Integrated Dell Remote Access Controller 6 (iDRAC6) Version 1.95

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-Übersicht

Der Integrated Dell Remote Access Controller6 (iDRAC6) ist eine Hardware- und Softwarelösung zur Systemverwaltung, die Remote-Verwaltungsfunktionalität, Wiederherstellung für abgestürzte Systeme sowie Stromsteuerungsfunktionen für Dell PowerEdge-Systeme bietet.

Der iDRAC6 verwendet einen integrierten System-auf-Chip-Mikroprozessor für das Remote-Überwachungs-/Steuerungssystem. Der iDRAC6 und der verwaltete PowerEdge-Server befinden sich gemeinsam auf der Systemplatine. Das Betriebssystem des Servers befasst sich mit der Ausführung von Anwendungen und der iDRAC6 mit der Überwachung und Verwaltung der Serverumgebung und des Serverstatus außerhalb des Betriebssystems.

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

Die iDRAC6-Netzwerkschnittstelle ist standardmäßig mit der statischen IP-Adresse 192.168.0.120 aktiviert. Sie muss konfiguriert werden, bevor ein Zugriff auf den iDRAC6 möglich ist. Nachdem der iDRAC6 auf dem Netzwerk konfiguriert wurde, kann auf ihn an seiner zugewiesenen IP-Adresse über die iDRAC6-Webschnittstelle, Telnet oder SSH (Secure Shell) sowie unterstützte Netzwerkverwaltungsprotokolle wie die IPMI (intelligente Plattform-Verwaltungsschnittstelle) zugegriffen werden.

Was ist neu an dieser Version?

- Unterstützung für DIMM-Konfigurationen und PCI-Karten (siehe Versionshinweise für Details.)
- Unterstützung für Internet Explorer 10 Browser.
- Die Länge des Certificate Signing Request (CSR) Standard-Verschlüsselungsschlüssels wurde auf 2048 Bit geändert.

iDRAC6 Express-Verwaltungsfunktionen

iDRAC6 Express bietet die folgenden Verwaltungsfunktionen:

- Registrierung des dynamischen Domänennamensystems (DDNS).
- Bietet Remote-Systemverwaltung und -überwachung unter Verwendung einer Webschnittstelle und der SM-CLP-Befehlszeile (Server Management Command Line Protocol) über eine serielle, Telnet- oder SSH-Verbindung.
- Bietet Unterstützung für Microsoft Active Directory-Authentifizierung – Fasst iDRAC6-Benutzer-IDs und -kennwörter in Active Directory unter Verwendung eines erweiterten Schemas oder Standardschemas zusammen.
- Bietet eine allgemeine Lösung zur Unterstützung LDAP-basierter Authentifizierung (Lightweight Directory Access Protocol) – Für diese Funktion ist auf Ihren Verzeichnisdiensten keine Schemaeweiterung erforderlich.
- Bietet Zugriff auf Systeminformationen und Komponentenstatus für Überwachungszwecke.
- Bietet Zugriff auf das Systemereignisprotokoll (das iDRAC6-Protokoll) und, unabhängig vom Status des Betriebssystems, Zugriff auf den Bildschirm des letzten Absturzes für das abgestürzte bzw. nicht mehr reagierende System.
- Bietet die Möglichkeit, dem Lifecycle Controller-Protokoll über die GUI oder die CLI Arbeitsnotizen hinzuzufügen.
- Ermöglicht Ihnen, die iDRAC6-Webschnittstelle über Dell OpenManage Server Administrator oder Dell OpenManage IT Assistant zu starten.
- Warnt Sie anhand einer E-Mail-Benachrichtigung oder eines SNMP-Traps vor potenziellen Problemen mit verwalteten Knoten.
- Bietet Remote-Stromverwaltungsfunktionen von einer Verwaltungskonsole aus, z. B. zum Herunterfahren und Zurücksetzen des Systems.
- Bietet Unterstützung für die intelligente Plattform-Verwaltungsschnittstelle (IPMI).
- Bietet eine sichere Remote-Systemverwaltung über die Webschnittstelle.
- Verhindert den unerlaubten Zugriff auf Remote-Systeme durch Sicherheitsverwaltung auf Kennwortebene.

- Bietet zuweisbare Berechtigungen für verschiedene Systemverwaltungsaufgaben durch rollenbasierte Autorität.
- Bietet Unterstützung für IPv6, wie den Zugriff auf die iDRAC6-Webschnittstelle mithilfe einer IPv6-Adresse, legt die IPv6-Adresse für den iDRAC-NIC fest und bestimmt eine Zielnummer zur Konfiguration eines IPv6-SNMP-Warnungsziels.
- Bietet eine über das Netzwerk zugängliche Verwaltung unter Verwendung des WS-MAN-Protokolls (Web Services for Management).
- Bietet Unterstützung für SM-CLP (Server Management-Command Line Protocol) und stellt damit Standards für SM-CLI-Implementierungen bereit.
- Ermöglicht Ihnen das Starten (oder Zurücksetzen) von einem Firmware-Image Ihrer Wahl über Zurücksetzen und Wiederherstellen der Firmware.

Weitere Informationen zu iDRAC6 Express finden Sie im *Hardware-Benutzerhandbuch* unter **dell.com/support/manuals**.

iDRAC6 Enterprise und VFlash-Datenträger

iDRAC6 Enterprise mit vFlash-Medien bietet zusätzliche Unterstützung für RACADM, virtuelle Konsole, Funktionen des virtuellen Datenträgers, einen dedizierten NIC und vFlash (mit einer optionalen Dell VFlash-Medienkarte). VFlash ermöglicht das Speichern von Notfall-Startimages und Diagnosehilfsprogrammen auf einem VFlash-Datenträger. Weitere Informationen zu iDRAC6 Enterprise- und VFlash-Datenträgern finden Sie im *Hardware-Benutzerhandbuch* unter **dell.com/support/manuals**.

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

Tabelle 1-1. iDRAC6-Funktionsliste

Funktion	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise mit vFlash
Schnittstellen- und Standardunterstützung				
IPMI 2.0	✓	✓	✓	✓
Webbasierte GUI	✗	✓	✓	✓
SNMP	✗	✓	✓	✓
WSMAN	✗	✓	✓	✓
SMASH-CLP (nur SSH)	✗	✓	✓	✓
RACADM-Befehlszeile (SSH und lokal)	✗	✓	✓	✓
RACADM-Befehlszeile (Remote)	✗	✗	✓	✓
Konnektivität				
Netzwerkmodi Freigegeben/Failover	✓	✓	✓	✓
IPv4	✓	✓	✓	✓
VLAN-Tagging	✓	✓	✓	✓
IPv6	✗	✓	✓	✓
Dynamisches DNS	✗	✓	✓	✓
Dedizierte NIC	✗	✗	✓	✓
Sicherheit und Authentifizierung				
Rollenbasierte Autorität	✓	✓	✓	✓
Local Users (Lokale Benutzer)	✓	✓	✓	✓
SSL-Verschlüsselung	✓	✓	✓	✓
Active Directory	✗	✓	✓	✓

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

Funktion	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise mit vFlash
Allgemeine LDAP-Unterstützung	✗	✓	✓	✓
Zweifaktor-Authentifizierung[1]	✗	✓	✓	✓
Einmalanmeldung	✗	✓	✓	✓
PK-Authentifizierung (für SSH)	✗	✗	✓	✓
Remote-Verwaltung und Störungsbeseitigung				
Remote-Firmware-Aktualisierung	✓[2]	✓	✓	✓
Serverstromregelung	✓[2]	✓	✓	✓
Seriell-über-LAN (mit Proxy)	✓	✓	✓	✓
Seriell-über-LAN (ohne Proxy)	✓	✓	✓	✓
Power Capping (Strombegrenzung)	✓	✓	✓	✓
Erfassung des Bildschirms „Letzter Absturz“	✗	✓	✓	✓
Start-Capture	✗	✓	✓	✓
Virtueller Datenträger[3]	✗	✗	✓	✓
Virtuelle Konsole[3]	✗	✗	✓	✓
Gemeinsame Nutzung der virtuellen Konsole[3]	✗	✗	✓	✓
Remote-Start der virtuellen Konsole	✗	✗	✓	✓
vFlash	✗	✗	✗	✓

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

Funktion	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise mit vFlash
Überwachung				
Sensorüberwachung und Warnmeldungen	✓[2]	✓	✓	✓
Echtzeit-Stromüberwachung	✓	✓	✓	✓
Echtzeit-Stromdiagramme	✗	✓	✓	✓
Historische Stromzähler	✗	✓	✓	✓
Protokollierung				
Systemereignisprotokoll (SEL)	✓	✓	✓	✓
RAC-Protokoll	✗	✓	✓	✓
Remote-Syslog	✗	✗	✓	✓
Lifecycle Controller				
Unified Server Configurator	✓[4]	✓	✓	✓
Remote-Dienste (über WS-MAN)	✗	✓	✓	✓
Teilersetzung	✗	✗	✗	✓

[1]Für die Zweifaktor-Authentifizierung ist Internet Explorer erforderlich.

[2]Funktion ist nur über IPMI verfügbar, nicht über eine Web-GUI.

[3]Die virtuelle Konsole und der virtuelle Datenträger sind verfügbar, wobei sowohl das Java- als auch das Active-X-Plugin verwendet werden.

[4]Die Verwendung des über BMC verfügbaren Unified Server Configurator beschränkt sich auf die Betriebssysteminstallation und die Diagnose.

✓ = Unterstützt; ✗ = Nicht unterstützt

Der iDRAC6 enthält die folgenden Sicherheitsfunktionen:

- Einfache Anmeldung, Zweifaktor-Authentifizierung und Authentifizierung mit öffentlichem Schlüssel.
- Benutzerauthentifizierung durch Active Directory (optional), LDAP-Authentifizierung (optional) oder durch hardwaregespeicherte Benutzer-IDs und Kennwörter.
- Rollenbasierte Berechtigung, die es Administratoren ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren.
- Benutzer-ID- und Kennwort-Konfiguration über die Webschnittstelle oder SM-CLP.
- SM-CLP- und Webschnittstellen, die 128-Bit- und 40-Bit-Verschlüsselung mit SSL 3.0-Standard unterstützen (für Länder, in denen 128-Bit nicht zulässig ist).
- Konfiguration der Sitzungszeitüberschreitung (in Sekunden) über die Webschnittstelle oder SM-CLP.
- Konfigurierbare IP-Schnittstellen (wo anwendbar).

  ANMERKUNG: Telnet unterstützt keine SSL-Verschlüsselung.
- Secure Shell (SSH), verwendet eine verschlüsselte Übertragungsschicht für höhere Sicherheit.
- Beschränkung der Anmeldungsfehlversuche pro IP-Adresse, mit Anmeldungsblockierung der IP-Adresse, wenn die Grenze überschritten wird.
- Fähigkeit, den IP-Adressenbereich für Clients, die eine Verbindung zum iDRAC6 herstellen, zu beschränken.

Unterstützte Plattformen

Informationen zu den aktuell unterstützten Plattformen finden Sie in der iDRAC6-Infodatei und 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 den *iDRAC6 1.95-Versionshinweisen* und in der *Dell Systems Software Support-Matrix* unter **dell.com/support/manuals**.

ANMERKUNG: Aufgrund schwerwiegender Sicherheitslücken wird SSL 2.0 nicht mehr unterstützt. Für die ordnungsgemäße Ausführung muss Ihr Browser so konfiguriert sein, dass SSL 3.0 aktiviert wird. Internet Explorer 6.0 ist nicht unterstützt.

Unterstützte Remote-Zugriffsverbindungen

Tabelle 1-2 führt die Verbindungsfunktionen auf.

Tabelle 1-2. Unterstützte Remote-Zugriffsverbindungen

Verbindung	Funktionen
iDRAC6-NIC	• 10/100-Mbit/s-Ethernet • DHCP-Unterstützung • SNMP-Traps und E-Mail-Ereignisbenachrichtigung • Unterstützung für SM-CLP-Befehls-Shell (Telnet, SSH und RACADM) und für Verfahren wie iDRAC6-Befehle für Konfiguration, Systemstart, Reset, Hochfahren und Herunterfahren • Unterstützung für IPMI-Dienstprogramme wie IPMItool und ipmish

iDRAC6-Anschlüsse

Tabelle 1-3 führt die Anschlüsse auf, die der iDRAC6 auf 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.

Tabelle 1-3. iDRAC6-Server-Abhöranschlüsse

Port Number (Schnittstellennummer)	Funktion
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	Tastatur/Maus der virtuellen Konsole, Dienst des virtuellen Datenträgers, sicherer Dienst des virtuellen Datenträgers und Video der virtuellen Konsole

* 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-Online-Hilfe enthält detaillierte Informationen zur Verwendung der webbasierten Schnittstelle.
- Das *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC* enthält Informationen zu den RACADM-Unterbefehlen, den unterstützten Schnittstellen und iDRAC6-Eigenschaften-Datenbankgruppen und Objektdefinitionen.
- Das *Dell Lifecycle Controller-Benutzerhandbuch* enthält Informationen zum Unified Server Configurator (USC), dem Unified Server Configurator – Lifecycle Controller Enabled (USC – LCE) und Remote-Services.
- Informationen zur iDRAC6- und IPMI-Schnittstelle finden Sie im *Benutzerhandbuch für Dienstprogramme des Dell OpenManage Baseboard-Verwaltungs-Controllers*.
- Die *Dell Systems Software Support-Matrix* bietet Informationen über verschiedene Dell-Systeme, über die von diesen Systemen unterstützten Betriebssysteme und über 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 *Dell OpenManage Server Administrator-Benutzerhandbuch* für Informationen über die Installation und Verwendung von Server Administrator.
- Das *Benutzerhandbuch zu Dell Update Packages* für 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:

- Informationen zum Installieren eines iDRAC6 finden Sie im *Hardware-Benutzerhandbuch*.
- 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.
- In der zusammen mit der Rack-Lösung gelieferten *Rack-Installationsanleitung* wird beschrieben, wie das System in einem Rack installiert wird.
- Das *Handbuch zum Einstieg* enthält eine Übersicht über die Systemfunktionen, die Einrichtung des Systems und technische Daten.
- Im *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.

- Versionsinformationen oder Infodateien können vorhanden sein. Diese geben den letzten Stand der Änderungen am System oder an der Dokumentation wieder und enthalten erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.

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

Zum Einstieg mit iDRAC6

Der iDRAC6 ermöglicht Ihnen, ein Dell-System im Remote-Zugriff zu überwachen und zu reparieren und auf dem System Fehlerbehebungsmaßnahmen durchzuführen, selbst wenn es außer Betrieb ist. Der iDRAC6 bietet Funktionen wie Virtuelle Konsole, Virtueller Datenträger, Smart Card-Authentifizierung und Einfache Anmeldung (SSO).

Die *Management Station* ist das System, von dem aus ein Administrator ein Dell-System, das über einen iDRAC6 verfügt, im Remote-Zugriff verwaltet. Die mit dieser Methode überwachten Systeme werden *verwaltete Systeme* genannt.

Optional können Sie die Dell OpenManage-Software sowohl auf der Management Station als auch auf dem verwalteten System installieren. Ohne die Managed System-Software kann der RACADM nicht lokal verwendet werden, und der iDRAC6 kann den Bildschirm des letzten Absturzes nicht erfassen.

Um den iDRAC6 einzustellen, führen Sie die nachfolgenden allgemeinen Schritte aus:

ANMERKUNG: Dieses Verfahren kann je nach System unterschiedlich sein. Genaue Anleitungen zum Ausführen dieses Verfahrens befinden sich im *Hardware-Benutzerhandbuch* zu Ihrem System, das auf der Dell Support-Website unter **dell.com/support/manuals**/manuals zur Verfügung steht.

1. Konfigurieren Sie die Eigenschaften, Netzwerkeinstellungen und Benutzer des iDRAC6 – Der iDRAC6 kann sowohl unter Verwendung des iDRAC6-Konfigurationsdienstprogramms, als auch über die webbasierte Schnittstelle oder den RACADM konfiguriert werden.
2. **(Optional)** Konfigurieren Sie bei der Verwendung eines Windows-Systems das MicrosoftActive Directory, um Zugriff auf den iDRAC6 bereitzustellen, wodurch Ihnen ermöglicht wird, iDRAC6-Benutzerberechtigungen zu den vorhandenen Benutzern in der Active Directory-Software hinzuzufügen und zu steuern.
3. **(Optional)** Konfigurieren Sie die Smart Card-Authentifizierung – Smart Card bietet eine zusätzliche Sicherheitsstufe für Ihr Unternehmen.
4. Konfigurieren Sie Remote-Zugriffspunkte, wie z. B. virtuelle Konsole und virtueller Datenträger.

5 Konfigurieren Sie die Sicherheitseinstellungen.

6 Konfigurieren Sie Warnmeldungen für eine effiziente Systemverwaltung.

7 Konfigurieren Sie die iDRAC6-IPMI-Einstellungen (Intelligente Plattform-Verwaltungsschnittstelle), um die auf Standards beruhenden IPMI-Hilfsprogramme zur Verwaltung der Systeme auf Ihrem Netzwerk zu verwenden.

3

Grundlegende Installation des iDRAC6

Dieser Abschnitt enthält Informationen über die Installation und Einrichtung der iDRAC6-Hardware und -Software.

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Artikel aus dem Lieferumfang des Systems zur Verfügung stehen, bevor Sie die iDRAC6-Software installieren und konfigurieren:

- iDRAC6-Hardware (gegenwärtig installiert oder Teil des optionalen Einbausatzes)
- iDRAC6-Installationsverfahren (in diesem Kapitel enthalten)
- DVD *Dell Systems Management Tools and Documentation*

iDRAC6 Express/Enterprise-Hardware installieren

ANMERKUNG: Die iDRAC6-Verbindung emuliert eine USB-Tastaturverbindung. Infolgedessen meldet das System bei einem Neustart nicht, wenn keine Tastatur angeschlossen ist.

iDRAC6 Express/Enterprise kann auf Ihrem System vorinstalliert sein oder separat geliefert werden. Anweisungen zu den ersten Schritten mit dem auf dem System installierten iDRAC6 stehen unter „Übersicht zu Softwareinstallation und -konfiguration“ auf Seite 38 zur Verfügung.

Ist iDRAC6 Express/Enterprise auf Ihrem System nicht installiert, schlagen Sie im *Hardware-Benutzerhandbuch* auf Ihrer Plattform die Hardware-Installationsanleitungen nach.

System zur Verwendung eines iDRAC6 konfigurieren

Konfiguration des Systems zur Verwendung eines iDRAC6 mit dem iDRAC6-Konfigurationsdienstprogramm.

So führen Sie das iDRAC6-Konfigurationsdienstprogramm aus:

1. Schalten Sie das System ein oder starten Sie es neu.
2. Drücken Sie <Strg><E>, wenn Sie während des POST dazu aufgefordert werden.

   Wenn Ihr Betriebssystem zu laden beginnt, bevor Sie <Strg><E> gedrückt haben, lassen Sie das System vollständig hochfahren, starten Sie das System neu, und versuchen Sie es noch einmal.
3. Konfigurieren Sie das LOM.
   a. Verwenden Sie die Pfeiltasten, **um LAN-Parameter auszuwählen**, und drücken Sie <Eingabe>. **Die NIC-Auswahl** wird angezeigt.
   b. Wählen Sie mit den Pfeiltasten eine der folgenden NIC-Optionen aus:
      - **Dediziert** – Wählen Sie diese Option aus, um das Remote-Zugriffsgerät zur Verwendung der dedizierten Netzwerkschnittstelle auf dem iDRAC6 Enterprise zu aktivieren. Diese Schnittstelle wird nicht an das Host-Betriebssystem freigegeben und leitet den Verwaltungsdatenverkehr auf ein separates physisches Netzwerk um, wodurch er vom Anwendungsdatenverkehr getrennt wird. Diese Option steht nur dann zur Verfügung, wenn auf dem System ein iDRAC6 Enterprise installiert ist. Ändern Sie nach Einsetzen der iDRAC6 Enterprise-Karte die Option **NIC-Auswahl** auf jeden Fall auf **Dediziert**. Dieser Schritt kann über das iDRAC6-Konfigurationsdienstprogramm, die iDRAC6-Webschnittstelle oder RACADM vorgenommen werden.
      - **Freigegeben** – Wählen Sie diese Option aus, um die Netzwerkschnittstelle an das Host-Betriebssystem freizugeben. Die Netzwerkschnittstelle des Remote-Zugriffsgeräts ist vollständig funktionsfähig, wenn das Host-Betriebssystem für NIC-Teaming konfiguriert ist. Das Remote-Zugriffsgerät empfängt Daten über NIC 1 und NIC 2, sendet Daten jedoch nur über NIC 1. Wenn NIC 1 fehlschlägt, ist der Zugriff auf das Remote-Zugriffsgerät nicht möglich.

- **Freigegeben für Failover: LOM2** – Wählen Sie diese Option aus, um die Netzwerkschnittstelle an das Host-Betriebssystem freizugeben. Die Netzwerkschnittstelle des Remote-Zugriffsgeräts ist vollständig funktionsfähig, wenn das Host-Betriebssystem für NIC-Teaming konfiguriert ist. Das Remote-Zugriffsgerät empfängt Daten über NIC 1 und NIC 2, sendet Daten jedoch nur über NIC 1. Wenn NIC 1 ausfällt, schaltet das Remote-Zugriffsgerät für alle Datenübertragungen auf NIC 2. Das Remote-Zugriffsgerät verwendet NIC 2 weiterhin für die Datenübertragung. Wenn NIC 2 ausfällt, schaltet das Remote-Zugriffsgerät alle Datenübertragungen zurück auf NIC 1, jedoch nur, nachdem der ursprüngliche NIC 1-Fehler korrigiert wurde.
- **Freigegeben für Failover: Alle LOMs** – Wählen Sie diese Option aus, um die Netzwerkschnittstelle an das Host-Betriebssystem freizugeben. Die Netzwerkschnittstelle des Remote-Zugriffsgeräts ist vollständig funktionsfähig, wenn das Host-Betriebssystem für NIC-Teaming konfiguriert ist. Das Remote-Zugriffsgerät empfängt Daten über NIC 1, NIC 2, NIC 3 und NIC 4, sendet Daten jedoch nur über NIC 1. Wenn NIC 1 ausfällt, schaltet das Remote-Zugriffsgerät alle Datenübertragungen auf NIC 2. Wenn NIC 2 ausfällt, schaltet das Remote-Zugriffsgerät alle Datenübertragungen auf NIC 3. Wenn NIC 3 ausfällt, schaltet das Remote-Zugriffsgerät alle Datenübertragungen auf NIC 4. Wenn NIC 4 ausfällt, schaltet das Remote-Zugriffsgerät für alle Datenübertragungen zum NIC 1 zurück, allerdings nur, wenn der NIC 1-Fehler korrigiert wurde.

4 Konfigurieren Sie die LAN-Parameter des Netzwerk-Controllers zur Verwendung von DHCP oder einer statischen IP-Adressen-Quelle.

   a Wählen Sie mit der Abwärtspfeiltaste **LAN-Parameter** aus, und drücken Sie <Eingabe>.

   b Wählen Sie die **IP-Adressen-Quelle** mit den Pfeiltasten aus.

   c Wählen Sie mit den Pfeiltasten **DHCP**, **AutoConfig** oder **Statisch** aus.

   d Wenn Sie **Statisch** ausgewählt haben, konfigurieren Sie die Einstellungen für **IP-Adresse**, **Subnetzmaske** und **Standard-Gateway**.

   e Drücken Sie die <Esc>-Taste.

5 Drücken Sie die <Esc>-Taste.

6 Wählen Sie **Änderungen speichern und beenden** aus.

Übersicht zu Softwareinstallation und -konfiguration

Dieser Abschnitt bietet eine detaillierte Übersicht über die iDRAC6-Softwareinstallations- und -Konfigurationsverfahrens. Weitere Informationen zu den iDRAC6-Softwarekomponenten finden Sie unter „Software auf dem verwalteten System installieren“ auf Seite 39.

iDRAC6-Software installieren

So installieren Sie die iDRAC6-Software:

1. Installieren Sie die iDRAC6-Software auf dem verwalteten System. Siehe „Software auf dem verwalteten System installieren“ auf Seite 39.
2. Installieren Sie die iDRAC6-Software auf der Management Station. Siehe „Software auf der Management Station installieren“ auf Seite 39.

iDRAC6 konfigurieren

So konfigurieren Sie iDRAC6:

1. Wählen Sie eines der folgenden Konfigurationshilfsprogramme aus:
   - Webbasierte Schnittstelle – siehe „iDRAC6 mittels der Webschnittstelle konfigurieren“ auf Seite 47.
   - RACADM-CLI (siehe *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC* unter **dell.com/support/manuals**)
   - Telnet-Konsole – siehe „Telnet-Konsole verwenden“ auf Seite 95.

   ANMERKUNG: Die Verwendung von mehr als einem iDRAC6-Konfigurationshilfsprogramm zur gleichen Zeit kann zu unerwarteten Ergebnissen führen.
2. Konfigurieren Sie die iDRAC-Netzwerkeinstellungen. Siehe „iDRAC6-Netzwerkeinstellungen konfigurieren“ auf Seite 118.
3. iDRAC6-Benutzer hinzufügen und konfigurieren Siehe „iDRAC6-Benutzer hinzufügen und konfigurieren“ auf Seite 139.
4. Konfigurieren Sie den Webbrowser, um auf die webbasierte Schnittstelle zuzugreifen. Siehe „Konfigurieren eines unterstützten Webbrowsers“ auf Seite 44.

