSH vom lokalen RACADM aus zu aktivieren, melden Sie sich am verwalteten Server an und geben Sie in der Eingabeaufforderung die folgenden Befehle ein:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Ändern Sie zum Deaktivieren des Telnet- oder SSH-Diensts den Wert von `1` zu `0`:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 0

racadm config -g cfgSerial -o cfgSerialSshEnable 0
```

Geben Sie zum Ändern der Telnet-Anschlussnummer auf dem iDRAC6 den folgenden Befehl ein:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort
<neue Anschlussnummer>
```

Geben Sie z. B. zum Ändern des Telnet-Anschlusses von der Standardeinstellung 23 auf 8022 den folgenden Befehl ein:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort
8022
```

Eine vollständige Liste verfügbarer RACADM-CLI-Befehle finden Sie unter „RACADM-Befehlszeilenschnittstelle verwenden“ auf Seite 295.

Remote- und SSH-/Telnet-RACADM

Remote-RACADM ist ein Dienstprogramm auf Client-Seite, das von einer Management Station aus über die bandexterne Netzwerkschnittstelle ausgeführt werden kann. Eine Remote-Option (**-r**) wird zur Verfügung gestellt, mit der eine Verbindung zum verwalteten System hergestellt werden kann und RACADM-Unterbefehle von einer Remote-Konsole oder Management Station aus ausgeführt werden können. Um die Remote-Fähigkeit verwenden zu können, sind ein gültiger Benutzername (Option **-u**), ein gültiges Kennwort (Option **-p**) sowie die iDRAC6-IP-Adresse erforderlich. SSH-/Telnet-RACADM wird verwendet, um über eine SSH- oder Telnet-Aufforderung einen Bezug zur RACADM-Befehlsanwendung herzustellen.

Die maximale Anzahl gleichzeitiger Remote-RACADM-Sitzungen beträgt vier. Diese Sitzungen sind unabhängig und erfolgen zusätzlich zu den Telnet- und SSH-Sitzungen. iDRAC6 kann zusätzlich zu den vier RACADM-Sitzungen gleichzeitig vier SSH-Sitzungen und vier Telnet-Sitzungen unterstützen.

ANMERKUNG: Konfigurieren Sie die IP-Adresse auf dem iDRAC6, bevor Sie die RACADM-Remote-Fähigkeit verwenden.

ANMERKUNG: Wenn das System, von dem aus Sie auf das Remote-System zugreifen, kein iDRAC6-Zertifikat in seinem standardmäßigen Zertifikatspeicher enthält, wird beim Eingeben eines RACADM-Befehls eine Meldung eingeblendet.

```
Sicherheitswarnung: Zertifikat ist ungültig - Name
auf Zertifikat ist ungültig oder stimmt nicht mit
Standortnamen überein

Ausführung wird fortgesetzt. Verwenden Sie die
Option -S für racadm, um die Ausführung bei
zertifikatbezogenen Fehlern anzuhalten.
```

RACADM setzt die Ausführung des Befehls fort. Wenn Sie jedoch die Option `–S` verwenden, hält RACADM die Ausführung des Befehls an und blendet die folgende Meldung ein:

```
Sicherheitswarnung: Zertifikat ist ungültig - Name
auf Zertifikat ist ungültig oder stimmt nicht mit
Standortnamen überein

Racadm setzt die Ausführung des Befehls nicht fort.

FEHLER: Verbindung zum iDRAC6 konnte unter der
angegebenen IP-Adresse nicht hergestellt werden.
```

ANMERKUNG: Wenn Sie die RACADM-Remote-Fähigkeit verwenden, müssen Sie Schreibberechtigungen für die Ordner haben, in denen Sie die RACADM-Unterbefehle für Dateivorgänge verwenden, z. B.:

```
racadm getconfig -f <Dateiname>
```

oder

```
racadm sslcertdownload -t <Typ>[-f <Dateiname>]
```

Remote-RACADM-Verwendung

`racadm -r <iDRAC6-IP-Adresse> -u <Benutzername> -p <Kennwort> <Unterbefehl> <Unterbefehloptionen>`

`racadm -i -r <iDRAC6-IP-Adresse> <Unterbefehl> <Unterbefehloptionen>`

Zum Beispiel:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
```

```
racadm -i -r 192.168.0.120 getsysinfo
```

Wenn die HTTPS-Anschlussnummer des iDRAC6 auf einen vom Standardanschluss (443) abweichenden benutzerdefinierten Anschluss geändert wurde, muss die folgende Syntax verwendet werden:

`racadm -r <iDRAC6-IP-Adresse>:<Anschluss> -u <Benutzername> -p <Kennwort> <Unterbefehl> <Unterbefehloptionen>`

`racadm -i -r <iDRAC6-IP-Adresse>:<Anschluss> <Unterbefehl> <Unterbefehloptionen>`

Remote-RACADM-Optionen

Tabelle 13-6 listet die Optionen für den Remote-RACADM-Befehl auf.

Tabelle 13-6. RACADM-Befehlsoptionen

Option	Beschreibung
-r <*RAC-IP-Adr*>	Bestimmt die Remote-IP-Adresse des Controllers.
-r <*RAC-IP-Adr*>**:** <*Anschlussnummer*>	Verwenden Sie :<*Anschlussnummer*>, wenn die iDRAC6-Anschlussnummer nicht dem Standardanschluss (443) entspricht.
-i	Weist RACADM an, den Benutzer interaktiv nach dem Benutzernamen und dem Kennwort zu fragen.
-u <*Benutzername*>	Gibt den Benutzernamen an, der verwendet wird, um die Befehlstransaktion zu authentifizieren. Wenn die Option **-u** verwendet wird, muss auch die Option **-p** verwendet werden, wobei die Option **-i** (interaktiv) nicht zulässig ist.
-p <*Kennwort*>	Gibt das Kennwort an, das zur Authentifizierung der Befehlstransaktion verwendet wird. Wenn die Option **-p** verwendet wird, ist die Option **-i** nicht erlaubt.
-S	Legt fest, dass RACADM auf ungültige Zertifikate überprüfen soll. RACADM hält die Ausführung des Befehls unter Ausgabe einer Fehlermeldung an, wenn ein ungültiges Zertifikat ermittelt wird.

ANMERKUNG: Die Verwendung von Zeichen, außer den nicht-alphanumerischen Zeichen, wie $, % , <, > , | usw., wird für RACADM-Befehlsargumente nicht empfohlen. Die Verwendung solcher anderen Zeichen kann zu einem unerwarteten Verhalten führen.

iDRAC6-Konfigurationsdatei verwenden

Eine iDRAC6-Konfigurationsdatei ist eine Textdatei, die eine Darstellung der Werte in der iDRAC6-Datenbank enthält. Der RACADM-Unterbefehl **getconfig** kann zum Erstellen einer Konfigurationsdatei verwendet werden, die die aktuellen Werte des iDRAC6 enthält. Sie können dann die Datei bearbeiten und den RACADM-Unterbefehl **config -f** zum Zurückladen der Datei in den iDRAC6 oder zum Kopieren der Konfiguration auf andere iDRAC6 verwenden.

iDRAC6-Konfigurationsdatei erstellen

Die Konfigurationsdatei ist eine unformatierte Textdatei. Es können alle gültigen Dateinamen verwendet werden - die gebräuchliche Dateierweiterung **.cfg** wird jedoch empfohlen.

Die Konfigurationsdatei kann:

- mit einem Textbearbeitungsprogramm erstellt werden
- über den RACADM-Unterbefehl **getconfig** vom iDRAC6 abgerufen werden
- über den RACADM-Unterbefehl **getconfig** vom iDRAC6 abgerufen und dann bearbeitet werden

Geben Sie zum Abrufen einer Konfigurationsdatei über den RACADM-Befehl **getconfig** den folgenden Befehl ein:

```
racadm -r <Remote-iDRAC6-IP> -u <Benutzer> -p
<Kennwort> getconfig -f myconfig.cfg
```

Anhand dieses Befehls wird die Datei **myconfig.cfg** im aktuellen Verzeichnis erstellt.

Syntax der Konfigurationsdatei

ANMERKUNG: Bearbeiten Sie die Konfigurationsdatei mit einem Klartext-Bearbeitungsprogramm, z. B. **Notepad** (Windows) oder **vi** (Linux). Das Dienstprogramm **racadm** parst nur ASCII-Text. Formatierung verwirrt den Parser, wodurch die iDRAC6-Datenbank beschädigt werden kann.

In diesem Abschnitt wird das Format der Konfigurationsdatei beschrieben.

- Zeilen, die mit einem # beginnen, sind Kommentare.

  Ein Kommentar *muss* in der ersten Spalte der Zeile beginnen. Ein #-Zeichen wird in jeder anderen Spalte als normales #-Zeichen behandelt.

  Beispiel:

  ```
  #
  # Dies ist eine Anmerkung
  [cfgUserAdmin]
  cfgUserAdminPrivilege=4
  ```

- Alle Gruppeneinträge müssen sich zwischen den Zeichen *[* und *]* befinden.

  Das Anfangszeichen *[*, das einen Gruppennamen anzeigt, *muss* in Spalte eins sein. Der Gruppenname *muss* vor allen anderen Objekten in dieser Gruppe angegeben werden. Objekte, die keinen zugewiesenen Gruppennamen enthalten, erzeugen Fehler. Die Konfigurationsdaten sind in Gruppen angeordnet, die im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist, definiert sind.

  Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objekts an.

  Beispiel:

  `[cfgLanNetworking]` (*Gruppenname*)

  `cfgNicIpAddress=192.168.1.1` (*Objektname*)

- Parameter werden als *Objekt*=*Wert*-Paare ohne Leerzeichen zwischen Objekt, = und Wert angegeben.

  Auf den Wert folgende Leerzeichen werden ignoriert. Ein Leerzeichen innerhalb einer Wertezeichenkette bleibt unverändert. Alle Zeichen rechts neben = werden unverändert übernommen (z. B. ein zweites = oder ein #, *[*, *]* usw.).

  Um den Inhalt einer indizierten Gruppe anzuzeigen, verwenden Sie den folgenden Befehl:

  `racadm getconfig -g <Gruppenname> -i <Index>`

- Bei indizierten Gruppen *muss* der Objektanker das erste Objekt nach dem *[ ]*-Paar sein. Im Folgenden finden Sie Beispiele für aktuelle indizierte Gruppen:

  `[cfgUserAdmin]`

  `cfgUserAdminIndex=11`

- Wenn der Parser auf eine indizierte Gruppe trifft, wird der Index der Gruppe als Anker verwendet. Sämtliche Modifizierungen der Objekte innerhalb der indizierten Gruppe werden ebenfalls mit dem Indexwert assoziiert.

Zum Beispiel:

```
[cfgUserAdmin]

# cfgUserAdminIndex=11

cfgUserAdminUserName=

# cfgUserAdminPassword=******** (nur Schreiben)

cfgUserAdminEnable=0

cfgUserAdminPrivilege=0x00000000

cfgUserAdminIpmiLanPrivilege=15

cfgUserAdminIpmiSerialPrivilege=15

cfgUserAdminSolEnable=0
```

- Die Indizes sind vom Typ Nur-Lesen und können nicht modifiziert werden. Objekte der indizierten Gruppe sind an den Index gebunden, unter dem sie gelistet sind, und jede gültige Konfiguration zum Objektwert ist nur für diesen bestimmten Index anwendbar
- Für jede indizierte Gruppe steht ein vordefinierter Satz von Indizes zur Verfügung. Weitere Informationen finden Sie im *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

iDRAC6-IP-Adresse in einer Konfigurationsdatei modifizieren

Wenn Sie die iDRAC6-IP-Adresse in der Konfigurationsdatei modifizieren, sind alle unnötigen Einträge des Typs <*Variable*>=<*Wert*> zu entfernen. Es verbleibt nur die tatsächliche Bezeichnung der variablen Gruppe mit „[„ und “]“ einschließlich der beiden <*Variable*>=<*Wert*>-Einträge, die sich auf die Änderung der IP-Adresse beziehen.

Zum Beispiel:

```
#

# Objektgruppe "cfgLanNetworking"

#
```

```
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Die Datei wird wie folgt aktualisiert:

```
#
# Objektgruppe "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# Kommentar, der Rest dieser Zeile wird ignoriert
cfgNicGateway=10.35.9.1
```

Konfigurationsdatei in den iDRAC6 laden

Der Befehl `racadm config -f <Dateiname>` parst die Konfigurationsdatei, um zu überprüfen, ob gültige Gruppen- und Objektnamen vorhanden sind und Syntaxregeln befolgt werden. Weist die Datei keine Fehler auf, aktualisiert der Befehl die iDRAC6-Datenbank mit dem Dateiinhalt.

ANMERKUNG: Wenn Sie nur die Syntax überprüfen, jedoch nicht die iDRAC6-Datenbank aktualisieren möchten, fügen Sie dem Unterbefehl **config** die Option-**c** hinzu.

Fehler in der Konfigurationsdatei werden mit der Zeilennummer sowie einer Meldung markiert, die das Problem beschreibt. Bevor die Konfigurationsdatei den iDRAC6 aktualisieren kann, müssen alle Fehler korrigiert werden.

ANMERKUNG: Verwenden Sie den Unterbefehl **racresetcfg**, um die Datenbank und die iDRAC6-NIC-Einstellungen auf die ursprünglichen Standardeinstellungen zurückzusetzen und alle Benutzer und Benutzerkonfigurationen zu entfernen. Während der Stammbenutzer verfügbar ist, werden die Einstellungen anderer Benutzer ebenfalls auf die Standardeinstellungen zurückgesetzt.

Bevor Sie den Befehl `racadm config -f <Dateiname>` ausführen, können Sie den Unterbefehl `racresetcfg` ausführen, um den iDRAC6 auf seine Standardeinstellungen zurückzusetzen. Stellen Sie sicher, dass die zu ladende Konfigurationsdatei alle gewünschten Objekte, Benutzer, Indizes und anderen Parameter enthält.

Führen Sie zum Aktualisieren des iDRAC6 mit der Konfigurationsdatei den folgenden Befehl aus:

```
racadm -r <Remote-iDRAC6-IP> -u <Benutzer> -p
<Kennwort> config -f myconfig.cfg
```

Nachdem der Befehl abgeschlossen wurde, können Sie den RACADM-Unterbefehl **getconfig** ausführen, um zu bestätigen, dass die Aktualisierung erfolgreich verlaufen ist.

Mehrere iDRAC6 konfigurieren

Unter Verwendung einer Konfigurationsdatei können Sie andere iDRAC6-Systeme mit identischen Eigenschaften konfigurieren. Führen Sie zur Konfiguration mehrerer iDRAC die folgenden Schritte aus:

1. Erstellen Sie die Konfigurationsdatei über iDRAC6-Einstellungen, die Sie auf die anderen replizieren möchten. Geben Sie folgenden Befehl ein:

   ```
   racadm -r <Remote-iDRAC6-IP> -u <Benutzer> -p
   <Kennwort> getconfig -f <Dateiname>
   ```

   wobei <*Dateiname*> der Name einer Datei zum Speichern der iDRAC6-Eigenschaften ist, wie z. B. **myconfig.cfg**.

   Das nachstehende Beispiel zeigt, wie Sie Remote-RACADM-Befehle zum Konfigurieren mehrerer iDRAC6 verwenden können. Erstellen Sie eine Batch-Datei auf der Management Station und rufen Sie remote racadm-Befehle aus der Batch-Datei ab.

   Zum Beispiel:

   ```
   racadm -r <Server-IP 1> -u <Benutzer> -p
   <Kennwort> config -f myconfig.cfg