5 Deaktivieren Sie die Microsoft Windows-Option für den automatischen Neustart. Siehe „Die Windows-Option "Automatischer Neustart" deaktivieren“ auf Seite 356.

6 Aktualisieren Sie die iDRAC6-Firmware. Siehe „iDRAC6-Firmware aktualisieren“ auf Seite 41.

Software auf dem verwalteten System installieren

Die Installation von Software auf dem verwalteten System ist optional. Ohne die Managed System-Software kann der RACADM nicht lokal verwendet werden, und der iDRAC6 kann den Bildschirm des letzten Absturzes nicht erfassen.

Installieren Sie die Managed System-Software, indem Sie die Software unter Verwendung der DVD *Dell Systems Management Tools and Documentation* auf dem verwalteten System installieren. Installationsanweisungen für diese Software finden Sie in der *Schnellinstallationsanleitung* auf der Dell Support-Website unter **support.dell.com\manuals**.

Die Managed System-Software installiert Ihre Auswahl der entsprechenden Version von Dell OpenManage Server Administrator auf dem verwalteten System.

ANMERKUNG: Installieren Sie die iDRAC6 Management Station-Software und die iDRAC6 Managed System-Software nicht auf demselben System.

Wenn Server Administrator nicht auf dem verwalteten System installiert ist, können Sie weder den Bildschirm des letzten Systemabsturzes anzeigen noch die Funktion **Autom. Wiederherstellung** verwenden.

Weitere Informationen zum Bildschirm des letzten Absturzes finden Sie unter „Bildschirm des letzten Systemabsturzes anzeigen“ auf Seite 378.

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

Informationen über Server Administrator, IT Assistant und Unified Server Configurator finden Sie im *Server Administrator-Benutzerhandbuch*, im *IT Assistant-Benutzerhandbuch* und im *Lifecycle Configurator-Benutzerhandbuch*. Diese stehen auf der Dell Support-Website unter **dell.com/support/manuals** zur Verfügung.

RACADM auf einer Linux-Management Station installieren und entfernen

Zur Verwendung der Remote-RACADM-Funktionen installieren Sie RACADM auf einer Management Station, die Linux ausführt.

ANMERKUNG: Wenn Sie **Setup** auf der DVD *Dell Systems Management Tools and Documentation* ausführen, wird das RACADM-Dienstprogramm für alle unterstützten Betriebssysteme auf der Management Station installiert.

RACADM installieren

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.

RACADM deinstallieren

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 RAC-Software verwendet wurde.

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

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

iDRAC6-Firmware aktualisieren

Verwenden Sie eine der folgenden Methoden, um die iDRAC6-Firmware zu aktualisieren.

- Webbasierte Schnittstelle (siehe „iDRAC6-Firmware mittels der webbasierten Benutzerschnittstelle aktualisieren“ auf Seite 42)
- RACADM-CLI (siehe „iDRAC6-Firmware über RACADM aktualisieren“ auf Seite 42)
- Dell Update Packages (siehe „iDRAC6-Firmware mittels Dell Update Packages für unterstützte Windows- und Linux-Betriebssysteme aktualisieren“ auf Seite 43)

Bevor Sie beginnen

Bevor Sie die iDRAC6-Firmware mit lokalem RACADM oder Dell Update Packages aktualisieren, führen Sie die folgenden Verfahren aus. Andernfalls schlägt die Firmware-Aktualisierung eventuell fehl.

1. Installieren und aktivieren Sie die entsprechende IPMI und die entsprechenden Treiber des verwalteten Knotens.
2. Wenn das System das Windows-Betriebssystem ausführt, aktivieren und starten Sie den **Windows Management Instrumentation**-Dienst (WMI).
3. Wenn Sie iDRAC6 Enterprise verwenden und das System SUSE Linux Enterprise Server (Version 10) für Intel EM64T ausführt, starten Sie den **Raw**-Dienst.
4. Trennen Sie die Verbindung zum virtuellen Datenträger und heben Sie die Bereitstellung auf (unmount).

   ANMERKUNG: Wird die iDRAC6-Firmware-Aktualisierung aus irgendeinem Grund unterbrochen, kann es bis zu 30 Minuten dauern, bis eine erneute Aktualisierung möglich ist.
5. Stellen Sie sicher, dass der USB aktiviert ist.

iDRAC6-Firmware herunterladen

Zum Aktualisieren der iDRAC6-Firmware laden Sie die neueste Firmware von der Dell Support-Website unter **support.dell.com** herunter und speichern die Datei auf dem lokalen System.

Die folgenden Softwarekomponenten sind in Ihrem iDRAC6-Firmware-Paket enthalten:

- Kompilierte iDRAC6-Firmware-Codes und -Daten
- Webbasierte Benutzerschnittstelle, JPEG und andere Benutzeroberflächendateien
- Standard-Konfigurationsdateien

iDRAC6-Firmware mittels der webbasierten Benutzerschnittstelle aktualisieren

Ausführliche Informationen finden Sie unter „iDRAC6 Firmware/Systemdienste-Wiederherstellungsimage aktualisieren“ auf Seite 80.

iDRAC6-Firmware über RACADM aktualisieren

Sie können die iDRAC6-Firmware mittels des CLI-basierten RACADM-Hilfsprogramms aktualisieren. Wenn auf dem verwalteten System Server Administrator installiert ist, können Sie die Firmware mit lokalem RACADM aktualisieren.

1. Laden Sie das iDRAC6-Firmware-Abbild von der Dell Support-Website unter **support.dell.com** auf das verwaltete System herunter.

   Zum Beispiel:

   ```
   C:\downloads\firmimg.d6
   ```

2. Führen Sie den folgenden RACADM-Befehl aus:

   ```
   racadm fwupdate -pud c:\downloads\
   ```

   Sie können die Firmware auch mit Remote-RACADM aktualisieren.

   Zum Beispiel:

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

Hierbei ist *Pfad* der Speicherort auf dem TFTP-Server, auf dem **firmimg.d6** einschließlich der TFTP-Server-IP-Adresse gespeichert ist.

Pfad: <*TFTP-Server-IP*> -d < *Firmware-Image-Pfad auf dem TFTP-Server*>

- Szenario 1: Ist das firmimg.d6-Image im tftp-Stammordner enthalten, lautet der Pfad: <*TFTPServerIP*>
- Szenario 2: Ist das firmimg.d6-Image im Unterordner des tftp-Stammordners enthalten, lautet der Pfad: <*TFTPServerIP*> -d / <*Unterordnerpfad*>

iDRAC6-Firmware mittels Dell Update Packages für unterstützte Windows- und Linux-Betriebssysteme aktualisieren

Die Dell Update Packages für unterstützte Windows- und Linux-Betriebssysteme können von der Dell Support-Website unter **support.dell.com** heruntergeladen und ausgeführt werden. Weitere Informationen finden Sie im *Dell Update Packages-Benutzerhandbuch* auf der Dell Support-Website unter **support.dell.com\manuals**.

ANMERKUNG: Wird die iDRAC6-Firmware mit dem Dell Update Packages-Dienstprogramm in Linux aktualisiert, werden u. U. folgende Meldungen auf der Konsole angezeigt:

```
usb 5-2: device descriptor read/64, error -71
```
(usb 5-2: Gerät-Desktiptor read/64, Fehler -71)

```
usb 5-2: device descriptor not accepting
address 2, error -71
```
(usb 5-2: Gerät-Desktiptor akzeptiert Adresse 2 nicht, Fehler -71)

Dies sind Schönheitsfehler, die ignoriert werden können. Diese Meldungen werden durch das Zurücksetzen der USB-Geräte während der Firmware-Aktualisierung verursacht. Sie sind harmlos.

Konfigurieren eines unterstützten Webbrowsers

Die folgenden Abschnitte enthalten Anweisungen zur Konfiguration von unterstützten Webbrowsern.

Konfiguration des Webbrowsers, um eine Verbindung zur webbasierten iDRAC6-Schnittstelle herzustellen

Wenn Sie von einer über einen Proxyserver mit dem Internet verbundenen Management Station aus eine Verbindung zur iDRAC6-Webschnittstelle herstellen, müssen Sie den Webbrowser so konfigurieren, dass er von diesem Server aus auf das Internet zugreift.

So konfigurieren Sie Internet Explorer, um auf einen Proxy-Server zuzugreifen:

1. Öffnen Sie ein Webbrowser-Fenster.
2. Klicken Sie auf **Extras** und dann auf **Internetoptionen**.
3. Klicken Sie im Fenster **Internetoptionen** auf das Register **Verbindungen**.
4. Klicken Sie unter **LAN-Einstellungen (Lokales Netzwerk)** auf **LAN-Einstellungen**.
5. Wenn das Kästchen **Proxyserver verwenden** ausgewählt ist, wählen Sie das Kästchen **Proxyserver für lokale Adressen umgehen** aus.
6. Klicken Sie zweimal auf **OK**.

Liste vertrauenswürdiger Domänen

Wenn Sie über den Webbrowser auf die webbasierte iDRAC6-Schnittstelle zugreifen, werden Sie möglicherweise dazu aufgefordert, die iDRAC6-IP-Adresse der Liste vertrauenswürdiger Domänen hinzuzufügen, wenn die IP-Adresse auf der Liste fehlt. Wenn Sie diesen Vorgang ausgeführt haben, klicken Sie auf **Aktualisieren** oder starten Sie den Webbrowser neu, um eine neue Verbindung zur webbasierten iDRAC6-Schnittstelle herzustellen.

Lokalisierte Versionen der webbasierten Schnittstelle anzeigen

Windows

Die webbasierte iDRAC6-Schnittstelle wird in den folgenden Windows-Betriebssystemsprachen unterstützt:

- Englisch
- Französisch
- Deutsch

- Spanisch
- Japanisch
- Chinesisch (vereinfacht)

So zeigen Sie eine lokalisierte Version der webbasierten iDRAC6-Schnittstelle in Internet Explorer an:

1. Klicken Sie auf das Menü **Extras** und wählen Sie **Internetoptionen** aus.
2. Klicken Sie im Fenster **Internetoptionen** auf **Sprachen**.
3. Klicken Sie im Fenster **Spracheinstellung** auf **Hinzufügen**.
4. Wählen Sie im Fenster **Sprache hinzufügen** eine unterstützte Sprache aus.

   Um mehr als eine Sprache auszuwählen, drücken Sie <Strg>.
5. Wählen Sie Ihre bevorzugte Sprache aus, und klicken Sie auf **Nach oben**, um die Sprache an die Spitze der Liste zu verschieben.
6. Klicken Sie auf **OK**.
7. Klicken Sie im Fenster **Spracheinstellung** auf **OK**.

Linux

Wenn Sie die virtuelle Konsole auf einem Red Hat Enterprise Linux-Client (Version 4) mit einer grafischen Benutzeroberfläche (GUI) für vereinfachtes Chinesisch ausführen, erscheinen das Viewer-Menü und der Titel eventuell in willkürlichen Zeichen. Dieses Problem wird durch eine falsche Verschlüsselung für vereinfachtes Chinesisch im Red Hat Enterprise Linux-Betriebssystem (Version 4) verursacht. Um dieses Problem zu lösen, greifen Sie auf die aktuellen Verschlüsselungseinstellungen zu und ändern Sie sie, indem Sie folgende Schritte ausführen:

1. Öffnen Sie ein Terminal.
2. Geben Sie „locale“ ein und drücken Sie die Eingabetaste. Die folgende Ausgabe wird 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. Wenn die Werte „zh_CN.UTF-8“ einschließen, sind keine Änderungen erforderlich. Wenn die Werte „zh_CN.UTF-8“ nicht einschließen, fahren Sie mit Schritt 4 fort.
4. Wechseln Sie zur Datei **/etc/sysconfig/i18n**.
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.
7. Starten Sie den iDRAC6 neu.

Wenn Sie von einer beliebigen anderen Sprache zu vereinfachtem Chinesisch wechseln, müssen Sie sicherstellen, dass die Korrektur noch gültig ist. Ist dies nicht der Fall, wiederholen Sie das Verfahren.

Informationen zu erweiterten iDRAC6-Konfigurationen finden Sie unter „Erweiterte iDRAC6-Konfiguration“ auf Seite 93.

4

iDRAC6 mittels der Webschnittstelle konfigurieren

Der iDRAC6 bietet eine Webschnittstelle, über die Sie die iDRAC6-Eigenschaften und -Benutzer konfigurieren, Remote-Verwaltungsaufgaben ausführen sowie Fehler und Probleme auf einem (verwalteten) Remote-System feststellen und beheben können. Verwenden Sie die iDRAC6-Webschnittstelle für die tägliche Systemverwaltung. Dieses Kapitel gibt darüber Auskunft, wie allgemeine Systemverwaltungsaufgaben über die iDRAC6-Webschnittstelle ausgeführt werden, und enthält Verknüpfungen zu zugehörigen Informationen.

Die meisten Konfigurationsaufgaben über die Webschnittstelle können auch über RACADM-Befehle oder über SM-CLP-Befehle (Server Management-Command Line Protocol) ausgeführt werden.

Befehle des lokalen RACADM werden vom verwalteten Server aus ausgeführt.

SM-CLP- und SSH/Telnet-RACADM-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-SM-CLP-Befehlszeilenoberfläche verwenden“ auf Seite 253. Weitere Informationen zu den RACADM-Befehlen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

VORSICHTSHINWEIS: Wenn Sie den Browser durch Klicken auf „Aktualisieren“ oder durch Drücken von F5 aktualisieren, werden Sie möglicherweise von der Web-GUI-Sitzung (grafische Benutzeroberfläche) abgemeldet oder zur Seite „Systemzusammenfassung“ umgeleitet.

Zugriff auf die Webschnittstelle

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

1. Öffnen Sie einen unterstützten Webbrowser.

   Um mit einer IPv4-Adresse auf die Webschnittstelle zuzugreifen, fahren Sie mit Schritt 2 fort.

   Um mit einer IPv6-Adresse auf die Webschnittstelle zuzugreifen, fahren Sie mit Schritt 3 fort.

2. Greifen Sie mit einer IPv4-Adresse auf die Webschnittstelle zu. Sie müssen IPv4 aktiviert haben.

   Geben Sie Folgendes in die **Adressenleiste** des Browsers ein:

   `https://<iDRAC-IPv4-Adresse>`

   Drücken Sie dann die Eingabetaste.

3. Greifen Sie mit einer IPv6-Adresse auf die Webschnittstelle zu. Sie müssen IPv6 aktiviert haben.

   Geben Sie Folgendes in die **Adressenleiste** des Browsers ein:

   `https://[<iDRAC-IPv6-Adresse>]`

   Drücken Sie dann die Eingabetaste.

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

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

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

5. Geben Sie in das Feld **Adresse** `https://<iDRAC-IP-Adresse>` ein und drücken Sie die Eingabetaste.

   Wurde die Standard-HTTPS-Portnummer (443) geändert, geben Sie Folgendes ein:

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

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

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

Anmeldung

Sie können sich als iDRAC6-Benutzer oder als Microsoft Active Directory-Benutzer anmelden. Standardmäßig sind der Benutzername und das Kennwort für einen iDRAC6-Benutzer **root** bzw. **calvin**.

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

Um sich anzumelden, führen Sie die folgenden Schritte aus.

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

     Bei der Eingabe des Benutzernamens für lokale Benutzer wird zwischen Groß- und Kleinschreibung unterschieden. Beispiele sind `root`, `it_user` oder john_doe.
   - Ihren Active Directory-Benutzernamen.

     Active Directory-Namen können in einem der folgenden Formate eingegeben werden: <*Benutzername*>, <*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`.
2. Geben Sie in das Feld **Kennwort** Ihr iDRAC6-Benutzerkennwort oder Ihr Active Directory-Benutzerkennwort ein. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden.
3. Wählen Sie im Dropdown-Feld **Domäne** *Dieser iDRAC* aus, um sich als iDRAC6-Benutzer anzumelden, oder wählen Sie eine der verfügbaren Domänen aus, um sich als Active Directory-Benutzer anzumelden.

   ANMERKUNG: Als Active Directory-Benutzer wählen Sie im Dropdown-Menü *Dieser iDRAC* aus, wenn Sie den Domänennamen als Teil des Benutzernamens angegeben haben.
4. 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 angezeigt, wenn Sie sich angemeldet haben.

ANMERKUNG: Wenn Sie den Browser schließen, ohne sich abzumelden, kann dies dazu führen, dass die Sitzung so lange offen bleibt, bis eine Zeitüberschreitung eintritt. Es wird dringend empfohlen, zum Beenden der Sitzung auf die Schaltfläche „Abmeldung" zu klicken, da die Sitzung andernfalls möglicherweise aktiv bleibt, bis die Sitzungszeitüberschreitung eintritt.

ANMERKUNG: Wenn Sie die iDRAC6-Webschnittstelle im Microsoft Internet Explorer mit der Schließen-Schaltfläche („x") oben rechts im Fenster 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. Microsoft Internet Explorer Version 7 und 8 bieten die Option, Register und Fenster zu öffnen.

Jedes Register übernimmt die Merkmale des zuletzt geöffneten Registers.

Drücken Sie auf `<Strg-T>`, um ein neues Register in der aktiven Sitzung zu öffnen, und melden Sie sich erneut an.

Drücken Sie auf `<Strg-N>`, um ein neues Browser-Fenster in der aktiven Sitzung zu öffnen. Sie werden mit den bereits authentifizierten Anmeldeinformationen angemeldet.

Durch das Schließen eines Registers laufen alle Register der iDRAC6-Webschnittstelle ab.

Wenn Sie sich in einem Register mit Hauptbenutzerberechtigungen und dann in einem anderen Register als Administrator anmelden, sind für beide Register die Berechtigungen des ersten Registers erforderlich.

Das Verhalten der Register in Mozilla Firefox 3 ist identisch mit dem Registerverhalten in Microsoft Internet Explorer, Version 7 und 8.

Tabelle 4-1. Benutzerrechte-Verhalten in unterstützten Browsern

Browser	Registerverhalten	Fensterverhalten
Microsoft Internet Explorer 6	Entfällt	Neue Sitzung
Microsoft IE7 und IE8	Von letzter geöffneter Sitzung	Neue 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 konfigurieren“ auf Seite 38.

Netzwerk- und IPMI-LAN-Einstellungen konfigurieren

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

ANMERKUNG: Für die meisten DHCP-Server ist ein Server zum Speichern eines Client-Bezeichner-Tokens in der Reservierungstabelle erforderlich. Der Client (z. B. iDRAC) 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.

ANMERKUNG: Wenn STP (Spanning Tree-Protokoll) für die Ausführung aktiviert ist, stellen Sie sicher, dass auch PortFast oder eine ähnliche Technologie wie folgt eingeschaltet ist:
– An den Anschlüssen für den mit dem iDRAC6 verbundenen Schalter
– An den Anschlüssen, die an die Management Station angeschlossen sind, auf der eine virtuelle iDRAC-Konsolensitzung ausgeführt wird

ANMERKUNG: Eventuell wird die folgende Meldung eingeblendet, wenn das System während des POST anhält: `Drücken Sie zum Fortfahren die Taste F1 und zum Ausführen des System-Setup-Programms die Taste F2` Eine mögliche Ursache für diesen Fehler könnte eine Netzwerküberlastung sein, die dazu führt, dass die Verbindung zum iDRAC6 unterbrochen wird. Starten Sie das System neu, wenn die Netzwerküberlastung nachgelassen hat.

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

2 Auf der Seite **Netzwerk** können Sie Netzwerkeinstellungen, allgemeine iDRAC6-Einstellungen, IPv4-Einstellungen, IPv6-Einstellungen, IPMI-Einstellungen und VLAN-Einstellungen vornehmen. Siehe Tabelle 4-2, Tabelle 4-3, Tabelle 4-4, Tabelle 4-5, Tabelle 4-6 und Tabelle 4-7.

3 Klicken Sie nach Eingabe der erforderlichen Einstelllungen auf **Anwenden**.

Die neuen Einstellungen auf der Seite Netzwerk werden gespeichert.

ANMERKUNG: Wenn Sie Änderungen an den Einstellungen der NIC-IP-Adresse vornehmen, werden alle Benutzersitzungen geschlossen, und die Benutzer müssen unter Verwendung der aktualisierten IP-Adresseneinstellungen eine neue Verbindung zur iDRAC6-Webschnittstelle herstellen. Alle anderen Änderungen erfordern das Zurücksetzen des NIC, wodurch eine kurzzeitige Unterbrechung der Verbindungen verursacht werden kann.

Tabelle 4-2. Netzwerkeinstellungen

Einstellung	Beschreibung
NIC-Auswahl	Konfiguriert den aktuellen Modus aus den vier möglichen Modi: • Dediziert • Freigegeben (LOM1) • Freigegeben für Failover: LOM2 • Freigegeben für Failover: Alle LOMs **ANMERKUNG:** Die Option **Dediziert** ist nur für iDRAC Enterprise-Karten verfügbar, und die Option **Freigegeben für Failover: Alle LOMs** ist eventuell nur für einige wenige Systeme verfügbar. iDRAC6 kommuniziert nicht lokal über denselben physischen Anschluss, wenn die NIC-Auswahl entweder auf den Modus **Freigegeben** oder auf den Modus **Freigegeben für Failover** gesetzt ist. Der Grund dafür ist, dass ein Netzwerk-Switch keine Pakete über denselben Anschluss sendet, über den er sie empfangen hat. Wenn die NIC-Auswahl auf **Freigegeben für Failover** (LOM 2 oder alle LOMs) eingestellt ist, empfiehlt es sich, die LOMs nicht mit unterschiedlichen Netzwerk-Broadcast-Domänen zu verbinden. Es wird empfohlen, LOMs nicht mit Add-In-Netzwerk-Controllern im Teaming-Betrieb zusammenzufassen, wenn iDRAC für einen freigegebenen Modus konfiguriert ist. Jede Art von Team zwischen den LOMs ist annehmbar, unabhängig vom NIC-Auswahlmodus (freigegeben/freigegeben mit Failover LOM2/freigegeben mit Failover alle LOMs.)

Tabelle 4-2. Netzwerkeinstellungen *(fortgesetzt)*

Einstellung	Beschreibung
MAC-Adresse	Zeigt die MAC-Adresse (Media Access Control) an, die die einzelnen Knoten in einem Netzwerk eindeutig identifiziert.
NIC aktivieren	Wenn markiert, weist dies darauf hin, dass die NIC aktiviert ist und die verbleibenden Steuerungen dieser Gruppe aktiviert werden. Wenn ein NIC deaktiviert ist, wird jegliche Datenübertragung zum und vom iDRAC6 über das Netzwerk blockiert. Die Standardeinstellung ist **Ein**.
Automatische Verhandlung	Wenn auf **Ein** eingestellt, werden die Netzwerkgeschwindigkeit und der Modus durch Kommunizieren mit dem nächstgelegenen Router oder Switch angezeigt. Wenn auf **Aus** eingestellt, können Sie die Netzwerkgeschwindigkeit und den Duplexmodus manuell einstellen. Falls **NIC-Auswahl** *nicht* auf **Dediziert** eingestellt ist, wird die Einstellung „Automatische Verhandlung“ immer aktiviert sein (**Ein**). **ANMERKUNG:** Wenn der Server ausgeschaltet ist, unterstützen die integrierten LOM-Schnittstellen eine maximale Taktrate von 100 Mbps. Aus diesem Grund wird durch die Konfiguration der LOMs und des Schalters zum Unterstützen der automatischen Verhandlung die Konnektivität zu iDRAC über Systemstromübergänge sichergestellt.
Netzwerkgeschwindigkeit	Ermöglicht Ihnen, die Netzwerkgeschwindigkeit entsprechend der Netzwerkumgebung auf 100 Mb oder 10 Mb einzustellen. Diese Option steht nicht zur Verfügung, wenn „Automatische Verhandlung“ auf **Ein** eingestellt ist.
Duplexmodus	Ermöglicht Ihnen, den Duplexmodus entsprechend der Netzwerkumgebung auf Voll- oder Halbduplex einzustellen. Diese Option ist nicht verfügbar, wenn **Automatische Verhandlung** auf **Ein** eingestellt ist.
NIC MTU	Ermöglicht Ihnen, die MTU-Größe (maximale Paketgröße) im NIC einzustellen.

Tabelle 4-3. Allgemeine Einstellungen

Einstellung	Beschreibung
iDRAC auf DNS registrieren	Registriert den iDRAC6-Namen auf dem DNS-Server. Die Standardeinstellung ist **Deaktiviert**.
DNS iDRAC-Name	Zeigt den iDRAC6-Namen nur an, wenn **iDRAC auf DNS registrieren** ausgewählt ist. Der Standardname lautet idrac-*service_tag*, wobei *service_tag* die Service-Tag-Nummer des Dell-Servers ist, z. B. idrac-00002.
Domänenname automatisch konfigurieren	Verwendet den Standard-DNS-Domänennamen. Wenn das Kontrollkästchen nicht ausgewählt ist und die Option **iDRAC auf DNS registrieren** ausgewählt ist, können Sie den DNS-Domänennamen im Feld **DNS-Domänenname** ändern. Die Standardeinstellung ist **Deaktiviert**.
DNS-Domänenname	Der Standard-**DNS-Domänenname** ist leer. Wenn das Kontrollkästchen **Domänenname automatisch konfigurieren** markiert ist, ist diese Option deaktiviert.

Tabelle 4-4. IPv4-Einstellungen

Einstellung	Beschreibung
IPv4 aktivieren	Wenn der NIC aktiviert ist, wird die IPv4-Protokoll-Unterstützung ausgewählt und die anderen Felder in diesem Abschnitt werden aktiviert.
DHCP aktivieren	Fordert den iDRAC6 auf, eine IP-Adresse für den NIC vom Server für das dynamische Host-Konfigurationsprotokoll (DHCP) abzurufen. Die Standardeinstellung ist **Aus**.
IP-Adresse	Gibt die iDRAC6-NIC-IP-Adresse an.
Subnetzmaske	Ermöglicht Ihnen, eine statische IP-Adresse für den iDRAC6-NIC einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, wählen Sie das Kontrollkästchen DHCP verwenden (für NIC-IP-Adresse) ab.
Gateway	Die Adresse eines Routers oder Switches. Der Wert wird im Punkttrennungs-Format angegeben, z. B. 192.168.0.1.

Tabelle 4-4. IPv4-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung *(fortgesetzt)*
DHCP zum Abrufen von DNS-Serveradressen verwenden	Aktivieren Sie das DHCP zum Abrufen von DNS-Server-Adressen, 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. Die Standardeinstellung ist **aus**. **ANMERKUNG:** Wenn das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** markiert ist, können IP-Adressen nicht in die Felder **Bevorzugter DNS-Server** und **Alternativer DNS-Server** eingetragen werden.
Bevorzugter DNS-Server	IP-Adresse des DNS Servers.
Alternativer DNS-Server	Alternative IP-Adresse des DNS Servers.

Tabelle 4-5. IPv6-Einstellungen

Einstellung	Beschreibung
IPv6 aktivieren	Wenn das Kontrollkästchen markiert ist, ist IPv6 aktiviert. Wenn das Kontrollkästchen nicht markiert ist, ist IPv6 deaktiviert. Die Standardeinstellung ist deaktiviert.
Automatische Konfiguration aktivieren	Wählen Sie dieses Kontrollkästchen aus, um dem iDRAC6 zu ermöglichen, die IPv6-Adresse des iDRAC6-NIC vom DHCPv6-Server (dynamisches Host-Konfigurationsprotokoll) abzurufen. Wenn die automatische Konfiguration aktiviert wird, werden auch die statischen Werte für IP-Adresse 1, Präfixlänge und IP-Gateway deaktiviert und geleert.
IP-Adresse 1	Konfiguriert die IPv6-Adresse für den iDRAC-NIC. Zum Ändern dieser Einstellung müssen Sie zuerst **Automatische Konfiguration** deaktivieren, indem Sie das entsprechende Kontrollkästchen abwählen.

Tabelle 4-5. IPv6-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
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** deaktivieren, indem Sie das entsprechende Kontrollkästchen abwählen.
Gateway	Konfiguriert den statischen Gateway für den iDRAC-NIC. Zum Ändern dieser Einstellung müssen Sie zuerst **Automatische Konfiguration** deaktivieren, indem Sie das entsprechende Kontrollkästchen abwählen.
Lokale Adresse verbinden	Gibt die lokale iDRAC6-NIC-IPv6-Link-Adresse an.
IP-Adresse 2...15	Gibt die zusätzliche iDRAC6-NIC-IPv6-Adresse an, sofern eine verfügbar ist.
DHCP zum Abrufen von DNS-Serveradressen verwenden	Aktivieren Sie das DHCP zum Abrufen von DNS-Server-Adressen, indem Sie das Kontrollkästchen **DHCP 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. Die Standardeinstellung ist Aus. **ANMERKUNG:** Wenn das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** markiert ist, können IP-Adressen nicht in die Felder **Bevorzugter DNS-Server** und **Alternativer DNS-Server** eingetragen werden.
Bevorzugter DNS-Server	Konfiguriert die statische IPv6-Adresse für den bevorzugten DNS-Server. Zum Ändern dieser Einstellung müssen Sie zuerst **DHCP zum Abrufen von DNS-Serveradressen verwenden** deaktivieren.
Alternativer DNS-Server	Konfiguriert die statische IPv6-Adresse für den alternativen DNS-Server. Zum Ändern dieser Einstellung müssen Sie zuerst **DHCP zum Abrufen von DNS-Serveradressen verwenden** deaktivieren.

Tabelle 4-6. IPMI-Einstellungen

Einstellung	Beschreibung
IPMI-über-LAN aktivieren	Wenn markiert, weist dies darauf hin, dass der IPMI LAN-Kanal aktiviert ist. Die Standardeinstellung ist **Aus**.
Beschränkung der Kanalberechtigungsebene	Konfiguriert die niedrigste 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: 0 bis 20 Hexadezimalzeichen (keine Leerstellen erlaubt). Der Standardwert besteht ausschließlich aus Nullen.

Tabelle 4-7. VLAN-Einstellungen

Einstellung	Beschreibung
VLAN-ID aktivieren	Wenn aktiviert, wird nur abgestimmter VLAN-ID-Datenverkehr (virtuelles LAN) akzeptiert.
VLAN ID	VLAN-ID-Feld von 802.1g-Feldern. Geben Sie einen gültigen Wert für die VLAN-ID ein (eine Zahl zwischen 1 und 4094).
Priorität	Prioritätsfeld von 802.1g-Feldern. Geben Sie eine Zahl zwischen 0 und 7 ein, um die Priorität der VLAN-ID einzustellen.

IP-Filterung und IP-Blockierung konfigurieren

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

1. Klicken Sie auf **iDRAC-Einstellungen→ Netzwerk/Sicherheit** und klicken Sie dann auf das Register **Netzwerk**, um die Seite **Netzwerk** zu öffnen.
2. Klicken Sie auf **Erweiterte Einstellungen**, um die Netzwerksicherheitseinstellungen zu konfigurieren.

   Tabelle 4-8 beschreibt die Einstellungen der **Seite Netzwerksicherheit**.
3. Klicken Sie nach der Konfiguration der Einstellungen auf **Anwenden**.

   Speichert alle neuen Einstellungen, die Sie auf der Seite Netzwerksicherheit vorgenommen haben.

Tabelle 4-8. Einstellungen der Seite „Netzwerksicherheit"

Einstellungen	Beschreibung
IP-Bereich aktiviert	Aktiviert die Funktion zur Überprüfung des IP-Bereichs. Die Funktion definiert einen Bereich von IP-Adressen, die auf den iDRAC zugreifen können. Die Standardeinstellung ist **aus**.
IP-Bereichs-Adresse	Bestimmt das akzeptable IP-Adressen-Bitmuster, abhängig von den Einsen (1) in der Subnetzmaske. Dieser Wert wird mit binärem UND mit der Subnetzmaske des IP-Bereichs verbunden, um den oberen Teil der zulässigen IP-Adresse zu bestimmen. Jeder IP-Adresse, die dieses Bitmuster in ihrem oberen Bitbereich enthält, wird erlaubt, eine iDRAC6-Sitzung herzustellen. Anmeldeversuche von IP-Adressen, die sich außerhalb dieses Bereichs befinden, schlagen fehl. Die Standardwerte in jeder Eigenschaft erlauben einem Adressenbereich von 192.168.1.0 bis 192.168.1.255, eine iDRAC6-Sitzung herzustellen.
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 **aus**.
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 dem Anmeldeversuche von einer IP-Adresse auf Grund übermäßiger Fehler zurückgewiesen werden. Die Standardeinstellung ist **3600**.

Plattformereignisse konfigurieren

Die Plattformereigniskonfiguration bietet einen Mechanismus zur Konfiguration des iDRAC6, damit bei bestimmten Ereignismeldungen ausgewählte Maßnahmen getroffen werden können. Die Maßnahmen umfassen: 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 4-9 aufgeführt.

Tabelle 4-9. Plattformereignisfilter

Stichwort-verzeichnis	Plattformereignis
1	Assertion Lüfter kritisch
2	Assertion Batteriewarnung
3	Assertion Batterie kritisch
4	Assertion Spannung kritisch
5	Assertion Temperaturwarnung
6	Assertion Temperatur kritisch
7	Assertion Eingriff kritisch
8	Redundanz herabgesetzt
9	Redundanz verloren
10	Assertion Prozessorwarnung
11	Assertion Prozessor kritisch
12	Assertion Prozessor nicht vorhanden/kritisch
13	Assertion Netzteilwarnung
14	Assertion Netzteil kritisch
15	Assertion Netzteil nicht vorhanden/kritisch
16	Assertion Ereignisprotokoll kritisch
17	Assertion Watchdog kritisch
18	Assertion Systemstromwarnung
19	Assertion Systemstrom kritisch

Tabelle 4-9. Plattformereignisfilter *(fortgesetzt)*

Stichwort-verzeichnis	Plattformereignis
20	Assertion wechselbarer Flash-Datenträger nicht vorhanden – Zur Information
21	Assertion wechselbarer Flash-Datenträger – Kritisch
22	Assertion wechselbarer Flash-Datenträger – Warnung

Wenn ein Plattformereignis auftritt (z. B. eine Batteriewarnungsassertion), 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 über einen unterstützten Webbrowser am Remote-System an. Siehe „Zugriff auf die Webschnittstelle“ auf Seite 48.
2. Klicken Sie auf **System→ Warnungen→ Plattformereignisse**.
3. Wählen Sie unter **Plattformereignisfilter-Konfiguration** die Option **Aktiviert** aus, um **Plattformereignisfilter-Warnungen zu aktivieren**.

   ANMERKUNG: **Plattformereignisfilter-Warnungen aktivieren** muss aktiviert sein, damit eine Warnung an ein gültiges, konfiguriertes Ziel gesendet werden kann (PET oder E-Mail).
4. Führen Sie in der Tabelle **Liste der Plattformereignisfilter** Folgendes für die Filter aus, die Sie konfigurieren möchten:
   - Wählen Sie eine der folgenden Maßnahmen:
     - System neu starten
     - System aus- und wieder einschalten (Power Cycle)
     - System ausschalten
     - Keine Maßnahme

- Markieren Sie in der Spalte **Warnung erstellen** das Kontrollkästchen zum Aktivieren der Warnungserstellung oder heben Sie die Markierung des Kontrollkästchens auf, um die Warnungserstellung für die ausgewählte Maßnahme zu deaktivieren.

ANMERKUNG: Warnung erstellen muss aktiviert sein, damit eine Warnung an ein gültiges, konfiguriertes Ziel gesendet werden kann (PET).

5 Klicken Sie auf **Anwenden**. Die Einstellungen werden gespeichert.

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 über einen unterstützten Webbrowser am Remote-System an.

2 Vergewissern Sie sich, dass Sie die unter „Plattformereignisfilter (PEF) konfigurieren“ auf Seite 60 beschriebenen Verfahren ausgeführt haben.

3 Klicken Sie auf **System→ Warnungen→ Traps-Einstellungen**.

4 Gehen Sie in der **IPv4-Ziel-Liste** oder in der **IPv6-Ziel-Liste** bzgl. der **Zielnummer** folgendermaßen vor, um die IPv4- oder IPv6-SNMP-Warnungsziele zu konfigurieren:

   a Markieren Sie das Kontrollkästchen **Zustand** oder heben Sie dessen Markierung auf. Ein markiertes Kontrollkästchen weist darauf hin, dass die IP-Adresse zum Empfangen von Warnungen aktiviert ist. Ein Kontrollkästchen mit aufgehobener Markierung bedeutet, dass die IP-Adresse zum Empfangen von Warnungen deaktiviert ist.

   b Geben Sie unter **Ziel-IPv4-Adresse** oder **Ziel-IPv6-Adresse** eine gültige IP-Adresse eines Plattformereignis-Trap-Ziels ein.

   c Klicken Sie unter **Test-Trap** auf **Senden**, um die konfigurierte Warnung zu testen.

ANMERKUNG: Ihr Benutzerkonto muss über die Berechtigung **Testwarnungen** verfügen, damit Sie einen Test-Trap senden können. Weitere Informationen finden Sie unter Tabelle 6-6.

Die von Ihnen festgelegten Änderungen werden entweder in der IPv4- oder der IPv6-**Ziel-Liste** angezeigt.

5 Geben Sie in das Feld **Community-Zeichenkette** den iDRAC-SNMP-Community-Namen ein.

ANMERKUNG: Die Ziel-Community-Zeichenkette muss mit der iDRAC6-Community-Zeichenkette übereinstimmen.

6 Klicken Sie auf **Anwenden**. Die Einstellungen werden gespeichert.

ANMERKUNG: Wenn Sie einen Plattformereignisfilter deaktivieren, wird auch der Trap deaktiviert, der diesem „fehlerhaft" werdenden Sensor zugeordnet ist. Ist die Option **Plattformereignisfilter-Warnungen aktivieren** ausgewählt, werden Traps, die mit Übergängen des Typs „fehlerhaft zu funktionstüchtig" assoziiert werden, immer generiert. Beispiel: Wenn Sie die Option **Warnung erstellen** für den **Assertionsfilter wechselbarer Flash-Datenträger nicht vorhanden – Zur Information** deaktivieren und die SD-Karte entfernen, wird der zugeordnete Trap nicht angezeigt. Der Trap wird erstellt, wenn Sie die SD-Karte erneut einlegen. Wenn Sie jedoch die Option **Plattformereignisfilter-Warnungen aktivieren** auswählen, wird ein Trap erstellt, wenn Sie die SD-Karte entfernen oder einlegen.

Konfiguration von E-Mail-Warnungen

ANMERKUNG: Wenn Ihr Mail-Server Microsoft Exchange Server 2007 ist, ist sicherzustellen, dass der iDRAC-Domänenname so konfiguriert ist, dass der Mail-Server die E-Mail-Warnungen des iDRAC empfängt.

ANMERKUNG: E-Mail-Warnungen unterstützen sowohl IPv4- als auch IPv6-Adressen.

1 Melden Sie sich über einen unterstützten Webbrowser am Remote-System an.

2 Vergewissern Sie sich, dass Sie die unter „Plattformereignisfilter (PEF) konfigurieren" auf Seite 60 beschriebenen Verfahren ausgeführt haben.

3 Klicken Sie auf **System→ Warnungen→ E-Mail-Warnungseinstellungen**.

4 Gehen Sie in der Tabelle **Ziel-E-Mail-Adressen** folgendermaßen vor, um eine Zieladresse für die **E-Mail-Warnungsnummer** zu konfigurieren:

   a Markieren Sie das Kontrollkästchen **Zustand** oder heben Sie dessen Markierung auf. Ein markiertes Kontrollkästchen weist darauf hin, dass die E-Mail-Adresse zum Empfangen der Warnungen aktiviert ist. Ein Kontrollkästchen mit aufgehobener Markierung bedeutet, dass die E-Mail-Adresse zum Empfangen von Warnungsmeldungen deaktiviert ist.

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

c Geben Sie in das Feld **E-Mail-Beschreibung** eine kurze Beschreibung ein.

5 Klicken Sie unter **Test-E-Mail** auf **Senden**, um die konfigurierten E-Mail-Warnungseinstellungen zu testen.

6 Geben Sie in das Feld **SMTP- [E-Mail-] Server-IP-Adresse** eine gültige IP-Adresse oder einen vollständig qualifizierten Domänennamen (FQDN) des für die Konfiguration zu verwendenden SMTP-Servers ein.

ANMERKUNG: Die **SMTP- (E-Mail-) Server-IP-Adresse** muss zum erfolgreichen Senden einer Test-E-Mail auf der Seite **E-Mail-Warnungseinstellungen** konfiguriert werden. Der SMTP-Server verwendet die eingestellte IP-Adresse zum Kommunizieren mit dem iDRAC6, um E-Mail-Warnungen zu senden, wenn ein Plattformereignis auftritt.

7 Klicken Sie auf **Anwenden**. Die Einstellungen werden gespeichert.

IPMI unter Verwendung der Webschnittstelle konfigurieren

1 Melden Sie sich über einen unterstützten Webbrowser am Remote-System an.

2 Konfigurieren Sie IPMI-über-LAN.

a Klicken Sie in der Struktur unter **System** auf **iDRAC-Einstellungen**.

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

c Wählen Sie auf der Seite **Netzwerk** unter **IPMI-Einstellungen** die Option **IPMI über LAN aktivieren** aus und klicken Sie auf **Anwenden**.

d Aktualisieren Sie die IPMI-LAN-Kanalberechtigungen, falls erforderlich.

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 Dropdown-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-LAN-Einstellungen** den Verschlüsselungsschlüssel in das Feld **Verschlüsselungsschlüssel** ein und klicken Sie auf **Anwenden**.

ANMERKUNG: Der Verschlüsselungsschlüssel muss aus einer geraden Anzahl von maximal 40 Hexadezimalzeichen bestehen.

3 IPMI Seriell über LAN (SOL) konfigurieren.

a Klicken Sie in der Struktur unter **System** auf **iDRAC-Einstellungen**.

b Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Seriell-über-LAN**.

c Wählen Sie auf der Seite **Seriell-über-LAN** die Option **Seriell-über-LAN aktivieren** aus.

d Aktualisieren Sie die IPMI-SOL-Baudrate.

ANMERKUNG: Um die serielle Konsole über LAN umzuleiten, stellen Sie sicher, dass die SOL-Baudrate mit der Baudrate des verwalteten Systems übereinstimmt.

e Klicken Sie auf das Dropdown-Menü **Baudrate**, wählen Sie die entsprechende Baudrate aus, und klicken Sie auf **Anwenden**.

f Aktualisieren Sie die erforderliche Mindestberechtigung. Diese Eigenschaft definiert die Mindestbenutzerberechtigung, die zur Verwendung der Funktion **Seriell-über-LAN** erforderlich ist.

Klicken Sie auf das Dropdown-Menü **Beschränkung der Kanalberechtigungsebene** und wählen Sie dann entweder **Benutzer** oder **Operator** oder **Administrator** aus.

g Klicken Sie auf **Anwenden**.

4 Konfigurieren Sie IPMI-Seriell.

a Klicken Sie auf dem Register **Netzwerksicherheit** auf **Seriell**.

b Ändern Sie im Menü **Seriell** den seriellen IPMI-Verbindungsmodus auf die entsprechende Einstellung.

Klicken Sie unter **IPMI-Seriell** auf das Dropdown-Menü **Verbindungsmoduseinstellung**, und wählen Sie den entsprechenden Modus aus.

c Stellen Sie die IPMI-Seriell-Baudrate ein.

Klicken Sie auf das Dropdown-Menü **Baudrate**, wählen Sie die entsprechende Baudrate aus und klicken Sie auf **Anwenden**.

d Stellen Sie **Beschränkung der Kanalberechtigungsebene** und **Datenflusssteuerung** ein.

e Klicken Sie auf **Anwenden**.

f Stellen Sie sicher, dass der serielle MUX im BIOS-Setup-Programm des verwalteten Systems korrekt eingestellt ist.

- Starten Sie das System neu.
- Drücken Sie während des POST <F2>, um das BIOS-Setup-Programm zu öffnen.
- Wechseln Sie zu **Serielle Kommunikation**.
- Stellen Sie im Menü **Serial Connection** (Serielle Verbindung) sicher, dass **External Serial Connector** (Externe serielle Schnittstelle) auf **Remote Access Device** (Remote-Zugriffsgerät) gesetzt ist.
- Speichern und beenden Sie das BIOS-Setup-Programm.
- Starten Sie das System neu.

Wenn sich IPMI-Seriell im Terminalmodus befindet, können Sie die folgenden zusätzlichen Einstellungen konfigurieren:

- Löschsteuerung
- Echosteuerung
- Zeilenbearbeitung
- Neue Zeilenfolgen
- Neue Zeilenfolgen eingeben

Weitere Informationen über diese Eigenschaften finden Sie in der IPMI 2.0-Spezifikation. Weitere Informationen über Terminalmodusbefehle finden Sie im *Benutzerhandbuch für Dienstprogramme des Dell OpenManage Baseboard-Verwaltungs-Controllers* unter **dell.com/support/manuals**.

iDRAC6-Benutzer konfigurieren

Genauere Informationen finden Sie unter „iDRAC6-Benutzer hinzufügen und konfigurieren“ auf Seite 139.

iDRAC6-Datenübertragung mit SSL und digitalen Zertifikaten sichern

Dieser Abschnitt enthält Informationen über die folgenden Datensicherheitsfunktionen, die im iDRAC integriert sind:

- Secure Sockets Layer (SSL)
- Zertifikatsignierungsanforderung (CSR)
- Auf SSL über die webbasierte Schnittstelle zugreifen
- CSR erstellen
- Serverzertifikat hochladen
- Serverzertifikat anzeigen

Secure Sockets Layer (SSL)

Der iDRAC6 beinhaltet einen Web Server, der zur Verwendung des SSL-Sicherheitsprotokolls nach Industriestandard konfiguriert wurde, um verschlüsselte Daten über ein Netzwerk zu übertragen. SSL basiert auf einer Verschlüsselungstechnologie mit öffentlichem und privatem Schlüssel und ist eine allgemein akzeptierte Technologie, die authentifizierte und verschlüsselte Kommunikationen zwischen Clients und Servern ermöglicht, 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 128-Bit-SSL-Verschlüsselungsstandard, die sicherste Form von Verschlüsselung, die für Webbrowser in Nordamerika allgemein verfügbar ist.

Der iDRAC6-Web Server enthält standardmäßig ein selbstsigniertes Dell-SSL-Digitalzertifikat (Server-ID). Um bei Internetübertragungen eine hohe Sicherheit zu gewährleisten, ersetzen Sie das SSL-Zertifikat des Web Servers durch ein Zertifikat, das von einer bekannten Zertifizierungsstelle signiert wurde. 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 (CA) wie VeriSign oder Thawte senden.

Zertifikatsignierungsanforderung (CSR)

Eine CSR ist eine digitale Anforderung an eine CA für ein sicheres Serverzertifikat. Sichere Serverzertifikate ermöglichen Clients des Servers, die Identität des Servers, zu dem sie eine Verbindung hergestellt haben, als vertrauenswürdig einzustufen und eine verschlüsselte Sitzung mit dem Server auszuhandeln.

Eine Zertifizierungsstelle ist ein Unternehmen, das in der IT-Branche dafür anerkannt ist, hohe Ansprüche bezüglich der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger Sicherheitskriterien zu erfüllen. Beispiele für CAs umfassen Thawte und VeriSign. 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 im Zertifikat enthaltenen Informationen übereinstimmen.

Auf SSL über die webbasierte Schnittstelle zugreifen

1. Klicken Sie auf **iDRAC-Einstellungen→ Netzwerk/Sicherheit**.
2. Klicken Sie auf **SSL**, um die Seite **SSL** zu öffnen.

Auf der Seite **SSL** können Sie die folgenden Optionen ausführen:

- Eine Zertifikatsignierungsanforderung (CSR) zum Senden an eine CA erstellen. Die CSR-Informationen werden in der iDRAC6-Firmware gespeichert.
- Ein Serverzertifikat hochladen.
- Ein Serverzertifikat anzeigen.

Tabelle 4-10 beschreibt die o. g. Optionen auf der Seite **SSL**.

Tabelle 4-10. Optionen auf der Seite SSL

Feld	Beschreibung
Zertifikatsignierungsanforderung (CSR) erstellen	Mit dieser Option können Sie eine CSR erstellen, die Sie an eine CA senden, um ein sicheres Webzertifikat anzufordern. **ANMERKUNG:** Jede neue CSR überschreibt die vorherige CSR in der Firmware. Die Zertifikatsignierungsanforderung der Firmware muss mit dem von der Zertifizierungsstelle ausgegebenen Zertifikat übereinstimmen.
Serverzertifikat hochladen	Mit dieser Option können Sie ein vorhandenes Zertifikat hochladen, das Ihrem Unternehmen gehört und für die Zugriffsteuerung auf den iDRAC6 verwendet wird. **ANMERKUNG:** Der iDRAC6 akzeptiert lediglich X509-Base-64-kodierte Zertifikate. DER-kodierte Zertifikate werden nicht angenommen. Das Hochladen eines neuen Zertifikats ersetzt das Standardzertifikat, das Sie mit dem iDRAC6 erhalten haben.
Serverzertifikat anzeigen	Mit dieser Option können Sie ein vorhandenes Serverzertifikat anzeigen.

Zertifikatsignierungsanforderung erstellen

1. Wählen Sie auf der Seite **SSL** die Option **Zertifikatsignierungsanforderung (CSR) erstellen** und klicken Sie auf **Weiter**.
2. Geben Sie auf der Seite **Zertifikatsignierungsanforderung (CSR) erstellen** jeweils einen Wert für die einzelnen CSR-Attribute ein. Tabelle 4-11 beschreibt die CSR-Attribute.
3. Klicken Sie auf **Erstellen**, um die CSR zu erstellen, auf Ihren lokalen Computer herunterzuladen und in dem angegebenen Verzeichnis zu speichern.
4. Klicken Sie auf **Zurück zum SSL-Hauptmenü**, um zur SSL-Seite zurückzukehren.

Tabelle 4-11. Attribute für die Zertifikatsignierungsanforderung erstellen

Feld	Beschreibung
Allgemeiner Name	Der genaue Name, der zertifiziert werden soll (normalerweise der Domänenname des iDRAC, z. B. **xyzcompany.com**). Gültig sind alphanumerische Zeichen, Bindestriche und Punkte.
Name der Organisation	Der mit dieser Organisation assoziierte Name (zum Beispiel, XYZ Corporation). Gültig sind alphanumerische Zeichen, Bindestriche und Punkte.
Organisationseinheit	Der einer Organisationseinheit, z. B. eine IT-Abteilung zugeordnete Name. Gültig sind alphanumerische Zeichen, Bindestriche und Punkte.
Ort	Die Stadt oder ein anderer Standort des Unternehmens, das zertifiziert wird (z. B. München). Gültig sind alphanumerische Zeichen, Bindestriche und Punkte.
Name des Staates	Das Bundesland oder der Kanton, in dem sich das Unternehmen, das sich für eine Zertifizierung bewirbt, befindet (z. B. Bayern). Gültig sind alphanumerische Zeichen, Bindestriche und Punkte. Verwenden Sie keine Abkürzungen.
Name des Landes	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 des Unternehmens oder eine beliebige mit der CSR in Zusammenhang stehende E-Mail-Adresse ein. Dieses Feld ist optional.