   racadm -r <Server-IP 2> -u <Benutzer> -p
   <Kennwort> config -f myconfig.cfg

   ...
   ```

Weitere Informationen finden Sie unter „iDRAC6-Konfigurationsdatei erstellen“ auf Seite 320.

ANMERKUNG: Einige Konfigurationsdateien enthalten eindeutige iDRAC6-Informationen (z. B. die statische IP-Adresse), die vor dem Exportieren der Datei zu anderen iDRAC6 geändert werden müssen.

2 Bearbeiten Sie die im vorherigen Schritt erstellte Konfigurationsdatei und entfernen Sie alle Einstellungen oder kommentieren Sie alle Einstellungen aus, die Sie *nicht* replizieren möchten.

3 Kopieren Sie die bearbeitete Konfigurationsdatei auf ein Netzlaufwerk, auf dem alle verwalteten Server, deren iDRAC6 konfiguriert werden soll, auf sie zugreifen können.

4 Führen Sie für jeden iDRAC6, den Sie konfigurieren möchten, Folgendes aus:

   a Melden Sie sich am verwalteten Server an und öffnen Sie eine Eingabeaufforderung.

   b Wenn Sie den iDRAC6 von den Standardeinstellungen aus neu konfigurieren möchten, geben Sie den folgenden Befehl ein:

   ```
   racadm racresetcfg
   ```

   c Mit dem folgenden Befehl laden Sie die Konfigurationsdatei in den iDRAC6:

   ```
   racadm -r <Remote-iDRAC6-IP> -u <Benutzer> -p
   <Kennwort> config -f <Dateiname>
   ```

   wobei <*Dateiname*> der Name der von Ihnen erstellten Konfigurationsdatei ist. Schließen Sie den vollständigen Pfad mit ein, wenn sich die Datei nicht im Arbeitsverzeichnis befindet.

   d Setzen Sie den konfigurierten iDRAC6 durch Eingabe des folgenden Befehls zurück:

   ```
   racadm racreset
   ```

14

Energieüberwachung und Energieverwaltung

Dell PowerEdge-Systeme enthalten viele neue und erweiterte Stromverwaltungsfunktionen. Die gesamte Plattform, von der Hardware zur Firmware bis hin zur Systemverwaltungssoftware, wurde mit einem Schwerpunkt auf Energieeffizienz, Energieüberwachung und Energieverwaltung entwickelt.

ANMERKUNG: Die iDRAC6-Energieverwaltungslogik wendet ein Complex Programmable Logic Device (CPLD) an, das auf dem Blade-Server vorhanden ist. Einige wenige Plattformen unterstützen auch ein erweitertes CPLD. Aktualisierungen zu CPLD-Geräten stehen auf der Dell Support-Website unter **support.dell.com** in den Abschnitten **System-Firmware** und **Systemplatine** zur Verfügung. Es wird empfohlen, den Blade-Server mit der neuesten CPLD-Firmware-Version zu aktualisieren. Die aktuellen CPLD- und die erweiterten CPLD-Firmwareversionen (für geeignete Plattformen) werden in der iDRAC6 Web GUI angezeigt.

Dell PowerEdge-Systeme enthalten viele Funktionen zur Energieüberwachung und -verwaltung:

- **Energieüberwachung:** iDRAC6 dokumentiert den Verlauf von Strommesswerten und berechnet Durchschnitts- sowie Spitzenwerte und mehr. Mithilfe der iDRAC6-Webschnittstelle können Sie die Informationen auf dem Bildschirm **Energieüberwachung** anzeigen. Sie können die Informationen auch in Diagrammform einsehen, indem Sie unten im Bildschirm **Energieüberwachung** auf **Show Graph (Diagramm anzeigen)** klicken. Weitere Informationen finden Sie unter „Stromüberwachung“ auf Seite 328.
- **Strombudget:** Ein Systeminventar aktiviert beim Start die Kalkulation eines Systemstrombudgets für die aktuelle Konfiguration. Weitere Informationen finden Sie unter „Energiebudgetierung“ auf Seite 331.
- **Stromsteuerung:** iDRAC6 ermöglicht Ihnen, im Remote-Zugriff verschiedene Energieverwaltungsmaßnahmen im verwalteten System vorzunehmen. Weitere Informationen finden Sie unter „Energiesteuerung“ auf Seite 336.

Strom konfigurieren und verwalten

Sie können die iDRAC6-Webschnittstelle und die RACADM-Befehlszeilenschnittstelle (CLI) zum Verwalten und Konfigurieren der Stromsteuerungen im Dell PowerEdge-System verwenden. Genauer gesagt können Sie:

- Den Netzstromstatus des Servers ansehen. Siehe „Energieüberwachung anzeigen“ auf Seite 329.
- Informationen zum Strombudget für den Server anzeigen, einschließlich des Mindest- und potenziellen Höchststromverbrauchs. Siehe „Energiebudget anzeigen“ auf Seite 333.
- Den Schwellenwert für das Strombudget des Servers anzeigen. Siehe „Strombudget-Schwellenwert“ auf Seite 334.
- Die den PCIe-Erweiterungskarten im Server zugewiesene Stromleistung anzeigen. Siehe „Einsehen und Ändern der PCIe-Energiezuweisung“ auf Seite 335.
- Stromsteuerungsmaßnahmen auf dem Server (z. B. Strom ein, Strom aus, System-Reset, Aus- und Einschalten und Ordentliches Herunterfahren) ausführen. Siehe „Durchführen von Energiesteuerungsmaßnahmen an einem Server“ auf Seite 336.

Stromüberwachung

Der iDRAC6 überwacht kontinuierlich den Stromverbrauch in Dell PowerEdge-Servern. Der iDRAC6 errechnet folgende Stromwerte und zeigt die Informationen auf der Webschnittstelle oder der RACADM-CLI an:

- Kumulativer Systemstrom
- Spitzenstrom und Spitzenstromstärke des Systems
- Durchschnittliche, Mindest- und Höchstleistungsaufnahme
- Leistungsaufnahme (wird auch grafisch auf der Webschnittstelle dargestellt)
- Zeiten der höchsten und geringsten Leistungsaufnahme

Energieüberwachung anzeigen

Webschnittstelle verwenden

So zeigen Sie die Energieüberwachungsdaten an:

1. Melden Sie sich an der iDRAC6-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Energieüberwachung**.

   Der Bildschirm **Energieüberwachung** wird eingeblendet und zeigt folgende Informationen an:

Stromüberwachung

- **Status**: Eine **grüne Markierung** verweist auf einen normalen Energiestatus, **Warnung** verweist auf die Ausgabe einer Warnmeldung, und **Schwerwiegend** verweist auf die Ausgabe einer Fehlermeldung.
- **Sondenname**: Führt den Namen des Sensors auf.
- **Messwert**: Zeigt die von der Sonde gemeldete Wattleistung an.
- **Warnungsgrenzwert**: Zeigt den empfohlenen annehmbaren Stromverbrauch (in Watt und BTU/h) für den Systembetrieb an. Ein über diesen Wert hinausgehender Stromverbrauch führt zu Warnereignissen und zur Drosselung der CPU.
- **Ausfallgrenzwert**: Zeigt den höchsten annehmbaren Stromverbrauch (in Watt und BTU/h) für den Systembetrieb an. Ein über diesen Wert hinausgehender Stromverbrauch führt zu kritischen Ereignissen/Fehlerereignissen und das Blade wird heruntergefahren.

Stromstärke (A)

- **Standort**: Zeigt den Namen des Systemplatinen-Sensors an.
- **Messwert**: Der aktuelle Stromverbrauch in Wechselstrom-Ampere

Energieüberwachungsstatistik und Spitzenwertstatistik

- **Statistik:**
  - **Kumulative Systemenergie –** Zeigt den aktuellen kumulativen Energieverbrauch des Servers in kWh an. Der Wert gibt den totalen Energieverbrauch des Systems wieder. Sie können diesen Wert auf 0 zurücksetzen, indem Sie am Ende der Tabellenzeile auf **Reset** klicken.

- **Spitzenenergie des Systems** gibt den Spitzenwert des Systems in Watt-Wechselstrom an.
- **Spitzenstromstärke des Systems** gibt die Spitzenstromstärke des Systems an. Der Spitzenwert stellt den höchsten Wert dar, der zwischen der **Startzeit der Messung** und dem aktuellen Zeitpunkt aufgezeichnet wurde. Die Spitzenzeit war der Zeitpunkt, zu dem der Spitzenwert auftrat. Klicken Sie am Ende der Tabellenzeile auf **Reset**, um den Wert auf den momentanen Wert zurückzusetzen (der ungleich 0 ist, wenn der Server in Betrieb ist). Durch Klicken auf Reset wird auch die Startzeit der Messung auf die aktuelle Uhrzeit zurückgesetzt.
- **Startzeit der Messung** – Zeigt das Datum und die gespeicherte Zeit an, zu der der Wert für den Systemenergieverbrauch zuletzt gelöscht wurde und der neue Messzyklus begann. Für die Statistiken zu **Kumulative Systemenergie**, **Spitzenstromstärke des Systems** und **Spitzenenergie des Systems** geben die Spitzenwerte beim Reset sofort den aktuellen Wert an.
- **Laufzeit der Messung** für die **kumulative Systemenergie** zeigt das aktuelle Datum und die Zeit für die Kalkulation des anzuzeigenden Energieverbrauchs des Systems an. Bei **Spitzenstromstärke des Systems** und **Spitzenenergie des Systems** zeigen die **Spitzenzeit**-Felder die Zeiten des Auftretens dieser Spitzenwerte an.
- **Messwert**: Der Wert der entsprechenden Statistik – **Kumulativer Systemstrom**, **Spitzenstrom des Systems** und **Spitzenstromstärke des Systems**, seit der Zähler gestartet wurde.

ANMERKUNG: Energieüberwachungsstatistiken bleiben über wiederholte Systemrücksetzungen erhalten. Sie spiegeln daher alle Aktivitäten im Intervall zwischen der angegebenen Startzeit und aktuellen Zeit wider. Die in der Tabelle Leistungsaufnahme angezeigten Energiewerte sind kumulative Durchschnittswerte im entsprechenden Zeitintervall (vorangehende(r) Minute, Stunde, Tag und Woche). Da die Intervalle zwischen Start- und Endzeiten hier von den Stromüberwachungsstatistiken abweichen können, ist es möglich, dass Spitzenstromwerte (maximale Spitzenwattwerte gegenüber maximalem Stromverbrauch) voneinander abweichen.

Power Consumption (Leistungsbedarf)

- **Durchschnittliche Leistungsaufnahme**: Durchschnitt während der vorhergehenden Minute, der vorhergehenden Stunde, des vorhergehenden Tages und der vorhergehenden Woche.

- **Maximale Leistungsaufnahme** und **Minimale Leistungsaufnahme**: Die maximalen und minimalen Leistungsaufnahmen, die im gegebenen Zeitintervall gemessen wurden.
- **Zeit der maximalen Leistung** und **Zeit der minimalen Leistung**: Die Zeiten (nach Minute, Stunde, Tag oder Woche), in denen die maximale und minimale Leistungsaufnahme auftrat.

Diagramm anzeigen

Klicken Sie auf **Diagramm anzeigen**, um Diagramme anzuzeigen, die die Leistungsaufnahme des iDRAC6 während der letzten Stunde, 24 Stunden, drei Tage oder Woche in Watt anzeigen. Verwenden Sie das Dropdown-Menü über dem Diagramm, um den Zeitabschnitt auszuwählen.

ANMERKUNG: Die Dateieinträge im Diagramm zeigen jeweils Durchschnittsmesswerte über einen Zeitraum von 5 Minuten an. Aus diesem Grund können die Diagramme kurze Abweichungen oder den aktuellen Verbrauch eventuell nicht widerspiegeln.

Energiebudgetierung

Der Bildschirm **Energiebudget** zeigt die Schwellenwertgrenzen für die Energie an, die den Umfang der Netzleistungsaufnahme angeben, die ein System während Spitzenleistungszeiten dem Rechenzentrum mitteilt.

Bevor ein Server hochfährt, teilt iDRAC6 dem CMC seine Strombereichsanforderung mit. Der vor dem Einschalten des Systems von iDRAC für CMC bereitgestellte Strombereich ist größer als der tatsächlich vom Blade aufnehmbare Strom. Dieser Strombereich wird anhand der Informationen der begrenzten Hardware-Bestandsliste berechnet. Basierend auf der vom Server tatsächlich verbrauchten Energie kann ein kleinerer Strombereich (Power-Envelope) angefordert werden, nachdem der Server hochgefahren wurde. Wenn sich der Stromverbrauch im Laufe der Zeit erhöht und sich der Stromverbrauch des Servers der maximalen Zuweisung nähert, kann der iDRAC6 eine Erhöhung des maximalen potenziellen Stromverbrauchs anfordern und erhöht auf diese Weise den Power-Envelope. iDRAC6 erhöht seine Anforderung hinsichtlich der maximalen potenziellen Leistungsaufnahme nur für den CMC. Fällt der Verbrauch ab, fordert er keine geringere potenzielle Mindestenergie an. iDRAC fordert mehr Strom an, wenn der Stromverbrauch über den vom CMC zugewiesenen Stromwert hinausgeht.

Nach dem Einschalten und Initialisieren des Systems berechnet iDRAC einen neuen Strombereich, der 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.

iDRAC6 unterstützt auch eine Energiezuweisung zu den PCIe-Erweiterungskarten für geeignete Plattformen. Sie können die Energie, die den im Erweiterungssteckplatz im Server installierten PCIe-Erweiterungskarten zugewiesen ist, ändern. In geeignete Plattformen können zwei PCIe-Karten installiert werden. iDRAC stellt die Hüllkurvenleistung dynamisch sehr nah an die tatsächlichen Systemanforderungen für das Blade ein, fügt den Bedarf für den Erweiterungskarten-Steckplatz zu und fragt die kombinierte Energie vom CMC ab. Weitere Informationen zu Erweiterungskarten finden Sie im *Hardware-Benutzerhandbuch*, das auf der Dell Support-Website unter **support.dell.com/manuals** verfügbar ist. Informationen über die Modifikation der PCIe-Energiezuweisung finden Sie unter „Einsehen und Ändern der PCIe-Energiezuweisung“ auf Seite 335.

Nach dem Starten des Blades fährt das BIOS hoch und erkennt die tatsächliche Leistungsaufnahme der installierten PCIe-Erweiterungskarten. Dies geschieht während des POST. iDRAC behält den in der Vorinitialisierungsphase für die Erweiterungskarten verwendeten Wert bei, wenn beide Karten vorhanden sind. Sobald der aktualisierte Wert basierend auf den aktuell installierten PCIe-Karten erreicht wurde, kombiniert iDRAC diesen Wert mit der geschätzten Leistungsaufnahme der Erweiterungskarte und gibt einen neuen Energiewert für das Gesamt-Blade aus. Wenn die CMC nicht ausreichend Energie zuweist, schaltet iDRAC das Blade ab. Wenn das CMC genug Energie zuweist, kann BIOS den Hochfahrvorgang fortsetzen und der Server kann starten.

Wenn z. B. 500 W der Wert ist, den iDRAC während der Vorinitialisierung annimmt, wird dieser Wert verwendet, außer wenn Sie einen anderen Wert für die Zuweisung des PCIe-Erweiterungssteckplatzes einstellen. Wenn Sie einen anderen Wert einstellen, wird dieser Wert immer während der Vorinitialisierung verwendet. Der Wert wird bei Aus- und Einschaltzyklen beibehalten. Der Eingangswert wird dann mit der Anzahl von installierten Karten verglichen, wenn das System POST erreicht.

Energiebudget anzeigen

Der Server bietet Übersichten zum Status des Energiebudgets für das Energie-Subsystem auf dem Bildschirm **Energiebudget**.

Webschnittstelle verwenden

ANMERKUNG: Um Energieverwaltungsmaßnahmen auszuführen, benötigen Sie Administratorberechtigung.

1. Melden Sie sich an der iDRAC6-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **System**.
3. Klicken Sie auf das Register **Energieverwaltung** und dann auf **Energiebudget**.

   Der Bildschirm **Strombudget** wird angezeigt.

Die Tabelle **Informationen zum Energiebudget** zeigt die Minimal- und Maximalgrenzen der Energieschwellenwerte für die aktuelle Systemkonfiguration an. Diese geben den Umfang der Wechselstrom-Leistungsaufnahme an, die ein schwellenwertbegrenztes System während Spitzenleistungszeiten an das Rechenzentrum schickt.

- **Potenzielle Mindest-Leistungsaufnahme** – Zeigt den Schwellenwert für die niedrigste Leistungsaufnahme an.
- **Potenzielle Höchst-Leistungsaufnahme** – Zeigt den Schwellenwert für die höchste Leistungsaufnahme an. Dieser Wert ist auch die absolute maximale Leistungsaufnahme für die aktuelle Systemkonfiguration.

RACADM verwenden

Öffnen Sie auf einem verwalteten Server eine Befehlszeilenschnittstelle und geben Sie Folgendes ein:

```
racadm getconfig -g cfgServerPower
```

ANMERKUNG: Weitere Informationen zu cfgServerPower, einschließlich Ausgabedetails, finden Sie unter cfgServerPower im *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **support.dell.com/manuals** verfügbar ist.

Strombudget-Schwellenwert

Bei Aktivierung bestimmt der Energiebudget-Schwellenwert das Energielimit für das System. Die Systemleistung wird dynamisch angepasst, um die Leistungsaufnahme am festgelegten Schwellenwert zu halten.

Die tatsächliche Leistungsaufnahme kann bei niedriger Auslastung geringer sein und den Schwellenwert für einen Augenblick überschreiten, bis Leistungsanpassungen abgeschlossen sind.

ANMERKUNG: Der Energiebudget-Schwellenwert ist schreibgeschützt und kann im iDRAC6 weder aktiviert noch konfiguriert werden.

Webschnittstelle verwenden

1. Melden Sie sich an der iDRAC6-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **System**.
3. Klicken Sie auf das Register **Energieverwaltung** und dann auf **Energiebudget**.

   Der Bildschirm **Strombudget** wird angezeigt. Die Tabelle **Energiebudget-Schwellenwert** zeigt Informationen zur Energiegrenze des Systems an:

   - **Aktiviert** weist darauf hin, ob das System den Schwellenwert für das Energiebudget erfordert.
   - **Schwellenwert in Watt** und **Schwellenwert in BTU/h** zeigen jeweils den Grenzwert in Watt-Wechselstrom bzw. BTU/h an.
   - **Schwellenwert in Prozent (maximal)** zeigt den Prozentsatz des Energiebegrenzungsbereichs an.

RACADM verwenden

Um die Energiebudget-Schwellenwertdaten vom lokalen RACADM aus einzusehen, öffnen Sie eine Befehlszeilenschnittstelle auf dem verwalteten Server und geben Sie folgendes ein:

```
racadm getconfig -g cfgServerPower -o
cfgServerPowerCapWatts
```

Anzeige: <*Energiebegrenzungswert in Watt-Wechselstrom*>

```
racadm getconfig -g cfgServerPower -o
cfgServerPowerCapBTUhr
```

Anzeige: <*Energiebegrenzungswert in BTU/h*>

```
racadm getconfig -g cfgServerPower -o
cfgServerPowerCapPercent
```

Anzeige: <*Energiebegrenzungswert in %*>

ANMERKUNG: Weitere Informationen zu cfgServerPower, einschließlich Ausgabedetails, finden Sie unter cfgServerPower im *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **support.dell.com/manuals** verfügbar ist.

Einsehen und Ändern der PCIe-Energiezuweisung

Die PCIe-Energiezuweisung ermöglicht Ihnen, die den PCIe-Erweiterungskarten zugewiesene Maximalenergie einzusehen und zu ändern. Die zugewiesene Energie muss zwischen 100 W und 500 W liegen. Ein Zuweisen von zuviel Energie kann dazu führen, dass das Blade nicht startet, oder dass andere Blades im Gehäuse nicht starten. Wenn die PCIe-Erweiterungskarte mehr Energie aufnimmt als zugewiesen, schaltet das Blade ab. Bei der Änderung der PCIe-Energiezuweisung wird der neue Energiezuweisungswert beim Starten des Systems verwendet.

ANMERKUNG: Die PCIe-Energiezuweisungsinformation gilt nicht für alle Plattformen und wird nicht für Plattformen angezeigt, für die sie nicht gilt.

ANMERKUNG: Sie müssen Administratorberechtigungen haben (iDRAC konfigurieren und Serversteuerungsbefehle ausführen), um den PCIe-Energiezuweisungswert zu ändern.

Webschnittstelle verwenden

1. Melden Sie sich an der iDRAC6-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **System**.
3. Klicken Sie auf das Register **Energieverwaltung** und dann auf **Energiebudget**. Die **PCIe-Energiezuweisungstabelle** zeigt die aktuelle Energiezuweisung im Feld **Energieschwellenwert in Watt** an.
4. Geben Sie den erforderlichen Wert ein oder klicken Sie auf **Standardwert**, um einen Standardwert festzulegen. Gültige Werte reichen von 100 W bis 500 W. Der Standardwert ist 500 W.
5. Klicken Sie auf **Anwenden**, um den neuen Wert zu speichern. Der neue Wert wird beim Starten des Systems verwendet.

RACADM verwenden

Um die aktuell zugewiesene Energie für die PCIe-Erweiterungskarten einzusehen, die remote RACADM verwenden, öffnen Sie auf dem Remotesystem eine Befehlseingabeaufforderung und geben Sie folgenden Befehl ein:

```
racadm -r <iDRAC-IP> -u <Benutzer> -p <Kennwort>
config -g cfgServerPower -o
cfgServerPowerPCIeAllocation
```

Gibt *<Energiebegrenzungswert in Watt-Wechselstrom oder BTU/h>* aus. Der Standardwert ist 500 W.

Ändern des Energiezuweisungswertes (z. B. auf 250 W):

```
racadm -r <iDRAC-IP> -u <Benutzer> -p <Kennwort>
config -g cfgServerPower -o
cfgServerPowerPCIeAllocation 250
```

Stellt den Wert auf 250 W

ANMERKUNG: Das cfgServerPowerPCIeAllocation-Objekt wird nur auf Remote-RACADM unterstützt, nicht auf lokalem RACADM.

ANMERKUNG: Weitere Informationen finden Sie unter cfgServerPowerPCIeAllocation im *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **support.dell.com/manuals** verfügbar ist.

Energiesteuerung

Der iDRAC6 ermöglicht, im Remote-Zugriff die Maßnahmen Einschalten, Ausschalten, Reset, ordentliches Herunterfahren, nicht maskierbarer Interrupt (NMI) oder Aus- und Einschalten auszuführen. Verwenden Sie den Bildschirm **Energiesteuerung**, um während eines Neustarts und beim Ein- und Ausschalten ein ordnungsgemäßes Herunterfahren über das Betriebssystem durchzuführen.

Durchführen von Energiesteuerungsmaßnahmen an einem Server

ANMERKUNG: Um Energieverwaltungsmaßnahmen auszuführen, benötigen Sie **Administratorberechtigungen**.

Der iDRAC6 ermöglicht die Ausführung von Maßnahmen im Remote-Zugriff wie Einschalten, Reset, ordnungsgemäßes Herunterfahren, nicht maskierbarer Interrupt (NMI) oder Aus- und Einschalten (Power Cycle).

Webschnittstelle verwenden

1. Melden Sie sich an der iDRAC6-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **System**.
3. Klicken Sie auf die Registerkarte **Power Management** (Energieverwaltung).

   Die Seite **Energiesteuerung** wird angezeigt.
4. Wählen Sie einen der folgenden **Stromsteuerungsvorgänge** aus, indem Sie auf die Optionsschaltfläche klicken:
   - **System einschalten** – Schaltet den Server ein (entspricht dem Drücken des Netzschalters, wenn der Systemstrom ausgeschaltet ist). Diese Option ist deaktiviert, wenn das System bereits eingeschaltet ist.
   - **System ausschalten** – Schaltet den Server aus. Diese Option ist deaktiviert, wenn das System bereits ausgeschaltet ist.
   - **NMI (nicht maskierbarer Interrupt)**- Erstellt einen NMI, um den Systembetrieb anzuhalten. Ein NMI sendet eine Unterbrechung hoher Stufe an das Betriebssystem, was dazu führt, dass das System den Vorgang unterbricht, um kritische Diagnose- und Fehlerbehebungsaktivitäten zu ermöglichen. Diese Option ist deaktiviert, wenn das System bereits ausgeschaltet ist.
   - **Ordnungsgemäßes Herunterfahren** – Versucht, das Betriebssystem herunterzufahren und schaltet dann das System aus. Hierfür ist ein ACPI-abhängiges Betriebssystem (Advanced Configuration and Power Interface) erforderlich, das systemgesteuerte Energieverwaltung ermöglicht. Diese Option ist deaktiviert, wenn das System bereits ausgeschaltet ist.
   - **System zurücksetzen (Softwareneustart) –** Startet das System neu, ohne den Strom abzuschalten. Diese Option ist deaktiviert, wenn das System bereits ausgeschaltet ist.
   - **System aus- und einschalten (Hardwareneustart)** – Schaltet das System aus und startet es daraufhin neu. Diese Option ist deaktiviert, wenn das System bereits ausgeschaltet ist.
5. Klicken Sie auf **Anwenden**.

   Daraufhin werden Sie von einem Dialogfeld zur Bestätigung aufgefordert.
6. Klicken Sie auf **OK**, um die Energieverwaltungsmaßnahme durchzuführen, die Sie ausgewählt haben.

RACADM verwenden

Um Energiemaßnahmen über das lokale RACADM auszuführen, geben Sie bei Eingabeaufforderung den nachstehenden Befehl ein:

```
racadm serveraction <Maßnahme>
```

wobei `<Maßnahme>` `powerup`, `powerdown`, `powercycle`, `hardreset` oder `powerstatus` ist.

ANMERKUNG: Weitere Informationen zu severaction finden Sie unter serveraction im *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **support.dell.com/manuals** verfügbar ist.

15

iDRAC6-Enterprise verwenden SM-CLP-Befehlszeilenschnittstelle

Dieser Abschnitt enthält Informationen zum SMWG SM-CLP (Serververwaltungs-Workgroup, Serververwaltungs-Befehlszeilenprotokoll), das im iDRAC6 integriert ist.

ANMERKUNG: Für diesen Abschnitt wird angenommen, dass Sie mit der SMASH-Initiative (Systemverwaltungsarchitektur für Serverhardware) und den SMWG SM-CLP-Angaben vertraut sind. Weitere Informationen zu diesen Spezifikationen finden Sie auf der Website zur Distributed Management Task Force (DMTF) unter **www.dmtf.org**.

Das iDRAC6-SM-CLP ist ein Protokoll, das von DMTF und SMWG betrieben wird, um Standards für Systemverwaltungs-CLI-Umsetzungen bereitzustellen. Viele Ansätze basieren auf einer definierten SMASH-Architektur, die als Fundament für besser genormte Systemverwaltungskomponenten dienen soll. Das SMWG SM-CLP ist eine Unterkomponente der gesamten von DMTF verfolgten SMASH-Bemühungen.

SM-CLP enthält einen Teilsatz der Funktionalität, die von der Befehlszeilenschnittstelle des lokalen RACADM zur Verfügung gestellt wird, verfügt jedoch über einen unterschiedlichen Zugriffspfad. SM-CLP wird innerhalb des iDRAC6 ausgeführt, RACADM jedoch auf dem verwalteten Server Bei RACADM handelt es sich außerdem um eine Dell-proprietäre Schnittstelle, wobei SM-CLP eine Industriestandardschnittstelle ist.

ANMERKUNG: Informationen zu den Dell Profilen und den MOFs sind im Dell Enterprise Technology Center unter **www.delltechcenter.com** und alle DMTF-Informationen auf der DMTF-Website unter **www.dmtf.org/standards/profiles/** verfügbar. Außerdem stehen Dell Erweiterungen unter **www.delltechcenter.com/page/DCIM+-+Dell+CIM+Extensions** zur Verfügung.

Systemverwaltung mit SM-CLP

Das iDRAC6-SM-CLP ermöglicht die Verwaltung der folgenden Systemfunktionen über eine Befehlszeile:

- Serverenergieverwaltung – System einschalten, herunterfahren oder neu starten
- Verwaltung des Systemereignisprotokolls (SEL) – SEL-Datensätze anzeigen oder löschen
- iDRAC6-Benutzerkontenverwaltung
- Active Directory-Konfiguration
- iDRAC6-LAN-Konfiguration
- Erstellung einer SSL-Zertifikatsignaturanforderung (CSR)
- Konfiguration virtueller Datenträger

Support für iDRAC6-SM-CLP

SM-CLP wird von der iDRAC6-Firmware gehostet und unterstützt Telnet- und SSH-Verbindungen. Die iDRAC6-SM-CLP-Schnittstelle basiert auf der SM-CLP-Spezifikation Version 1.0, bereitgestellt von der DMTF-Organisation.

Die folgenden Abschnitte enthalten eine Übersicht über die SM-CLP-Funktion, die vom iDRAC6 gehostet wird.

ANMERKUNG: Wenn Sie über Telnet/SSH eine SM-CLP-Sitzung eingerichtet haben und diese Sitzung aufgrund einer Unterbrechung der Netzwerkverbindung nicht ordnungsgemäß geschlossen wird, wird möglicherweise eine Meldung eingeblendet, die besagt, dass die maximale Anzahl von Verbindungen erreicht worden sein könnte. Sie können dieses Problem beheben, indem Sie die SM-CLP-Sitzung über die GUI unter **System**→ **iDRAC-Einstellungen**→ **Netzwerk/Sicherheit**→ **Sitzungen** beenden, bevor Sie versuchen, eine neue Sitzung einzurichten.

ANMERKUNG: iDRAC6 unterstützt bis zu vier Telnet-Sitzungen und vier SSH-Sitzungen gleichzeitig. Nur *eine* der acht potentiellen Sitzungen kann jedoch das SM-CLP benutzen. Dies bedeutet, dass der iDRAC6 nur jeweils eine SM-CLP-Sitzung auf einmal unterstützt.

So starten Sie eine SM-CLP-Sitzung:

- Stellen Sie über SSH/Telnet eine Verbindung zum iDRAC6 her, wodurch Sie zur CLI (Konsole) gelangen.
- Geben Sie bei der $-Eingabeaufforderung „smclp“ ein, um die SM–CLP-Konsole zu starten.

Syntax:

```
telnet <iDRAC6-IP-Adresse>

$ (die CLI-Eingabeaufforderung wird angezeigt)

$smclp (geben Sie bei der CLI-Eingabeaufforderung
smclp ein)
```

SM-CLP-Funktionen

Die SM-CLP-Spezifikation enthält einen allgemeinen Satz von SM-CLP-Standardverben, die für die einfache Systemverwaltung über die CLI verwendet werden können.

SM-CLP fördert das Konzept von Verben und Zielen, um Systemkonfigurationsfähigkeiten über die CLI bereitzustellen. Das Verb zeigt den auszuführenden Vorgang an und das Ziel ist die Einheit (oder das Objekt), auf der der Vorgang ausgeführt wird.

Im Folgenden wird die Syntax der SM-CLP-Befehlszeile dargestellt:

```
<Verb> [<Optionen>] [<Ziel>] [<Eigenschaften>]
```

Tabelle 15-1 enthält eine Liste der Verben, die die iDRAC6-CLI unterstützt, die Syntax der einzelnen Befehle sowie eine Liste der Optionen, die das Verb unterstützt.

Tabelle 15-1. Unterstützte SM-CLP-CLI-Verben

Verb	Beschreibung	Optionen
CD	Navigiert mithilfe der Shell durch den Adressbereich des verwalteten Systems. Syntax: `cd [Optionen] [Ziel]`	–default, –examine, –help, –output, –version
delete	Löscht eine Objektinstanz. Syntax: `delete [Optionen] Ziel`	–examine, –help, –output, –version
Beenden	Beendet die SM-CLP-Shell-Sitzung. Syntax: `exit [Optionen]`	–help, –output, –version

Tabelle 15-1. Unterstützte SM-CLP-CLI-Verben *(fortgesetzt)*

Verb	Beschreibung	Optionen
Hilfe	Zeigt Hilfe für SM-CLP-Befehle an. `Hilfe`	-examine, -help, -output, -version
reset	Setzt das Ziel zurück. Syntax: `reset [Optionen] [Ziel]`	–examine, –help, –output, –version
set	Stellt die Eigenschaften eines Ziels ein Syntax: `set [Optionen] [Ziel] <Eigenschaftenname>=<Wert>`	–examine, –help, –output, –version
Anzeigen	Zeigt die Zieleigenschaften, Verben und Unterziele an. Syntax: `show [Optionen] [Ziel] <Eigenschaftenname>=<Wert>`	-all, -default, –display, –examine, –help, –level, –output, –version
start	Startet ein Ziel. Syntax: `start [Optionen] [Ziel]`	–examine, –force, –help, –output, –version
stop	Fährt ein Ziel herunter. Syntax: `stop [Optionen] [Ziel]`	–examine, –force, –help, –output, –version, –wait
Version	Zeigt die Versionsattribute eines Ziels an. Syntax: `version [Optionen]`	–examine, –help, –output, –version

Tabelle 15-2 beschreibt die SM-CLP-Optionen. Einige Optionen haben abgekürzte Formen, wie in der Tabelle gezeigt.

Tabelle 15-2. Unterstützte SM-CLP-Optionen

SM-CLP-Option	Beschreibung
-all, -a	Beauftragt das Verb, alle möglichen Funktionen auszuführen.
-destination	Bestimmt den Speicherort, an dem ein Image im Dump-Befehl gespeichert wird. Syntax: –destination <URI>
-display, -d	Filtert die Befehlsausgabe. Syntax: `-display <Eigenschaften | Ziele | Verben>[, <Eigenschaften | Ziele | Verben>]*`
-examine, -x	Weist den Befehlsprozessor an, die Befehlssyntax zu validieren, ohne den Befehl auszuführen.
-force, -f	Wenn ein kontrolliertes Herunterfahren nicht erfolgreich ist, verwenden Sie diese Option, um ein erzwungenes Herunterfahren des Zielsystems durchzuführen. Syntax: `stop -force <Ziel>`
-help, -h	Zeigt Hilfe für das Verb an.
-level, -l	Weist das Verb an, an Zielen auf zusätzlichen Stufen unterhalb des festgelegten Ziels zu arbeiten. Syntax: `-level <n | alle>`

-output, -o	Legt das Format für die Ausgabe fest.
	Syntax:
	`-output format=<Text | clpcsv | Schlüsselwort | clpxml>`
	oder
	`-o format=<Text | clpcsv | Schlüsselwort | clpxml>`

-version, -v	Zeigt die SM-CLP-Versionsnummer an.

MAP-Adressbereich navigieren

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.

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 iDRAC6 anmelden. Wechseln Sie von root abwärts, indem Sie das Verb `cd` verwenden.

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.

Targets

Eine Liste der Ziele, die über das SM-CLP verfügbar sind, finden Sie im Dokument zur SM–CLP-Zuweisung, das im Dell Enterprise Technology Center unter **www.delltechcenter.com** zur Verfügung steht.

Verb show verwenden

Um mehr über ein Ziel zu erfahren, verwenden Sie das Verb `show`. Dieses Verb zeigt die Eigenschaften des Ziels, untergeordnete Ziele, Zuordnungen, sowie eine Liste der SM-CLP-Verben an, die an diesem Ort 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/oemdcim_mfaaccount1
```

Wenn Sie nur eine Eigenschaft anzeigen möchten, können Sie die Klammern auslassen.

Option -level verwenden

Die Option **show -level** führt **show** über zusätzliche Ebenen unterhalb des festgelegten Ziels aus. Wenn Sie alle Ziele und Eigenschaften im Adressbereich anzeigen möchten, verwenden Sie 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 **www.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
```

Beispiele für iDRAC6-SM-CLP

Die folgenden Unterabschnitte enthalten Beispiele, wie Sie sich unter Verwendung der SSH-Schnittstelle am iDRAC6 anmelden und eine SM-CLP-Sitzung starten können, um die folgenden Verfahren auszuführen:

- Serverenergieverwaltung
- SEL-Verwaltung
- MAP-Zielnavigation
- Eigenschaften des Anzeigesystems

Server-Energieverwaltung

Tabelle 15-3 enthält Beispiele für die Verwendung des SM-CLP zum Ausführen von Energieverwaltungsvorgängen auf einem verwalteten Server.

Geben Sie „`smclp`“ ein, um die SM-CLP-Konsole zu starten.

Tabelle 15-3. Stromverwaltungsvorgänge des Servers

Operation	Syntax

Am iDRAC6 mithilfe der SSH-Schnittstelle anmelden	`>ssh 192.168.0.120`
	`>Anmeldung: root`
	`>Kennwort:`
	Geben Sie „`smclp`“ ein, um die SM–CLP-Konsole zu starten.

Schalten Sie den Server aus.	`->stop /admin1/system1` `system1 erfolgreich angehalten`
Server aus dem ausgeschalteten Zustand hochfahren	`->start /admin1/system1` `system1 erfolgreich gestartet`
Server neu starten	`->reset /admin1/system1\` `RESET erfolgreich für system1`

SEL-Verwaltung

Tabelle 15-4 enthält Beispiele für die Verwendung des SM-CLP zum Ausführen von SEL-bezogenen Vorgängen auf dem verwalteten System.

MAP-Zielnavigation

Tabelle 15-5 enthält Beispiele für die Verwendung des Verbs **cd**, um innerhalb des MAP zu navigieren. In allen Beispielen wird angenommen, dass das ausgängliche Standardziel '/' ist.

Tabelle 15-4. SEL-Verwaltungsvorgänge

Operation	Syntax

SEL anzeigen	`->show -d targets,properties,verbs /admin1/system1/logs1/log1`
	
	Gibt möglicherweise Folgendes zurück:
	`Ziele:`
	`record1/`
	`record2/...`
	
	`Eigenschaften:`
	`OverwritePolicy=7`
	`LogState=4`
	`CurrentNumberOfRecords=60`
	`MaxNumberOfRecords=512`
	`ElementName=Record Log 1`
	`HealthState=5`
	`EnabledState=2`
	`RequestedState=12`
	`EnabledDefault=2`
	`TransitioningToState=12`
	`InstanceID=DCIM: SEL Log`
	`OperationalStatus={2}`
	
	`Verben:`
	`Anzeigen`
	`Beenden`
	`Version`
	`CD`
	`Hilfe`

Tabelle 15-4. SEL-Verwaltungsvorgänge *(fortgesetzt)*

Operation	Syntax
SEL-Datensatz anzeigen	->show /admin1/system1/logs1/log1/record4 **Gibt möglicherweise Folgendes zurück:** ufip=/admin1/system1/logs1/log1/record4 Associations:LogManagesRecord= >/admin1/system1/logs1/log1 Eigenschaften: RecordData=*0.0.65*4 2*1245152621*65 65*4*31*0*true*111*1*255*255* RecordFormat= *IPMI_SensorNumber.IPMI_OwnerLUN.IPMI_OwnerID*I PMI_RecordID*IPMIRecordType*IPMI_TimeStamp*IPMI _GeneratorID*IPMI_EvMRev*IPMI_SensorType*IPMI_S ensorNumber*IPMI_AssertionEvent*IPMI_EventType* IPMI_EventData1*IPMI_EventData2*IPMI_EventData3 *IANA* Description=:0:Assert:OEM specific ElementName=DCIM System Event Log Entry InstanceID=DCIM:SEL LOG:4 LogInstanceID=idrac:Unknown:Unknown SEL Log LogName=DCIM System Event Log Entry RecordID=DCIM:SEL LOG:4 CreationTimeStamp=20090616114341.000000+000
	Verben: Anzeigen Beenden Version CD Hilfe delete

Tabelle 15-4. SEL-Verwaltungsvorgänge *(fortgesetzt)*

Operation	Syntax

SEL löschen	`->delete /admin1/system1/logs1/log1/record*`
	Rückgaben:
	`Einträge wurden erfolgreich gelöscht`

Tabelle 15-5. Map-Zielnavigationsvorgänge

Operation	Syntax

Zum Systemziel wechseln und einen Neustart durchführen	`->cd admin1/system1`
	`->reset`
	ANMERKUNG: Das aktuelle Standardziel ist /.

Zum SEL-Ziel wechseln und die Protokolldatensätze anzeigen	`->cd admin1`
	`->cd system1`
	`->cd logs1`
	`->cd log1`
	`->show`
	entspricht
	`->cd admin1/system1/logs1/log1`
	`->show`

Aktuelles Ziel anzeigen	`->cd .`
Eine Stufe höher gehen	`->cd ..`
Shell beenden	`->exit`

16

WS-MAN-Schnittstelle verwenden

Web Services for Management (WS–MAN) ist ein SOAP-basiertes Protokoll (Simple Object Access Protocol), das zur Systemverwaltung verwendet wird. WS–MAN bietet ein dialogfähiges Protokoll für Geräte zum netzwerkübergreifenden Freigeben und Austauschen von Daten. iDRAC6 verwendet WS–MAN zum Übermitteln von DMTF-CIM-basierten Verwaltungsinformationen (Distributed Management Task Force; Common Information Model); die CIM-Informationen definieren die Semantik- und Informationstypen, die in einem verwalteten System manipuliert werden können. Die Dell–integrierten Serverplattform-Verwaltungsschnittstellen werden zu Profilen organisiert, wobei jedes Profil die spezifischen Schnittstellen für eine bestimmte Verwaltungsdomäne oder für einen bestimmten Funktionsbereich definiert. Desweiteren hat Dell eine Anzahl von Modell- und Profilerweiterungen definiert, die Schnittstellen für zusätzliche Fähigkeiten zur Verfügung stellen.

Die durch WS-MAN zur Verfügung gestellten Daten werden durch die iDRAC6-Instrumentierungsschnittstelle bereitgestellt, die den DMTF-Profilen und den Dell-Erweiterungsprofilen zugeordnet ist.

Funktionen von WS-Management

Die WS–Management-Spezifikation fördert die Interoperabilität zwischen Verwaltungsanwendungen und verwalteten Ressourcen. Durch das Identifizieren eines Kernsatzes von Web Services-Spezifikationen und Gebrauchsanforderungen zum Herausstellen eines gemeinsamen Satzes von Vorgängen, die im Mittelpunkt der Systemverwaltung stehen, ist WS–Management zu Folgendem in der Lage:

- ERMITTELN des Vorhandenseins von Verwaltungsressourcen und das Navigieren zwischen ihnen
- ERHALTEN, EINSTELLEN, ERSTELLEN und LÖSCHEN individueller Verwaltungsressourcen, wie z. B. Einstellungen und dynamische Werte

- AUFLISTEN des Inhalts von Containern und Sammlungen, wie z. B. große Tabellen und Protokolle
- AUSFÜHREN spezieller Verwaltungsmethoden mit stark typisierten Eingabe- und Ausgabeparametern

Unterstützte CIM-Profile

Tabelle 16-1. Unterstützte CIM-Profile

Standard-DMTF
1 Basisserver Bestimmt CIM-Klassen zum Darstellen des Hostservers.
2 Basismetrik Bestimmt CIM-Klassen zum Liefern der Fähigkeit, Metriken zu entwickeln und zu steuern, die für verwaltete Elemente erfasst werden.
3 Serviceprozessor Bestimmt CIM-Klassen zum Entwickeln von Serviceprozessoren.
4 USB-Umleitung Bestimmt CIM-Klassen zum Beschreiben von Informationen zu USB-Umleitungen. Für KVM-Geräte sollte dieses Profil verwendet werden, wenn die Geräte als USB-Geräte verwaltet werden sollen.
5 Physischer Bestand Bestimmt CIM-Klassen zum Darstellen der physischen Aspekte der verwalteten Elemente. iDRAC6 verwendet dieses Profil, um die FRU-Informationen des Hostservers und seiner Komponenten sowie die physische Topologie darzustellen.
6 SM-CLP-Administrator-Domäne Bestimmt CIM-Klassen zum Darstellen der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für die Implementierung von CLP.
7 Stromzustandsverwaltung Bestimmt CIM-Klassen für Stromsteuerungsvorgänge. iDRAC6 verwendet dieses Profil für die Stromsteuerungsvorgänge des Hostservers.
8 CLP-Dienst Bestimmt CIM-Klassen zum Darstellen der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für die Implementierung von CLP.
9 IP-Schnittstelle Bestimmt CIM-Klassen zum Darstellen einer IP-Schnittstelle auf einem verwalteten System.

Tabelle 16-1. Unterstützte CIM-Profile *(fortgesetzt)*

10 DHCP-Client
Bestimmt CIM-Klassen zum Darstellen eines DHCP-Clients und seiner zugehörigen Fähigkeiten und Konfiguration.

11 DNS-Client
Bestimmt CIM-Klassen zum Darstellen eines DNS-Clients in einem verwalteten System.

12 Datensatzprotokoll
Bestimmt CIM-Klassen zum Darstellen unterschiedlicher Protokolltypen. iDRAC6 verwendet dieses Profil, um das Systemereignisprotokoll (SEL) und das iDRAC6-RAC-Protokoll darzustellen.

13 Rollenbasierte Authentifizierung
Bestimmt CIM-Klassen zum Darstellen von Rollen. iDRAC6 verwendet dieses Profil zum Konfigurieren von iDRAC6-Kontoberechtigungen.

14 SMASH-Sammlungen
Bestimmt CIM-Klassen zum Darstellen der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für die Implementierung von CLP.

15 Profilregistrierung
Bestimmt CIM-Klassen zur Ankündigung der Profil-Implementierungen. iDRAC6 verwendet dieses Profil, um die eigenen implementierten Profile, wie in dieser Tabelle dargestellt, anzukündigen.

16 Einfache Identitätsverwaltung
Bestimmt CIM-Klassen zum Darstellen der Identitäten. iDRAC6 verwendet dieses Profil zum Konfigurieren von iDRAC6-Konten.

17 Ethernet-Anschluss
Bestimmt CIM-Klassen zum Darstellen eines Ethernet-Anschlusses, seines zugehörigen Controllers, sowie Ethernet-Schnittstellen in einem verwalteten System. In diesem Profil werden Zuordnungen zu den physischen Aspekten des Anschlusses und Profilimplementierungs-Versionsinformationen modelliert.

18 Sensor
Bestimmt CIM-Klassen zur Beschreibung der Sensoren in einem verwalteten System. Außerdem werden Zuordnungsklassen bestimmt, die die Beziehung der Sensoren zu den überwachten Geräten beschreiben.

Dell-Erweiterungen

1 Active Directory-Client
Bestimmt CIM- und Dell-Erweiterungsklassen zum Konfigurieren des iDRAC6 Active Directory-Clients und der lokalen Berechtigungen für Active Directory-Gruppen.

Tabelle 16-1. Unterstützte CIM-Profile *(fortgesetzt)*

2 Virtueller Datenträger
Bestimmt CIM- und Dell-Erweiterungsklassen zum Konfigurieren des virtuellen iDRAC6-Datenträgers. Erweitert das *USB-Umleitung*sprofil.

3 BS-Bereitstellung
Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der Konfiguration von BS-Bereitstellungsfunktionen. Sie erweitert die Verwaltungsfähigkeit des Verweisens auf Profile, indem die Fähigkeit hinzugefügt wird, BS-Bereitstellungsvorgänge zu unterstützen. Hierzu werden die vom Serviceprozessor gelieferten BS-Bereitstellungsfunktionen manipuliert.

4 Software-Bestandsaufnahme
Bestimmt CIM- und Dell-Erweiterungen zur Darstellung kürzlich installierter BIOS-, Komponenten-Firmware-, Diagnose-, Unified Server Configurator- und Driver Pack-Versionen. Außerdem werden die im Lifecycle Controller verfügbaren Versionen von BIOS- und Firmware-Aktualisierungsabbilder für ein Rollback und eine Neuinstallation dargestellt.

5 Software-Aktualisierung
Bestimmt CIM- und Dell-Erweiterungen zur Darstellung der Serviceklasse und Methoden zur Aktualisierung des BIOS, der Diagnose, Driver Packs sowie der Komponenten- und Lifecycle Controller-Firmware. Die Aktualisierungsmethoden unterstützen die Aktualisierung über CIFS-, NFS-, FTP- und HTTP-Netzwerkfreigaben sowie über Aktualisierungsabbilder des Lifecycle Controllers. Aktualisierungsanfragen werden als Auftrag formuliert und können für sofort oder später geplant werden, wobei verschiedene Neustart-Aktionen für die Aktualisierung angewendet werden können.

6 Aufgabensteuerung
Bestimmt CIM- und Dell-Erweiterungen zur Verwaltung von Aufträgen, die durch Aktualisierungsanfragen erzeugt werden. Aufträge können erstellt, gelöscht, geändert und in Auftragsreihen eingeteilt werden, um Auftragsreihenfolgen festzulegen und mehrere Aktualisierungen bei nur einem Neustart durchzuführen.

7 LC-Verwaltung
Bestimmt CIM- und Dell-Erweiterungen für den Erhalt und die Einstellung von Attributen zur Verwaltung der Auto-Discovery- und Part Replacement-Funktionen des Lifecycle Controllers.

8 Dauerhafte Speicherung
Definiert CIM- und Dell-Erweiterungsklassen für die Verwaltung der Partitionen auf den virtuellen Flash-Medien von Dell-Plattformen.

Tabelle 16-1. Unterstützte CIM-Profile *(fortgesetzt)*

9	Einfacher NIC Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der Konfiguration von NIC-Netzwerk-Controllern
10	BIOS und Startverwaltung Definiert CIM- und Dell-Erweiterungsklassen zur Darstellung von Dell BIOS-Attributen und zur Konfiguration der Startreihenfolge des Host.
11	Einfaches RAID Definiert CIM- und Dell-Erweiterungsklassen zur Darstellung der Konfiguration der RAID-Speicherung des Host.
12	iDRAC-Karte Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der iDRAC6-Bestandsinformationen.
13	Speicher Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der DIMM-Bestandsinformationen des Hosts.
14	CPU Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der CPU-Bestandsinformationen des Hosts.
15	Systeminfo Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der Plattform-Bestandsinformationen des Hosts.
16	PCI-Gerät Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der PCI-Geräte-Bestandsinformationen des Hosts.
17	Grafikkarte Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der Videokarten-Bestandsinformationen des Hosts.

Die iDRAC6-WS–MAN-Implementierung verwendet SSL auf Anschluss 443 für Transportsicherheit und unterstützt die grundlegende Authentifizierung. Web-Services-Schnittstellen können verwendet werden, indem Client-Infrastrukturen wie Windows WinRM und Powershell CLI, Open Source-Dienstprogramme wie WSMANCLI und Anwendungs-Programmierumgebungen wie Microsoft .NET genutzt werden.

Zusätzliche Implementierungsanleitungen, White-Papers, Profile, MOFs und Codebeispiele stehen im Dell Enterprise Technology Center unter **www.delltechcenter.com** zur Verfügung. Weitere Informationen finden Sie auch an folgenden Stellen:

- DMTF-Website: **www.dmtf.org/standards/profiles/**
- WS–MAN, Anmerkungen zur Version oder Infodatei.

17

Betriebssystemmithilfe deriVMCLI bereitstellen

Das Befehlszeilendienstprogramm des integrierten virtuellen Datenträgers (iVMCLI) ist eine Befehlszeilenschnittstelle, die die Funktionen des virtuellen Datenträgers von der Management Station zum iDRAC6 im Remote-System bereitstellt. Mit iVMCLI und geskripteten Methoden können Sie das Betriebssystem auf mehreren Remote-Systemen in Ihrem Netzwerk einsetzen.

Dieser Abschnitt enthält Informationen zum Einbinden des iVMCLI-Dienstprogramms in das Unternehmensnetzwerk.

Bevor Sie beginnen

Stellen Sie vor Verwendung des iVMCLI-Dienstprogramms sicher, dass die gewünschten Remote-Systeme und das Unternehmensnetzwerk den in den folgenden Abschnitten aufgeführten Anforderungen entsprechen.

Remote-System-Anforderungen

- iDRAC6 wird in jedem Remote-System konfiguriert.

Netzwerkanforderungen

Eine Netzwerkfreigabe muss die folgenden Komponenten enthalten:

- Betriebssystemdateien
- Erforderliche Treiber
- Start-Imagedatei(en) des Betriebssystems

  Die Imagedatei muss das ISO-Image einer Betriebssystem-CD oder einer CD/DVD mit einem dem Industriestandard entsprechenden startfähigen Format sein.

Startfähige Imagedatei erstellen

Bevor Sie die Imagedatei für die Remote-Systeme bereitstellen, ist sicherzustellen, dass ein unterstütztes System von der Datei gestartet werden kann. Um die Abbilddatei zu überprüfen, übertragen Sie sie unter Verwendung der iDRAC6-Webbenutzerschnittstelle auf ein Testsystem und führen Sie dann einen Neustart des Systems durch.

Die folgenden Abschnitte enthalten spezifische Informationen über das Erstellen von Abbilddateien für Linux- und Windows-Systeme.

Imagedatei für Linux-Systeme erstellen

Verwenden Sie das Datenvervielfältigungs-Dienstprogramm (dd), um eine startfähige Abbilddatei für das Linux-System zu erstellen.

Um das Dienstprogramm auszuführen, öffnen Sie eine Eingabeaufforderung und geben Sie Folgendes ein:

```
dd if=<Eingabegerät> of=<Ausgabedatei>
```

Zum Beispiel:

```
dd if=/dev/sdc0 of=mycd.img
```

Imagedatei für Windows-Systeme erstellen

Achten Sie bei der Auswahl eines Datenreplikator-Dienstprogramms für Windows-Imagedateien darauf, dass es sich um ein Dienstprogramm handelt, welches die Imagedatei und die CD/DVD-Startsektoren kopiert.

Vorbereitung auf die Bereitstellung

Remote-Systeme konfigurieren

1. Erstellen Sie eine Netzwerkfreigabe, auf die über die Management Station zugegriffen werden kann.
2. Kopieren Sie die Betriebssystemdateien zur Netzwerkfreigabe.
3. Wenn Sie über eine startfähige, vorkonfigurierte Imagedatei zur Bereitstellung des Betriebssystems an die Remote-Systeme verfügen, können Sie diesen Schritt überspringen.

Wenn Sie über keine startfähige, vorkonfigurierte Imagedatei verfügen, erstellen Sie die Datei. Schließen Sie alle für die Betriebssystem-Bereitstellungsverfahren zu verwendenden Programme und/oder Skripte ein.

Um z. B. ein Windows-Betriebssystem bereitzustellen, kann die Abbilddatei Programme enthalten, die den von Microsoft Systems Management Server (SMS) verwendeten Bereitstellungsmethoden ähnlich sind.

Wenn Sie die Imagedatei erstellen, gehen Sie wie folgt vor:

- Befolgen Sie die netzwerkbasierten Standardinstallationsverfahren.
- Kennzeichnen Sie das Bereitstellungsabbild als „schreibgeschützt“, um sicherzustellen, dass jedes Zielsystem startet und dasselbe Bereitstellungsverfahren ausführt.

4 Führen Sie eines der folgenden Verfahren aus:

- Integrieren Sie **IPMItool** und die Befehlszeilenschnittstelle des virtuellen Datenträgers (iVMCLI) in die bestehende Bereitstellungsanwendung Ihres Betriebssystems. Verwenden Sie das Beispielskript **ivmdeploy** als Orientierungshilfe beim Verwenden des Dienstprogramms.
- Verwenden Sie das vorhandene **ivmdeploy**-Skript, um das Betriebssystem bereitzustellen.

ANMERKUNG: ivmdeploy verwendet intern iVMCLI und ipmitool. Sie müssen über die Berechtigung *IPMI über LAN* verfügen, um dieses Hilfsprogramm zu verwenden. Der virtuelle Datenträger muss sich außerdem im verbundenen Zustand befinden, wenn das Skript ivmdeploy verwendet wird.

Betriebssystem bereitstellen

Verwenden Sie das iVMCLI-Dienstprogramm und das im Dienstprogramm enthaltene Skript **ivmdeploy**, um das Betriebssystem auf den Remote-Systemen bereitzustellen.

Sehen Sie sich, bevor Sie beginnen, das Beispielskript **ivmdeploy** an, das im iVMCLI-Dienstprogramm enthalten ist. Das Skript führt die detaillierten Schritte an, die zur Bereitstellung des Betriebssystems an Remote-Systemen im Netzwerk erforderlich sind.

Das folgende Verfahren enthält eine allgemeine Übersicht zur Bereitstellung des Betriebssystems auf Remote-Zielsystemen.

1. Listen Sie die iDRAC6-IP-Adressen der Remote-Systeme auf, die in der Textdatei **ip.txt** bereitgestellt werden (eine IP-Adresse pro Zeile).
2. Legen Sie eine startfähige Betriebssystem-CD oder -DVD in das Laufwerk des Client-Datenträgers ein.
3. Führen Sie an der Befehlszeile **ivmdeploy** aus.

Geben Sie zum Ausführen des ivmdeploy-Skripts den folgenden Befehl an der Befehlszeile ein:

```
ivmdeploy -r ip.txt -u <iDRAC-Benutzer> -p
<iDRAC-Kennwort> -c {<ISO9660-Abbild> | <Pfad>}
```

wobei

- <*iDRAC-Benutzer*> der iDRAC6-Benutzername ist – z. B. **root**
- <*iDRAC-Kennwort*> das Kennwort für den iDRAC6-Benutzer ist – z. B. **calvin**
- <*iso9660-Img*> ist der Pfad zu einem ISO9660-Image der Betriebssystem-Installations-CD-ROM oder -DVD
- <*Pfad*> der Pfad zu dem Gerät ist, das die Betriebssystem-Installations-CD-ROM oder -DVD enthält

Das Skript **ivmdeploy** leitet seine Befehlszeilenoptionen an das Dienstprogramm **iVMCLI** weiter. Einzelheiten zu diesen Optionen finden Sie unter „Befehlszeilenoptionen“ auf Seite 362. Das Skript verarbeitet die Option **-r** etwas anders als die Option **iVMCLI -r**. Wenn das Argument der Option **-r** der Name einer vorhandenen Datei ist, liest das Skript iDRAC6-IP-Adressen aus der festgelegten Datei und führt das Dienstprogramm **iVMCLI** einmal pro Zeile aus. Wenn das Argument der Option **-r** kein Dateiname ist, muss es die Adresse eines einzelnen iDRAC6 sein. In diesem Fall arbeitet die Option **-r** wie für das Dienstprogramm **iVMCLI** beschrieben.

Das ivmdeploy-Skript unterstützt die Installation nur von CD/DVD oder einem CD/DVD-ISO9660-Abbild. Wenn Sie die Installation über eine Diskette oder ein Diskettenabbild vornehmen müssen, können Sie das Skript zur Verwendung der Option **iVMCLI -f** modifizieren.

Befehlszeilendienstprogramm des virtuellen Datenträgers verwenden

Das Befehlszeilendienstprogramm des virtuellen Datenträgers (iVMCLI) ist eine skriptfähige Befehlszeilenschnittstelle, die die Funktionen des virtuellen Datenträgers von der Management Station zum iDRAC6 bereitstellt.

Das Dienstprogramm iVMCLI bietet folgende Funktionen:

ANMERKUNG: 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.

- Wechseldatenträgergeräte oder Imagedateien, die mit den Plugins des virtuellen Datenträgers übereinstimmen
- Automatisches Beenden, wenn die Einmal-Starten-Option der iDRAC6-Firmware aktiviert ist.
- Sichere Datenübertragung zum iDRAC6 mittels SSL-Verschlüsselung.

Stellen Sie vor dem Ausführen des Dienstprogramms sicher, dass Sie für den iDRAC6 über Benutzerberechtigungen des virtuellen Datenträgers verfügen.

VORSICHTSHINWEIS: Es wird empfohlen, beim Starten des iVMCLI-Befehlszeilendienstprogramms die interaktive Flag-Option „-i" zu benutzen. So stellen Sie eine höhere Sicherheit durch die Geheimhaltung des Benutzernamens und des Kennworts sicher, denn auf vielen Windows- und Linux-Betriebssystemen sind Benutzername und Kennwort in reinem Text sichtbar, wenn Prozesse von anderen Benutzern untersucht werden.

Wenn das Betriebssystem Administratorberechtigungen oder eine betriebssystemspezifische Berechtigung oder Gruppenmitgliedschaft unterstützt, sind Administratorberechtigungen auch zum Ausführen des iVMCLI-Befehls erforderlich.

Der Administrator des Client-Systems steuert Benutzergruppen und -berechtigungen und somit auch die Benutzer, die das Dienstprogramm ausführen können.

Auf Windows-Systemen müssen Sie über Hauptbenutzerberechtigungen verfügen, um das iVMCLI-Dienstprogramm auszuführen.

Auf Linux-Systemen können Sie ohne Administratorberechtigungen auf das iVMCLI-Dienstprogramm zugreifen, indem Sie den Befehl **sudo** verwenden. Dieser Befehl ist ein zentrales Mittel zur Bereitstellung von Nicht-Administrator-Zugriff und protokolliert alle Benutzerbefehle.

Um Benutzer in der iVMCLI-Gruppe hinzuzufügen oder zu bearbeiten, verwendet der Administrator den Befehl **visudo**. Benutzer ohne Administratorberechtigungen können den Befehl **sudo** der iVMCLI-Befehlszeile (oder dem iVMCLI-Skript) als Präfix hinzufügen, um Zugriff auf den iDRAC6 im Remote-System zu erhalten und das Dienstprogramm auszuführen.

iVMCLI-Dienstprogramm installieren

Das iVMCLI-Dienstprogramm befindet sich auf der DVD *Dell Systems Management Tools and Documentation*, die im Dell OpenManage System Management-Softwarepaket enthalten ist. Legen Sie zum Installieren des Dienstprogramms die DVD in das System ein und folgen Sie den Anweisungen auf dem Bildschirm.

Die DVD *Dell Systems Management Tools and Documentation* enthält die neuesten Softwareprodukte zur Systemverwaltung, einschließlich Diagnose, Speicherverwaltung, Remote-Zugriffsdienst und RACADM-Dienstprogramm. Diese DVD enthält auch Infodateien mit den neuesten Produktinformationen über die Systems Management Software.

Darüber hinaus enthält die DVD *Dell Systems Management Tools and Documentation* das Beispielskript **ivmdeploy**, das veranschaulicht, wie die iVMCLI- und RACADM-Dienstprogramme zum Bereitstellen von Software für mehrere Remote-Systeme verwendet werden.

ANMERKUNG: Das ivmdeploy-Skript hängt bei seiner Installation von den anderen, in seinem Verzeichnis vorhandenen Dateien ab. Wenn Sie das Skript von einem anderen Verzeichnis aus verwenden möchten, müssen Sie alle Dateien mitkopieren.

Befehlszeilenoptionen

Die iVMCLI-Schnittstelle ist sowohl auf Windows- als auch auf Linux-Systemen identisch. Das Dienstprogramm verwendet Optionen, die mit den RACADM-Dienstprogramm-Optionen übereinstimmen. Eine Option zur Angabe der iDRAC6-IP-Adresse erfordert beispielsweise dieselbe Syntax für das RACADM- und das iVMCLI-Dienstprogramm.

Das iVMCLI-Befehlsformat sieht folgendermaßen aus:

`iVMCLI [Parameter] [Betriebssystem_Shell-Optionen]`

Bei der Befehlszeilensyntax wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter „iVMCLI-Parameter“ auf Seite 363.

Wenn das Remote-System die Befehle akzeptiert und der iDRAC6 die Verbindung genehmigt, wird der Befehl weiterhin ausgeführt, bis eine der folgenden Situationen eintritt:

- Die iVMCLI-Verbindung wird aus einem beliebigen Grund abgebrochen.
- Der Prozess wird mit einer Betriebssystemsteuerung manuell abgebrochen. Beispiel: In Windows können Sie den Task-Manager verwenden, um das Verfahren abzubrechen.

ANMERKUNG: Wenn Sie den iVMCLI-Befehl verwenden und die Parameterwerte Leerzeichen zwischen Worten enthalten, müssen Sie für den gesamten Parameterwert Anführungszeichen verwenden. Betrachten Sie z. B. den Befehl zum Hinzufügen eines DVD-Abbildes von Ihrem System zum Betriebssystem auf dem Server:
F:\idrac>ivmcli -r 10.35.155.117 -u root -p calvin -c c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso

wobei -c hier einer der Parameter und **c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso** der Parameterwert ist, der Leerzeichen für ‘Dokumente und Einstellungen’ und ‘Meine Dokumente’ enthält. Aus diesem Grund werden für den gesamten Pfad der Abbilddatei Anführungszeichen verwendet. Ohne Anführungszeichen schlägt der Befehl fehl. Folgendes ist ebenfalls ungültig:

C:\“Dokumente und Einstellungen”\.....

iVMCLI-Parameter

iDRAC6-IP-Adresse

`-r <iDRAC-IP-Adresse>[:<iDRAC-SSL-Anschluss>]`

Dieser Parameter gibt die iDRAC6-IP-Adresse und den SSL-Anschluss an, die das Dienstprogramm zum Herstellen einer Verbindung des virtuellen Datenträgers zum Ziel-iDRAC6 benötigt. Wenn Sie eine ungültige IP-Adresse oder einen ungültigen DDNS-Namen eingeben, wird eine Fehlermeldung angezeigt, und der Befehl wird beendet.

<*iDRAC-IP-Adresse*> ist eine gültige, eindeutige IP-Adresse oder der iDRAC6-DDNS-Name (Dynamisches Domänennamensystem), falls unterstützt. Wenn <*iDRAC-SSL-Anschluss*> ausgelassen wird, wird der Anschluss 443 (Standard-Anschluss) verwendet. Solange der iDRAC6-Standard-SSL-Anschluss nicht geändert wird, ist der optionale SSL-Anschluss nicht erforderlich.

iDRAC6-Benutzername

`-u <iDRAC-Benutzername>`

Dieser Parameter gibt den iDRAC6-Benutzernamen an, der den virtuellen Datenträger ausführen wird.

Der <*iDRAC-Benutzername*> muss die folgenden Attribute aufweisen:

- Gültiger Benutzername
- iDRAC6-Benutzerberechtigung für den virtuellen Datenträger

Wenn die iDRAC6-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.

iDRAC6-Benutzerkennwort

`-p <iDRAC-Benutzerkennwort>`

Dieser Parameter gibt das Kennwort für den angegebenen iDRAC6-Benutzer an.

Wenn die iDRAC6-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.

Disketten-/Festplattengerät oder Imagedatei

`-f {<Gerätename> | <Abbilddatei>}`

wobei <*Gerätename*> ein gültiger Laufwerkbuchstabe (bei Windows-Systemen) oder ein gültiger Gerätekomponentenname ist, einschließlich der Partitionsnummer des bereitstellbaren Dateisystems, falls zutreffend (bei Linux-Systemen), und wobei <*Abbilddatei*> der Dateiname und Pfad einer gültigen Abbilddatei ist.

Dieser Parameter bestimmt das Gerät oder die Datei, das/die den virtuellen Disketten-/Festplatten-Datenträger liefert.

Beispiel: Eine Imagedatei wird wie folgt angegeben:

`-f c:\temp\myfloppy.img` (Windows-System)

`-f /tmp/myfloppy.img` (Linux-System)

Wenn die Datei nicht schreibgeschützt ist, kann der virtuelle Datenträger in die Imagedatei schreiben. Konfigurieren Sie das Betriebssystem so, dass eine Disketten-Imagedatei, die nicht überschrieben werden soll, mit einem Schreibschutz versehen wird.

Beispiel: Ein Gerät wird wie folgt angegeben:

`-f a:\` (Windows-System)

`-f /dev/sdb4 # 4th partition on device /dev/sdb` (Linux-System)

Wenn das Gerät eine Schreibschutzoption anbietet, können Sie diese verwenden, um sicherzustellen, dass der virtuelle Datenträger nicht auf den Datenträger schreibt.

Lassen Sie diesen Parameter aus der Befehlszeile aus, wenn Sie keine Disketten-Datenträger virtualisieren. Wenn ein ungültiger Wert festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl wird abgebrochen.

CD/DVD-Gerät oder -Imagedatei

`-c {<`*Gerätename*`> | <`*Imagedatei*`>}`

wobei <*Gerätename*> ein gültiger CD/DVD-Laufwerkbuchstabe (bei Windows-Systemen) oder ein gültiger CD/DVD-Gerätedateiname (bei Linux-Systemen) und <*Imagedatei*> der Dateiname und Pfad einer gültigen ISO-9660-Imagedatei ist.

Dieser Parameter legt das Gerät oder die Datei fest, die den virtuellen CD/DVD-ROM-Datenträger unterstützen:

Beispiel: Eine Imagedatei wird wie folgt angegeben:

`-c c:\temp\mydvd.img` (Windows-Systeme)

`-c /tmp/mydvd.img` (Linux-Systeme)

Beispiel: Ein Gerät wird wie folgt angegeben:

`-c d:\` (Windows-Systeme)

`-c /dev/cdrom` (Linux-Systeme)

Lassen Sie diesen Parameter aus der Befehlszeile aus, wenn Sie keine CD/DVD-Datenträger virtualisieren. Wenn ein ungültiger Wert festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl bricht ab.

Geben Sie mit dem Befehl mindestens einen Datenträgertyp (Disketten- oder CD/DVD-Laufwerk) an, es sei denn, es werden nur Switch-Optionen vorgegeben. Andernfalls wird eine Fehlermeldung angezeigt und der Befehl wird mit einem Fehler abgebrochen.

Stamm-CA-Zertifikatüberprüfung

`-s`

Dieser Parameter wird dazu verwendet, anzuzeigen, ob das iDRAC-CA-Zertifikat gültig ist. Ist das Zertifikat ungültig, wird die iVMCLI-Sitzung beendet und eine Fehlermeldung ausgegeben, die anzeigt, dass das Zertifikat ungültig ist. Ist das Zertifikat gültig, wird die iVMCLI-Sitzung eingerichtet.

Versionsanzeige

`-v`

Dieser Parameter wird zur Anzeige der iVMCLI-Dienstprogrammversion verwendet. Wenn keine anderen Nicht-Switch-Optionen geboten werden, wird der Befehl ohne Fehlermeldung abgebrochen.

Hilfeanzeige

`-h`

Dieser Parameter zeigt eine Zusammenfassung der iVMCLI-Dienstprogrammparameter an. Wenn keine anderen Nicht-Switch-Optionen bereitgestellt werden, wird der Befehl ohne Fehlermeldung abgebrochen.

Manuelle Anzeige

`-m`

Dieser Parameter zeigt eine detaillierte „man-Seite“ für das iVMCLI-Dienstprogramm an, einschließlich Beschreibungen aller möglicher Optionen.

Verschlüsselte Daten

`-e`

Wenn dieser Parameter in der Befehlszeile enthalten ist, verwendet die iVMCLI einen SSL-verschlüsselten Kanal zur Übertragung von Daten zwischen der Management Station und dem iDRAC6 im Remote-System. Wenn dieser Parameter nicht in der Befehlszeile enthalten ist, wird die Datenübertragung nicht verschlüsselt.

iVMCLI-Optionen der Betriebssystem-Shell

Die folgenden Betriebssystemfunktionen können in der iVMCLI-Befehlszeile verwendet werden:

- stderr/stdout-Umleitung - leitet jede gedruckte Dienstprogrammausgabe zu einer Datei um.

  Bei Verwendung des „größer als"-Zeichens (>), gefolgt von einem Dateinamen, wird z. B. die angegebene Datei mit der gedruckten Ausgabe des iVMCLI-Dienstprogramms überschrieben.

  ANMERKUNG: Das iVMCLI-Dienstprogramm liest nicht von der Standardeingabe (**stdin**). Infolgedessen ist keine **stdin**-Umleitung erforderlich.

- Ausführung im Hintergrund - Standardmäßig wird das iVMCLI-Dienstprogramm im Vordergrund ausgeführt. Verwenden Sie die Shell-Funktionen des Betriebssystems, um zu veranlassen, dass das Dienstprogramm im Hintergrund ausgeführt wird. Unter einem Linux-Betriebssystem wird z. B. durch das auf den Befehl folgende Et-Zeichen (&) veranlasst, dass das Programm als neuer Hintergrundprozess gestartet wird.

Diese letztere Methode ist bei Skriptprogrammen nützlich, da dem Skript nach dem Starten eines neuen Vorgangs für den iVMCLI-Befehl ermöglicht wird, fortzufahren (andernfalls würde das Skript blockieren, bis das iVMCLI-Programm beendet ist). Wenn auf diese Weise mehrere iVMCLI-Instanzen gestartet werden und eine oder mehrere Befehlsinstanzen manuell beendet werden müssen, sind die betriebssystemspezifischen Funktionen zum Auflisten und Beenden von Verfahren zu verwenden.

iVMCLI-Rückgabecodes

0 = Kein Fehler

1 = Kann keine Verbindung herstellen

2 = Fehler in der iVMCLI-Befehlszeile

3 = RAC-Firmware-Verbindung abgebrochen

Immer wenn Fehler auftreten, werden neben der Standardfehlerausgabe auch Textmeldungen auf Englisch ausgegeben.

18

iDRAC6-Konfigurationshilfsprogramm verwenden

Übersicht

Das iDRAC6-Konfigurationshilfsprogramm ist eine Vorstart-Konfigurationsumgebung, die es ermöglicht, Parameter für den iDRAC6 und das verwaltete System anzuzeigen und einzustellen. Genauer gesagt können Sie:

- Die Firmware-Revisionsnummern für die Firmware des iDRAC6 und der primären Rückwandplatine anzeigen
- Das lokale Netzwerk (LAN) des iDRAC6 konfigurieren, aktivieren oder deaktivieren
- IPMI über LAN aktivieren oder deaktivieren
- LAN-Parameter konfigurieren
- Systemdienste aktivieren, deaktivieren oder abbrechen
- Autom. Ermittlung aktivieren oder deaktivieren und den Bereitstellungsserver konfigurieren.
- Virtuelle Mediengeräte verbinden oder trennen
- vFlash aktivieren oder deaktivieren.
- Smart Card-Anmeldung und Einmalanmeldung (SSO) aktivieren oder deaktivieren.
- Systemdienste konfigurieren
- Den administrativen Benutzernamen bzw. das administrative Kennwort ändern
- Die iDRAC6-Konfiguration auf die Werkseinstellungen zurücksetzen
- SEL-Meldungen (Systemereignisprotokoll) anzeigen oder Meldungen aus dem Protokoll löschen

Die Tasks, die Sie unter Verwendung des iDRAC6-Konfigurationshilfsprogramms ausführen können, können auch mittels anderer Dienstprogramme ausgeführt werden, die vom iDRAC6 oder durch die Dell OpenManage-Software zur Verfügung gestellt werden, einschließlich Webschnittstelle, SM-CLP-Befehlszeilenschnittstelle, Befehlszeilenschnittstelle des lokalen und Remote-RACADM und, im Falle einer einfachen Netzwerkkonfiguration, bei iDRAC6-LCD während der erstmaligen iDRAC6-Konfiguration.

iDRAC6-Konfigurationshilfsprogramm starten

Zum ersten Zugriff auf das iDRAC6-Konfigurationshilfsprogramm oder nach dem Zurücksetzen des iDRAC6 auf die Standardeinstellungen müssen Sie eine iDRAC6-Virtuelle Konsole verwenden.

1. Drücken Sie auf der Tastatur, die mit der iDRAC6-Virtuelle Konsole verbunden ist, auf <Druck>, um das Menü iDRAC6-Virtuelle **Konsole-Onscreen-Konfiguration und -Berichterstattung (OSCAR)** anzuzeigen. Verwenden Sie die Taste <Nach oben> und <Nach unten>, um den Steckplatz zu markieren, der den Server enthält, und drücken Sie dann auf <Eingabe>.
2. Schalten Sie den Server ein oder starten Sie ihn neu, indem Sie an seiner Vorderseite den Netzschalter drücken.
3. Wenn die Meldung `<Strg-E> für Remote-Zugriff-Setup innerhalb von 5 Sek. drücken...` eingeblendet wird, drücken Sie umgehend auf <Strg><E>. Das iDRAC6-Konfigurationshilfsprogramm wird angezeigt.

ANMERKUNG: Wenn das Betriebssystem zu laden beginnt, bevor Sie auf <Strg><E> drücken, lassen Sie das System den Startvorgang beenden, starten Sie dann den Server erneut und wiederholen Sie den Vorgang.

Die ersten beiden Zeilen des Konfigurationsdienstprogramms enthalten Informationen über die iDRAC6-Firmware und über Firmware-Revisionen der primären Rückwandplatine. Die Revisionsangaben können nützlich sein, wenn Sie bestimmen möchten, ob ein Firmware-Upgrade erforderlich ist.

Die iDRAC6-Firmware ist der Teil der Firmware, der für externe Schnittstellen zuständig ist, wie z. B. für die Webschnittstelle, SM-CLP und Webschnittstellen. Die Firmware der primären Rückwandplatine ist der Teil der Firmware, der mit der Server-Hardwareumgebung in Verbindung steht und sie überwacht.

iDRAC6-Konfigurationshilfsprogramm verwenden

Unterhalb der Firmware-Revisionsmeldungen besteht der Rest des iDRAC6-Konfigurationshilfsprogramms aus einem Menü von Elementen, auf die Sie über die Nach oben- und Nach unten-Pfeiltasten zugreifen können.

- Wenn ein Menüelement zu einem Untermenü oder einem bearbeitbaren Textfeld führt, drücken Sie die Eingabetaste, um auf das Element zuzugreifen, und die Taste <Esc>, um es zu verlassen, wenn Sie es fertig konfiguriert haben.
- Wenn ein Element auswählbare Werte besitzt, wie **Ja/Nein** oder **Aktiviert/Deaktiviert**, drücken Sie die Nach links- oder Nach rechts-Pfeiltasten oder die Leertaste, um einen Wert auszuwählen.
- Kann ein Element nicht bearbeitet werden, wird es blau angezeigt. Einige Elemente werden abhängig von einer anderen Auswahl bearbeitbar.
- In der unteren Zeile des Bildschirms werden Anleitungen zum aktuellen Element angezeigt. Sie können <F1> drücken, um bzgl. des aktuellen Elements Hilfe anzuzeigen.
- Wenn Sie mit der Verwendung des iDRAC6-Konfigurationshilfsprogramms fertig sind, drücken Sie <Esc>, um das Menü Beenden anzuzeigen. Wählen Sie dort, ob Sie Ihre Änderungen speichern oder verwerfen oder ob Sie zum Dienstprogramm zurückkehren möchten.

In den folgenden Abschnitten werden die Menüelemente des iDRAC6-Konfigurationshilfsprogramms beschrieben.

iDRAC6-LAN

Mit den Nach links- und Nach rechts-Pfeiltasten und der Leertaste wählen Sie zwischen **Ein** und **Aus**.

Das iDRAC6-LAN ist in der Standardkonfiguration deaktiviert. Das LAN muss aktiviert sein, damit die Verwendung der iDRAC6-Einrichtungen zulässig ist, wie z. B. Webschnittstelle, Telnet-/SSH-Zugriff auf die SM-CLP-Befehlszeilenschnittstelle, virtuelle Konsole und virtueller Datenträger.

Wenn Sie wählen, das LAN zu deaktivieren, wird die folgende Warnung angezeigt:

```
iDRAC-bandexterne Schnittstelle wird deaktiviert,
wenn der LAN-Kanal AUS ist.
```

Die Meldung informiert Sie darüber, dass zusätzlich zu den Einrichtungen, auf die Sie über die direkte Verbindung zu den iDRAC6-HTTP-, HTTPS-, Telnet- oder SSH-Anschlüssen zugreifen, der bandexterne Verwaltungsnetzwerk-Datenverkehr, wie z. B. von einer Management Station aus zum iDRAC6 gesendete IPMI-Meldungen, nicht empfangen werden kann, wenn das LAN deaktiviert ist. Die Schnittstelle des lokalen RACADM bleibt verfügbar und kann zur Neukonfiguration des iDRAC6-LAN verwendet werden.

Drücken Sie auf eine beliebige Taste, um die Meldung zu löschen und fortzufahren.

IPMI über LAN

Drücken Sie zum Auswählen zwischen **Ein** und **Aus** auf die Pfeile <Nach links> oder <Nach rechts> oder auf die <Leertaste>. Wenn **Aus** ausgewählt ist, akzeptiert der iDRAC6 keine IPMI-Meldungen, die über die LAN-Schnittstelle eingehen.

Wenn Sie **Aus** auswählen, wird eine Warnmeldung angezeigt.

Drücken Sie auf eine beliebige Taste, um die Meldung zu löschen und fortzufahren. Erläuterungen zu dieser Meldung finden Sie unter „iDRAC6-LAN“ auf Seite 372.

LAN-Parameter

Drücken Sie die Eingabetaste, um das Untermenü der LAN-Parameter anzuzeigen. Wenn Sie die Konfiguration der LAN-Parameter abgeschlossen haben, drücken Sie <Esc>, um zum vorhergehenden Menü zurückzukehren.

Tabelle 18-1. LAN-Parameter

Element	Beschreibung
Allgemeine Einstellungen	
MAC-Adresse	Dies ist die nicht bearbeitbare MAC-Adresse der iDRAC6-Netzwerkschnittstelle.
VLAN aktivieren	Zeigt **Ein/Aus** an. **Ein** aktiviert die Filterung des virtuellen LAN für iDRAC6.
VLAN ID	Zeigt einen beliebigen VLAN-ID-Wert zwischen 1 und 4094 an.
VLAN	Zeigt die Priorität des VLAN zwischen 0 und 7 an.
iDRAC6-Namen registrieren	Wählen Sie **Ein** aus, um den iDRAC6-Namen im DNS-Dienst zu registrieren. Wählen Sie **Aus** aus, wenn Sie nicht möchten, dass Benutzer den iDRAC6-Namen im DNS auffinden.
iDRAC6-Name	Wenn **iDRAC-Name registrieren** auf **Ein** eingestellt ist, drücken Sie die Eingabetaste, um das Textfeld **Aktueller DNS-iDRAC-Name** zu bearbeiten. Drücken Sie die Eingabetaste, wenn Sie den iDRAC6-Namen fertig bearbeitet haben. Drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln. Der iDRAC6-Name muss ein gültiger DNS-Host-Name sein.
Domänenname von DHCP	Wählen Sie **Ein**, wenn Sie den Domänennamen von einem DHCP-Dienst auf dem Netzwerk abrufen möchten. Wählen Sie **Aus**, wenn Sie den Domänennamen festlegen möchten.
Domänenname	Wenn **Domänenname von DHCP Aus** ist, drücken Sie die Eingabetaste, um das Textfeld **Aktueller Domänenname** zu bearbeiten. Drücken Sie die Eingabetaste, wenn Sie mit der Bearbeitung fertig sind. Drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln. Der Domänenname muss sich auf eine gültige DNS-Domäne beziehen, z. B. `meinefirma.com`.
Zeichenkette des Host-Namens	Drücken Sie zur Bearbeitung die Eingabetaste. Geben Sie den Namen des Host für PET-Warnhinweise ein.

Tabelle 18-1. LAN-Parameter *(fortgesetzt)*

Element	Beschreibung
LAN-Warnung aktiviert	Wählen Sie **Ein**, um den PET LAN-Warnhinweis zu aktivieren.
Warnungsregel, Eintrag 1	Wählen Sie **Aktivieren** oder **Deaktivieren** aus, um das erste Warnungsziel zu aktivieren.
Warnungsziel 1	Wenn **LAN-Warnung aktiviert** auf **Ein** gesetzt ist, geben Sie die IP-Adresse ein, zu der PET LAN-Warnhinweise weitergeleitet werden.
IPv4-Einstellungen	Aktivieren oder deaktivieren Sie die Unterstützung der IPv4-Verbindung.
IPv4	Wählen Sie für IPv4-Protokollunterstützung **Aktiviert** oder **Deaktiviert.** Die Standardeinstellung ist aktiviert.
Verschlüsselungsschlüssel RMCP+	Drücken Sie die Eingabetaste, um den Wert zu bearbeiten, und <Esc>, wenn Sie den Vorgang abgeschlossen haben. Der Verschlüsselungsschlüssel RMCP+ ist eine aus 40 Zeichen bestehende hexadezimale Zeichenkette (Zeichen 0-9, a-f und A-F). RMCP+ ist eine IPMI-Erweiterung, die Authentifizierung und Verschlüsselung zur IPMI hinzufügt. Der Standardwert ist eine aus 40 Nullen bestehende Zeichenkette.
IP-Adressen-Quelle	Wählen Sie zwischen **DHCP** und **Statisch** aus. Wenn DHCP ausgewählt ist, werden die Felder **Ethernet-IP-Adresse**, **Subnetzmaske** und **Standard-Gateway** von einem DHCP-Server abgerufen. Wenn im Netzwerk kein DHCP-Server gefunden wird, werden die Felder auf Null gesetzt. Wenn **Statisch** ausgewählt ist, werden die Elemente **Ethernet-IP-Adresse**, **Subnetzmaske** und **Standard-Gateway** bearbeitbar.
Ethernet-IP-Adresse	Wenn die **IP-Adressenquelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse ein, die dem iDRAC6 zugewiesen werden soll. Die Standardadresse ist 192.168.0.120.

Tabelle 18-1. LAN-Parameter *(fortgesetzt)*

Element	Beschreibung
Subnetzmaske	Wenn die **IP-Adressenquelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene Subnetzmaskenadresse an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die Subnetzmaske für den iDRAC6 ein. Der Standardwert ist **255.255.255.0**.
Standard-Gateway	Wenn die **IP-Adressenquelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse des Standard-Gateways an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse des Standard-Gateways ein. Die Standardeinstellung ist **192.168.0.1.**
DNS-Server von DHCP	Wählen Sie **Ein**, um DNS-Server-Adressen von einem DHCP-Dienst im Netzwerk abzurufen. Wählen Sie **Aus**, um die unten stehenden DNS-Server-Adressen zu bestimmen.
DNS-Server 1	Wenn **DNS-Server von DHCP** auf **Aus** gesetzt ist, geben Sie die IP-Adresse des ersten DNS-Servers ein.
DNS-Server 2	Wenn **DNS-Server von DHCP Aus** ist, geben Sie die IP-Adresse des zweiten DNS-Servers ein.
IPv6-Einstellungen:	
IPv6	Aktivieren oder deaktivieren Sie die Unterstützung für die IPv6-Verbindung.
IPv6-Adressenquelle	Wählen Sie zwischen **AutoConfig** und **Statisch** aus. Wenn **AutoConfig** ausgewählt ist, werden die Felder **IPv6-Adresse 1**, **Präfixlänge** und **Standard-Gateway** vom DHCP abgerufen. Ist **Statisch** ausgewählt, können die Einträge **IPv6-Adresse 1**, **Präfixlänge** und **Standard-Gateway** bearbeitet werden.
IPv6-Adresse 1	Wenn die **IP-Adressenquelle** auf **AutoConfig** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse ein, die dem iDRAC6 zugewiesen werden soll.

Tabelle 18-1. LAN-Parameter *(fortgesetzt)*

Element	Beschreibung
Präfixlänge	Konfiguriert die Präfixlänge der IPv6-Adresse. Es kann ein Wert im Bereich von 1 bis 128 sein.
Standard-Gateway	Wenn die **IP-Adressenquelle** auf **AutoConfig** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse des Standard-Gateways an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse des Standard-Gateways ein.
IPv6-Link-Local-Adresse	Dies ist die nicht bearbeitbare **IPv6-Link-Local-Adresse** der iDRAC6-Netzwerkschnittstelle.
IPv6-Adresse 2-15	Dies ist die nicht bearbeitbare **IPv6-Adresse 2...IPv6-Adresse 15** der iDRAC6-Netzwerkschnittstelle.
DNS-Server von DHCPv6	Wählen Sie **Ein**, um DNS-Server-Adressen von einem DHCP-Dienst im Netzwerk abzurufen. Wählen Sie **Aus**, um die unten stehenden DNS-Server-Adressen zu bestimmen.
DNS-Server 1	Wenn **DNS-Server von DHCP** auf **Aus** gesetzt ist, geben Sie die IP-Adresse des ersten DNS-Servers ein.
DNS-Server 2	Wenn **DNS-Server von DHCP Aus** ist, geben Sie die IP-Adresse des zweiten DNS-Servers ein.

Konfiguration virtueller Laufwerke

Virtueller Datenträger

Verwenden Sie die Tasten <Nach links> und <Nach rechts>, um **Automatisch verbunden**, **Verbunden** oder **Abgetrennt** auszuwählen.

- Wenn Sie **Verbunden** auswählen, werden die virtuellen Datenträgergeräte mit dem USB-Bus verbunden. Hierdurch werden sie während **Virtuelle Konsole**-Sitzungen zur Verwendung verfügbar gemacht.
- Wenn Sie **Abgetrennt** auswählen, können Benutzer während **Virtuelle Konsole**-Sitzungen nicht auf virtuelle Datenträgergeräte zugreifen.
- Wenn Sie **Automatisch verbunden** auswählen, werden die Geräte des virtuellen Datenträgers automatisch mit dem Server verbunden, wenn eine Virtuelle Datenträger-Sitzung gestartet wird.

ANMERKUNG: Um ein USB-Flashlaufwerk mit der Funktion Virtuelle Datenträger zu verwenden, muss der **Emulationstyp des USB-Flashlaufwerks** im BIOS-Setup-Dienstprogramm auf **Festplatte** eingestellt sein. Sie können auf das BIOS-Setup-Dienstprogramm zugreifen, indem Sie während des Serverstarts auf <F2> drücken. Wenn der **Emulationstyp des USB-Flashlaufwerks** auf **Automatisch** eingestellt ist, wird das Flashlaufwerk dem System als Diskettenlaufwerk angezeigt.

vFlash

Verwenden Sie die Tasten <Nach links> und <Nach rechts>, um **Aktiviert** oder **Deaktiviert** auszuwählen.

- **Aktiviert –** vFlash steht für die Partitionsverwaltung zur Verfügung.
- **Deaktiviert –** vFlash steht für die Partitionsverwaltung nicht zur Verfügung.

VORSICHTSHINWEIS: vFlash kann nicht deaktiviert werden, wenn eine oder mehrere Partitionen verbunden sind oder sich in Verwendung befinden.

vFlash initialisieren

Wählen Sie diese Option aus, um die vFlash-Karte zu initialisieren. Durch den Initialisierungsvorgang werden vorhandene Daten auf der SD-Karte gelöscht und alle vorhandenen Partitionen werden entfernt. Sie können keinen Initialisierungsvorgang ausführen, wenn eine oder mehrere Partitionen verbunden sind oder sich in Verwendung befinden. Diese Option steht nur zur Verfügung, wenn sich im iDRAC Enterprise-Kartensteckplatz eine Karte befindet, die größer als 256 MB ist und wenn vFlash aktiviert ist.

Drücken Sie die Eingabetaste, um die vFlash-SD-Karte zu initialisieren.

Der Initialisierungsvorgang kann aus folgenden Gründen fehlschlagen:

- SD-Karte ist momentan nicht vorhanden.
- vFlash is currently in use by another process.
- vFlash ist nicht aktiviert.
- Die SD-Karte ist schreibgeschützt.
- Eine oder mehrere Partitionen sind momentan in Gebrauch.
- Eine oder mehrere Partitionen sind momentan verbunden.

vFlash-Eigenschaften

Drücken Sie die Eingabetaste, um die folgenden Eigenschaften der vFlash-SD-Karte anzuzeigen:

- **Name** – Zeigt den Namen der vFlash-SD-Karte an, die in den vFlash-SD-Kartensteckplatz des Servers eingelegt ist. Wenn es sich dabei um eine SD-Karte von Dell handelt, wird vFlash-SD-Karte angezeigt. Wenn es sich um eine SD-Karte handelt, die nicht von Dell ist, wird SD-Karte angezeigt.
- **Größe** – Zeigt die Größe der vFlash-SD-Karte in Gigabyte (GB) an.
- **Verfügbarer Speicherplatz** – Zeigt den unverbrauchten Speicherplatz auf der vFlash-SD-Karte in Megabyte (MB) an. Dieser Speicherplatz ist verfügbar, um weitere Partitionen auf der vFlash-SD-Karte zu erstellen. Für SD-Karten wird der verfügbare Speicherplatz mit 256 MB angezeigt.
- **Schreibgeschützt** - Zeigt an, ob die vFlash-SD-Karte schreibgeschützt ist oder nicht.
- **Funktionszustand** – Zeigt den allgemeinen Funktionszustand der vFlash-SD-Karte an. Dieser kann lauten:
  - OK
  - Warnung
  - Kritisch

Drücken Sie die <Esc>-Taste, um den Vorgang zu beenden.

Smart Card/SSO

Diese Option konfiguriert die Funktionen **Smart Card-Anmeldung** und **Einmalige Anmeldung (SSO)**. Die vorhandenen Optionen lauten **Aktiviert** und **Deaktiviert**.

ANMERKUNG: Wenn Sie die Funktion **Einmalige Anmeldung (SSO)** aktivieren, ist die Funktion **Smart Card-Anmeldung** deaktiviert.

System Services (Systemdienste)

System Services (Systemdienste)

Verwenden Sie die Tasten <Nach links> und <Nach rechts>, um **Aktiviert** oder **Deaktiviert** auszuwählen. Wenn aktiviert, können bestimmte iDRAC6-Funktionen mithilfe des Lifecycle-Controllers konfiguriert werden. Weitere Informationen finden Sie im *Lifecycle Controller-Benutzerhandbuch*, das auf der Dell Support-Website unter **dell.com/support/manuals** zur Verfügung steht.

ANMERKUNG: Durch Änderung dieser Option wird der Server neu gestartet, wenn Sie auf **Speichern** und **Beenden** klicken, um die neuen Einstellungen anzuwenden.

Systemdienste abbrechen

Verwenden Sie die Tasten <Nach oben> und <Nach unten>, um **Ja** oder **Nein** auszuwählen.

Wenn Sie **Ja** auswählen, werden alle Lifecycle Controller-Sitzungen geschlossen, und der Server wird neu gestartet, wenn Sie auf **Speichern** und **Beenden** klicken, um die neuen Einstellungen anzuwenden.

Systeminventar beim Neustart erfassen

Wählen Sie **Aktiviert** aus, um die Inventarerfassung während des Startvorgangs zuzulassen. Weitere Informationen finden Sie im *Dell Lifecycle Controller-Benutzerhandbuch*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

ANMERKUNG: Eine Änderung dieser Option führt zu einem Neustart des Servers, nachdem Sie Ihre Einstellungen gespeichert und das iDRAC6-Konfigurationsdienstprogramm verlassen haben.

LAN-Benutzerkonfiguration

Der LAN-Benutzer ist das iDRAC6-Administratorkonto, das standardmäßig **root** ist. Drücken Sie <Eingabe>, um das Untermenü der LAN-Benutzerkonfiguration anzuzeigen. Wenn Sie die Konfiguration des LAN-Benutzers abgeschlossen haben, drücken Sie <Esc>, um zum vorhergehenden Menü zurückzukehren.

Tabelle 18-2. Seite LAN-Benutzerkonfiguration

Element	Beschreibung
AutoErmittlung	Die Funktion AutoErmittlung ermöglicht die automatisierte Ermittlung nicht bereitgestellter Systeme im Netzwerk; sie richtet außerdem auf *sichere* Weise erste Anmeldeinformationen ein, sodass diese ermittelten Systeme verwaltet werden können. Diese Funktion ermöglicht dem iDRAC6, den Bereitstellungsserver ausfindig zu machen. iDRAC6 und der Bereitstellungsdienstserver authentifizieren sich gegenseitig. Der Remote-Bereitstellungsserver sendet die Anmeldeinformationen des Benutzers, sodass der iDRAC6 mit diesen Anmeldeinformationen ein Benutzerkonto einrichten kann. Sobald das Benutzerkonto eingerichtet ist, kann eine Remote-Konsole unter Verwendung der im Ermittlungsprozess angegebenen Anmeldeinformationen eine WSMAN-Verbindung zum iDRAC6 herstellen und die sicheren Anweisungen dann an den iDRAC6 senden, um ein Betriebssystem im Remote-Zugriff bereitzustellen. Weitere Informationen zur Remote-Bereitstellung von Betriebssystemen finden Sie im *Dell Lifecycle Controller-Benutzerhandbuch*, das auf der Dell Support-Website unter **dell.com/support/manuals** zur Verfügung steht. Führen Sie im Voraus die folgenden Maßnahmen in einer *gesonderten* Sitzung des **iDRAC6-Konfigurationshilfsprogramms** aus, *bevor Sie die Autom. Ermittlung manuell aktivieren*: • NIC aktivieren (Blade-Server) • IPv4 aktivieren (Blade-Server) • DHCP aktivieren • Domänenname vom DHCP abrufen • Admin-Konto deaktivieren (Konto Nr. 2) • DNS-Serveradresse vom DHCP abrufen • DNS-Domänenname vom DHCP abrufen Wählen Sie **Aktiviert** aus, um die Funktion AutoErmittlung zu aktivieren. Standardmäßig ist diese Funktion **deaktiviert**. Wenn Sie ein Dell-System bestellt haben, auf dem Autom. Ermittlung **aktiviert** ist, wird der iDRAC6 auf dem Dell-System mit aktiviertem DHCP und ohne standardmäßige Anmeldeinformationen für die Remote-Anmeldung versandt.

Tabelle 18-2. Seite LAN-Benutzerkonfiguration *(fortgesetzt)*

Element	Beschreibung
AutoErmittlung *(Fortsetzung ...)*	Vor dem Hinzufügen des Dell-Systems zum Netzwerk und dem Verwenden der Autom. Ermittlung ist Folgendes sicherzustellen: • DHCP-Server (Dynamisches Host-Konfigurationsprotokoll)/ DNS (Domänennamensystem) sind konfiguriert. • Bereitstellungs-Webdienste sind installiert, konfiguriert und registriert.
Bereitstellungsserver	Über dieses Feld können Sie den Bereitstellungsserver konfigurieren. Die Adresse des Bereitstellungsservers kann eine Kombination aus IPv4-Adressen oder Hostnamen sein und sollte eine Länge von 255 Zeichen nicht überschreiten. Die Adressen bzw. Hostnamen sollten jeweils durch ein Komma voneinander getrennt sein. Wenn Sie die Funktion AutoErmittlung aktiviert haben, werden Benutzer-Anmeldeinformationen vom konfigurierten Bereitstellungsserver abgerufen, sodass nach erfolgreichem Abschluss des Vorgangs AutoErmittlung zukünftig eine Remote-Bereitstellung möglich ist. Weitere Informationen finden Sie im *Dell Lifecycle Controller-Benutzerhandbuch*, das auf der Dell Support-Website unter **dell.com/support/manuals** zur Verfügung steht.
Kontozugriff	Wählen Sie **Aktiviert** aus, um das Administratorkonto zu aktivieren. Wählen Sie **Deaktiviert** aus, um das Administratorkonto zu deaktivieren oder wenn AutoErmittlung aktiviert ist.
IPMI-LAN-Berechtigung	Wählen Sie zwischen **Admin**, **Benutzer**, **Operator** und **Kein Zugriff** aus.
Kontobenutzername	Drücken Sie <Eingabe>, um den Benutzernamen zu bearbeiten, und dann <Esc>, wenn Sie den Vorgang beendet haben. Die Standardeinstellung für Benutzername ist **Stamm**.
Kennwort eingeben	Geben Sie das neue Kennwort für das Administratorkonto ein. Die Zeichen werden während der Eingabe nicht auf der Anzeige wiedergegeben.

Tabelle 18-2. Seite LAN-Benutzerkonfiguration *(fortgesetzt)*

Element	Beschreibung
Kennwort bestätigen	Geben Sie das neue Kennwort für das Administratorkonto erneut ein. Wenn die eingegebenen Zeichen nicht mit den im Feld **Kennwort eingeben** eingegebenen Zeichen übereinstimmen, wird eine Meldung angezeigt und das Kennwort muss erneut eingegeben werden.

Auf Standardeinstellung zurücksetzen

Verwenden Sie das Menüelement **Auf Standardeinstellung zurücksetzen**, um alle iDRAC6-Konfigurationselemente auf die Werkseinstellungen zurückzusetzen. Dies kann eventuell dann erforderlich sein, wenn Sie das Kennwort des administrativen Benutzers vergessen haben oder den iDRAC6 von den Standardeinstellungen aus neu konfigurieren möchten.

ANMERKUNG: In der Standardkonfiguration ist der iDRAC6-Netzwerkbetrieb deaktiviert. Sie können den iDRAC6 erst dann über das Netzwerk neu konfigurieren, wenn Sie das iDRAC6-Netzwerk im iDRAC6-Konfigurationshilfsprogramm aktiviert haben.

Drücken Sie <Eingabe>, um das Element auszuwählen. Die folgende Warnmeldung wird angezeigt:

```
Durch das Zurücksetzen auf die Werkseinstellungen
werden die nichtflüchtigen Remote-
Benutzereinstellungen wiederhergestellt. Vorgang
fortsetzen?

< NEIN (Abbrechen) >

< JA (Fortfahren) >
```

Wählen Sie zum Zurücksetzen des iDRAC6 auf die Standardeinstellungen **JA** aus und drücken Sie auf <Eingabe>.

Wenn dieser Vorgang fehlschlägt, wird eine der folgenden Fehlermeldungen angezeigt:

- Reset-Befehl war nicht erfolgreich. Versuchen Sie es bitte später – iDRAC ist ausgelastet.
- Einstellungen konnten nicht auf ihre Standardwerte zurückgesetzt werden – Zeitüberschreitung.
- Reset-Befehl konnte nicht gesendet werden. Versuchen Sie es bitte später – iDRAC ist ausgelastet.

Menü des Systemereignisprotokolls

Das Menü **Systemereignisprotokoll** ermöglicht Ihnen, Meldungen des Systemereignisprotokolls (SEL) anzuzeigen und die Protokollmeldungen zu löschen. Drücken Sie <Eingabe>, um das **Systemereignisprotokoll-Menü** anzuzeigen. Das System zählt die Protokolleinträge und zeigt dann die Gesamtanzahl von Einträgen sowie die jüngste Meldung an. Das SEL speichert maximal 512 Meldungen.

Um SEL-Meldungen anzuzeigen, wählen Sie **Systemereignisprotokoll anzeigen** aus und drücken Sie auf <Eingabe>. Zum Navigieren:

- Verwenden Sie die Pfeiltaste <Nach links>, um die vorherige (ältere) Nachricht anzuzeigen, und die Pfeiltaste <Nach rechts>, um die nächste (neuere) Nachricht anzuzeigen.
- Geben Sie eine spezifische Datensatznummer an, um zu diesem Datensatz zu wechseln.

Drücken Sie zum Beenden des Systemereignisprotokolls auf <Esc>.

ANMERKUNG: Das SEL kann nur im iDRAC6-Konfigurationshilfsprogramm oder in der iDRAC6-Webschnittstelle gelöscht werden.

Wählen Sie zum Löschen des SEL **Systemereignisprotokoll löschen** aus und drücken Sie die Eingabetaste.

Wenn Sie mit der Verwendung des SEL-Menüs fertig sind, drücken Sie <Esc>, um zum vorhergehenden Menü zurückzukehren.

iDRAC6-Konfigurationshilfsprogramm beenden

Wenn Sie mit den Änderungen der iDRAC6-Konfiguration fertig sind, drücken Sie auf die Taste <Esc>, um das Menü Beenden anzuzeigen.

- Wählen Sie **Änderungen speichern** und beenden aus und drücken Sie dann auf <Eingabe>, um Ihre Änderungen beizubehalten. Wenn dieser Vorgang fehlschlägt, wird eine der folgenden Meldungen angezeigt:
  - iDRAC6 Kommunikationsfehler - Wird angezeigt, wenn nicht auf iDRAC zugegriffen werden kann.
  - Einige der Einstellungen können nicht angewendet werden - Wird angezeigt, wenn einige Einstellungen nicht angewendet werden können.

- Wählen Sie **Änderungen ablehnen und beenden** aus und drücken Sie <Eingabe>, um alle vorgenommenen Änderungen zu ignorieren.
- Wählen Sie **Zu Setup zurückkehren** aus und drücken Sie die Eingabetaste, um zum iDRAC6-Konfigurationshilfsprogramm zurückzukehren.

19

Wiederherstellung und Fehlerbehebung beim verwalteten System

In diesem Abschnitt wird erklärt, wie Tasks bezüglich der Diagnose und Fehlerbehebung eines im Remote-Zugriff verwalteten Servers mithilfe von iDRAC6-Dienstprogrammen ausgeführt werden. Er enthält die folgenden Unterabschnitte:

- Problemanzeigen - hilft, Meldungen und andere Systemanzeigen zu finden, die zu einer Problemdiagnose führen können
- Hilfsprogramme zur Problemlösung - beschreibt iDRAC6-Hilfsprogramme, die Sie zur Fehlerbehebung des Systems verwenden können
- Fehlerbehebung und häufig gestellte Fragen - Antworten auf typische Situationen, die Ihnen unterlaufen könnten.

Sicherheit geht vor – für Sie und Ihr System

Für bestimmte in diesem Abschnitt beschriebene Verfahren müssen Sie am Gehäuse, am Dell PowerEdge™-System oder anderen Hardwaremodulen arbeiten. Versuchen Sie nicht, an der Hardware des Systems zu arbeiten, es sei denn, Sie befolgen die Erklärungen in diesem Handbuch und an anderer Stelle in der Systemdokumentation.

VORSICHTSHINWEIS: Manche Reparaturarbeiten dürfen nur von qualifizierten Servicetechnikern durchgeführt werden. 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.

Problemanzeigen

In diesem Abschnitt werden die Anzeichen beschrieben, die auf ein Problem im System hinweisen können.

LED-Anzeigen

LEDs am Gehäuse oder an den im System installierten Komponenten sind in der Regel die ersten Anzeichen eines Systemproblems. Die folgenden Komponenten und Module besitzen Status-LEDs:

- Gehäuse-LCD-Anzeige
- Server
- Lüfter
- CMCs
- E/A-Module
- Netzteile

Die einzelne LED des Gehäuse-LCD fasst den Status aller Komponenten im System zusammen. Eine ständig leuchtende blaue LED des LCD zeigt an, dass auf dem System keine Fehlerzustände festgestellt wurden. Eine blinkende gelbe LED des LCD zeigt an, dass ein bzw. mehrere Fehlerzustände festgestellt wurden.

Wenn am Gehäuse-LCD eine gelbe LED blinkt, können Sie über das LCD-Menü herausfinden, welche Komponente fehlerhaft ist. Hilfe zur Verwendung des LCD finden Sie im *Benutzerhandbuch zur Dell Chassis Management Controller-Firmware*.

Tabelle 19-1 beschreibt die Bedeutung der LED-Anzeigen des Dell PowerEdge-Systems:

Tabelle 19-1. Blade-Server-LED-Anzeigen

LED-Anzeige	Bedeutung
ständig grün (*nur für Netzschalter*)	Der Server ist eingeschaltet. Ein Fehlen der grünen LED bedeutet, dass der Server nicht eingeschaltet ist.
ständig blau	Der iDRAC6 funktioniert fehlerfrei.
blinkt gelb	Der iDRAC6 hat einen Fehlerzustand festgestellt oder aktualisiert gerade die Firmware.
blinkt blau	Ein Benutzer hat die Locator-ID für diesen Server aktiviert.

Anzeigen für Hardwareprobleme

Anzeichen dafür, dass bei einem Modul ein Hardwareproblem vorliegt, schließen folgende ein:

- Gerät kann nicht hochgefahren werden
- Laute Lüfter
- Verlust der Netzwerkkonnektivität
- Warnungen zu Batterie, Temperatur, Spannung oder Energieüberwachungssensor
- Festplattenfehler
- Fehler des USB-Datenträgers
- Physischer Schaden durch Fallenlassen, Wasser oder andere äußerliche Einwirkung

Wenn Probleme dieser Art auftreten, stellen Sie den entstandenen Schaden fest und versuchen Sie dann, das Problem folgendermaßen zu beheben:

- Setzen Sie das Modul noch einmal ein und starten Sie es erneut
- Versuchen Sie, das Modul in einem anderen Schacht des Gehäuses einzusetzen
- Versuchen Sie, Festplatten oder USB-Schlüssel auszutauschen
- Schließen Sie die Strom- und Netzwerkkabel erneut an, oder tauschen Sie sie aus

Wenn das Problem mit diesen Schritten nicht behoben werden kann, ziehen Sie das *Hardware-Benutzerhandbuch* zurate, um spezifische Fehlerbehebungsinformationen für das Hardwaregerät zu erhalten.

Weitere Problemanzeigen

Tabelle 19-2. Problemanzeigen

Achten Sie auf Folgendes:	Aktion:
Warnmeldungen der Systemverwaltungssoftware	Weitere Informationen finden Sie in der Dokumentation zur Systemverwaltungssoftware.
Meldungen im Systemereignisprotokoll	Siehe „Systemereignisprotokoll (SEL) überprüfen“ auf Seite 389.

Tabelle 19-2. Problemanzeigen *(fortgesetzt)*

Achten Sie auf Folgendes:	Aktion:
Meldungen der POST-Codes beim Start	Siehe „POST-Codes überprüfen“ auf Seite 391.
Meldungen auf dem Bildschirm Letzter Absturz	Siehe „Bildschirm Letzter Systemabsturz anzeigen“ auf Seite 391.
Alarmmeldungen auf dem Serverstatusbildschirm des LCD	Siehe „Serverstatusbildschirm auf Fehlermeldungen überprüfen“ auf Seite 394.
Meldungen im iDRAC6-Protokoll	Siehe „iDRAC6-Protokoll anzeigen“ auf Seite 404.

Hilfsprogramme zum Lösen von Problemen

In diesem Abschnitt werden iDRAC6-Einrichtungen beschrieben, die Sie zur Diagnose von Problemen auf dem System verwenden können, besonders wenn Probleme im Remote-Zugriff gelöst werden sollen.

- Überprüfen des Systemzustands
- Systemereignisprotokoll auf Fehlermeldungen überprüfen
- POST-Codes überprüfen
- Bildschirm des letzten Systemabsturzes anzeigen
- Die letzten Startsequenzen anzeigen
- Serverstatusbildschirm auf dem LCD auf Fehlermeldungen überprüfen
- iDRAC6-Protokoll anzeigen
- Systeminformationen anzeigen
- Verwalteten Server im Gehäuse identifizieren
- Diagnosekonsole verwenden
- Strom auf einem Remote-System verwalten

Überprüfen des Systemzustands

Wenn Sie sich an der iDRAC6-Webschnittstelle anmelden, zeigt der Bildschirm zur **Systemzusammenfassung** den Funktionszustand der Systemkomponenten an. Tabelle 19-3 beschreibt die Bedeutung der Systemzustandsanzeigen.

Tabelle 19-3. Serverzustandsanzeigen

Anzeige	Beschreibung
	Eine grüne Markierung zeigt eine unproblematische (normale) Statusbedingung an.
	Ein gelbes Dreieck, das ein Ausrufezeichen enthält, zeigt eine (nichtkritische) Warnungs-Statusbedingung an.
	Ein rotes X zeigt eine kritische (Ausfall) Statusbedingung an.
	Ein Fragezeichen-Symbol zeigt an, dass der Status unbekannt ist.

Klicken Sie im Abschnitt **Serverzustand** auf eine beliebige Komponente, um Informationen zur Komponente anzuzeigen. Sensormesswerte werden für Batterien, Temperaturen, Spannungen und Energieüberwachung angezeigt, was bei der Diagnose gewisser Problemtypen hilfreich ist. Die Informationsbildschirme zum iDRAC6 und CMC enthalten nützliche Informationen zum aktuellem Status und zur Konfiguration.

Systemereignisprotokoll (SEL) überprüfen

Auf der Seite **SEL-Protokoll** werden Meldungen zu Ereignissen angezeigt, die auf dem verwalteten Server auftreten.

Führen Sie zum Anzeigen des **Systemereignisprotokolls** folgende Schritte aus:

1. Klicken Sie auf **System** und dann auf das Register **Protokolle**.
2. Klicken Sie auf **Systemereignisprotokoll**, um die Seite **Systemereignisprotokoll** anzuzeigen.

   Die Seite **Systemereignisprotokoll** blendet eine Systemzustandsanzeige (siehe Tabelle 19-3), einen Zeitstempel sowie eine Beschreibung des Ereignisses ein.
3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Systemereignisprotokoll**, um fortzufahren (siehe Tabelle 19-4).

Tabelle 19-4. SEL-Schaltflächen

Schaltfläche	Aktion
Protokoll löschen	Löscht das SEL. **ANMERKUNG:** Die Schaltfläche **Protokoll löschen** wird nur angezeigt, wenn Sie die Berechtigung **Protokolle löschen** besitzen.
Speichern unter	Öffnet ein Popup-Fenster, das es ermöglicht, das SEL in einem Verzeichnis Ihrer Wahl zu speichern. **ANMERKUNG:** Wenn Sie Internet Explorer verwenden und beim Speichern auf ein Problem stoßen, laden Sie die kumulative Sicherheitsaktualisierung für Internet Explorer von der Support-Website von Microsoft unter **support.microsoft.com** herunter. **ANMERKUNG:** Wenn Sie Internet Explorer verwenden und das SEL-Protokoll nicht mit **Speichern unter** speichern können, kann das an einer Browsereinstellung liegen. 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 • Dateien herunterladen **VORSICHTSHINWEIS: Um sicherzustellen, dass der für den Zugriff auf iDRAC verwendete Computer sicher ist, darf die Option *Starten von Applikationen und unsichere Dateien* unter *Verschiedenes* nicht aktiviert sein.**
Erweiterte Einstellungen	Öffnet die Seite **Systemereignisprotokoll – Erweiterte Einstellungen**, auf der Sie die OEM-Ereignisnachrichten von dem im Systemereignisprotokoll (SEL) angezeigten, verwalteten System aktivieren/deaktivieren können. Klicken Sie auf **Anwenden,** um die Einstellung zu übernehmen.

Befehlszeile zum Anzeigen des Systemereignisprotokolls verwenden

Der Befehl lautet:

racadm getsel <Optionen>

Wenn keine Argumente vorgegeben werden, wird das gesamte Protokoll angezeigt.

So zeigen Sie die Anzahl der Einträge im SEL an:

```
racadm getsel-i
```

ANMERKUNG: Weitere Informationen zu den Optionen finden Sie im *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Mit dem Befehl `clrsel` werden alle vorhandenen Aufzeichnungen aus dem SEL entfernt.