Serverzertifikat hochladen

1 Wählen Sie auf der Seite **SSL** die Option **Serverzertifikat hochladen** aus und klicken Sie auf **Weiter**.

Die Seite **Serverzertifikat hochladen** wird angezeigt.

2 Geben Sie im Feld **Dateipfad** den Pfad des Zertifikats in das Feld **Wert** ein, oder klicken Sie auf **Durchsuchen**, um zur Zertifikatdatei zu navigieren.

ANMERKUNG: Der Wert **Dateipfad** zeigt den relativen Dateipfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad eingeben, der den vollständigen Pfad und den vollständigen Dateinamen sowie die Dateierweiterung enthält.

3 Klicken Sie auf **Anwenden**.

4 Klicken Sie auf **Zurück zum SSL-Hauptmenü**, um zur Seite **SSL-Hauptmenü** zurückzukehren.

Serverzertifikat anzeigen

1 Wählen Sie auf der Seite **SSL** die Option **Serverzertifikat anzeigen** aus und klicken Sie auf **Weiter**.

Die Seite **Serverzertifikat anzeigen** zeigt das Serverzertifikat an, das Sie auf den iDRAC hochgeladen haben.

Tabelle 4-12 erläutert die Felder und zugehörigen Beschreibungen, die in der Tabelle **Zertifikat** aufgeführt sind.

2 Klicken Sie auf **Zurück zum SSL-Hauptmenü**, um zur Seite **SSL-Hauptmenü** zurückzukehren.

Tabelle 4-12. Zertifikatinformationen

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

Active Directory konfigurieren und verwalten

Auf dieser Seite können Sie Active Directory-Einstellungen konfigurieren und verwalten.

ANMERKUNG: Sie müssen die Berechtigung **iDRAC konfigurieren** besitzen, um Active Directory zu verwenden oder zu konfigurieren.

ANMERKUNG: Bevor Sie die Active Directory-Funktion konfigurieren oder verwenden, muss sichergestellt sein, dass der Active Directory-Server für die Kommunikation mit dem iDRAC6 konfiguriert ist.

ANMERKUNG: Ausführliche Informationen zur Active Directory-Konfiguration und zur Konfiguration von Active Directory mit Erweitertem Schema oder Standardschema finden Sie unter „iDRAC6-Verzeichnisdienst verwenden" auf Seite 155.

So greifen Sie auf die Seite **Active Directory-Konfiguration und Verwaltung** zu :

1. Klicken Sie auf **iDRAC-Einstellungen→ Netzwerk/Sicherheit**.
2. Klicken Sie auf **Active Directory**, um die Seite **Active Directory-Konfiguration und Verwaltung** zu öffnen.

   Tabelle 4-13 führt die Optionen der Seite **Active Directory-Konfiguration und Verwaltung** auf.
3. Klicken Sie auf **Active Directory konfigurieren**, um Active Directory zu konfigurieren. Ausführliche Informationen zur Konfiguration finden Sie unter „iDRAC6-Verzeichnisdienst verwenden" auf Seite 155.
4. Klicken Sie auf **Einstellungen testen**, um die Active Directory-Konfiguration unter Verwendung der angegebenen Einstellungen zu testen. Ausführliche Informationen zur Option zum Testen der Einstellungen finden Sie unter „iDRAC6-Verzeichnisdienst verwenden" auf Seite 155.

Tabelle 4-13. Optionen der Seite „Active Directory-Konfiguration und Verwaltung"

Attribut	Beschreibung
Allgemeine Einstellungen	
Active Directory aktiviert	Gibt an, ob Active Directory aktiviert oder deaktiviert ist.
Einfache Anmeldung aktiviert	Gibt an, ob die einfache Anmeldung aktiviert oder deaktiviert ist. Falls aktiviert, können Sie sich am iDRAC6 anmelden, ohne Ihre Benutzeranmeldeinformationen für die Domäne, z. B. Benutzername und Kennwort, einzugeben. Markieren Sie das Kontrollkästchen, um die Anmeldung zu aktivieren.
Schemaauswahl	Gibt an, ob derzeit das Standardschema oder das erweiterte Schema mit Active Directory verwendet wird. **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	Dieser Wert enthält bis zu 40 Benutzerdomäneneinträge. Wenn der Wert konfiguriert ist, wird die Liste der Benutzerdomänennamen auf der Anmeldeseite als Pulldown-Menü für den anmeldenden Benutzer zur Auswahl angezeigt. Wenn dieser Wert nicht konfiguriert ist, können sich Active Directory-Benutzer weiterhin anmelden, indem sie den Benutzernamen in den folgenden Formaten eingeben: Benutzer_name@Domänen_name, Domänen_name/Benutzer_name oder Domänen_name\Benutzer_name.
Zeitüberschreitung	Gibt die Wartezeit für den Abschluss von Active Directory-Abfragen in Sekunden an. Der Standardwert beträgt 120 Sekunden.

Tabelle 4-13. Optionen der Seite „Active Directory-Konfiguration und Verwaltung“ *(fortgesetzt)*

Attribut	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-Serveradresse 1-3 (FQDN oder IP)	Gibt den FQDN (vollständig qualifizierter Domänennamen) des Domänen-Controllers oder die IP-Adresse an. Mindestens eine der 3 Adressen muss konfiguriert werden. iDRAC6 versucht, nacheinander mit jeder der konfigurierten Adressen eine Verbindung aufzubauen, bis eine Verbindung hergestellt ist. Wenn das erweiterte Schema ausgewählt ist, sind dies die Adressen der Domänen-Controller, auf denen sich das iDRAC6-Geräteobjekt und die Zuordnungsobjekte befinden. Wenn das Standardschema ausgewählt ist, sind dies die Adressen der Domänen-Controller, auf denen sich die Benutzerkonten und Rollengruppen befinden.

Tabelle 4-13. Optionen der Seite „Active Directory-Konfiguration und Verwaltung“ *(fortgesetzt)*

Attribut	Beschreibung
Zertifikatsvalidierung aktiviert	iDRAC6 verwendet beim Herstellen einer Verbindung zum Active Directory das Netzwerkprotokoll Secure Socket Layer (SSL). Standardmäßig verwendet der iDRAC6 das in den iDRAC6 geladene Zertifizierungsstellenzertifikat, um das SSL-Serverzertifikat (Security Socket Layer) des Domänen-Controllers während des SSL-Handshake zu überprüfen und gewährleistet dadurch hohe Sicherheit. Die Zertifikatsvalidierung kann für Testzwecke deaktiviert werden, oder der Systemadministrator entscheidet sich, den Domänen-Controllern im Sicherheitsbereich ohne Überprüfung der SSL-Zertifikate zu vertrauen. Diese Option gibt an, ob die Zertifikatsvalidierung aktiviert oder deaktiviert ist.
Active Directory-CA-Zertifikat	
Zertifikat	Das Zertifikat der Zertifizierungsstelle, die alle SSL-Serverzertifikate (Security Socket Layer) des Domänen-Controllers unterzeichnet.
Einstellungen zum erweiterten Schema	**iDRAC-Name**: Gibt den Namen an, der den iDRAC eindeutig im Active Directory 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 iDRAC für die Verwendung mit Active Directory mit erweitertem Schema konfiguriert wurde.

Tabelle 4-13. Optionen der Seite „Active Directory-Konfiguration und Verwaltung“ *(fortgesetzt)*

Attribut	Beschreibung
Einstellungen zum Standardschema	**Globaler Katalogserver-Adresse 1-3 (FQDN oder IP)**: Gibt den FQDN (vollständig qualifizierter Domänenname) der IP-Adresse des globalen Katalogservers an. Mindestens eine der 3 Adressen muss konfiguriert werden. iDRAC6 versucht, nacheinander mit jeder der konfigurierten Adressen eine Verbindung aufzubauen, bis eine Verbindung hergestellt ist. Der globale Katalogserver ist für das Standardschema nur dann 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 die Gruppendomäne an. **Gruppenberechtigung**: Gibt die Gruppenberechtigungsebene an. Diese Einstellungen werden nur angezeigt, wenn der iDRAC für die Verwendung mit einem Active Directory-Standardschema konfiguriert wurde. Wählen Sie die Option **Lookup des Global Catalog-Servers mit DNS** aus, und geben Sie den **Root-Domänennamen** ein, der für die DNS-Suche zur Ermittlung von globalen Katalogservern in 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.

Konfiguration und Verwaltung von allgemeinem LDAP

iDRAC6 bietet eine generische Lösung zur Unterstützung der LDAP-basierten (Lightweight Directory Access Protocol) Authentifizierung. Für diese Funktion ist keine Schemaerweiterung Ihrer Verzeichnisdienste erforderlich. Informationen zum Konfigurieren des allgemeinen LDAP-Verzeichnisdienstes finden Sie unter „Allgemeiner LDAP-Verzeichnisdienst“ auf Seite 195.

iDRAC6-Dienste konfigurieren

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

1. Klicken Sie auf **iDRAC-Einstellungen→ Netzwerk/Sicherheit**. Klicken Sie auf das Register **Dienste**, um die Konfigurationsseite **Dienste** anzuzeigen.
2. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Lokale Konfiguration - siehe Tabelle 4-14.
   - Web Server - siehe Tabelle 4-15 für Informationen zu Web Server-Einstellungen.
   - SSH - siehe Tabelle 4-16 für Informationen zu SSH-Einstellungen.
   - Telnet - siehe Tabelle 4-17 für Informationen zu Telnet-Einstellungen
   - Remote-RACADM - siehe Tabelle 4-18 für Informationen zu Remote-RACADM-Einstellungen
   - SNMP-Agent - siehe Tabelle 4-19 für Informationen zu SNMP-Einstellungen
   - Automatisierter System-Wiederherstellungsagent (ASR-Agent) - siehe Tabelle 4-20 für Informationen zu ASR-Agent-Einstellungen
3. Klicken Sie auf **Annehmen**, um die Einstellungen auf der Seite **Dienste** zu übernehmen.

Tabelle 4-14. Lokale Konfiguration

Einstellung	Beschreibung
Lokale iDRAC-Konfiguration mittels Options-ROM deaktivieren	Deaktiviert die lokale Konfiguration des iDRAC mithilfe des Options-ROM. Das Options-ROM befindet sich im BIOS und enthält eine Benutzeroberfläche, welche die BMC- und iDRAC-Konfiguration gestattet. Das Options-ROM fordert Sie auf, das Setup-Modul durch Drücken von <Strg+E> zu öffnen.
Lokale iDRAC-Konfiguration mittels RACADM deaktivieren	Deaktiviert die lokale Konfiguration des iDRAC mithilfe von RACADM.

Tabelle 4-15. Web Server-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert den iDRAC6-Web Server. Wenn markiert, weist das Kontrollkästchen darauf hin, dass der Web Server aktiviert ist. Die Standardeinstellung ist **aktiviert**.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger Web Server-Sitzungen, die für dieses System zulässig sind. Dieses Feld kann nicht bearbeitet werden. Die maximale Anzahl gleichzeitiger Sitzungen beträgt fünf.
Aktive Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich dem Wert der **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 den Einstellungen der Zeitüberschreitung werden sofort wirksam und beenden die aktuelle Webschnittstellensitzung. Der Web Server wird ebenfalls zurückgesetzt. Bitte warten Sie einige Minuten ab, bevor Sie eine neue Webschnittstellensitzung starten. Der Zeitüberschreitungsbereich beträgt 60 bis 10800 Sekunden. Der Standardeinstellung ist 1800 Sekunden.

Tabelle 4-15. Web Server-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
HTTP-Schnittstellennummer	Der Anschluss, den der iDRAC6 auf eine Browser-Verbindung abhört. Die Standardeinstellung ist **80**.
HTTPS-Schnittstellennummer	Der Anschluss, den der iDRAC6 auf eine sichere Browser-Verbindung abhört. Die Standardeinstellung ist **443**.

Tabelle 4-16. SSH-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert SSH. Wenn markiert, ist SSH aktiviert.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger SSH-Sitzungen, die für dieses System zulässig sind. Sie können dieses Feld nicht bearbeiten. **ANMERKUNG:** iDRAC6 unterstützt bis zu 2 SSH-Sitzungen gleichzeitig.
Aktive Sitzungen	Die Anzahl von aktuellen SSH-Sitzungen auf dem System, kleiner/gleich der Einstellung für den Wert der **Max. Sitzungen**. 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, den der iDRAC6 auf eine SSH-Verbindung abhört. Die Standardeinstellung ist **22**.

Tabelle 4-17. Telnet-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert Telnet. Wenn markiert, ist Telnet aktiviert.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger Telnet-Sitzungen, die für dieses System zulässig sind. Sie können dieses Feld nicht bearbeiten. **ANMERKUNG:** iDRAC6 unterstützt bis zu 2 Telnet-Sitzungen gleichzeitig.
Aktive Sitzungen	Die Anzahl von aktuellen Telnet-Sitzungen auf dem System, kleiner/gleich der Einstellung für den Wert der **Max. Sitzungen**. Sie können dieses Feld nicht bearbeiten.
Zeitüberschreitung	Die Leerlaufzeitüberschreitung 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, den der iDRAC6 auf eine Telnet-Verbindung abhört. Die Standardeinstellung ist **23**.

Tabelle 4-18. Remote-RACADM- Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert/deaktiviert Remote-RACADM. Wenn markiert, ist Remote-RACADM aktiviert.
Aktive Sitzungen	Die Anzahl der aktuellen Remote-RACADM-Sitzungen auf dem System. Sie können dieses Feld nicht bearbeiten.

Tabelle 4-19. SNMP-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert/deaktiviert SNMP. Wenn markiert, ist SNMP aktiviert.
SNMP-Community-Name	Aktiviert/deaktiviert den SNMP-Community-Namen. Wenn markiert, ist der SNMP-Community-Name aktiviert. Definieren Sie die zu verwendende SNMP-Community-Zeichenkette. Der Community-Name kann aus bis zu 31 Zeichen (ohne Leerzeichen) bestehen. Die Standardeinstellung ist **öffentlich**.

Tabelle 4-20. Einstellung des automatisierten System-Wiederherstellungsagenten

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert/deaktiviert den automatisierten System-Wiederherstellungsagenten. Wenn markiert, ist der automatisierte System-Wiederherstellungsagent aktiviert.

iDRAC6 Firmware/Systemdienste-Wiederherstellungsimage aktualisieren

ANMERKUNG: Wenn die iDRAC6-Firmware beschädigt wird, was geschehen kann, wenn der iDRAC6-Firmware-Aktualisierungsvorgang vorzeitig abgebrochen wird, können Sie den iDRAC6 mithilfe der iDRAC6-Webschnittstelle wiederherstellen.

ANMERKUNG: Die Firmware-Aktualisierung behält standardmäßig die aktuellen iDRAC6-Einstellungen bei. Während des Aktualisierungsvorgangs haben Sie die Möglichkeit, die iDRAC6-Konfiguration auf die Werkseinstellungen zurückzusetzen. Wenn Sie die Konfiguration auf die Werkseinstellungen einstellen, müssen Sie das Netzwerk mithilfe des iDRAC6-Konfigurationsdienstprogramms konfigurieren.

1. Öffnen Sie die webbasierte iDRAC6-Schnittstelle und melden Sie sich am Remote-System an.
2. Klicken Sie auf **iDRAC-Einstellungen** und dann auf das Register **Aktualisierung**.

3 Klicken Sie auf der Seite **Hochladen/Zurücksetzen (Schritt 1 von 3)** auf **Durchsuchen**, um das von der Website **www.support.dell.com** heruntergeladene Firmware-Image bzw. das Systemdienst-Wiederherstellungs-Image auszuwählen.

ANMERKUNG: Wenn Sie Firefox ausführen, erscheint der Textcursor nicht im Feld **Firmware-Image**.

Zum Beispiel:

`C:\Updates\V1.0\<Image_Name>`.

ODER

`\\192,168.1,10\Updates\V1.0\<Image_Name>`

Standardmäßig ist der Name des Firmware-Image **firmimg.d6**.

4 Klicken Sie auf **Hochladen**.

Die Datei wird auf den iDRAC6 hochgeladen. Dieser Vorgang kann einige Minuten dauern.

Die folgende Meldung wird bis zum Abschluss des Vorgangs angezeigt:

`Datei wird hochgeladen...`

5 Auf der Seite **Status (Seite 2 von 3)** können Sie die Ergebnisse der Überprüfung einsehen, die auf der hochgeladenen Imagedatei durchgeführt wurde.

- Wenn die Systemwiederherstellungs-Image-Datei erfolgreich hochgeladen wurde und sie alle Überprüfungsvorgänge bestanden hat, wird der Name der Image-Datei angezeigt. Wenn ein Firmware-Image hochgeladen wurde, werden die aktuelle und die neue Firmware-Version angezeigt.

  ODER

- Wenn das Image nicht erfolgreich hochgeladen wurde oder es die Überprüfungsvorgänge nicht bestanden hat, wird eine entsprechende Fehlermeldung eingeblendet, und die Aktualisierung kehrt zur Seite **Hochladen/Zurücksetzen (Schritt 1 von 3)** zurück. Sie können versuchen, den iDRAC6 erneut zu aktualisieren, oder auf **Abbrechen** klicken, um den iDRAC6 in den normalen Betriebsmodus zurückzusetzen.

6 Im Fall eines Firmware-Image bietet Ihnen die Option **Konfiguration beibehalten** die Möglichkeit, die bestehende iDRAC6-Konfiguration beizubehalten oder zu löschen. Diese Option ist standardmäßig ausgewählt.

ANMERKUNG: Wenn Sie die Markierung des Kontrollkästchens für **Konfiguration beibehalten** aufheben, wird der iDRAC6 auf seine Standardeinstellungen zurückgesetzt. Das LAN ist in den Standardeinstellungen mit einer statischen IPv4-Adresse aktiviert. Sie werden u. U. nicht in der Lage sein, sich an der iDRAC6-Webschnittstelle anzumelden. Sie müssen die LAN-Einstellungen während des BIOS-POST unter Verwendung des iDRAC6-Konfigurationshilfsprogramms neu konfigurieren.

7 Klicken Sie zum Starten des Aktualisierungsvorgangs auf **Aktualisieren**.

8 Auf der Seite **Aktualisierung (Schritt 3 von 3)** können Sie den Status der Aktualisierung einsehen. Der Fortschritt des in Prozent gemessenen Aktualisierungsvorgangs wird in der Spalte **Fortschritt** angezeigt.

ANMERKUNG: Der Aktualisierungsvorgang wird während des Aktualisierungsmodus im Hintergrund auch dann fortgesetzt, wenn Sie zu einer anderen Seite wechseln.

Wenn die Firmware-Aktualisierung erfolgreich abgeschlossen ist, wird der iDRAC6 automatisch zurückgesetzt. Sie müssen das aktuelle Browserfenster schließen und eine neue iDRAC6-Verbindung in einem neuen Browserfenster herstellen. Wenn ein Fehler auftritt, wird eine entsprechende Fehlermeldung eingeblendet.

Wenn die Aktualisierung der Systemdienste-Wiederherstellung erfolgreich abgeschlossen ist/fehlschlägt, wird eine entsprechende Statusmeldung angezeigt.

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 webbasierte iDRAC6-Schnittstelle und melden Sie sich am Remote-System an.

Klicken Sie auf **System→ iDRAC-Einstellungen** und dann auf das Register **Aktualisierung**.

2 Klicken Sie auf der Seite **Hochladen/Zurücksetzen (Schritt 1 von 3)** auf **Zurücksetzen**. Die aktuelle und die zurückzusetzende Firmware-Version werden auf der Seite **Status (Schritt 2 von 3)** angezeigt.

Konfiguration beibehalten bietet Ihnen die Möglichkeit, die bestehende iDRAC6-Konfiguration beizubehalten oder zu löschen. Diese Option ist standardmäßig ausgewählt.

ANMERKUNG: Wenn Sie die Markierung des Kontrollkästchens für **Konfiguration beibehalten** aufheben, wird der iDRAC6 auf seine Standardeinstellungen zurückgesetzt. Das LAN ist in den Standardeinstellungen aktiviert. Sie werden u. U. nicht in der Lage sein, sich an der iDRAC6-Webschnittstelle anzumelden. Sie müssen die LAN-Einstellungen unter Verwendung des iDRAC6-Konfigurationshilfsprogramms während des BIOS-POST oder unter Verwendung des RACADM-Befehls (lokal auf dem Server verfügbar) neu konfigurieren.

3 Klicken Sie zum Starten des Firmware-Aktualisierungsvorgangs auf **Aktualisierung**.

Auf der Seite **Aktualisierung (Schritt 3 von 3)** können Sie den Status des Zurücksetzungsvorgangs einsehen. Der in Prozent gemessene Vorgang wird in der Spalte **Fortschritt** angezeigt.

ANMERKUNG: Der Aktualisierungsvorgang wird während des Aktualisierungsmodus im Hintergrund auch dann fortgesetzt, wenn Sie zu einer anderen Seite wechseln.

Wenn die Firmware-Aktualisierung erfolgreich abgeschlossen ist, wird der iDRAC6 automatisch zurückgesetzt. Sie müssen das aktuelle Browserfenster schließen und eine neue iDRAC6-Verbindung in einem neuen Browserfenster herstellen.

Remote-Syslog

Mit der iDRAC6-Enterprise-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. Damit die Protokolle im Remote-Syslog-Server eingegeben werden können, ist sicherzustellen, dass zwischen dem iDRAC6 und dem Remote-Syslog-Server 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 (User Datagram Protocol), 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 bzw. wenn die Protokolle im RAC-Protokoll und SEL-Protokoll des iDRAC6 eingetragen werden.

Remote-Syslog kann über die Remote-Webschnittstelle aktiviert werden:

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 4-21 führt die Remote-Syslog-Einstellungen auf.

Tabelle 4-21. 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 (Schnittstellen-nummer)	Geben Sie die Schnittstellennummer des Remote-Syslog-Servers ein. Die Schnittstellennummer muss zwischen 1 und 65535 liegen. 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.

Das erste Startlaufwerk kann über die Remote-Webschnittstelle ausgewählt werden:

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

Tabelle 4-22 führt die Einstellungen für **Erstes Startlaufwerk** auf.

Tabelle 4-22. 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 RFS-Funktion (Remote-Dateifreigabe) von iDRAC6 ermöglicht Ihnen, eine ISO- oder IMG-Imagedatei anzugeben, die sich auf einer Netzwerkfreigabe befindet, und diese dem Betriebssystem des verwalteten Servers als virtuelles Laufwerk zur Verfügung zu stellen, indem es als CD/DVD oder Diskette unter Verwendung eines Netzwerkdateisystems (Network File System, NFS) oder allgemeinen Internetdateisystems (Common Internet File System, CIFS) bereitgestellt wird.

Das Format des Pfads des freigegebenen CIFS-Image lautet:

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

Das Format des Pfads des freigegebenen NFS-Image lautet:

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

ANMERKUNG: Wenn Sie NFS verwenden, stellen Sie sicher, dass Sie den genauen <*Pfad zum Image*> einschließlich der Image-Dateierweiterung angeben, da zwischen Groß- und Kleinschreibung unterschieden wird.

ANMERKUNG: <*IP-Adresse*> muss eine IPv4-Adresse sein. Die IPv6-Adresse wird momentan nicht unterstützt.

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

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

Die RFS-Funktion verwendet die zugrunde liegende Implementierung des virtuellen Datenträgers in 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 zur RFS-Bereitstellung 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 stehen auch in iDRAC6 zur Verfügung.

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→ Remote-Dateifreigabe** aus.

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

Tabelle 4-23 führt die Einstellungen der Remote-Dateifreigabe auf.

Tabelle 4-23. 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. **Verbindung wird hergestellt**: Es wird gerade eine Verbindung zur Freigabe hergestellt.

Klicken Sie auf **Verbinden**, um eine Verbindung zu RFS herzustellen. Nachdem die Verbindung erfolgreich hergestellt worden ist, wird **Verbinden** deaktiviert.

ANMERKUNG: Auch wenn Sie Remote-Dateifreigabe konfiguriert habe, zeigt die GUI diese Information 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` <*image_location*>; Image-Speicherort auf der Netzwerkfreigabe; doppelte Anführungszeichen um den Speicherort setzen
- `-s` ; aktuellen Status anzeigen

ANMERKUNG: Die maximal unterstützte Anzahl von Zeichen für **Benutzername** und für **Kennwort** ist 40, und für **Imagedateipfad** 511. Alle Zeichen einschließlich alphanumerischer Zeichen und Sonderzeichen sind für diese drei Felder gestattet, mit Ausnahme der folgenden:

- ' (einfaches Anführungszeichen)
- " (doppeltes Anführungszeichen)
- , (Komma)
- < (kleiner als)
- > (größer als)

Internes zweifaches SD-Modul

Das interne zweifache SD-Modul (IDSDM) bietet Redundanz auf der Hypervisor-SD-Karte, indem eine andere SD-Karte verwendet wird, die den Inhalt der ersten SD-Karte spiegelt. Die zweite SD-Karte kann zusammen mit der anderen SD-Karte auf IDSDM eingestellt werden, indem die Option **Redundanz** auf dem Bildschirm **Integrierte Geräte** im System-BIOS-Setup auf **Spiegelungsmodus** eingestellt wird. Weitere Informationen über die BIOS-Optionen für IDSDM finden Sie im *Hardware-Benutzerhandbuch*, das auf der Dell Support-Website unter **sdell.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. Wenn sie auf **Aus** eingestellt ist, ist das IDSDM für das System nicht als Startgerät sichtbar.

Eine der beiden SD-Karten kann der Master sein. Beispiel: Wenn zwei SD-Karten im IDSDM installiert sind, während kein Netzstrom am System anliegt, wird SD1 als aktive Karte bzw. Master-Karte betrachtet. SD2 ist die Backup-Karte, und alle Schreibvorgänge des Dateisystem-IDSDM werden auf beiden Karten vorgenommen. Lesevorgänge finden jedoch nur über SD1 statt. Immer wenn SD1 ausfällt oder entfernt wird, wird SD2 automatisch zur aktiven (Master-) Karte. Die vFlash-SD-Karte wird im Spiegelungsmodus deaktiviert.

Tabelle 4-24. IDSDM-Status

IDSDM – Spiegelungsmodus	SD1-Karte	SD2-Karte	vFlash-SD-Karte
Enabled (Aktiviert)	Aktiv	Aktiv	Inaktiv
Disabled (Deaktiviert)	Aktiv	Inaktiv	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 auf **Wechselbarer Flash-Datenträger**. 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 der SD-Karten oder beide SD-Karten funktionieren nicht ordnungsgemäß.
- **Status des internen SD-Moduls** – Zeigt den Zustand der SD-Karte für SD1-, SD2- und vFlash-Karten 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 eine Warnung ausgegeben wurde.
  - Position – Position der SD-Karten.
  - Onlinestatus – SD1-, SD2- und vFlash-Karten können sich in einem der unter Tabelle 4-25 aufgeführten Zustände befinden.

Tabelle 4-25. Zustand der SD-Karte

SD-Karte	Status	Beschreibung
SD1 und SD2	Boot (Start-vorgang)	Der Controller wird hochgefahren.
	Aktiv	Die Karte ist bereit für die Annahme von SD-Lese-/Schreibanforderungen.
	Standby	Die Karte ist die sekundäre Karte. Sie erhält eine Kopie aller SD-Einträge.
	Failed (Fehlge-schlagen)	Während eines Lese- oder Schreibvorgangs einer SD-Karte wird ein Fehler gemeldet.
	Nicht vorhanden	Die SD-Karte wurde nicht erkannt.
	Offline	Zum Zeitpunkt des Starts unterscheidet sich die Kartenidentifikations-Signatur der Karte vom Wert des nichtflüchtigen Speichers, oder die Karte ist das Ziel eines aktiven Kopiervorgangs.
	Schreibge-schützt	Die Karte ist durch die physische Sperre auf der SD-Karte schreibgeschützt. Das IDSDM kann keine schreibgeschützte Karte verwenden.
vFlash	Aktiv	Die Karte ist bereit für die Annahme von SD-Lese-/Schreibanforderungen.
	Nicht vorhanden	Die SD-Karte wurde nicht erkannt.

5

Erweiterte iDRAC6-Konfiguration

Dieser Abschnitt bietet Informationen zur erweiterten iDRAC6-Konfiguration und wird Benutzern empfohlen, die fortgeschrittene Kenntnisse im Bereich Systemverwaltung haben und die iDRAC6-Umgebung an ihre speziellen Bedürfnissen anpassen möchten.

Bevor Sie beginnen

Die grundlegende Installation bzw. Einrichtung der iDRAC6-Hardware und -Software sollte zu diesem Zeitpunkt abgeschlossen sein. Weitere Informationen finden Sie unter „Grundlegende Installation des iDRAC6“ auf Seite 35.

iDRAC6 zur Anzeige der seriellen Ausgabe im Remote-Zugriff über SSH/Telnet konfigurieren

Sie können den iDRAC6 durch Ausführen der folgenden Schritte für die serielle Remote-Konsole konfigurieren:

Konfigurieren Sie zuerst das BIOS, um die serielle Konsole zu aktivieren:

1. Schalten Sie das System ein oder starten Sie es neu.
2. Drücken Sie die Taste <F2> umgehend, wenn folgende Meldung angezeigt wird:

   ```
   <F2> = System Setup
   ```

3. Scrollen Sie nach unten und wählen Sie durch Drücken der Eingabetaste **Serial Communication** (Serielle Kommunikation) aus.
4. Stellen Sie die Optionen der Seite **Serial Communication** folgendermaßen ein:

   ```
   Serial Communication... Eingeschaltet mit serieller
   Umleitung über COM2
   ```

   ANMERKUNG: Sie können die serielle Kommunikation auf **Eingeschaltet mit serieller Umleitung über COM1** einstellen, solange das Adressfeld des seriellen Anschlusses, serielles Gerät2, auch auf COM1 eingestellt ist.

```
Serielle Anschlussadresse... Serielles Gerät1 =
COM1, Serielles Gerät2 = COM2

Externer serieller Anschluss... Serielles Gerät1

Failsafe-Baudrate... 115200

Remote-Terminaltyp... vt100/vt220

Umleitung nach Start... aktiviert
```

Wählen Sie danach **Save Changes** (Änderungen speichern) aus.

5 Drücken Sie <Esc>, um das **System-Setup**-Programm zu beenden und die Konfiguration des System-Setup-Programms abzuschließen.

iDRAC6-Einstellungen zur SSH/Telnet-Aktivierung konfigurieren

Als nächstes konfigurieren Sie die iDRAC6-Einstellungen zur Aktivierung von SSH/Telnet, was entweder über RACADM oder die iDRAC6-Webschnittstelle erfolgen kann.

Führen Sie die folgenden Befehle aus, um die iDRAC6-Einstellungen zur Aktivierung von SSH/Telnet unter Verwendung von RACADM zu konfigurieren:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Sie können RACADM-Befehle auch im Remote-Zugriff ausführen. Siehe „RACADM im Remote-Zugriff verwenden“ auf Seite 121.

Führen Sie die folgenden Schritte aus, um die iDRAC6-Einstellungen zur Aktivierung von SSH/Telnet unter Verwendung der iDRAC6-Webschnittstelle zu konfigurieren:

1 Erweitern Sie die Struktur unter **System**, und klicken Sie auf **iDRAC-Einstellungen**.

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

3 Wählen Sie **Aktiviert** in den Abschnitten **SSH** oder **Telnet** aus.

4 Klicken Sie auf **Änderungen übernehmen**.

Mit dem nächsten Schritt wird eine Verbindung zum iDRAC6 über Telnet oder SSH hergestellt.

Eine Textkonsole über Telnet oder SSH starten

Nachdem Sie sich über die Management Station-Terminal-Software mit Telnet oder SSH am iDRAC6 angemeldet haben, können Sie die Textkonsole des verwalteten Systems umleiten, indem Sie den Telnet-/SSH-Befehl **console com2** verwenden. Es wird nur jeweils ein **console com2**-Client unterstützt.

Öffnen Sie zum Herstellen einer Verbindung zur Textkonsole des verwalteten Systems eine iDRAC6-Eingabeaufforderung (über eine Telnet- oder SSH-Sitzung angezeigt) und geben Sie Folgendes ein:

```
console com2
```

Der Befehl `console -h com2` zeigt den Inhalt des seriellen Verlaufspuffers an, bevor er auf Eingaben über die Tastatur oder neue Zeichen vom seriellen Anschluss wartet.

Die Standardgröße (bzw. maximale Größe) des Verlaufspuffers beträgt 8192 Zeichen. Sie können diese Zahl auf einen kleineren Wert einstellen, indem Sie den folgenden Befehl verwenden:

```
racadm config -g cfgSerial -o cfgSerialHistorySize
<Zahl>
```

Informationen zum Konfigurieren von Linux für die Konsolenumleitung während des Startvorgangs finden Sie unter „Linux während des Starts für die serielle Konsole konfigurieren“ auf Seite 100.

Telnet-Konsole verwenden

Telnet unter Verwendung von Microsoft Windows XP oder Windows 2003 ausführen

Wenn auf Ihrer Management Station Windows XP oder Windows 2003 ausgeführt wird, tritt möglicherweise ein Problem mit den Zeichen in einer iDRAC6-Telnet-Sitzung auf. Dieses Problem kann in der Form einer eingefrorenen Anmeldung auftreten, bei der die Eingabetaste nicht reagiert und die Eingabeaufforderung für das Kennwort nicht angezeigt wird.

Um dieses Problem zu beheben, laden Sie Hotfix 824810 von der Microsoft Support-Website unter **support.microsoft.com** herunter. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 824810.

Telnet mittels Windows 2000 ausführen

Wenn Ihre Management Station Windows 2000 ausführt, können Sie nicht mit der Taste <F2> auf das BIOS-Setup zugreifen. Verwenden Sie zum Beheben dieses Problems den Telnet-Client, der mit den Windows-Diensten für UNIX 3.5 geliefert wurde (empfohlener Gratis-Download von Microsoft). Rufen Sie **www.microsoft.com/downloads/** auf, und suchen Sie nach *Windows-Dienste für UNIX 3.5*.

Microsoft Telnet für die virtuelle Telnet-Konsole aktivieren

ANMERKUNG: Einige Telnet-Clients auf Microsoft-Betriebssystemen zeigen den BIOS-Setup-Bildschirm eventuell nicht richtig an, wenn die virtuelle BIOS-Konsole auf die VT100/VT220-Emulation eingestellt ist. Wenn dieses Problem auftritt, können Sie die Anzeige aktualisieren, indem Sie die virtuelle BIOS-Konsole zum ANSI-Modus ändern. Um dieses Verfahren im BIOS-Setup-Menü auszuführen, wählen Sie **Virtuelle Konsole→ Remote-Terminaltyp→ ANSI** aus.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete virtuelle Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine ordnungsgemäße Textanzeige sicherzustellen. Andernfalls werden einige Textanzeigen möglicherweise nicht richtig dargestellt.

1. Aktivieren Sie **Telnet** in den **Windows-Komponentendiensten**.
2. Stellen Sie eine Verbindung zum iDRAC6 in der Management Station her.

   Öffnen Sie eine Eingabeaufforderung, geben Sie folgenden Befehl ein, und drücken Sie die Eingabetaste:

   `telnet <IP-Adresse>:<Anschlussnummer>`

   wobei *`IP-Adresse`* die IP-Adresse für den iDRAC6 ist und *`Anschlussnummer`* die Telnet-Anschlussnummer (falls Sie einen neuen Anschluss verwenden).

Die Rücktaste für die Telnet-Sitzung konfigurieren

Je nach verwendetem Telnet-Client kann die Verwendung der Rücktaste zu unerwarteten Ergebnissen führen. Die Sitzung kann beispielsweise ein `^h`-Echo verursachen. Die meisten Microsoft- und Linux-Telnet-Clients können jedoch für die Verwendung der Rücktaste konfiguriert werden.

So konfigurieren Sie Microsoft-Telnet-Clients zur Verwendung der Rücktaste:

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

   ```
   telnet
   ```

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

   ```
   set bsasdel
   ```

   Die folgende Meldung wird angezeigt:

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

So konfigurieren Sie eine Linux-Telnet-Sitzung zur Verwendung der Rücktaste:

1. Öffnen Sie eine Eingabeaufforderung und geben Sie Folgendes ein:

   ```
   stty erase ^h
   ```
2. Geben Sie in der Eingabeaufforderung Folgendes ein:

   ```
   telnet
   ```

Secure Shell (SSH) verwenden

Es ist wichtig, dass die Geräte und die Geräteverwaltung des Systems sicher sind. Integrierte angeschlossene Geräte bilden den Kern vieler Geschäftsprozesse. Wenn diese Geräte gefährdet sind, kann dies gleichzeitig auch eine Gefährdung Ihres Geschäfts bedeuten, was neue Sicherheitsanforderungen an die Geräte-Verwaltungssoftware der Befehlszeilenoberfläche (CLI) stellt.

Secure Shell (SSH) ist eine Befehlszeilensitzung, die dieselben Fähigkeiten wie eine Telnet-Sitzung aufweist, jedoch mit verbesserter Sicherheit. Der iDRAC6 unterstützt SSH-Version 2 mit Kennwortauthentifizierung. SSH wird auf dem iDRAC6 aktiviert, wenn Sie die iDRAC6-Firmware installieren oder aktualisieren.

Sie können entweder PuTTY oder OpenSSH auf der Management Station verwenden, um eine Verbindung zum iDRAC6 des verwalteten Systems herzustellen. Wenn während des Anmeldungsverfahrens ein Fehler auftritt, gibt der Secure Shell-Client eine Fehlermeldung aus. Der Meldungstext hängt vom Client ab 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).

Es werden nur zwei SSH-Sitzungen gleichzeitig 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.

Geben Sie zum Aktivieren der SSH auf dem iDRAC6 Folgendes ein:

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Geben Sie zum Ändern des SSH-Anschlusses Folgendes ein:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort
<Schnittstellennummer>
```

Weitere Informationen zu den Eigenschaften cfgSerialSshEnable und cfgRacTuneSshPort finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Die iDRAC6-SSH-Umsetzung unterstützt mehrfache Verschlüsselungsschemata, wie in Tabelle 5-1 dargestellt.

Tabelle 5-1. Verschlüsselungsschemata

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

ANMERKUNG: SSHv1 wird nicht unterstützt.

Linux während des Starts für die serielle Konsole konfigurieren

Die folgenden Schritte beziehen sich speziell auf den Linux Grand Unified Bootloader (GRUB). Ähnliche Änderungen sind bei der Verwendung eines anderen Bootloaders erforderlich.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete virtuelle Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine ordnungsgemäße Textanzeige sicherzustellen. Andernfalls werden einige Textanzeigen möglicherweise nicht richtig dargestellt.

Bearbeiten Sie die Datei **/etc/grub.conf** wie folgt:

1. Suchen Sie in der Datei die Abschnitte zur allgemeinen Einstellung und fügen Sie die folgenden zwei Zeilen hinzu:

   ```
   serial --unit=1 --speed=57600
   terminal --timeout=10 serial
   ```

2. Hängen Sie zwei Optionen an die Kernel-Zeile an:

   ```
   kernel ............. console=ttyS1,115200n8r
   console=tty1
   ```

3. Wenn **/etc/grub.conf** eine `splashimage`-Direktive enthält, kommentieren Sie sie aus.

Tabelle 5-2 enthält ein Beispiel einer **/etc/grub.conf**-Datei, die die in diesem Verfahren beschriebenen Änderungen zeigt.

Tabelle 5-2. Beispieldatei: /etc/grub.conf

```
# grub.conf, erstellt durch
#
# Beachten Sie, dass „grub“ nach Vornehmen von
Änderungen an dieser Datei
# nicht erneut ausgeführt werden muss.
# HINWEIS:  Sie haben keine /boot-Partition. Dies
bedeutet, dass
#          alle Kernel und initrd-Pfade relativ zu /
sind, z. B.
```

Tabelle 5-2. Beispieldatei: /etc/grub.conf *(fortgesetzt)*

```
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=
/dev/sda1
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial -unit=1 -speed=57600
terminal -timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=
/dev/sda1 hda=ide-scsi console=ttyS0 console=
ttyS1,115200n8r
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

Verwenden Sie bei der Verarbeitung der Datei **/etc/grub.conf** die folgenden Richtlinien:

1. Deaktivieren Sie die grafische GRUB-Schnittstelle und verwenden Sie die textbasierte Schnittstelle; andernfalls wird der GRUB-Bildschirm nicht in der virtuellen RAC-Konsole angezeigt. Zum Deaktivieren der grafischen Schnittstelle kommentieren Sie die Zeile aus, die mit `splashimage` beginnt.
2. Um mehreren GRUB-Optionen das Starten von Sitzungen der virtuellen Konsole über die serielle RAC-Verbindung zu ermöglichen, fügen Sie die folgende Zeile allen Optionen hinzu:

   `console=ttyS1,115200n8r console=tty1`

   Tabelle 5-2 zeigt `console=ttyS1,57600` nur zur ersten Option hinzugefügt.

Anmeldung an der virtuellen Konsole nach dem Start aktivieren

Bearbeiten Sie die Datei **/etc/inittab** wie folgt:

Fügen Sie eine neue Zeile hinzu, um `agetty` auf der seriellen COM2-Schnittstelle zu konfigurieren:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

Tabelle 5-3 zeigt eine Beispieldatei mit der neuen Zeile.

Tabelle 5-3. Beispieldatei: /etc/innitab

```
#
# inittab  Diese Datei beschreibt, wie das INIT-
Verfahren
#          das System auf einer bestimmten
Ausführungsstufe einrichtet.
#
# Autor:  Miquel van Smoorenburg
#          Geändert für RHS Linux von Marc Ewing und
Donnie Barnes
#
# Standard-Ausführungsstufe. Die von RHS verwendeten
Ausführungsstufen lauten:
#   0 - Halt (initdefault NICHT auf diesen Wert
einstellen)
#   1 - Einzelbenutzer-Modus
#   2 - Multibenutzer-Modus, ohne NFS (gleich wie 3,
wenn kein
#       Netzwerkbetrieb vorhanden ist)
#   3 - Voller Multibenutzer-Modus
#   4 - Nicht verwendet
#   5 - X11
#   6 - Neu starten (initdefault NICHT auf diesen
Wert einstellen)
#
id:3:initdefault:

# Systeminitialisierung.
si::sysinit:/etc/rc.d/rc.sysinit
```

Tabelle 5-3. Beispieldatei: /etc/innitab *(fortgesetzt)*

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Auf jeder Ausführungsstufe auszuführende Befehle.
ud::once:/sbin/update

# Trap STRG-ALT-ENTF
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# Wenn die USV Stromausfall anzeigt, davon ausgehen,
dass einige
# Minuten Strom verbleiben. Planen Sie ein
Herunterfahren in 2 Minuten.
# Es wird hierbei natürlich angenommen, dass Strom
anliegt und die
# USV angeschlossen ist und korrekt funktioniert.
pf::powerfail:/sbin/shutdown -f -h +2 „Stromausfall;
System fährt herunter“
# Wenn Strom wiederhergestellt wurde, bevor das
Herunterfahren eingeleitet wurde, brechen Sie ab.
pr:12345:powerokwait:/sbin/shutdown -c „Strom
wiederhergestellt; Herunterfahren abgebrochen“
```

Tabelle 5-3. Beispieldatei: /etc/innitab *(fortgesetzt)*

```
# gettys in Standard-Ausführungsstufen ausführen
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# xdm in Ausführungsstufe 5 ausführen
# xdm ist jetzt ein separater Dienst
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Bearbeiten Sie die Datei **/etc/securetty** wie folgt:

Fügen Sie eine neue Zeile mit dem Namen des seriellen tty für COM2 hinzu:

```
ttyS1
```

Tabelle 5-4 zeigt eine Beispieldatei mit der neuen Zeile.

Tabelle 5-4. Beispieldatei: /etc/securetty

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

ANMERKUNG: Verwenden Sie die Sequenz der Untbr-Taste (~B), um auf einer seriellen Konsole mithilfe des IPMI-Hilfsprogramms die Befehle der magischen Linux **S-Abf**-Taste auszuführen.

iDRAC6 für serielle Verbindung konfigurieren

Zum Herstellen einer seriellen Verbindung zum iDRAC6 kann jede der folgenden Schnittstellen verwendet werden:

- iDRAC6-CLI
- Direktverbindung - grundlegender Modus
- Direktverbindung - Terminalmodus

Führen Sie zum Einrichten Ihres Systems für die Verwendung einer dieser Schnittstellen die folgenden Schritte aus:

1. Konfigurieren Sie das **BIOS**, um die serielle Verbindung zu aktivieren.
   a. Schalten Sie das System ein oder starten Sie es neu.
   b. Drücken Sie die Taste <F2> umgehend, wenn folgende Meldung angezeigt wird:

      ```
      <F2> = System Setup
      ```

   c. Scrollen Sie nach unten und wählen Sie durch Drücken der Eingabetaste **Serial Communication** (Serielle Kommunikation) aus.
   d. Stellen Sie den Bildschirm **Serial Communication** folgendermaßen ein:

      ```
      Externer serieller Anschluss... Remote-
      Zugriffsgerät
      ```

   e. Wählen Sie **Änderungen speichern** aus.
   f. Drücken Sie <Esc>, um das **System-Setup**-Programm zu beenden und die Konfiguration des System-Setup-Programms abzuschließen.
2. Stellen Sie eine Verbindung mit dem DB-9-Kabel oder Nullmodemkabel von der Management Station zum Server des verwalteten Knotens her. Siehe „DB-9- oder Nullmodemkabel für die serielle Konsole anschließen“ auf Seite 111.
3. Vergewissern Sie sich, ob die Verwaltungs-Terminalemulationssoftware für die serielle Verbindung konfiguriert ist. Siehe „Terminalemulationssoftware der Management Station konfigurieren“ auf Seite 112.
4. Konfigurieren Sie die iDRAC6-Einstellungen zum Aktivieren serieller Verbindungen. Sie können die Konfiguration über RACADM oder über die iDRAC6-Webschnittstelle durchführen.

Führen Sie die folgenden Befehle aus, um die iDRAC6-Einstellungen für die Aktivierung der seriellen Verbindung mittels RACADM zu konfigurieren:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

Führen Sie die folgenden Schritte aus, um die iDRAC6-Einstellungen für die Aktivierung der seriellen Verbindung mittels der iDRAC6-Webschnittstelle zu konfigurieren:

1. Erweitern Sie die Struktur unter **System**, und klicken Sie auf **iDRAC-Einstellungen**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Seriell**.
3. Wählen Sie **Aktiviert** im Abschnitt **Serieller RAC** aus.
4. Klicken Sie auf **Änderungen übernehmen**.

Wenn Sie seriell mit den vorhergehenden Einstellungen verbunden sind, müsste jetzt eine Anmeldeaufforderung angezeigt werden. Geben Sie den Benutzernamen und das Kennwort des iDRAC6 ein (die Standardwerte sind `root` bzw. `calvin`).

Über diese Schnittstelle können Funktionen wie RACADM ausgeführt werden. Beispiel: Geben Sie zum Ausdrucken des Systemereignisprotokolls den folgenden RACADM-Befehl ein:

```
racadm getsel
```

iDRAC6 bei Direktverbindung für Terminalmodus und grundlegenden Modus konfigurieren

Führen Sie mithilfe von RACADM den folgenden Befehl aus, um die iDRAC6-Befehlszeilenoberfläche zu deaktivieren:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

Führen Sie dann den folgenden RACADM-Befehl aus, um bei Direktverbindung den grundlegenden Modus zu aktivieren:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialConnectionMode 1
```

Führen Sie dann den folgenden RACADM-Befehl aus, um bei Direktverbindung den Terminalmodus zu aktivieren:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialConnectionMode 0
```

Dieselben Maßnahmen können auch mithilfe der iDRAC6-Webschnittstelle ausgeführt werden.

1. Erweitern Sie die Struktur unter **System**, und klicken Sie auf **iDRAC-Einstellungen**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Seriell**.
3. Wählen Sie **Aktiviert** im Abschnitt **Serieller RAC** ab.

   Für Direktverbindung mit grundlegendem Modus:

   Ändern Sie im Abschnitt **Serielle IPMI** das Drop-Down-Menü **Einstellungen des Datenübertragungsmodus** in **Direktverbindung - grundlegender Modus**.

   Für Direktverbindung mit Terminalmodus:

   Ändern Sie im Abschnitt **Serielle IPMI** das Drop-Down-Menü **Einstellungen des Datenübertragungsmodus** in **Direktverbindung - Terminalmodus**.
4. Klicken Sie auf **Änderungen übernehmen**. Weitere Informationen über Direktverbindung mit grundlegendem Modus und Direktverbindung mit Terminalmodus finden Sie unter „Seriellen Modus und Terminalmodus konfigurieren“ auf Seite 115.