```
racadm clrsel
```

POST-Codes überprüfen

Die Seite **POST-Codes** zeigt den letzten POST-Code des Systems vor dem Start des Betriebssystems an. 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.

ANMERKUNG: Den Text für die Nummern der POST-Code-Meldungen finden Sie auf der LCD-Anzeige oder im *Hardwarebenutzerhandbuch*.

Zum Anzeigen der Post-Codes klicken Sie auf **System→ Protokolle→ Post-Code**. Auf dem Bildschirm **Post-Code** wird eine Systemzustandsanzeige (siehe Tabelle 19-3), ein Hexadezimalcode sowie eine Beschreibung des Codes eingeblendet.

Bildschirm Letzter Systemabsturz anzeigen

ANMERKUNG: Die Funktion Bildschirm Letzter Absturz muss im Server Administrator und in der iDRAC6-Webschnittstelle konfiguriert werden. Anleitungen zum Konfigurieren dieser Funktion finden Sie unter „Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz“ auf Seite 86.

Auf der Seite **Bildschirm Letzter Absturz** wird der letzte Absturzbildschirm mit Informationen über die Ereignisse vor dem Systemabsturz angezeigt. Das Bild des letzten Systemabsturzes wird im Dauerspeicher des iDRAC6

gespeichert und steht per Remote-Zugriff zur Verfügung. Der Bildschirm zum letzten Absturz ist auch dann verfügbar, wenn iDRAC zurückgesetzt wird, da der Bildschirm im NVRAM gespeichert ist.

Um den **Bildschirm Letzter Absturz** anzuzeigen, klicken Sie auf **System→ Protokolle→ Bildschirm Letzter Absturz**. Im Bildschirm **Bildschirm Letzter Absturz** wird der zuletzt gespeicherte Absturzbildschirm angezeigt.

Klicken Sie auf **Speichern**, um den Bildschirm Letzter Absturz in einem Verzeichnis Ihrer Wahl zu speichern.

Klicken Sie auf **Löschen**, um den Bildschirm Letzter Absturz zu löschen.

ANMERKUNG: Die Schaltflächen **Speichern** und **Löschen** werden nicht angezeigt, wenn kein gespeicherter Absturzbildschirm vorhanden ist.

ANMERKUNG: Aufgrund von Schwankungen im Zeitgeber für Autom. Wiederherstellung kann der **Bildschirm Letzter Absturz** eventuell nicht erfasst werden, wenn der System-Reset-Zeitgeber mit einem zu hohen Wert konfiguriert ist. Die Standardeinstellung ist 480 Sekunden. Stellen Sie den System-Reset-Zeitgeber mit dem Server Administrator oder IT Assistant auf 60 Sekunden ein, und stellen Sie sicher, dass der **Bildschirm Letzter Absturz** korrekt funktioniert. Weitere Informationen hierzu finden Sie unter „Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz“ auf Seite 86.

Die letzten Startsequenzen anzeigen

Wenn Sie Startprobleme feststellen, können Sie sich die Bildschirmaktivität der Geschehnisse während der letzten drei Startsequenzen auf der Seite **Systemstartprotokoll** anzeigen lassen. Die Wiedergabe der Startbildschirme tritt mit einer Rate von 1 Frame pro Sekunde auf. iDRAC6 zeichnet zum Zeitpunkt des Starts 50 Frames auf. Wenn iDRAC zurückgesetzt wird, ist das Systemstartvideo nicht mehr verfügbar, da dieses im RAM gespeichert und beim Zurücksetzen von iDRAC gelöscht wird.

Tabelle 19-5 führt die verfügbaren Steuerungsmaßnahmen auf.

ANMERKUNG: Sie müssen über Administratorberechtigungen verfügen, um die Wiedergabe der Systemstartprotokoll-Sequenzen anzuzeigen.

Tabelle 19-5. Systemstartprotokoll-Optionen

Schaltfläche/Option	Beschreibung
Startreihenfolge auswählen	Ermöglicht die Auswahl der Startreihenfolge zum Laden und Abspielen. • Systemstartprotokoll 1 — Lädt die letzte Startsequenz. • Systemstartprotokoll 2 — Lädt die (vorletzte) Startsequenz, die vor dem Systemstartprotokoll 1 aufgetreten ist. • Systemstartprotokoll 3 — Lädt die (drittletzte) Startsequenz, die vor dem Systemstartprotokoll 2 aufgetreten ist.
Speichern unter	Erstellt eine komprimierte .zip-Datei, die alle Systemstartprotokollbilder der aktuellen Sequenz enthält. Der Benutzer muss über Administratorberechtigungen verfügen, um diese Maßnahme durchzuführen.
Vorhergehender Bildschirm	Bringt Sie zum vorhergehenden Bildschirm in der Wiedergabekonsole, falls vorhanden.
Wiedergabe	Startet die Bildschirmwiedergabe vom aktuellen Bildschirm in der Wiedergabekonsole.
Pause (Anhalten)	Hält die Bildschirmwiedergabe auf dem aktuellen in der Wiedergabekonsole angezeigten Bildschirm an.
Beenden	Beendet die Bildschirmwiedergabe und lädt den ersten Bildschirm dieser Startsequenz.
Nächster Bildschirm	Bringt Sie zum nächsten Bildschirm in der Wiedergabekonsole, falls vorhanden.
Drucken	Druckt das Systemstartprotokollbild, das auf dem Bildschirm angezeigt wird.
Refresh (Aktualisieren)	Lädt die Seite Systemstartprotokoll neu.

Arbeitnotizen anzeigen und hinzufügen

Auf der Seite **Arbeitsnotizen** werden die im Lifecycle-Protokoll gespeichert en Arbeitsnotizeinträge angezeigt. Zum Anzeigen der Seite **Arbeitsnotizen** erweitern Sie die Struktur unter **System**, und klicken Sie auf **Systeme→ Protokolle→ Arbeitsnotizen**.

Die für die einzelnen Arbeitsnotizeinträge aufgezeichneten Zeitstempel und die Inhalte der Arbeitsnotizen werden angezeigt. Das Zeitstempelformat lautet JJJJ/MM/TT/hh:mm:ss, basierend auf dem 24-Stunden-Zeitsystem.

Jeder bei iDRAC angemeldete Benutzer kann dem Protokoll Arbeitsnotizen hinzufügen. Jede neue Arbeitsnotiz darf aus maximal 50 Zeichen bestehen. Klicken Sie auf **Speichern**, um dem Protokoll die Notiz hinzuzufügen.

ANMERKUNG: Sie können bestimmte Sonderzeichen außer „<" und „&". Wenn Sie diese Zeichen benutzen, können Sie die Arbeitsnotiz nicht speichern.

ANMERKUNG: Zum Hinzufügen von Arbeitsnotizen müssen Sie über eine Anmeldeberechtigung für iDRAC verfügen. Unter „iDRAC6-Benutzer hinzufügen und konfigurieren" auf Seite 104 finden Sie Hilfeanleitungen zum Konfigurieren von Benutzerberechtigungen.

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. In der folgenden Tabelle werden alle Fehlermeldungen sowie die Schweregrade der Fehler aufgeführt.

Tabelle 19-6. Serverstatus-Bildschirm

Schweregrad	Meldung	Ursache
Warnung	Umgebungstemperatur der Systemplatine: Temperatursensor für Systemplatine, Warnungsereignis	Umgebungstemperatur des Servers hat einen Warnungsschwellenwert überschritten
Kritisch	Umgebungstemperatur der Systemplatine: Temperatursensor für Systemplatine, Fehlerereignis	Umgebungstemperatur des Servers hat einen Fehlerschwellenwert überschritten
Kritisch	CMOS-Batterie der Systemplatine: Batteriesensor der Systemplatine, Ausfall bestätigt	CMOS-Batterie nicht vorhanden oder weist keine Spannung auf

Tabelle 19-6. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Warnung	Systemebene der Systemplatine: Stromsensor für Systemplatine, Warnungsereignis	Strom hat eine Warnungsschwelle überschritten
Kritisch	Systemebene der Systemplatine: Stromsensor für Systemplatine, Fehlerereignis	Strom hat eine Fehlerschwelle überschritten
Kritisch	CPU<Nummer> <Name des Spannungssensors>: Spannungssensor für CPU<Nummer>, bestätigter Zustand wurde bestätigt	Spannung außerhalb des Bereichs
Kritisch	Systemplatine <Name des Spannungssensors>: Spannungssensor für Systemplatine, bestätigter Zustand wurde bestätigt	Spannung außerhalb des Bereichs
Kritisch	CPU<Nummer> <Name des Spannungssensors>: Spannungssensor für CPU<Nummer>, bestätigter Zustand wurde bestätigt	Spannung außerhalb des Bereichs
Kritisch	CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, IERR wurde bestätigt	CPU-Fehler
Kritisch	CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, thermische Auslösung wurde bestätigt	CPU überhitzt
Kritisch	CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, Konfigurationsfehler wurde bestätigt	Falscher Prozessortyp oder an falschem Ort

Tabelle 19-6. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, Bestätigung des Vorhandenseins wurde aufgehoben	Erforderliche CPU fehlt oder ist nicht vorhanden.
Kritisch	Video-Riser-Karte der Systemplatine: Modulsensor der Systemplatine, Entfernen des Geräts wurde bestätigt	Erforderliches Modul wurde entfernt
Kritisch	Mezz B<Steckplatznummer> Status: Add-In-Kartensensor für Mezz B<Steckplatznummer>, Installationsfehler wurde bestätigt	Falsche Mezzanine-Karte für E/A-Architektur installiert
Kritisch	Mezz C<Steckplatznummer> Status: Add-In-Kartensensor für Mezz C<Steckplatznummer>, Installationsfehler wurde bestätigt	Falsche Mezzanine-Karte für E/A-Architektur installiert
Kritisch	Rückwandplatine, Laufwerk <Nummer>: Laufwerksteckplatzsensor für Rückwandplatine, Laufwerk entfernt	Speicherlaufwerk wurde entfernt
Kritisch	Rückwandplatine, Laufwerk <Nummer>: Laufwerksteckplatzsensor für Rückwandplatine, Laufwerkfehler wurde bestätigt	Speicherlaufwerk fehlerhaft
Kritisch	Systemplatine, PFault störsicher: Spannungssensor für Systemplatine, bestätigter Zustand wurde bestätigt	Dieses Ereignis wird erstellt, wenn sich die Systemplatinenspannungen nicht im normalen Bereich befinden.

Tabelle 19-6. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, abgelaufener Zeitgeber wurde bestätigt	Der iDRAC6-Watchdog-Zeitgeber ist abgelaufen und es wurde keine Maßnahme festgelegt.
Kritisch	Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, Neustart wurde bestätigt	Der iDRAC6-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist) und die Maßnahme wurde auf Neustart festgelegt.
Kritisch	Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, Ausschalten des Stroms wurde bestätigt	Der iDRAC6-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist) und die Maßnahme wurde auf Ausschalten gesetzt.
Kritisch	Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, Aus- und Einschalten des Stroms wurde bestätigt	Der iDRAC6-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist) und die Maßnahme wurde auf Aus- und Einschalten gesetzt.
Kritisch	Systemplatinen-SEL: Ereignisprotokollsensor für Systemplatine, volles Protokoll wurde bestätigt	Das SEL-Gerät stellt fest, dass dem SEL nur ein Eintrag hinzugefügt werden kann, bevor es voll ist.
Warnung	ECC, korr. Fehl.: Speichersensor, korrigierbarer ECC (<DIMM-Position>) wurde bestätigt	Korrigierbare ECC-Fehler haben eine kritische Rate erreicht.

Tabelle 19-6. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	ECC, nicht korrigierbarer Fehler: Speichersensor, nicht korrigierbarer ECC (<DIMM-Position>) wurde bestätigt	Ein nicht korrigierbarer ECC-Fehler wurde festgestellt.
Kritisch	E/A-Kanalüberprüfung: Sensor für kritische Ereignisse, E/A-Kanalüberprüfungs-NMI wurde bestätigt	Im E/A-Kanal wird eine kritische Unterbrechung generiert.
Kritisch	PCI-Paritätsfehler: Sensor für kritische Ereignisse, PCI PERR wurde bestätigt	Auf dem PCI-Bus wurde ein Paritätsfehler festgestellt.
Kritisch	PCI-Systemfehler: Sensor für kritische Ereignisse, PCI-SERR (<Steckplatznummer oder PCI-Geräte-ID>) wurde bestätigt	PCI-Fehler durch Gerät festgestellt
Kritisch	SBE-Protokoll deaktiviert: Ereignisprotokollsensor, Deaktivierung der Protokollierung korrigierbarer Speicherfehler wurde bestätigt	Einzelbitfehler-Protokollierung wird deaktiviert, wenn zu viele SBE protokolliert werden
Kritisch	Protokollierung deaktiviert: Ereignisprotokollsensor, Deaktivierung der gesamten Ereignisprotokollierung wurde bestätigt	Die gesamte Fehlerprotokollierung ist deaktiviert
Nicht wiederherstellbar	CPU-Protokollfehler: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt	Das Prozessorprotokoll ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht wiederherstellbar	CPU-Bus-PERR: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt	Der Prozessor-Bus-PERR ist in einen nicht wiederherstellbaren Zustand übergegangen.

Tabelle 19-6. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Nicht wiederherstellbar	CPU-Initialisierungsfehler: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt	Die Prozessorinitialisierung ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht wiederherstellbar	CPU-Maschinenüberprüfung: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt	Die Prozessormaschinenüberprüfung ist in einen nicht wiederherstellbaren Zustand übergegangen.
Kritisch	Speicher reserviert: Speichersensor, Redundanz verloren (<DIMM-Position>) wurde bestätigt	Speicherreserve ist nicht mehr redundant.
Kritisch	Speicher gespiegelt: Speichersensor, Redundanz verloren (<DIMM-Position>) wurde bestätigt	Gespiegelter Speicher ist nicht mehr redundant.
Kritisch	Speicher-RAID: Speichersensor, Redundanz verloren (<DIMM-Position>) wurde bestätigt	RAID-Speicher ist nicht mehr redundant
Warnung	Speicher hinzugefügt: Speichersensor, Bestätigung des Vorhandenseins (<DIMM-Position>) wurde aufgehoben	Hinzugefügtes Speichermodul wurde entfernt.
Warnung	Speicher entfernt: Speichersensor, Bestätigung des Vorhandenseins (<DIMM-Position>) wurde aufgehoben	Speichermodul wurde entfernt.
Kritisch	Speicherkonfigurationsfehler: Speichersensor, Konfigurationsfehler (<DIMM-Position>) wurde bestätigt	Speicherkonfiguration für das System ist falsch.

Tabelle 19-6. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Warnung	Speicherredundanz-Zunahme: Speichersensor, Redundanz herabgesetzt (<DIMM-Position>) wurde bestätigt	Speicherredundanz ist herabgesetzt, aber nicht verloren
Kritisch	Schwerwiegender PCIE-Fehler: Sensor für kritische Ereignisse, schwerwiegender Busfehler wurde bestätigt	Schwerwiegender Fehler auf dem PCIE-Bus festgestellt.
Kritisch	Chipset-Fehler: Sensor für kritische Ereignisse, PCI-PERR wurde bestätigt	Chip-Fehler wurde festgestellt.
Warnung	Speicher-ECC-Warnung: Speichersensor, Übergang zu nicht kritisch von OK (<DIMM-Position>) wurde bestätigt	Die Rate der korrigierbaren ECC-Fehler geht über eine normale Rate hinaus.
Kritisch	Speicher-ECC-Warnung: Speichersensor, Übergang zu kritisch von weniger schwerwiegend (<DIMM-Position>) wurde bestätigt	Korrigierbare ECC-Fehler haben eine kritische Rate erreicht.
Kritisch	POST-Fehler: POST-Sensor, Kein Speicher installiert	Kein Speicher auf Platine festgestellt
Kritisch	POST-Fehler: POST-Sensor, Speicherkonfigurationsfehler	Speicher wurde erkannt, kann jedoch nicht konfiguriert werden.
Kritisch	POST-Fehler: POST-Sensor, Fehler durch unbrauchbaren Speicher	Speicher wurde konfiguriert, ist jedoch unbrauchbar.
Kritisch	POST-Fehler: POST-Sensor, Shadow-BIOS fehlerhaft	System-BIOS, Shadow-Fehler
Kritisch	POST-Fehler: POST-Sensor, CMOS fehlerhaft	CMOS-Fehler

Tabelle 19-6. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	POST-Fehler: POST-Sensor, DMA-Controller fehlerhaft	DMA-Controller-Fehler
Kritisch	POST-Fehler: POST-Sensor, Unterbrechungs-Controller fehlerhaft	Unterbrechungs-Controller-Fehler
Kritisch	POST-Fehler: POST-Sensor, Zeitgeberaktualisierung fehlerhaft	Fehler bei der Zeitgeberaktualisierung
Kritisch	POST-Fehler: POST-Sensor, Fehler bei programmierbarem Intervallzeitgeber	Fehler beim programmierbaren Intervallzeitgeber
Kritisch	POST-Fehler: POST-Sensor, Paritätsfehler	Paritätsfehler
Kritisch	POST-Fehler: POST-Sensor, SIO fehlerhaft	SIO-Fehler
Kritisch	POST-Fehler: POST-Sensor, Tastatur-Controller fehlerhaft	Keyboard controller failure
Kritisch	POST-Fehler: POST-Sensor, Unterbrechungsinitialisierung der Systemverwaltung fehlerhaft	Initialisierungsfehler bei Systemverwaltungsunterbrechung
Kritisch	POST-Fehler: POST-Sensor, Test zum Herunterfahren des BIOS fehlerhaft	Fehler beim BIOS-Herunterfahren-Test
Kritisch	POST-Fehler: POST-Sensor, BIOS-POST-Speichertest fehlerhaft	BIOS-POST-Speicherüberprüfungsfehler
Kritisch	POST-Fehler: POST-Sensor, Konfiguration des Dell Remote Access Controllers fehlerhaft	Konfigurationsfehler bei Dell Remote Access Controller
Kritisch	POST-Fehler: POST-Sensor, CPU-Konfiguration fehlerhaft	CPU-Konfigurationsfehler
Kritisch	POST-Fehler: POST-Sensor, Falsche Speicherkonfiguration	Falsche Speicherkonfiguration

Tabelle 19-6. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	POST-Fehler: POST-Sensor, POST-Fehler	Allgemeiner Fehler nach Video
Kritisch	Hardwareversions-Fehler: Sensor für Versionsänderung, Hardware-Inkompatibilität wurde bestätigt	Inkompatible Hardware wurde festgestellt
Kritisch	Hardwareversions-Fehler: Sensor für Versionsänderung, Hardware-Inkompatibilität (BMC-Firmware) wurde bestätigt	Hardware ist inkompatibel mit Firmware
Kritisch	Hardwareversions-Fehler: Sensor für Versionsänderung, Hardware-Inkompatibilität (BMC-Firmware und CPU-Übereinstimmungsfehler) wurde bestätigt	CPU und Firmware nicht kompatibel
Kritisch	Speicherübertemperatur: Speichersensor, korrigierbarer ECC <DIMM-Position> wurde bestätigt	Überhitzung des Speichermoduls
Kritisch	Speicher, SB-CRC schwerwiegend: Speichersensor, nicht korrigierbarer ECC wurde bestätigt	Southbridge-Speicher fehlerhaft
Kritisch	Speicher, NB-CRC schwerwiegend: Speichersensor, nicht korrigierbarer ECC wurde bestätigt	Northbridge-Speicher fehlerhaft
Kritisch	Watchdog-Zeitgeber: Watchdog-Sensor, Neustart wurde bestätigt	Watchdog-Zeitgeber verursachte Systemneustart
Kritisch	Watchdog-Zeitgeber: Watchdog-Sensor, Ablaufen des Zeitgebers wurde bestätigt	Watchdog-Zeitgeber abgelaufen, jedoch keine Maßnahme ergriffen

Tabelle 19-6. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Warnung	Link-Tuning: Sensor für Versionsänderung, Bestätigung der erfolgreichen Software- oder F/W-Änderung wurde aufgehoben	Link-Tuning-Einstellung für ordnungsgemäßen NIC-Betrieb konnte nicht aktualisiert werden
Warnung	Link-Tuning: Sensor für Versionsänderung, Bestätigung der erfolgreichen Hardwareänderung <Gerätesteckplatznummer> wurde aufgehoben	Link-Tuning-Einstellung für ordnungsgemäßen NIC-Betrieb konnte nicht aktualisiert werden
Kritisch	Link-T/Flex-Adr: Link-Tuning-Sensor, Bestätigung, dass die virtuelle MAC-Adresse (Bus-Nr. Geräte-Nr. Funktions-Nr.) nicht programmiert werden konnte	Flex-Adresse konnte für dieses Gerät nicht programmiert werden
Kritisch	Link-T/Flex-Adr: Link-Tuning-Sensor, Bestätigung, dass Geräte-Options-ROM Link-Tuning oder Flex-Adresse (Mezz <Position>) nicht unterstützen konnte	Options-ROM unterstützt weder Flex-Adresse noch Link-Tuning
Kritisch	Link-T/Flex-Adr: Link-Tuning-Sensor, Bestätigung, dass Daten zu Link-Tuning oder Flex-Adresse nicht vom BMC/iDRAC6 abgerufen werden konnten	Informationen zu Link-Tuning oder Flex-Adresse konnten nicht vom BMC/iDRAC6 abgerufen werden