Direktverbindung mit grundlegendem Modus ermöglicht es Ihnen, Hilfsprogramme wie ipmish direkt über die serielle Verbindung zu verwenden. Beispiel: Führen Sie zum Ausdrucken des Systemereignisprotokolls mittels ipmish über den grundlegenden IPMI-Modus den folgenden Befehl aus:

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin
sel get
```

Direktverbindung mit Terminalmodus ermöglicht es Ihnen, ASCII-Befehle an den iDRAC6 zu senden. Beispiel: Zum Ein-/Ausschalten des Servers über Direktverbindung mit Terminalmodus:

1. Stellen Sie eine Verbindung zum iDRAC6 über die Terminal-Emulations-Software her.
2. Geben Sie zum Anmelden den folgenden Befehl ein:

   ```
   [SYS PWD -U root calvin]
   ```

Als Antwort darauf wird Folgendes angezeigt:

```
[SYS]
```

```
[OK]
```

3 Geben Sie zum Überprüfen der erfolgreichen Anmeldung den folgenden Befehl ein:

```
[SYS TMODE]
```

Als Antwort darauf wird Folgendes angezeigt:

```
[OK TMODE]
```

4 Geben Sie zum Ausschalten des Servers (der Server wird umgehend ausgeschaltet) den folgenden Befehl ein:

```
[SYS POWER OFF]
```

5 Und zum Einschalten des Servers (der Server wird umgehend eingeschaltet):

```
[SYS POWER ON]
```

Zwischen serieller RAC-Schnittstellenkommunikation und serieller Konsole umschalten

Der iDRAC6 unterstützt Escape-Tastenfolgen, die eine Umschaltung zwischen serieller RAC-Schnittstellenkommunikation und serieller Konsole ermöglichen.

Um das System für dieses Verhalten einzurichten, gehen Sie wie folgt vor:

1 Schalten Sie das System ein oder starten Sie es neu.

2 Drücken Sie die Taste <F2> umgehend, wenn folgende Meldung angezeigt wird:

```
<F2> = System Setup
```

3 Scrollen Sie nach unten und wählen Sie durch Drücken der Eingabetaste **Serial Communication** (Serielle Kommunikation) aus.

4 Stellen Sie den Bildschirm **Serial Communication** folgendermaßen ein:

Serial Communication - Eingeschaltet mit serieller Umleitung über COM2

ANMERKUNG: Sie können die **serielle Kommunikation** auf **Eingeschaltet mit serieller Umleitung über COM1** einstellen, solange das **Adressfeld des seriellen Anschlusses, Serielles Gerät2**, auch auf COM1 eingestellt ist.

Serielle Anschlussadresse -- Serielles Gerät1 = COM1, Serielles Gerät2 = COM2

Externer serieller Anschluss -- Serielles Gerät2

Failsafe-Baudrate... 115200

Remote-Terminaltyp... vt100/vt220

Umleitung nach Start ... aktiviert

Wählen Sie danach **Save Changes** (Änderungen speichern) aus.

5. Drücken Sie <Esc>, um das **System-Setup**-Programm zu beenden und die Konfiguration des System-Setup-Programms abzuschließen.

Schließen Sie das Nullmodemkabel am externen seriellen Anschluss des verwalteten Systems und am seriellen Anschluss der Management Station an.

Verwenden Sie ein Terminal-Emulationsprogramm (HyperTerminal oder TeraTerm) auf der Management Station. Je nachdem, an welchem Punkt des Startprozesses sich der verwaltete Server befindet, werden entweder die POST-Bildschirme oder die Betriebssystem-Bildschirme angezeigt. Dies ist von der Konfiguration abhängig: SAC für Windows und Linux-Textmodus-Bildschirme für Linux. Setzen Sie die Terminaleinstellungen der Management Station auf Baud Rate-115200, data-8 bit, parity-none, stop-1 bit und Flow Control-None.

Um vom Modus der seriellen Konsole auf die serielle RAC-Schnittstellenkommunikation umzuschalten, verwenden Sie die folgende Tastenfolge:

```
<Esc> + <UMSCH> <9>
```

Mit der obigen Tastenfolge rufen Sie entweder die iDRAC-Anmeldeaufforderung auf (wenn der RAC auf den seriellen RAC-Modus gesetzt ist) oder den seriellen Anschlussmodus, in dem Terminalbefehle abgeben werden können (wenn der RAC auf den seriellen IPMI-Terminalmodus bei Direktverbindung eingestellt ist).

Um vom Modus der seriellen RAC-Schnittstellenkommunikation auf den Modus der seriellenKonsole umzuschalten, verwenden Sie die folgende Tastenfolge:

```
<Esc> + <UMSCH> <q>
```

Verwenden Sie im Terminalmodus zum Umschalten der Verbindung zum COM2-Anschluss des Systems:

```
<Esc> + <UMSCH> <q>
```

Verwenden Sie bei der Verbindung zum COM2-Anschluss des Systems zum Zurückwechseln in den Terminalmodus:

```
<Esc> + <UMSCH> <9>
```

DB-9- oder Nullmodemkabel für die serielle Konsole anschließen

Um mit einer seriellen Textkonsole auf das verwaltete System zuzugreifen, schließen Sie ein DB-9-Nullmodemkabel an den COM-Anschluss auf dem verwalteten System an. Damit die Datenübertragung auch über das Nullmodemkabel funktioniert, sollten die entsprechenden Einstellungen für serielle Übertragung im CMOS-Setup vorgenommen werden. Nicht alle DB-9-Kabel führen die Stiftbelegung/Signale, die für diese Verbindung erforderlich sind. Das DB-9-Kabel für diese Verbindung muss der in Tabelle 5-5 dargestellten Spezifikation entsprechen.

ANMERKUNG: Das DB-9-Kabel kann auch für die virtuelle BIOS-Textkonsole verwendet werden.

Tabelle 5-5. Erforderliche Stiftbelegung für das DB-9-Nullmodemkabel

Signalname	DB-9-Stift (Server-Stift)	DB-9-Stift (Workstation-Stift)
FG (Gehäusemasse)	-	-
TD (Daten senden)	3	2
RD (Daten empfangen)	2	3
RTS (Anforderung zu senden)	7	8
CTS (Sendebereitschaft)	8	7
SG (Betriebserde)	5	5
DSR (Datensatz bereit)	6	4
CD (Trägersignalerkennung)	1	4
DTR (Datenterminal bereit)	4	1 und 6

Terminalemulationssoftware der Management Station konfigurieren

iDRAC6 unterstützt eine serielle oder Telnet-Textkonsole von einer Management Station aus, auf der einer der folgenden Typen von Terminalemulationssoftware ausgeführt wird:

- Linux Minicom in einem Xterm
- Hilgraeve HyperTerminal Private Edition (Version 6.3)
- Linux Telnet in einem Xterm
- Microsoft Telnet

Um Ihre Art der Terminalsoftware zu konfigurieren, führen Sie die folgenden Schritte aus. Wenn Sie Microsoft Telnet verwenden, ist keine Konfiguration erforderlich.

Linux Minicom für die serielle Konsolenemulation konfigurieren

Minicom ist das Zugriffsdienstprogramm des seriellen Anschlusses für Linux. Die folgenden Schritte beziehen sich auf die Konfiguration der Minicom-Version 2.0. Andere Versionen von Minicom können geringfügig abweichen, erfordern jedoch die selben grundlegenden Einstellungen. Verwenden Sie die Informationen in „Erforderliche Minicom-Einstellungen für die Emulation der seriellen Konsole“ auf Seite 114 zur Konfiguration anderer Minicom-Versionen.

Minicom Version 2.0 für die Emulation der seriellen Konsole konfigurieren

ANMERKUNG: Um sicherzustellen, dass der Text ordnungsgemäß angezeigt wird, wird empfohlen, ein Xterm-Fenster zur Anzeige der Telnet-Konsole zu verwenden, statt der in der Linux-Installation enthaltenen Standardkonsole.

1. Um eine neue Xterm-Sitzung zu starten, geben Sie bei der Eingabeaufforderung `xterm &` ein.
2. Bewegen Sie im Xterm-Fenster den Mauspfeil in die untere rechte Ecke des Fensters, und ändern Sie die Größe des Fensters auf 80 x 25.
3. Wenn Sie keine Minicom-Konfigurationsdatei haben, fahren Sie mit dem nächsten Schritt fort.

   Wenn Sie eine Minicom-Konfigurationsdatei haben, geben Sie `minicom <Minicom Konfigurationsdateiname>` ein, und fahren Sie mit Schritt 17 fort.

4. Geben Sie an der Xterm-Eingabeaufforderung `minicom -s` ein.
5. Wählen Sie die Option **Seriellen Anschluss einrichten** aus und drücken Sie die Taste <Eingabe>.
6. Drücken Sie <a> und wählen Sie das entsprechende serielle Gerät (z. B. **/dev/ttyS0**) aus.
7. Drücken Sie <e>, und stellen Sie die Option **Bps/Par/Bits** auf **57600 8N1** ein.
8. Drücken Sie <f>, und stellen Sie die **Hardware-Datenflusssteuerung** auf **Ja** und die **Software-Datenflusssteuerung** auf **Nein** ein.
9. Um das Menü **Seriellen Anschluss einrichten** zu beenden, drücken Sie die Taste <Eingabe>.
10. Wählen Sie **Modem und Wählen** aus und drücken Sie die Taste <Eingabe>.
11. Drücken Sie im Menü **Modem-Wählen und Parameter-Setup** die <Rücktaste>, um die Einstellungen **init**, **reset**, **connect** und **hangup** zu löschen, sodass sie leer sind.
12. Drücken Sie die Eingabetaste, um jeden leeren Wert zu speichern.
13. Wenn alle angegebenen Felder gelöscht sind, drücken Sie die Taste <Eingabe>, um das Menü **Modem-Wählen und Parameter-Setup** zu beenden.
14. Wählen Sie **Setup als config_name speichern** aus und drücken Sie die Taste <Eingabe>.
15. Wählen Sie **Minicom beenden** aus und drücken Sie die Taste <Eingabe>.
16. Geben Sie bei der Befehls-/Shell-Eingabeaufforderung `minicom <Minicom Konfigurationsdateiname>` ein.
17. Um das Minicom-Fenster auf 80 x 25 zu erweitern, ziehen Sie an der Ecke des Fensters.
18. Drücken Sie <Strg+a>, <z>, <x>, um Minicom zu beenden.

ANMERKUNG: Wenn Sie Minicom für die serielle virtuelle Textkonsole verwenden, um das BIOS des verwalteten Systems zu konfigurieren, wird empfohlen, in Minicom die Farbeinstellung einzuschalten. Geben Sie zum Einschalten der Farbe den folgenden Befehl ein: `minicom -c on`

Stellen Sie sicher, dass das Minicom-Fenster eine Eingabeaufforderung anzeigt. Wenn die Eingabeaufforderung angezeigt wird, wurde Ihre Verbindung erfolgreich hergestellt, und Sie können jetzt mithilfe des seriellen Befehls **connect** eine Verbindung zur Konsole des verwalteten Systems herstellen.

Erforderliche Minicom-Einstellungen für die Emulation der seriellen Konsole

Verwenden Sie Tabelle 5-6 zum Konfigurieren einer beliebigen Minicom-Version .

Tabelle 5-6. Minicom-Einstellungen für die Emulation der seriellen Konsole

Beschreibung der Einstellung	Erforderliche Einstellung
Bit/s/Par/Bit	57600 8N1
Hardware-Datenflusssteuerung	Ja
Software-Datenflusssteuerung	Nein
Terminalemulation	ANSI
Einwahl per Modem und Parameter-Einstellungen	Löschen Sie die Einstellungen **init**, **reset**, **connect** und **hangup**, sodass sie leer sind
Fenstergröße	80 x 25 (um die Größe zu ändern, ziehen Sie die Ecke des Fensters)

HyperTerminal für die serielle Konsole konfigurieren

HyperTerminal ist das Zugriffsdienstprogramm des seriellen Anschlusses von Microsoft Windows. Um die Größe Ihres Bildschirms der virtuellen Konsole angemessen einzustellen, verwenden Sie Hilgraeve HyperTerminal Private Edition, Version 6.3.

VORSICHTSHINWEIS: Alle Versionen der Microsoft Windows-Betriebssysteme enthalten die Terminalemulationssoftware Hilgraeve HyperTerminal. Die integrierte Version enthält jedoch viele der Funktionen, die während des Vorgangs der virtuellen Konsole erforderlich sind, nicht. Verwenden Sie daher Edition 6.3 oder eine Terminal-Emulations-Software, die den Emulationsmodus VT100/VT220 oder ANSI unterstützt. Ein vollständiger VT100/VT220- oder ANSI-Terminalemulator, der die virtuelle Konsole auf Ihrem System unterstützt, ist beispielsweise HyperTerminal Private von Hilgraeve.

So konfigurieren Sie HyperTerminal für die serielle Konsole:

1. Starten Sie das HyperTerminal-Programm.
2. Geben Sie einen Namen für die neue Verbindung ein und klicken Sie auf **OK**.
3. Wählen Sie neben **Verbindung herstellen mit:** den COM-Anschluss auf der Management Station (z. B. COM2) aus, an dem Sie das DB-9-Nullmodemkabel angeschlossen haben, und klicken Sie auf **OK**.
4. Konfigurieren Sie die Einstellungen des COM-Anschlusses wie unter Tabelle 5-7 gezeigt.
5. Klicken Sie auf **OK**.
6. Klicken Sie auf **Datei→ Eigenschaften** und dann auf das Register **Einstellungen**.
7. Stellen Sie die **Telnet-Terminal-ID:** auf **ANSI**.
8. Klicken Sie auf **Terminal-Setup** und stellen Sie die **Bildschirmzeilen** auf **26**.
9. Stellen Sie die **Spalten** auf 80 und klicken Sie auf **OK**.

Tabelle 5-7. Einstellungen des COM-Anschlusses der Management Station

Beschreibung der Einstellung	Erforderliche Einstellung
Bits pro Sekunde	57600
Datenbits	8
Parität	NONE
Stoppbits	1
Datenflusssteuerung	Hardware

Seriellen Modus und Terminalmodus konfigurieren

IPMI und seriellen iDRAC6 konfigurieren

1. Erweitern Sie die Struktur unter **System**, und klicken Sie auf **iDRAC-Einstellungen**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Seriell**.
3. Konfigurieren Sie die seriellen IPMI-Einstellungen.

   Eine Beschreibung der seriellen IPMI-Einstellungen ist unter Tabelle 5-8 verfügbar.

4 Konfigurieren Sie die seriellen iDRAC6-Einstellungen.

Eine Beschreibung zu den seriellen iDRAC6-Einstellungen ist unter Tabelle 5-9 verfügbar.

5 Klicken Sie auf **Änderungen anwenden**, um die IPMI- und seriellen iDRAC6-Änderungen zu übernehmen.

6 Klicken Sie auf der Seite **Seriell** auf die entsprechende Schaltfläche, um fortzufahren. In der *iDRAC6-Online-Hilfe* finden Sie eine Beschreibung der auf der Seite **Serielle Konfiguration** verfügbaren Einstellungen.

Tabelle 5-8. Serielle IPMI-Einstellungen

Einstellung	Beschreibung
Verbindungsmodus-einstellungen	• Direktverbindung, grundlegender Modus - grundlegender serieller IPMI-Modus • Direktverbindung, Terminalmodus - serieller IPMI-Terminalmodus
Baudrate	• Legt die Datengeschwindigkeit fest. Wählen Sie **9600 Bit/s**, **19,2 kBit/s**, **57,6 kBit/s** oder **115,2 kBit/s** aus.
Flow Control (Datenflusssteuerung)	• Keine - Hardware-Datenflusssteuerung Aus • RTS/CTS – Hardware-Datenflusssteuerung Ein
Beschränkung der Kanalberechti-gungsebene	• Administrator • Operator • Benutzer

Tabelle 5-9. Serielle iDRAC6-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert die serielle iDRAC6-Konsole. Markiert=Aktiviert; Unmarkiert=Deaktiviert
Zeitüberschreitung	Die maximale Leerlaufzeit (in Sekunden), bevor die Leitung getrennt wird. Der Bereich beträgt 60 bis 1920 Sekunden. Die Standardeinstellung beträgt 300 Sekunden. Wählen Sie 0 Sekunden, um die Zeitüberschreitungsfunktion zu deaktivieren.

Tabelle 5-9. Serielle iDRAC6-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
Umleitung aktiviert	Aktiviert oder deaktiviert die virtuelle Konsole. Markiert = Aktiviert; Unmarkiert = Deaktiviert
Baudrate	Die Datengeschwindigkeit auf dem externen seriellen Anschluss. Die Werte betragen **9600 Bit/s**, **19,2 kBit/s**, **57,6 kBit/s** und **115,2 kBit/s**. Die Standardeinstellung ist **57,6 kBit/s**.
Escape-Taste	Gibt die <Esc>-Taste an. Die Standardeinstellung sind die Zeichen ^ \.
Größe Verlaufspuffer	Die Größe des seriellen Verlaufspuffers, der die letzten in die virtuelle Konsole geschriebenen Zeichen enthält. Maximum und Standard = 8192 Zeichen.
Anmeldungsbefehl	Die bei gültiger Anmeldung auszuführende iDRAC6-Befehlszeile.

Terminalmodus konfigurieren

1. Erweitern Sie die Struktur unter **System**, und klicken Sie auf **iDRAC-Einstellungen**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Seriell**.
3. Klicken Sie auf der Seite **Seriell** auf **Terminalmodus-Einstellungen**.
4. Konfigurieren Sie die Terminalmodus-Einstellungen.

   Eine Beschreibung der Terminalmodus-Einstellungen finden Sie unter Tabelle 5-10.
5. Klicken Sie auf **Änderungen übernehmen**.
6. Klicken Sie auf der Seite **Terminalmodus-Einstellungen** auf die entsprechende Schaltfläche, um fortzufahren. In der *iDRAC6-Online-Hilfe* finden Sie eine Beschreibung der auf der Seite **Terminalmodus-Einstellungen** verfügbaren Schaltflächen.

Tabelle 5-10. Terminalmodus-Einstellungen

Einstellung	Beschreibung
Zeilenbearbeitung	Aktiviert oder deaktiviert die Zeilenbearbeitung.
Löschsteuerung	Wählen Sie eine der folgenden Optionen: • iDRAC gibt ein <Rückt><Leer><Rückt>-Zeichen aus, wenn <Rückt> oder <Entf> empfangen wird. - • iDRAC gibt ein <Entf>-Zeichen aus, wenn <Rückt> oder <Entf> empfangen wird. -
Echo-Steuerung	Aktiviert oder deaktiviert Echo.
Handshaking-Steuerung	Aktiviert oder deaktiviert Handshaking.
Neue Zeilenreihenfolge	Wählen Sie None, <CR-LF>, <NULL>, <CR>, <LF-CR> oder <LF> aus.
Neue Zeilenreihenfolge eingeben	Wählen Sie <CR> oder <NULL> aus.

iDRAC6-Netzwerkeinstellungen konfigurieren

VORSICHTSHINWEIS: Durch Ändern der iDRAC6-Netzwerkeinstellungen wird möglicherweise die aktuelle Netzwerkverbindung getrennt.

Konfigurieren Sie die iDRAC6-Netzwerkeinstellungen mithilfe eines der folgenden Hilfsprogramme:

- Webbasierte Schnittstelle – Siehe „iDRAC6-NIC konfigurieren“ auf Seite 51.
- RACADM-CLI – Siehe cfgLanNetworking im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.
- iDRAC6-Konfigurationsdienstprogramm – Siehe „System zur Verwendung eines iDRAC6 konfigurieren“ auf Seite 36.

ANMERKUNG: Wird der iDRAC6 in einer Linux-Umgebung bereitgestellt, finden Sie entsprechende Informationen unter „RACADM installieren“ auf Seite 40.

Über ein Netzwerk auf den iDRAC6 zugreifen

Nachdem Sie den iDRAC6 konfiguriert haben, können Sie im Remote-Zugriff mittels einer der folgenden Schnittstellen auf das verwaltete System zugreifen:

- Webbasierte Schnittstelle
- RACADM
- Telnet-Konsole
- SSH
- IPMI

Tabelle 5-11 beschreibt alle iDRAC6-Schnittstellen.

Tabelle 5-11. iDRAC6-Schnittstellen

Schnittstelle	Beschreibung
Webbasierte Schnittstelle	Ermöglicht Remote-Zugriff auf den iDRAC6 über eine grafische Benutzeroberfläche. Die webbasierte Schnittstelle ist in die iDRAC6-Firmware integriert und Zugriff darauf erfolgt über die NIC-Schnittstelle von einem unterstützten Webbrowser auf der Management Station aus.

RACADM	Ermöglicht Remote-Zugriff auf den iDRAC6 mittels einer Befehlszeilenoberfläche. RACADM verwendet die iDRAC6-IP-Adresse, um RACADM-Befehle auszuführen.
	ANMERKUNG: Die racadm-Option „Remote-Fähigkeit“ wird nur auf Management Stations unterstützt. Weitere Informationen finden Sie unter„RACADM im Remote-Zugriff verwenden“ auf Seite 121.
	ANMERKUNG: Wenn Sie die racadm-Remote-Fähigkeit verwenden, müssen Sie über Schreibberechtigung in den Ordnern verfügen, in denen Sie die RACADM-Unterbefehle für Dateivorgänge verwenden, z. B.:
	`racadm getconfig -f <Dateiname>`
	oder:
	`racadm sslcertupload -t 1 -f c:\cert\cert.txt Unterbefehle`

Tabelle 5-11. iDRAC6-Schnittstellen *(fortgesetzt)*

Schnittstelle	Beschreibung
Telnet-Konsole	Bietet Zugriff auf den iDRAC6 und Unterstützung für serielle und RACADM-Befehle, einschließlich der Befehle **powerdown**, **powerup**, **powercycle** und **hardreset**. **ANMERKUNG:** Telnet ist kein sicheres Protokoll, da es alle Daten, einschließlich der Kennwörter, in Klartext überträgt. Verwenden Sie bei Übertragung vertraulicher Informationen die SSH-Schnittstelle.
SSH-Schnittstelle	Bietet dieselben Fähigkeiten wie die Telnet-Konsole und verwendet eine verschlüsselte Transportschicht für höhere Sicherheit.
IPMI-Schnittstelle	Bietet über den iDRAC6 Zugriff auf die grundlegenden Verwaltungsfunktionen des Remote-Systems. Die Schnittstelle umfasst IPMI-über-LAN, IPMI-über-Seriell und Seriell-über-LAN. Weitere Informationen hierzu finden Sie im *Benutzerhandbuch für Dienstprogramme des Dell OpenManage Baseboard-Verwaltungs-Controllers* unter **support.dell.com\manuals**.

ANMERKUNG: Der Standard-Benutzername des iDRAC6 lautet `root` und das Standardkennwort `calvin`.

Sie können mithilfe eines unterstützten Webbrowsers sowohl über den iDRAC6-NIC als auch über den Server Administrator oder IT Assistant auf die webbasierte iDRAC6-Schnittstelle zugreifen.

Um mit Server Administrator auf die iDRAC6-Remote-Zugriffsschnittstelle zuzugreifen, gehen Sie wie folgt vor:

- Starten Sie Server Administrator.
- Von der Systemstruktur im linken Fensterbereich der Server Administrator-Startseite klicken Sie auf **System → Hauptsystemgehäuse → Remote-Access-Controller**.

Weitere Informationen finden Sie im *Server Administrator-Benutzerhandbuch*.

RACADM im Remote-Zugriff verwenden

ANMERKUNG: Konfigurieren Sie die IP-Adresse auf dem iDRAC6, bevor Sie die RACADM-Remote-Fähigkeit verwenden. Weitere Informationen zum Einrichten des iDRAC6 sowie eine Liste in Bezug stehender Dokumente finden Sie unter „Grundlegende Installation des iDRAC6“ auf Seite 35.

RACADM bietet eine Remote-Fähigkeitsoption (**-r**), mit der eine Verbindung zum verwalteten System hergestellt werden kann und RACADM-Unterbefehle über eine virtuelle Remote-Konsole oder eine Management Station ausgeführt werden können. Um die Remote-Fähigkeit verwenden zu können, sind ein gültiger Benutzername (Option **-u**) und Kennwort (Option **-p**) sowie die iDRAC6-IP-Adresse erforderlich.

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. Weitere Informationen über iDRAC6-Zertifikate finden Sie unter „iDRAC6-Datenübertragung mit SSL und digitalen Zertifikaten sichern“ auf Seite 66.

```
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.
```

Stellen Sie auf Linux-Systemen sicher, dass Sie die folgenden Zwischenschritte ausführen, damit die Zertifikatüberprüfung unter Verwendung des Remote-RACADM erfolgreich verläuft:

1. Konvertieren Sie das Zertifikat vom DER-Format in das PEM-Format (unter Verwendung des Hilfsprogramms openssl cmdline):

   ```
   openssl x509 -inform pem -in <yourdownloadedderformatcert.crt> –outform pem -out <outcertfileinpemformat.pem> –text
   ```

2. Suchen Sie den Speicherort des Standard-CA-Zertifizierungsbündels auf der Management Station. Beispiel: Für RHEL5 64-Bit lautet er / etc/pki/tls/cert.pem.

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

   Verwenden Sie zum Beispiel den cat-Befehl:

   ```
   - cat testcacert.pem >> cert.pem
   ```

RACADM Übersicht

```
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>
```

RACADM-Optionen

Tabelle 5-12 listet die Optionen für den RACADM-Befehl auf.

Tabelle 5-12. 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 dem Standardanschluss (443) nicht 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.

RACADM-Remote-Fähigkeit aktivieren und deaktivieren

ANMERKUNG: Es wird empfohlen, diese Befehle auf Ihrem lokalen System auszuführen.

Die RACADM-Remote-Fähigkeit ist standardmäßig aktiviert. Wenn deaktiviert, geben Sie den folgenden RACADM-Befehl zum Aktivieren ein:

```
racadm config -g cfgRacTuning -o
cfgRacTuneRemoteRacadmEnable 1
```

Zum Deaktivieren der Remote-Fähigkeit geben Sie Folgendes ein:

```
racadm config -g cfgRacTuning -o
cfgRacTuneRemoteRacadmEnable 0
```

RACADM-Unterbefehle

Tabelle 5-13 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.

Bei der Eingabe eines RACADM-Unterbefehls muss dem Befehl das Präfix `racadm` vorangestellt werden, z. B.:

```
racadm help
```

Tabelle 5-13. RACADM-Unterbefehle

Befehl	Beschreibung
Hilfe	Listet iDRAC6-Unterbefehle auf.
Hilfe - *<Unterbefehl>*	Listet die Verwendung für den angegebenen Unterbefehl auf.
arp	Zeigt den Inhalt der ARP-Tabelle an. Es dürfen keine ARP-Tabelleneinträge hinzugefügt oder gelöscht werden.
clearasrscreen	Löscht den letzten ASR-Bildschirm (Absturz, letzter blauer Bildschirm).
clrraclog	Löscht das iDRAC6-Protokoll. Es wird ein einzelner Eintrag vorgenommen, um anzuzeigen, von welchem Benutzer und zu welcher Uhrzeit das Protokoll gelöscht wurde.
config	Konfiguriert den iDRAC6.
getconfig	Zeigt die aktuellen iDRAC6-Konfigurationseigenschaften an.
coredump	Zeigt den letzten Coredump des iDRAC6 an.
coredumpdelete	Löscht den im iDRAC6 gespeicherten Coredump.
fwupdate	Führt iDRAC6-Firmware-Aktualisierungen durch oder zeigt deren Status an.
getssninfo	Zeigt Informationen über aktive Sitzungen an.
getsysinfo	Zeigt allgemeine Informationen zum iDRAC6 und zum System an.
getractime	Zeigt die iDRAC6-Uhrzeit an.
ifconfig	Zeigt die aktuelle iDRAC6-IP-Konfiguration an.
netstat	Zeigt die Routingtabelle und die aktuellen Verbindungen an.

Tabelle 5-13. RACADM-Unterbefehle *(fortgesetzt)*

Befehl	Beschreibung
ping	Überprüft, ob die Ziel-IP-Adresse unter Verwendung des Inhalts der aktuellen Routingtabelle vom iDRAC6 aus erreichbar ist.
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.
getniccfg	Zeigt die derzeitige IP-Konfiguration für den Controller an.
getsvctag	Zeigt die Service-Tags des Systems an.
racdump	Liest den iDRAC6-Status sowie Zustandsinformationen zum Debuggen aus.
racreset	Setzt den iDRAC6 zurück.
racresetcfg	Setzt den iDRAC6 auf die Standardkonfiguration zurück.
serveraction	Führt Energieverwaltungsvorgänge auf dem verwalteten System aus.
getraclog	Zeigt das iDRAC6-Protokoll an.
clrsel	Löscht die Einträge des Systemereignisprotokolls.
gettracelog	Zeigt das iDRAC6-Ablaufverfolgungsprotokoll an. Bei Verwendung mit `-i` zeigt der Befehl die Anzahl von Einträgen im iDRAC6-Ablaufverfolgungsprotokoll an.
sslcsrgen	Erstellt die SSL-CSR und lädt sie herunter.
sslcertupload	Lädt ein Zertifizierungsstellenzertifikat (CA) oder Serverzertifikat auf den iDRAC6 hoch.
sslcertdownload	Lädt ein Zertifizierungsstellenzertifikat (CA) herunter.
sslcertview	Zeigt ein Zertifizierungsstellenzertifikat (CA) oder Serverzertifikat im iDRAC6 an.
sslkeyupload	Lädt den SSL-Schlüssel vom Client auf den iDRAC6 hoch.
testtrap	Zwingt den iDRAC6, ein Test-SNMP-Trap über den iDRAC6-NIC zu senden, um die Trap-Konfiguration zu überprüfen.
vmdisconnect	Erzwingt das Schließen einer Verbindung des virtuellen Datenträgers.
closessn	Schließt eine Kommunikationssitzung auf dem Gerät.
getsel	Zeigt die SEL-Einträge an.

Tabelle 5-13. RACADM-Unterbefehle *(fortgesetzt)*

Befehl	Beschreibung
krbkeytabupload	Eine Kerberos-Keytab-Datei hochladen.
localConRedir Disable	Deaktiviert die Server-Konsole. Es gibt keine Videoausgabe an der Videoschnittstelle des Servers.
testemail	Testet die E-Mail-Warnungsfunktion für den RAC
usercertupload	Lädt ein Benutzerzertifikat oder ein Benutzer-Zertifizierungsstellenzertifikat vom Client auf den iDRAC6 hoch.
usercertview	Zeigt das Benutzerzertifikat oder das Benutzer-Zertifizierungsstellenzertifikat an, das auf dem iDRAC6 vorhanden ist.
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.

Häufig gestellte Fragen zu RACADM-Fehlermeldungen

Nach dem Ausführen eines iDRAC6-Resets (mithilfe des Befehls racadm racreset) gebe ich einen Befehl aus, worauf die folgende Meldung angezeigt wird:

```
FEHLER: Verbindung zum RAC konnte unter angegebener
IP-Adresse nicht hergestellt werden.
```

Was bedeutet diese Meldung?

Sie müssen warten, bis der iDRAC6-Reset abgeschlossen ist, bevor Sie einen anderen Befehl ausgeben.

Wenn ich die racadm-Befehle und -Unterbefehle verwende, erhalte ich Fehlermeldungen, die ich nicht verstehe.

Bei der Verwendung von RACADM-Befehlen und -Unterbefehlen können ein oder mehrere der folgenden Fehler auftreten:

- Lokale RACADM-Fehlermeldungen – Probleme wie Syntax, typografische Fehler und falsche Namen.
- Remote RACADM-Fehlermeldungen – Probleme wie falsche IP-Adresse, falscher Benutzername oder falsches Kennwort.

Wenn ich die iDRAC6-IP-Adresse von meinem System aus pinge und meine iDRAC6-Karte dann während der Ping-Antwort zwischen den Modi „Dediziert“ und „Freigegeben“ umschalte, erhalte ich keine Antwort.

Löschen Sie die ARP-Tabelle auf dem System.

Remote-RACADM ist nicht in der Lage, eine Verbindung zu iDRAC über SUSE Linux Enterprise Server (SLES) 11 SP1 herzustellen.

Stellen Sie sicher, dass Sie die offiziellen openssl- und libopenssl-Versionen installiert haben. Führen Sie den folgenden Befehl aus, um die RPM-Pakete zu installieren:

```
rpm -ivh --force < Dateiname >
```

Hierbei ist `<Dateiname>` die openssl- oder libopenssl rpm-Paketdatei.

Zum Beispiel:

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
rpm -ivh --force libopenssl0_9_8-0.9.8h-
30.22.21.1.x86_64.rpm
```

Mehrere iDRAC6-Controller konfigurieren

Mit RACADM können Sie einen oder mehrere iDRAC6 mit identischen Eigenschaften konfigurieren. Wenn Sie einen spezifischen iDRAC6-Controller mit dessen Gruppen-ID und Objekt-ID abfragen, erstellt RACADM die **.cfg**-Konfigurationsdatei aus den abgerufenen Informationen. Der Dateiname kann vom Benutzer angegeben werden, z. B. **racadm.cfg**. Wenn Sie die Datei in einen oder mehrere iDRAC6 exportieren, können Sie Ihre Controller in kürzester Zeit mit identischen Eigenschaften konfigurieren.

ANMERKUNG: Einige Konfigurationsdateien enthalten eindeutige iDRAC6-Informationen (z. B. die statische IP-Adresse), die vor dem Exportieren der Datei in andere iDRAC6 geändert werden müssen.

Führen Sie zum Konfigurieren mehrerer iDRAC6-Controller die folgenden Anweisungen aus:

1. Verwenden Sie RACADM, um den Ziel-iDRAC6 abzufragen, der die entsprechende Konfiguration enthält.

   ANMERKUNG: Die erstellte **.cfg**-Datei enthält keine Benutzerkennwörter.

   Öffnen Sie eine Eingabeaufforderung und geben Sie Folgendes ein:

   ```
   racadm getconfig-f myfile.cfg
   ```

   ANMERKUNG: Das Umleiten der iDRAC6-Konfiguration zu einer Datei unter Verwendung von **getconfig -f** wird nur bei den lokalen und Remote-RACADM-Schnittstellen unterstützt.

2. Ändern Sie die Konfigurationsdatei mit einem einfachen Texteditor **(optional)**.

3. Verwenden Sie die neue Konfigurationsdatei, um einen Ziel-iDRAC6 zu ändern.

   Geben Sie bei der Eingabeaufforderung Folgendes ein:

   ```
   racadm config -f myfile.cfg
   ```

4. Setzen Sie den konfigurierten Ziel-iDRAC6 zurück.

   Geben Sie bei der Eingabeaufforderung Folgendes ein:

   ```
   racadm racreset
   ```

Der Unterbefehl `getconfig -f racadm.cfg` fordert die iDRAC6-Konfiguration an und erstellt die Datei **racadm.cfg**. Die Datei kann, falls erforderlich, mit einem anderen Namen konfiguriert werden.

Sie können den Befehl **getconfig** dazu verwenden, die folgenden Maßnahmen auszuführen:

- Alle Konfigurationseigenschaften in einer Gruppe anzeigen (nach Gruppenname und -index)
- Alle Konfigurationseigenschaften für einen Benutzer nach Benutzernamen anzeigen

Der Unterbefehl **config** lädt die Informationen in den anderen iDRAC6. Verwenden Sie **config**, um die Benutzer- und Kennwortdatenbank über Server Administrator zu synchronisieren.

Die ursprüngliche Konfigurationsdatei, **racadm.cfg**, wird durch den Benutzer benannt. Im folgenden Beispiel trägt die Konfigurationsdatei den Namen **myfile.cfg**. Um diese Datei zu erstellen, geben Sie bei der Eingabeaufforderung Folgendes ein:

```
racadm getconfig-f myfile.cfg
```

VORSICHTSHINWEIS: Es wird empfohlen, diese Datei mit einem einfachen Texteditor zu bearbeiten. Das RACADM-Dienstprogramm verwendet einen ASCII-Textparser. Formatierungen verwirren den Parser, wodurch die RACADM-Datenbank beschädigt werden kann.

iDRAC6-Konfigurationsdatei erstellen

Die iDRAC6-Konfigurationsdatei **<***Dateiname***>.cfg** wird mit dem Befehl `racadm config -f <Dateiname>.cfg` verwendet. Sie können die Konfigurationsdatei zum Erstellen einer Konfigurationsdatei (ähnlich einer **INI**-Datei) verwenden und den iDRAC6 von dieser Datei aus konfigurieren. Sie können einen beliebigen Dateinamen verwenden und die Dateierweiterung **.cfg** ist nicht erforderlich (obwohl in diesem Teilabschnitt mit dieser Erweiterung auf die Datei Bezug genommen wird).

Die **CFG**-Datei kann:

- Created (erstellt)
- über den Befehl `racadm getconfig -f <Dateiname>.cfg` abgerufen werden
- über den Befehl `racadm getconfig -f <Dateiname>.cfg` abgerufen und dann bearbeitet werden

ANMERKUNG: Informationen zum Befehl **getconfig** finden Sie in der Beschreibung zum getconfig-Befehl im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Die **CFG**-Datei wird zunächst geparst, um zu prüfen, ob gültige Gruppen und Objektnamen vorhanden sind und ob einige einfache Syntaxregeln befolgt werden. Fehler werden mit der Zeilennummer markiert, in der der Fehler erkannt wurde, und eine einfache Meldung beschreibt das Problem. Die vollständige Datei wird auf Richtigkeit geparst und alle Fehler werden angezeigt. Schreibbefehle werden nicht zum iDRAC6 übertragen, wenn in der **.cfg**-Datei ein Fehler festgestellt wird. Der Benutzer muss *alle* Fehler beheben, bevor eine Konfiguration vorgenommen werden kann. Die Option **-c** kann für den Unterbefehl **config** verwendet werden. Dadurch wird lediglich die Syntax überprüft, es werden jedoch *keine* Schreibvorgänge zum iDRAC6 vorgenommen.

Verwenden Sie die folgenden Richtlinien zum Erstellen einer **.cfg**-Datei:

- 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 aufgeführt sind, und alle gültigen Konfigurationen des Objektwerts gelten nur für diesen bestimmten Index.
- Für jede indizierte Gruppe steht ein vordefinierter Satz von Indizes zur Verfügung. Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.
- Verwenden Sie den Unterbefehl **racresetcfg**, um den iDRAC6 auf die ursprünglichen Standardeinstellungen zurückzusetzen, und führen Sie dann den Befehl `racadm config -f <Dateiname>.cfg` aus. Stellen Sie sicher, dass die **CFG**-Datei alle erforderlichen Objekte, Benutzer, Indizes und anderen Parameter enthält.

VORSICHTSHINWEIS: 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.

Parsing-Regeln

- Alle Zeilen, die mit '#' beginnen, werden als Kommentare behandelt.

  Eine Kommentarzeile *muss* in Spalte 1 beginnen. Das Zeichen '#' in einer anderen Spalte wird als '#'-Zeichen behandelt.

  Einige Modemparameter können '#' -Zeichen in der Zeichenkette enthalten. Ein Escape-Zeichen ist nicht erforderlich. Sie können einen **.cfg**-Befehl aus einem `racadm getconfig -f <Dateiname>.cfg`-Befehl erstellen und dann einen `racadm config -f <Dateiname>.cfg`-Befehl auf einem anderen iDRAC6 ausführen, ohne dass Sie Escape-Zeichen hinzufügen müssen.

  Beispiel:

  ```
  #

  # Dies ist eine Anmerkung

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<Modem init # Dies
  ist kein Kommentar>
  ```

- Alle Gruppeneinträge müssen in "[" und "]"-Zeichen eingeschlossen sein.

  Das "[" -Startzeichen, das einen Gruppennamen angibt, *muss* in Spalte 1 beginnen. 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=143.154.133.121 {Objektname}
  ```

- Alle Parameter werden als „Objekt=Wert“-Paare ohne Leerzeichen zwischen „Objekt“, „=“ und „Wert“ angegeben.

  Leerzeichen nach dem Wert werden ignoriert. Ein Leerzeichen innerhalb einer Wertezeichenkette bleibt unverändert. Jedes Zeichen rechts von '=' wird wie vorhanden angenommen (zum Beispiel, ein zweites '=' oder ein '#', '[', ']' und so weiter). Bei diesen Zeichen handelt es sich um gültige Modemchat-Skriptzeichen.

  Siehe Beispiel unter vorherigem Punkt.

  Der Befehl `racadm getconfig -f <Dateiname>.cfg` setzt einen Kommentar vor die Index-Objekte, durch die dem Benutzer die enthaltenen Kommentare angezeigt werden.

  Um den Inhalt einer indizierten Gruppe anzuzeigen, verwenden Sie den folgenden Befehl:

  ```
  racadm getconfig -g <Gruppenname> -i <Index 1-16>
  ```

- Für indizierte Gruppen *muss* es sich bei dem Objektanker um das erste Objekt nach dem "[ ]"-Paar handeln. Im Folgenden finden Sie Beispiele für aktuelle indizierte Gruppen:

  ```
  [cfgUserAdmin]

  cfgUserAdminIndex=11
  ```

  Wenn Sie `racadm getconfig -f <MeinBeispiel>.cfg` eingeben, erstellt der Befehl eine **.cfg**-Datei für die aktuelle iDRAC6-Konfiguration Diese Konfigurationsdatei kann als Beispiel und als Ausgangspunkt für Ihre eindeutige **CFG**-Datei verwendet werden.

iDRAC6-IP-Adresse ändern

Wenn Sie die iDRAC6-IP-Adresse in der Konfigurationsdatei ändern, entfernen Sie alle unnötigen **<*Variable*>=Wert**-Einträge. Es verbleibt lediglich die tatsächliche Bezeichnung der variablen Gruppe mit "[" und "]" zusammen mit den beiden **<*Variable*>=Wert**-Einträgen, die sich auf die IP-Adressenänderung 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
```

Mit dem Befehl **racadm config -f myfile.cfg** wird die Datei geparst, und Fehler werden nach Zeilennummer identifiziert. Eine korrekte Datei aktualisiert die entsprechenden Einträge. Außerdem kann derselbe **getconfig**-Befehl (siehe vorheriges Beispiel) zur Bestätigung der Aktualisierung verwendet werden.

Mit dieser Datei können Sie unternehmensweite Änderungen herunterladen oder neue Systeme über das Netzwerk konfigurieren.

ANMERKUNG: „Anchor“ ist ein interner Ausdruck und darf nicht in der Datei verwendet werden.

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 bieten dieselbe Konfigurationsfunktionalität wie das iDRAC6-Konfigurationsdienstprogramm bei Systemstart, wenn Sie die Aufforderung erhalten, <Strg><E> zu drücken. Weitere Informationen zum Konfigurieren von Netzwerkeigenschaften mit dem iDRAC6-Konfigurationshilfsprogramm finden Sie unter „System zur Verwendung eines iDRAC6 konfigurieren“ auf Seite 36.

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.

iDRAC6-Modi

Der iDRAC6 kann in einem von vier Modi konfiguriert werden:

- Dediziert
- Freigegeben
- Freigegeben für Failover: LOM2
- Freigegeben für Failover: Alle LOMs

Tabelle 5-14 bietet eine Beschreibung der einzelnen Modi.

Tabelle 5-14. iDRAC6-NIC-Konfigurationen

Modus	Beschreibung
Dediziert	Der iDRAC6 verwendet seinen eigenen NIC (RJ-45-Anschluss) und die iDRAC6-MAC-Adresse für Netzwerkverkehr.
Freigegeben	Der iDRAC6 verwendet LOM1 auf dem Planar.
Freigegeben für Failover: LOM2	Der iDRAC6 verwendet LOM1 und LOM2 als Team für Failover. Das Team verwendet die iDRAC6-MAC-Adresse.
Freigegeben für Failover: Alle LOMs	Der iDRAC6 verwendet LOM1, LOM2, LOM3 und LOM4 als Team für Failover. Das Team verwendet die iDRAC6-MAC-Adresse.

Häufig gestellte Fragen zur Netzwerksicherheit

Wenn ich auf die webbasierte iDRAC6-Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die angibt, dass der Host-Name des SSL-Zertifikats nicht mit dem Host-Namen des iDRAC6 übereinstimmt.

Der iDRAC6 enthält ein Standard-iDRAC6-Serverzertifikat, um die Netzwerksicherheit für die webbasierte Schnittstelle und die Remote-RACADM-Funktionen zu gewährleisen. Wenn dieses Zertifikat verwendet wird, zeigt der Webbrowser eine Sicherheitswarnung an, weil das Standardzertifikat als **iDRAC6-Standardzertifikat** ausgegeben wird, das nicht mit dem Host-Namen des iDRAC6 (z. B. IP-Adresse) übereinstimmt.

Um dieses Sicherheitsproblem zu beseitigen, laden Sie ein iDRAC6-Serverzertifikat hoch, das auf die IP-Adresse oder den iDRAC-Namen des iDRAC6 ausgestellt ist. Wenn die Zertifikatsignierungsanforderung (CSR) erstellt wird, die zur Ausgabe des Zertifikats verwendet werden soll, stellen Sie sicher, dass der allgemeine Name (CN) der CSR mit der IP-Adresse (**falls Zertifikat auf IP ausgestellt**) des iDRAC6 (z. B. 192.168.0.120) oder dem registrierten DNS-iDRAC6-Namen (**falls Zertifikat auf den registrierten iDRAC-Namen ausgestellt**) übereinstimmt.

So stellen Sie sicher, dass die CSR dem eingetragenen DNS-iDRAC6-Namen entspricht:

1. Klicken Sie in der Struktur unter **System** auf **iDRAC-Einstellungen**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Netzwerk**.
3. Gehen Sie in der Tabelle **Allgemeine Einstellungen** wie folgt vor:
   a. Wählen Sie das Kontrollkästchen **iDRAC auf DNS registrieren** aus.
   b. Geben Sie den iDRAC6-Namen in das Feld **DNS-iDRAC-Name** ein.
4. Klicken Sie auf **Änderungen übernehmen**.

Weitere Informationen über die Erstellung von CSRs und über die Ausgabe von Zertifikaten finden Sie unter „iDRAC6-Datenübertragung mit SSL und digitalen Zertifikaten sichern“ auf Seite 393.

Warum sind die Remote-RACADM- und webbasierten Dienste nach einer Eigenschaftsänderung nicht verfügbar?

Es kann eine Weile dauern, bis die Remote-RACADM-Dienste und die webbasierte Schnittstelle nach einem Reset des iDRAC6-Web Servers verfügbar sind.

Der iDRAC6-Web Server wird nach den folgenden Ereignissen zurückgesetzt:

- Wenn die Netzwerkkonfiguration oder Netzwerk-Sicherheitseigenschaften mittels der webbasierten iDRAC6-Benutzeroberfläche geändert werden
- Wenn die Eigenschaft **cfgRacTuneHttpsPort** geändert wird (einschließlich der Änderung durch eine config -f-<*Konfigurationsdatei*>)
- Wenn **racresetcfg** verwendet wird
- Wenn der iDRAC6 zurückgesetzt wird
- Wenn ein neues SSL-Serverzertifikat hochgeladen wird

Warum registriert mein DNS-Server meinen iDRAC6 nicht?

Einige DNS-Server registrieren nur Namen mit höchstens 31 Zeichen.

Wenn ich auf die webbasierte iDRAC6-Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die angibt, dass das SSL-Zertifikat von einer nicht vertrauenswürdigen Zertifizierungsstelle (CA) ausgegeben wurde.

Der iDRAC6 enthält ein Standard-iDRAC6-Serverzertifikat, um die Netzwerksicherheit für die webbasierte Schnittstelle und die Remote-RACADM-Funktionen zu gewährleisen. Dieses Zertifikat wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgegeben. Um diese Sicherheitsproblem zu beseitigen, laden Sie ein von einer vertrauenswürdigen CA (z. B. Microsoft-CA, Thawte oder Verisign) ausgegebenes iDRAC6-Serverzertifikat hoch. Weitere Informationen über die Ausgabe von Zertifikaten finden Sie unter „iDRAC6-Datenübertragung mit SSL und digitalen Zertifikaten sichern“ auf Seite 393.

6

iDRAC6-Benutzer hinzufügen und konfigurieren

Erstellen Sie zur Verwaltung des Systems mit dem iDRAC6 und zur Aufrechterhaltung der Systemsicherheit eindeutige Benutzer mit spezifischen Verwaltungsberechtigungen (oder *rollenbasierter Autorität*). Für zusätzliche Sicherheit können Sie auch Warnungen konfigurieren, die spezifischen Benutzern per E-Mail geschickt werden, wenn ein bestimmtes Systemereignis vorkommt.

iDRAC6-Benutzer mithilfe der Webschnittstelle konfigurieren

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: Sie müssen die Berechtigung **Benutzer konfigurieren** besitzen, um einen iDRAC-Benutzer zu konfigurieren.

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

Die Seite **Benutzer** (siehe Tabelle 6-1) zeigt die folgenden Informationen für iDRAC6-Benutzer an: **Benutzer-ID**, **Zustand** (Aktiviert/Deaktiviert), **Benutzername**, **iDRAC**, **LAN**, **Serielle Schnittstelle** und **Seriell über LAN** (Aktiviert/Deaktiviert).

ANMERKUNG: Benutzer 1 ist für den anonymen IPMI-Benutzer reserviert; diese Konfiguration kann nicht geändert werden.

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

Auf der Seite **Benutzer-Hauptmenü** (siehe Tabelle 6-2 und Tabelle 6-7) können Sie einen Benutzer konfigurieren, ein Benutzerzertifikat anzeigen oder hochladen, das Zertifikat einer vertrauenswürdigen Zertifizierungsstelle hochladen und anzeigen, eine SSH-Datei mit öffentlichem Schlüssel (Secure Shell) hochladen oder einen festgelegten SSH-Schlüssel oder alle SSH-Schlüssel anzeigen oder löschen.

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

3 Konfigurieren Sie auf der Seite **Benutzerkonfiguration** Folgendes:

- Den Benutzernamen, das Kennwort und die Zugriffberechtigungen für einen vorhandenen iDRAC-Benutzer. Tabelle 6-3 beschreibt **Allgemeine Benutzereinstellungen.**
- Die IPMI-Berechtigungen des Benutzers. Tabelle 6-4 beschreibt die **IPMI-Benutzerberechtigungen** zum Konfigurieren der LAN-Berechtigungen des Benutzers.
- Die iDRAC-Benutzerberechtigungen. Tabelle 6-5 beschreibt die **iDRAC-Benutzerberechtigungen**.
- Die Zugriffberechtigungen der iDRAC-Gruppe. Tabelle 6-6 beschreibt die **iDRAC-Gruppenberechtigungen**.

4 Wenn dies abgeschlossen ist, klicken Sie auf **Änderungen übernehmen**.

5 Klicken Sie auf **Zurück zur Benutzerseite**, um zur Benutzerseite zurückzukehren.

Tabelle 6-1. Benutzerzustände und -berechtigungen

Einstellung	Beschreibung
Benutzer-ID	Zeigt eine sequenzielle Liste von Benutzer-ID-Nummern an. Jedes Feld unter **Benutzer-ID** enthält eine von 16 voreingestellten Benutzer-ID-Nummern. Dieses Feld darf nicht bearbeitet werden.
Status	Zeigt den Anmeldezustand des Benutzers an: aktiviert oder deaktiviert. (Die Standardeinstellung ist deaktiviert). **ANMERKUNG:** Benutzer 2 ist standardmäßig aktiviert.

Tabelle 6-1. Benutzerzustände und -berechtigungen *(fortgesetzt)*

Einstellung	Beschreibung
Benutzername	Zeigt den Anmeldenamen des Benutzers an. Gibt einen iDRAC6-Benutzernamen von bis zu 16 Zeichen an. Jeder Benutzer muss einen eindeutigen Benutzernamen besitzen. **ANMERKUNG:** Wenn der Benutzername geändert wird, erscheint der neue Name erst bei der nächsten Benutzeranmeldung in der Benutzeroberfläche.
iDRAC	Zeigt die Gruppe (Berechtigungsebene) an, welcher der Benutzer zugewiesen ist (Administrator, Operator, schreibgeschützt oder keine).
LAN	Zeigt die IPMI-LAN-Berechtigungsebene an, welcher der Benutzer zugewiesen ist (Administrator, Operator, schreibgeschützt oder keine).
Serieller Anschluss	Zeigt die Berechtigungsebene der seriellen IPMI-Schnittstelle an, welcher der Benutzer zugewiesen ist (Administrator, Operator, schreibgeschützt oder keine).
Seriell über LAN	Ermöglicht/verwehrt dem Benutzer, IPMI-Seriell-über-LAN zu verwenden.

Tabelle 6-2. Smart Card-Konfigurationsoptionen

Option	Beschreibung
Benutzerzertifikat hochladen	Ermöglicht dem Benutzer, das Benutzerzertifikat auf den iDRAC6 hochzuladen und in das Benutzerprofil zu importieren.
Benutzerzertifikat anzeigen	Zeigt die Seite des Benutzerzertifikats an, die auf den iDRAC hochgeladen wurde.
Zertifikat der vertrauenswürdigen CA hochladen	Ermöglicht Ihnen, das Zertifikat der vertrauenswürdigen Zertifizierungsstelle auf den iDRAC hochzuladen und in das Benutzerprofil zu importieren.