Kritisch	Link-T/Flex-Adr: Link-Tuning-Sensor, Bestätigung, dass Geräte-Option ROM Link-Tuning oder Flex-Adresse (Mezz XX) nicht unterstützen konnte	Dieses Ereignis wird erstellt, wenn PCI Geräte-Option ROM für eine NIC weder die Link-Tuning- noch die Flex-Adresse-Funktion unterstützt

Tabelle 19-6. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	LinkT/FlexAddr: Link-Tuning-Sensor, Bestätigung, dass die virtuelle MAC-Adresse (<Position>) nicht programmiert werden konnte	Dieses Ereignis wird erstellt, wenn das BIOS die virtuelle MAC-Adresse, die auf dem NIC-Gerät vorgegeben ist, nicht programmieren kann
Kritisch	I/O Fatal Err: Unbehebbarer E/A-Gruppensensor, unbehebbarer E/A-Fehler (<Position>)	Dieses Ereignis wird in Verbindung mit einem CPU-IERR erstellt und zeigt an, welches Gerät diesen CPU-IERR verursacht hat
Warnung	PCIE NonFatal Er: Behebbarer E/A-Gruppensensor, PCIe-Fehler (<Position>)	Dieses Ereignis wird in Verbindung mit einem CPU-IERR erstellt.

iDRAC6-Protokoll anzeigen

Das iDRAC6-**Protokoll** ist ein beständiges Protokoll, das in der iDRAC6-Firmware geführt wird. Das Protokoll enthält eine Liste von Benutzermaßnahmen (wie z. B. An- und Abmelden, Änderungen der Sicherheitsregeln) und Warnungen, die vom iDRAC6 ausgegeben werden. Nach der iDRAC6-Firmware-Aktualisierung wird das Protokoll gelöscht.

Während das **Systemereignisprotokoll** (SEL) Einträge von Ereignissen enthält, die auf dem verwalteten Server auftreten, enthält das iDRAC-**Protokoll** Einträge von Ereignissen, die im iDRAC6 auftreten.

Zum Zugreifen auf das iDRAC6-**Protokoll**, klicken Sie auf **System→ iDRAC-Einstellungen→ Protokolle.** Der Bildschirm **iDRAC6-Protokoll** wird angezeigt. Auf diesem Bildschirm werden die Informationen angezeigt, die in Tabelle 19-7 angezeigt sind.

Tabelle 19-7. iDRAC6-Protokollinformationen

Feld	Beschreibung
Uhrzeit/Datum	Datum und Uhrzeit (z. B. `19. Dez. 16:55:47`). iDRAC6 stellt seine Uhr bei seiner Initialisierung gemäß der Uhr des verwalteten Servers ein. Wenn der verwaltete Server beim Start von iDRAC6 abgeschaltet ist, stellt iDRAC6 seine Uhr gemäß des CMC in dem Gehäuse, in dem sich das Blade befindet, ein. **ANMERKUNG:** Da die Zeitquelle für iDRAC6 je nach Stromzustand des verwalteten Servers (zum Zeitpunkt der iDRAC6-Initialisierung) unterschiedlich ist, muss der verwaltete Server auf die CMC-Zeit eingestellt werden. Wenn die System- bzw. CMC-Zeiten nicht gleich sind, werden in iDRAC6-Protokollen nach den iDRAC-Initialisierungsvorgängen inkonsistente Zeiten gemeldet.
Quelle	Die Schnittstelle, die das Ereignis verursacht hat.
Beschreibung	Eine kurze Beschreibung des Ereignisses und der Name des Benutzers, der sich am iDRAC6 angemeldet hat.

Klicken Sie auf **Protokoll löschen**, um die Protokolleinträge zu löschen. Die Schaltfläche **Protokoll löschen** wird nur angezeigt, wenn Sie über eine Berechtigung zum Löschen von Protokollen verfügen.

Klicken Sie auf **Speichern unter**, um das iDRAC6-Protokoll in einem Verzeichnis Ihrer Wahl zu speichern.

Wenn Sie Internet Explorer verwenden und beim Speichern auf ein Problem stoßen, laden Sie die kumulative Sicherheitsaktualisierung für Internet Explorer von der Support-Website von Microsoft unter **www.support.microsoft.com** herunter. Wenn Sie Internet Explorer verwenden und das iDRAC-Protokoll nicht mit **Speichern unter** speichern können, kann das an einer Browsereinstellung liegen. 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
- Dateien herunterladen

VORSICHTSHINWEIS: Um sicherzustellen, dass der für den Zugriff auf iDRAC verwendete Computer sicher ist, darf die Option *Starten von Applikationen und unsichere Dateien* unter *Verschiedenes* nicht aktiviert sein.

Anzeigen von Systeminformationen

Die Seite **Systemdetails** zeigt Informationen zu den folgenden Systemkomponenten an:

- Hauptsystemgehäuse
- Integrated Dell Remote Access Controller 6 – Enterprise

Klicken Sie zum Zugreifen auf die Systeminformationen auf **System→ Eigenschaften→ Systemdetails**.

Unter „Wiederherstellung und Fehlerbehebung beim verwalteten System“ auf Seite 385 finden Sie Informationen zur Systemzusammenfassung, dem Hauptsystemgehäuse und den iDRAC6.

Verwalteten Server im Gehäuse identifizieren

In das Dell PowerEdge M1000e-Gehäuse können bis zu 16 Server eingebaut werden. Um einen bestimmten Server im Gehäuse ausfindig zu machen, können Sie mit der iDRAC6-Webschnittstelle eine blaue, blinkende LED auf dem Server einschalten. Wenn Sie die LED einschalten, können Sie die Anzahl von Sekunden festlegen, die die LED blinken soll, um sicherzustellen, dass Sie das Gehäuse erreichen können, während die LED noch blinkt. Durch die Eingabe von **0** blinkt die LED, bis Sie sie deaktivieren.

So identifizieren Sie den Server:

1 Klicken Sie auf **System→ iDRAC-Einstellungen→ Fehlerbehebung**.

2 Wählen Sie auf dem Bildschirm **Identifizieren** die Option **Server identifizieren** aus.

3 Geben Sie im Feld **Server-Zeitüberschreitung identifizieren** die Anzahl von Sekunden ein, die die LED blinken soll. Geben Sie **0** ein, wenn die LED blinken soll, bis Sie sie deaktivieren.

4 Klicken Sie auf **Anwenden**.

Eine blaue LED auf dem Server wird während der festgelegten Anzahl von Sekunden blinken.

Wenn Sie **0** eingegeben haben, damit die LED weiterblinkt, führen Sie die folgenden Schritte aus, um Sie zu deaktivieren:

1. Klicken Sie auf **System→ iDRAC-Einstellungen→ Fehlerbehebung**.
2. Heben Sie auf dem Bildschirm **Identifizieren** die Auswahl von **Server identifizieren** auf.
3. Klicken Sie auf **Anwenden**.

Diagnosekonsole verwenden

Der iDRAC6 bietet einen Standardsatz von Netzwerkdiagnose-Hilfsprogrammen (siehe Tabelle 19-8), die den mit Microsoft Windows- oder Linux-basierten Systemen gelieferten Hilfsprogrammen ähnlich sind. Mit der iDRAC6-Webschnittstelle können Sie auf die Hilfsprogramme zum Netzwerk-Debuggen zugreifen.

Klicken Sie auf **iDRAC6 zurücksetzen**, um den iDRAC zurückzusetzen. Auf dem iDRAC wird ein normaler Startvorgang ausgeführt.

Führen Sie zum Zugriff auf die Seite **Diagnosekonsole** folgende Schritte aus:

1. Klicken Sie auf **System→ iDRAC-Einstellungen→ Fehlerbehebung**.
2. Wählen Sie das Register **Diagnosekonsole** aus.

Tabelle 19-8 beschreibt die Befehle, die auf der Seite **Diagnosekonsole** eingegeben werden können. Geben Sie einen Befehl ein und klicken Sie auf **Senden**. Die Debug-Ergebnisse werden auf der Seite **Diagnosekonsole** angezeigt.

Klicken Sie auf die Schaltfläche **Löschen**, um die durch den vorhergehenden Befehl angezeigten Ergebnisse zu löschen.

Klicken Sie zum Aktualisieren der Seite **Diagnosekonsole** auf **Aktualisieren**.

Tabelle 19-8. Diagnosebefehle

Befehl	Beschreibung
arp	Zeigt den Inhalt der Tabelle des Adressauflösungsprotokolls (ARP) an. ARP-Einträge dürfen nicht hinzugefügt oder gelöscht werden.
ifconfig	Zeigt den Inhalt der Netzwerkschnittstellentabelle an.
netstat	Druckt den Inhalt der Routingtabelle aus.

Tabelle 19-8. Diagnosebefehle *(fortgesetzt)*

Befehl	Beschreibung
ping <*IP-Adresse*>	Überprüft, ob die Ziel-IP-Adresse unter Verwendung des Inhalts der aktuellen Routingtabelle vom iDRAC6 aus erreichbar ist. Im Feld rechts von dieser Option muss eine Ziel-IP-Adresse eingegeben werden. Ein ICMP-Echo-Paket (Internet-Steuerungsmeldungsprotokoll) wird basierend auf dem aktuellen Inhalt der Routingtabelle zur Ziel-IP-Adresse gesendet.
ping6 <*IPv6-Adresse*>	Überprüft, ob die Ziel-IPv6-Adresse unter Verwendung des aktuellen Inhalts der Routingtabelle vom iDRAC6 aus erreichbar ist. In das Feld rechts neben dieser Option muss eine Ziel-IPv6-Adresse eingegeben werden. Basierend auf dem aktuellen Inhalt der Routingtabelle wird ein ICMP-Echo-Paket (Internetsteuerungs-Meldungsprotokoll) zur Ziel-IPv6-Adresse gesendet.
traceroute <*IP-Adresse*>	Wird verwendet, um die Route zu bestimmen, der Pakete über ein IP-Netzwerk folgen.
traceroute6 <*IPv6-Adresse*>	Wird verwendet, um die Route zu bestimmen, der Pakete über ein IPv6-Netzwerk folgen.
gettracelog	Zeigt das **iDRAC6-Ablaufverfolgungsprotokoll** an. Weitere Informationen finden Sie unter gettracelog im *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Netzstrom auf einem Remote-System verwalten

Mit dem iDRAC6 können im Remote-Zugriff mehrere Energieverwaltungsmaßnahmen auf dem verwalteten Server durchgeführt werden. Verwenden Sie die Seite **Energieverwaltung**, um während eines Neustarts und beim Ein- und Ausschalten des Systems ein ordentliches Herunterfahren durch das Betriebssystem durchzuführen.

ANMERKUNG: Sie müssen über die Berechtigung **Server-Maßnahmenbefehle ausführen** verfügen, um Energieverwaltungsmaßnahmen ausführen zu können. Unter „iDRAC6-Benutzer hinzufügen und konfigurieren“ auf Seite 104 finden Sie Hilfeanleitungen zum Konfigurieren von Benutzerberechtigungen.

1 Klicken Sie auf **System** und dann auf das Register **Energieverwaltung**→ **Stromsteuerung**.

2 Wählen Sie eine **Stromsteuerungsmaßnahme** aus, z. B. **System zurücksetzen (Softwareneustart)**.

Tabelle 19-9 bietet Informationen zu Stromsteuerungsmaßnahmen

3 Klicken Sie auf **Anwenden**, um die ausgewählte Maßnahme auszuführen.

Tabelle 19-9. Stromsteuerungsmaßnahmen

System einschalten	Schaltet den Systemstrom ein (äquivalent zum Drücken des Netzschalters, wenn der Serverstrom ausgeschaltet ist).
System ausschalten	Schaltet den Systemstrom ein (äquivalent zum Drücken des Netzschalters, wenn der Serverstrom eingeschaltet ist).
NMI (Non-Masking Interrupt, nicht-maskierbare Unterbrechung)	Sendet eine Unterbrechung hoher Stufe an das Betriebssystem, was dazu führt, dass das System den Vorgang unterbricht, um kritische Diagnose- und Fehlerbehebungsaktivitäten zu ermöglichen.
Ordentliches Herunterfahren	Versucht, das Betriebssystem ordentlich herunterzufahren und schaltet dann das System aus. Hierfür ist ein ACPI-fähiges Betriebssystem (Advanced Configuration and Power Interface) erforderlich, das die systemgesteuerte Stromverwaltung ermöglicht. **ANMERKUNG:** Ein ordentliches Herunterfahren des BS des Servers könnte unmöglich sein, wenn die Serversoftware nicht länger reagiert oder wenn Sie nicht als Administrator auf einer lokalen Windows-Konsole angemeldet sind. In dem Fall müssen Sie einen Neustart erzwingen, anstatt eines ordentlichen Herunterfahrens von Windows. Außerdem ist, je nach Version des Windows-BS, womöglich eine Regel bezüglich des Herunterfahrens konfiguriert, die das Herunterfahrverhalten ändert, wenn die Maßnahme vom iDRAC6 ausgelöst wird. Ziehen Sie die Microsoft-Dokumentation zurate, um sich über die Richtlinie „Shutdown: Allow system to be shut down without having to login“ (Herunterfahren: System ohne Anmeldung herunterfahren lassen) zu lokalen Computern zu informieren.

Tabelle 19-9. Stromsteuerungsmaßnahmen *(fortgesetzt)*

System Reset (Softwareneustart)	Startet das System neu, ohne es auszuschalten (Softwareneustart).
System aus- und wieder einschalten (Hardwareneustart)	Schaltet das System aus und startet es dann neu (Hardwareneustart).

Weitere Informationen erhalten Sie unter „Energieüberwachung und Energieverwaltung“ auf Seite 327 .

Fehlerbehebung und häufig gestellte Fragen

Tabelle 19-10 enthält häufig gestellte Fragen zu Problemen bei der Störungsbehebung.

Tabelle 19-10. Häufig gestellte Fragen/Fehlerbehebung

Frage	Antwort
Die LED auf dem Server blinkt gelb.	Überprüfen Sie das SEL auf Meldungen und löschen Sie das SEL dann, um die blinkende LED zu stoppen. Lesen Sie in der iDRAC6-Webschnittstelle den Abschnitt „Systemereignisprotokoll (SEL) überprüfen“ auf Seite 389. Lesen Sie im SM-CLP den Abschnitt „SEL-Verwaltung“ auf Seite 346. Lesen Sie im iDRAC6-Konfigurationsdienstprogramm den Abschnitt „Menü des Systemereignisprotokolls“ auf Seite 383
Auf dem Server ist eine blaue blinkende LED.	Ein Benutzer hat die Locator-ID für den Server aktiviert. Dies ist ein Signal, das zum Identifizieren des Servers im Gehäuse behilflich ist. Informationen zu dieser Funktion finden Sie unter „Verwalteten Server im Gehäuse identifizieren“ auf Seite 406.

Tabelle 19-10. Häufig gestellte Fragen/Fehlerbehebung *(fortgesetzt)*

Frage	Antwort

Wie kann ich die IP-Adresse des iDRAC6 finden?	**Von der CMC-Webschnittstelle:**
	1 Klicken Sie auf **Gehäuse→ Server** und dann auf das Register **Setup**.
	2 Klicken Sie auf **Deploy** (Bereitstellen)
	3 Lesen Sie die IP-Adresse für Ihren Server aus der angezeigten Tabelle ab.
	Von der virtuellen Konsole:
	• Starten Sie den Server neu und öffnen Sie das **iDRAC6-Konfigurationshilfsprogramm** durch Drücken von <Strg><E>.
	• Warten Sie, bis die IP-Adresse während des BIOS-POST angezeigt wird.
	• 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. Eine vollständige Liste der CMC RACADM-Unterbefehle finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*.
	• Verwenden Sie den lokalen RACADM-Befehl **getsysinfo,** um die IP-Adresse des iDRAC6 anzuzeigen.
	Zum Beispiel:
	`$ racadm getniccfg -m server-1`
	`DHCP Aktiviert = 1`
	`IP-Adresse = 192.168.0.1`
	`Subnetzmaske = 255.255.255.0`
	`Gateway = 192.168.0.1`
	Von lokalem RACADM:
	Geben Sie den folgenden Befehl an einer Eingabeaufforderung ein:
	`racadm getsysinfo`
	Vom LCD:
	1 Markieren Sie im Hauptmenü das Element **Server** und drücken Sie auf die Schaltfläche mit dem Häkchen.
	2 Wählen Sie den Server aus, dessen IP-Adresse Sie suchen, und drücken Sie auf die Schaltfläche mit dem Häkchen.

Tabelle 19-10. Häufig gestellte Fragen/Fehlerbehebung *(fortgesetzt)*

Frage	Antwort

Wie kann ich die IP-Adresse des CMC finden?	**Von der iDRAC6-Webschnittstelle aus:**
	• Klicken Sie auf **System→ iDRAC-Einstellungen→ CMC**.
	Die CMC-IP-Adresse wird auf dem CMC-**Zusammenfassungs**bildschirm angezeigt.
	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. Eine vollständige Liste der CMC RACADM-Unterbehefle finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*.
	`$ racadm getniccfg -m chassis`
	`NIC Aktiviert = 1`
	`DHCP Aktiviert = 1`
	`Statische IP-Adresse = 192.168.0.120`
	`Statische Subnetzmaske = 255.255.255.0`
	`Statischer Gateway = 192.168.0.1`
	`Aktuelle IP-Adresse = 10.35.155.151`
	`Aktuelle Subnetzmaske = 255.255.255.0`
	`Aktueller Gateway = 10.35.155.1`
	`Geschwindigkeit = Automatische Aushandlung`
	`Duplex = Automatische Aushandlung`
	ANMERKUNG: Die oben aufgeführte Maßnahme kann auch mit Remote-RACADM ausgeführt werden.

Die iDRAC6-Netzwerkverbindung funktioniert nicht.	• 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.

Tabelle 19-10. Häufig gestellte Fragen/Fehlerbehebung *(fortgesetzt)*

Frage	Antwort
Ich habe den Server in das Gehäuse eingesetzt und den Netzschalter gedrückt, aber nichts ist passiert.	• Der iDRAC6 benötigt bis zu 2 Minuten zum Initialisieren, bevor der Server hochgefahren werden kann. • Überprüfen Sie das Energiebudget des CMC. Das Energiebudget für das Gehäuse könnte möglicherweise überschritten sein.
Ich habe den Benutzernamen und das Kennwort für den iDRAC6-Administrator vergessen.	Sie müssen die Standardeinstellungen des iDRAC6 wiederherstellen. **1** Starten Sie den Server neu und drücken Sie <Strg><E>, wenn Sie zum Öffnen des **iDRAC6-Konfigurationshilfsprogramms** aufgefordert werden. **2** Markieren Sie im Menü **iDRAC6-Konfigurationshilfsprogramm** die Option **Auf Standardeinstellung zurücksetzen** und drücken Sie die Eingabetaste. **ANMERKUNG:** Sie können den iDRAC6 auch vom lokalen RACADM aus zurücksetzen, indem Sie `racadm racresetcfg` ausgeben. Weitere Informationen finden Sie unter„Auf Standardeinstellung zurücksetzen“ auf Seite 382.
Wie kann ich den Namen des Steckplatzes für meinen Server ändern?	**1** Melden Sie sich bei der CMC-Webschnittstelle an. **2** Öffnen Sie die **Gehäuse**struktur und klicken Sie auf **Server**. **3** Klicken Sie auf das Register **Setup**. **4** Geben Sie den neuen Namen für den Steckplatz in die Zeile für den Server ein. **5** Klicken Sie auf **Anwenden**.

Tabelle 19-10. Häufig gestellte Fragen/Fehlerbehebung *(fortgesetzt)*

Frage	Antwort
Wenn eine Virtuelle Konsole-Sitzung von der iDRAC6-Webschnittstelle aus gestartet wird, wird ein ActiveX-Sicherheits-Popup angezeigt.	Der iDRAC6 könnte möglicherweise keine vertrauenswürdige Site sein. Um zu verhindern, dass jedes Mal, wenn Sie eine Virtuelle Konsole-Sitzung beginnen, ein Sicherheits-Popup eingeblendet wird, fügen Sie den iDRAC6 im Client-Browser einfach der Liste vertrauenswürdiger Sites 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 iDRAC6 ein. **3** Klicken Sie auf **Add** (Hinzufügen). **4** Klicken Sie auf **Stufe anpassen**. **5** Wählen Sie im Fenster **Sicherheitseinstellungen** die Option **Bestätigen** unter **Unsignierte ActiveX-Steuerelemente herunterladen** aus.
Wenn ich eine Virtuelle Konsole-Sitzung starte, ist der Viewer-Bildschirm leer.	Wenn Sie die Berechtigung **Virtuelle Datenträger** besitzen, jedoch nicht die Berechtigung Virtuelle **Konsole**, können Sie den Viewer starten und somit auf die Funktion des virtuellen Datenträgers zugreifen. Jedoch wird hierbei die Konsole des verwalteten Servers nicht angezeigt.
Der iDRAC6 reagiert während des Startvorgangs nicht.	Enfernen Sie den Server und setzen Sie ihn erneut ein. Überprüfen Sie die CMC-Webschnittstelle, um zu sehen, ob der iDRAC6 als aktualisierbare Komponente angezeigt wird. Ist dies der Fall, befolgen Sie die Anleitungen unter „iDRAC6-Firmware mithilfe des CMC aktualisieren“ auf Seite 132. Wird das Problem hierdurch nicht gelöst, setzen Sie sich mit dem technischen Support in Verbindung.
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. Achten Sie außerdem im iDRAC6-Protokoll auf Fehlermeldungen von der iDRAC6-Webschnittstelle oder vom LCD.

Stichwortverzeichnis

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z