Tabelle 6-2. Smart Card-Konfigurationsoptionen

Option	Beschreibung
Zertifikat der vertrauenswürdigen Zertifizierungsstelle anzeigen	Zeigt das Zertifikat der vertrauenswürdigen Zertifizierungsstelle an, das auf den iDRAC hochgeladen wurde. Das Zertifikat der vertrauenswürdigen Zertifizierungsstelle wird von der Zertifizierungsstelle ausgestellt, die autorisiert ist, Zertifikate für Benutzer auszustellen.

Tabelle 6-3. Allgemeine Benutzereinstellungen

Benutzer-ID	Enthält eine von 16 voreingestellten Benutzer-ID-Nummern.
Benutzer aktivieren	Wenn das Feld markiert ist, weist dies darauf hin, dass der Benutzerzugriff auf den iDRAC6 aktiviert ist. Wenn das Feld nicht markiert ist, ist der Benutzerzugriff deaktiviert.
Benutzername	Ein Benutzername von bis zu 16 Zeichen. Die folgenden Zeichen werden unterstützt: • 0-9 • A-Z • a-z • Sonderzeichen: + %) ' > : $ [| ! & = * , - {] § # (? < ; _ } I
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.

Tabelle 6-3. Allgemeine Benutzereinstellungen *(fortgesetzt)*

Neues Kennwort	Geben Sie ein **Kennwort** mit bis zu 16 Zeichen ein. Die Zeichen werden nicht angezeigt und sind maskiert. Die folgenden Zeichen werden unterstützt: • 0-9 • A-Z • a-z • Sonderzeichen: + & ? > - } | . ! (' , _ [" @ #) * ; $] / § % = < : { I \
Neues Kennwort bestätigen	Geben Sie das Kennwort des iDRAC-Benutzers erneut ein, um es zu bestätigen.

Tabelle 6-4. IPMI-Benutzerberechtigungen

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

Tabelle 6-5. iDRAC-Benutzerberechtigungen

Eigenschaft	Beschreibung
Rollen	Legt die maximale iDRAC-Benutzerberechtigung des Benutzers als eine der folgenden Benutzergruppen fest: **Administrator**, **Operator**, **Schreibgeschützt** oder **Keine**. Informationen zu **iDRAC-Gruppenberechtigungen** finden Sie unter Tabelle 6-6.
Am iDRAC anmelden	Ermöglicht dem Benutzer, sich am iDRAC anzumelden.
iDRAC konfigurieren	Ermöglicht dem Benutzer, den iDRAC zu konfigurieren.
Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern zu erlauben, auf das System zuzugreifen. **VORSICHTSHINWEIS: Diese Berechtigung ist normalerweise Benutzern vorbehalten, die Mitglieder der Administratorrolle auf dem iDRAC sind. Benutzern, die die „Operator"-Rolle innehaben, kann diese Berechtigung jedoch 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 iDRAC-Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer, Serversteuerungsbefehle auszuführen.
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.

Tabelle 6-6. iDRAC-Gruppenberechtigungen

User Group (Benutzergruppe)	Gewährte Berechtigungen
Administrator	Am iDRAC anmelden, iDRAC konfigurieren, Benutzer konfigurieren, Protokolle löschen, Serversteuerungsbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen
Operator	Auswahl einer beliebigen Kombination der folgenden Berechtigungen: Am iDRAC anmelden, iDRAC konfigurieren, Benutzer konfigurieren, Protokolle löschen, Servermaßnahmenbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen
Schreibgeschützt	Am iDRAC anmelden
Keine	Keine zugewiesenen Berechtigungen

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 PKA über SSH eingerichtet ist und korrekt verwendet wird, müssen Sie bei der Anmeldung am iDRAC6 keinen Benutzernamen und 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 zugreifen wird. Es gibt zwei herkömmliche Möglichkeiten, das öffentliche/private Schlüsselpaar zu erstellen: unter Verwendung 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. RSA und DSA sind die einzigen unterstützten Schlüsselerstellungsalgorithmen. Geben Sie die Anzahl Bits für den Schlüssel ein. Die Zahl muss für RSA zwischen 768 und 4096 Bit und für DSA bei 1024 Bit liegen.
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 unter Verwendung der Option „Öffentlichen Schlüssel speichern“ in einer Datei speichern, um ihn später hochzuladen. Alle hochgeladenen Schlüssel müssen im RFC 4716- oder openssh-Format sein. Wenn sie dieses Format nicht aufweisen, muss eine Konvertierung in dieses Format vorgenommen werden.

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

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

die Option **-b** gibt die Bit-Verschlüsselungsgröße zwischen 768 und 4096 an.

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

Befolgen Sie die Anweisungen. Laden Sie nach Ausführung des Befehls den öffentlichen Schlüssel hoch.

VORSICHTSHINWEIS: Schlüssel, die über die Linux-Management Station unter Verwendung von ssh-keygen erstellt wurden, weisen ein anderes Format als 4716 auf. Konvertieren Sie die Schlüssel unter Verwendung von `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub` **in das Format 4716. An den Berechtigungen der Schlüsseldatei dürfen keine Änderungen vorgenommen werden. Die oben erläuterte Konvertierung ist unter Verwendung der Standardberechtigungen auszuführen.**

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 ähnlich wie Remote-RACADM, da die Sitzung endet, nachdem der Befehl ausgeführt wurde.

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
```

SSH-Schlüssel unter Verwendung der webbasierten iDRAC6-Schnittstelle hochladen, anzeigen und löschen

1. Klicken Sie auf **iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Benutzer**. Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer. Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Verwenden Sie die Optionen **SSH-Schlüsselkonfigurationen** zum Hochladen, Anzeigen oder Entfernen von SSH-Schlüsseln.

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 über Benutzerberechtigungen erhalten Sie unter „iDRAC6-Benutzer hinzufügen und konfigurieren" auf Seite 139.

Tabelle 6-7. SSH-Schlüsselkonfigurationen

Option	Beschreibung
SSH-Schlüssel hochladen	Ermöglicht dem lokalen Benutzer, eine öffentliche SSH-Schlüsseldatei (Sichere Shell) 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.

Die Seite **SSH-Schlüssel hochladen** ermöglicht Ihnen, eine öffentliche SSH-Schlüsseldatei (Sichere Shell) hochzuladen. Beim Hochladen eines Schlüssels wird der Inhalt der Schlüsseldatei in einem nicht-editierbaren Textfeld auf der Seite **SSH-Schlüssel anzeigen/entfernen** angezeigt.

Tabelle 6-8. 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**.
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 6-9. 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.

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.

Lokales RACADM und Remote-RACADM:

```
racadm sshpkauth -i <2 to 16> -k <1 to 4> -f
<Dateiname>
```

```
racadm sshpkauth -i <2 bis 16> -k <1 bis 4> -t
```

```
<Schlüsseltext>
```

Telnet/SSH/RACADM seriell:

```
racadm sshpkauth -i <2 bis 16> -k <1 bis 4> -t
```

```
<Schlüsseltext>
```

Beispiel:

Laden Sie einen gültigen Schlüssel zum iDRAC6-Benutzer 2 im ersten Schlüsselbereich unter Verwendung einer Datei hoch:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

Die PK SSH-Authentifizierungsdatei wurde erfolgreich zum RAC hochgeladen.

VORSICHTSHINWEIS: Die Option „Schlüsseltext" wird auf dem lokalen und Remote-RACADM unterstützt. Die Option „Datei" wird auf Telnet-/ssh-/seriellem 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
```

Informationen zu den Unterbefehlsoptionen finden Sie unter dem Unterbefehl `sshpkauth` im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Das RACADM-Dienstprogramm zur Konfiguration von iDRAC6-Benutzern verwenden

ANMERKUNG: Sie müssen als Benutzer **root** angemeldet sein, um RACADM-Befehle auf einem Remote-Linux-System ausführen zu können.

Einzelne oder mehrere iDRAC6-Benutzer können über die RACADM-Befehlszeile konfiguriert werden, die mit den iDRAC6-Agenten auf dem verwalteten System installiert wird.

Um mehrere iDRAC6 mit identischen Konfigurationseinstellungen zu konfigurieren, führen Sie eines der folgenden Verfahren aus:

- Erstellen Sie mit Hilfe der RACADM-Beispiele in diesem Abschnitt eine Stapeldatei mit RACADM-Befehlen, und führen Sie diese Stapeldatei dann auf jedem verwalteten System aus.
- Erstellen Sie die iDRAC6-Konfigurationsdatei gemäß der Beschreibung im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist, und führen Sie den Unterbefehl **racadm config** unter Verwendung derselben Konfigurationsdatei auf allen verwalteten Systemen aus.

Bevor Sie beginnen

Sie können in der iDRAC6-Eigenschaften-Datenbank bis zu 16 Benutzer konfigurieren. Bevor Sie einen iDRAC-Benutzer manuell aktivieren, prüfen Sie, ob aktuelle Benutzer vorhanden sind. Wenn Sie einen neuen iDRAC6 konfigurieren oder den Befehl **racadm racresetcfg** ausgeführt haben, ist der einzige aktuelle Benutzer `root` mit dem Kennwort `calvin`. Der Unterbefehl **racresetcfg** setzt den iDRAC6 auf die ursprünglichen Standardwerte zurück.

VORSICHTSHINWEIS: Verwenden Sie den Befehl racresetcfg mit Vorsicht, da *alle* Konfigurationsparameter auf die ursprünglichen Standardeinstellungen zurückgesetzt werden. Alle vorherigen Änderungen gehen verloren.

ANMERKUNG: Benutzer können im Laufe der Zeit aktiviert und deaktiviert werden. Infolgedessen kann ein Benutzer auf jedem iDRAC6 eine unterschiedliche Indexnummer besitzen.

Um nachzuprüfen, ob ein Benutzer existiert, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
racadm getconfig -u <Benutzername>
```

ODER

geben Sie den folgenden Befehl einmal für jeden Index von 1 - 16 ein:

```
racadm getconfig -g cfgUserAdmin -i <Index>
```

ANMERKUNG: Sie können auch `racadm getconfig -f <myfile.cfg>` eingeben, und die Datei **myfile.cfg**, in der alle iDRAC6-Konfigurationsparameter enthalten sind, anzeigen oder bearbeiten.

Mehrere Parameter und Objekt-IDs werden mit ihren aktuellen Werten angezeigt. Zwei Objekte von Bedeutung sind:

```
# cfgUserAdminIndex=XX

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, wird dieser Index von diesem Benutzernamen verwendet.

ANMERKUNG: Wenn Sie einen Benutzer mit dem Unterbefehl **racadm config** manuell aktivieren oder deaktivieren, *muss* der Index mit der Option **-i** angegeben werden. Beachten Sie, dass das im vorherigen Beispiel gezeigte Objekt **cfgUserAdminIndex** ein "#"-Zeichen enthält. Wenn der Befehl **racadm config -f racadm.cfg** ferner zur Angabe einer beliebigen Anzahl von zu schreibenden Gruppen/Objekten verwendet wird, kann der Index nicht angegeben werden. Ein neuer Benutzer wird zum ersten verfügbaren Index hinzugefügt. Dieses Verhalten bietet größere Flexibilität bei der Konfiguration mehrerer iDRAC6 mit denselben Einstellungen.

iDRAC6-Benutzer hinzufügen

Um der RAC-Konfiguration einen neuen Benutzer hinzuzufügen, können einige grundlegende Befehle verwendet werden. Führen Sie im Allgemeinen die folgenden Verfahren aus:

1. Legen Sie den Benutzernamen fest.
2. Legen Sie das Kennwort fest.
3. Legen Sie folgende Benutzerberechtigungen fest:
   - iDRAC
   - LAN
   - Serieller Anschluss
   - Seriell über LAN
4. Aktivieren Sie den Benutzer.

Beispiel

Im folgenden Beispiel wird beschrieben, wie man einen neuen Benutzer namens „John“ mit dem Kennwort „123456“ und ANMELDE-Berechtigungen am RAC hinzufügt.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 2 123456

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminIpmiLanPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminIpmiSerialPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminSolEnable 1

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminEnable 1
```

Verwenden Sie zur Überprüfung einen der folgenden Befehle:

```
racadm getconfig -u john
```

```
racadm getconfig –g cfgUserAdmin –i 2
```

iDRAC6-Benutzer entfernen

Wenn Sie RACADM verwenden, müssen Benutzer manuell und einzeln deaktiviert werden. Benutzer können nicht mittels einer Konfigurationsdatei gelöscht werden.

Im folgenden Beispiel wird die Befehlssyntax gezeigt, die zum Löschen eines iDRAC6-Benutzers verwendet werden kann:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i <Index> „"
```

Eine Null-Zeichenkette von doppelten Anführungszeichen („“) weist den iDRAC6 an, die Benutzerkonfiguration am angegebenen Index zu entfernen und die Benutzerkonfiguration auf die ursprünglichen Werkseinstellungen zurückzusetzen.

iDRAC6-Benutzer mit Berechtigungen aktivieren

Um einen Benutzer mit spezifischen administrativen Berechtigungen (rollenbasierte Autorität) zu aktivieren, machen Sie zuerst einen verfügbaren Benutzer-Index ausfindig, indem Sie die Schritte unter „Bevor Sie beginnen“ auf Seite 151 ausführen. Geben Sie dann die folgenden Befehlszeilen mit dem neuen Benutzernamen und dem neuen Kennwort ein:

ANMERKUNG: Eine Liste gültiger Bit-Maskenwerte für spezifische Benutzerberechtigungen ist im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC* enthalten, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist. Der Standard-Berechtigungswert ist 0, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i <Index>
<Benutzerberechtigungs-Bitmaskenwert>
```

7

iDRAC6-Verzeichnisdienst verwenden

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 7-1 zeigt die iDRAC6 Active Directory-Benutzerberechtigungen.

Tabelle 7-1. iDRAC6-Benutzerberechtigungen

Berechtigung	Beschreibung
Am iDRAC anmelden	Ermöglicht dem Benutzer, sich am iDRAC6 anzumelden
iDRAC konfigurieren	Ermöglicht dem Benutzer, den iDRAC6 zu konfigurieren

Tabelle 7-1. iDRAC6-Benutzerberechtigungen *(fortgesetzt)*

Berechtigung	Beschreibung
Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern zu erlauben, auf das System zuzugreifen
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
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 beim iDRAC6 anzumelden:

- Webbasierte Schnittstelle
- Remote-RACADM
- Serielle oder Telnet-Konsole

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 webbasierte Schnittstelle anmelden und die Benutzerdomänen bereits konfiguriert sind, führt die Anmeldeseite der webbasiserten Schnittstelle in einem Pulldown-Menü sämtliche Benutzerdomänen auf, die zur Auswahl stehen. Wenn Sie eine Benutzerdomäne aus dem Pulldown-Menü wählen, sollten Sie nur den Benutzernamen eingeben. Wenn Sie **Diesen iDRAC** auswählen, können Sie sich als Active Directory-Benutzer anmelden, wenn Sie die Anmeldesyntax verwenden, die zuvor in diesem Abschnitt beschrieben wurde.

Sie können sich auch unter Verwendung der Smart Card oder der einfachen Anmeldung am iDRAC6 anmelden. Weitere Informationen finden Sie unter „iDRAC6 für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren“ auf Seite 205.

ANMERKUNG: Der Windows 2008 Active Directory-Server unterstützt nur Zeichenketten des Typs <*Benutzername*>@<*Domänenname*> mit einer maximalen Länge von 256 Zeichen.

Voraussetzungen zum Aktivieren der Microsoft Active Directory-Authentifizierung für iDRAC6

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

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 für alle Domänen-Controller vorzunehmen, 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 158.

SSL auf einem Domänen-Controller aktivieren

Wenn Benutzer durch den iDRAC gegen einen Active Directory-Domänen-Controller authentifiziert werden, wird eine SSL-Sitzung mit dem Domänen-Controller gestartet. Der Domänen-Controller sollte jetzt ein von der Zertifizierungsstelle signiertes Zertifikat erstellen, das Stammzertifikat, das auch in den iDRAC geladen wird. Damit, anders ausgedrückt, die iDRAC-Authentifizierung auf einen *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 Zertifikat besitzen.

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.

Aktivieren Sie SSL auf jedem einzelnen Domänen-Controller, indem Sie das SSL-Zertifikat für jeden Controller installieren.

1. Klicken Sie auf **Start→ Verwaltung→ Domänensicherheitsregeln**.
2. Erweitern Sie den Ordner **Richtlinien öffentlicher Schlüssel,** klicken Sie mit der rechten Maustaste auf **Automatische Zertifikatanforderungs-Einstellungen** und klicken Sie auf **Automatische Zertifikatanforderung**.
3. Klicken Sie im **Setup-Assistent der automatischen Zertifikatanforderung** auf **Weiter** und wählen Sie **Domänen-Controller** aus.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Exportieren des Stamm-CA-Zertifikats des Domänen-Controllers auf den iDRAC6

ANMERKUNG: Wenn Ihr System Windows 2000 ausführt oder Sie eine eigenständige CA verwenden, können die nachfolgenden Schritte variieren.

1. Machen Sie den Domänen-Controller ausfindig, der den Microsoft Enterprise-CA-Dienst ausführt.
2. Klicken Sie auf **Start→Run** (Ausführen).
3. Geben Sie `MMC` in das Feld **Ausführen** 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 CA-Stammzertifikat, 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 zum iDRAC hoch.

    Informationen zum Hochladen des Zertifikats unter Verwendung von RACADM finden Sie unter „Konfiguration des Microsoft Active Directory mit erweitertem Schema unter Verwendung der webbasierten iDRAC6-Schnittstelle“ auf Seite 177 oder „Konfiguration des Microsoft Active Directory mit Standardschema unter Verwendung von RACADM“ auf Seite 190.

    Informationen zum Hochladen des Zertifikats unter Verwendung der webbasierten Schnittstelle finden Sie unter „Konfiguration des Microsoft Active Directory mit erweitertem Schema unter Verwendung der webbasierten iDRAC6-Schnittstelle“ auf Seite 177 oder „Konfiguration des Microsoft Active Directory mit Standardschema unter Verwendung der webbasierten iDRAC6-Schnittstelle“ auf Seite 186.

SSL-Zertifikat der iDRAC6-Firmware importieren

ANMERKUNG: Wenn der Active Directory-Server so eingestellt ist, dass der Client in der Initialisierungsphase einer SSL-Sitzung authentifiziert wird, muss das iDRAC6-Serverzertifikat auf den Active Directory Domänen-Controller hochgeladen werden. Dieser zusätzliche Schritt ist nicht erforderlich, wenn das Active Directory während der Initialisierungsphase einer SSL-Sitzung keine Client-Authentifizierung ausführt.

Um das SSL-Zertifikat der iDRAC6-Firmware in alle vertrauenswürdigen Zertifikatlisten der Domänen-Controller zu importieren, gehen Sie wie folgt vor.

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

ANMERKUNG: Wenn das SSL-Zertifikat der iDRAC6-Firmware von einer bekannten Zertifizierungsstelle stammt und diese Zertifizierungsstelle in der Liste der vertrauenswürdigen Stammzertifizierungsstellen des Domänen-Controllers verzeichnet ist, müssen die folgenden Schritte nicht ausgeführt werden.

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

Um das iDRAC6-SSL-Zertifikat herunterzuladen, führen Sie den folgenden RACADM-Befehl aus:

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

1. Öffnen Sie am Domänen-Controller ein Fenster der **MMC-Konsole** und wählen Sie **Zertifikate→ Vertrauenswürdige Stammzertifizierungsstellen** aus.
2. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, wählen Sie **Alle Aufgaben** und klicken Sie auf **Importieren**.
3. Klicken Sie auf **Weiter** und suchen Sie die SSL-Zertifikatdatei.
4. Installieren Sie das iDRAC6-SSL-Zertifikat in der **vertrauenswürdigen Stammzertifizierungsstelle** jedes Domänen-Controllers.

   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.

5 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.

6 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 des *erweiterten Schemas* 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.
- Konfiguration des Benutzerzugriffs auf verschiedenen iDRAC6 mit unterschiedlichen Berechtigungsebenen wird bereitgestellt.

Der Vorteil der Standardschema-Lösung besteht darin, dass keine Schemaerweiterung 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.

Dell-Erweiterung: dell

Grund-OID von Dell: 1.2.840.113556.1.8000.1280

RACLinkID-Bereich:12070 to 12079

Übersicht über die iDRAC-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 an Berechtigungen für ein oder mehrere iDRAC-Geräte verwendet. Dieses Modell ist unkompliziert und gibt dem Administrator höchste Flexibilität bei der Verwaltung verschiedener Benutzergruppen, iDRAC-Berechtigungen und iDRAC-Geräten im Netzwerk.

Active Directory - Objektübersicht

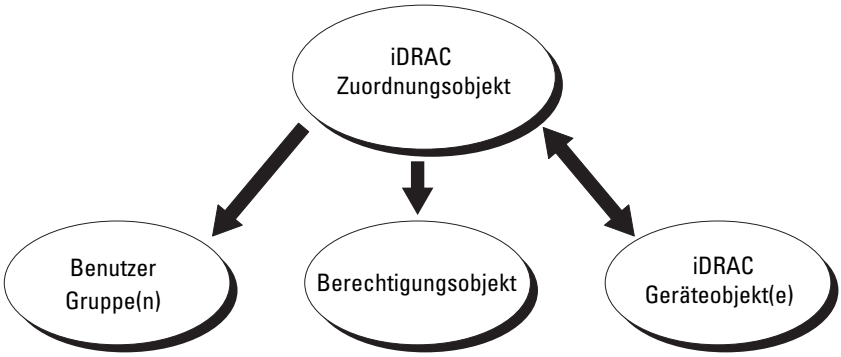
Für jeden physischen iDRAC auf dem Netzwerk, den Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein iDRAC-Geräteobjekt erstellen. Sie können mehrere Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt nach Bedarf mit beliebig vielen Benutzern, Benutzergruppen, oder iDRAC-Geräteobjekten verbunden werden kann. Die Benutzer und iDRAC-Benutzergruppen können Mitglieder beliebiger Domänen im Unternehmen sein.

Jedes Zuordnungsobjekt darf jedoch nur mit einem Berechtigungsobjekt verbunden werden (bzw. jedes Zuordnungsobjekt kann Benutzer, Benutzergruppen oder iDRAC-Geräteobjekte nur mit einem Berechtigungsobjekt verbinden). Dieses Beispiel ermöglicht dem Administrator, die Berechtigungen jedes Benutzers auf spezifischen iDRACs zu steuern.

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

Abbildung 7-1 zeigt, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für die gesamte Authentifizierung und Autorisierung erforderlich ist.

Abbildung 7-1. 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 es muss ein iDRAC-Geräteobjekt für jeden iDRAC auf dem Netzwerk vorhanden sein, das zum Zweck der Authentifizierung und Autorisierung mit dem iDRAC beim Active Directory integriert werden soll.

Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer bzw. Gruppen und auch iDRAC-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die *Benutzer*, die *Berechtigungen* auf den iDRACs haben.

Über die Dell-Erweiterung zum Active Directory-Benutzer- und -Computer-MMC-Snap-In können nur Berechtigungsobjekte und iDRAC-Objekte derselben Domäne mit dem Verbindungsobjekt verknüpft werden. Mit der Dell-Erweiterung können keine Gruppen oder iDRAC-Objekte aus anderen Domänen als Produktmitglied des Verbindungsobjektes hinzugefügt werden.

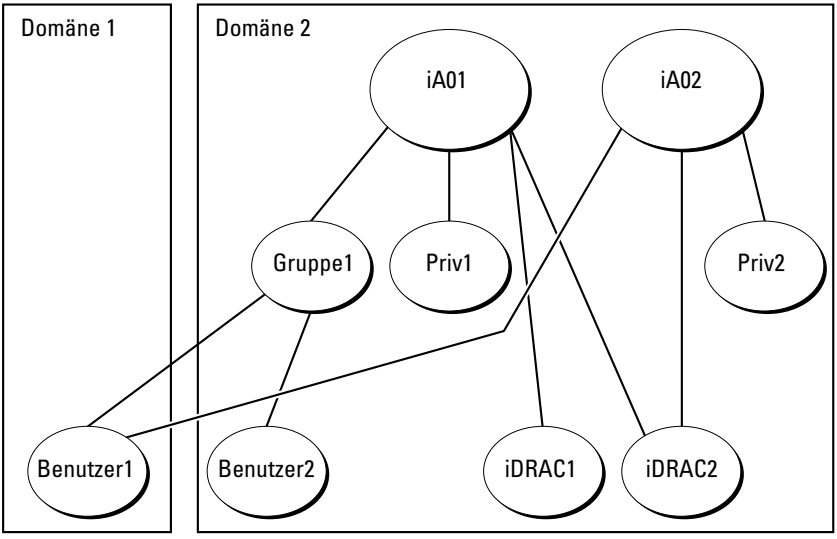
Benutzer, Benutzergruppen oder verschachtelte Benutzergruppen jeglicher Domäne können dem Verbindungsobjekt hinzugefügt werden. Lösungen mit erweitertem Schema unterstützen jede Art von Benutzergruppe sowie jede Benutzergruppe, die über mehrere Domänen verschachtelt und von Microsoft Active Directory 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 7-2 enthält ein Beispiel für das Ansammeln von Berechtigungen unter Verwendung des erweiterten Schemas.

Abbildung 7-2. Ansammeln von Berechtigungen für einen Benutzer



Die Abbildung zeigt zwei Zuordnungsobjekte - iA01 und iA02. 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 besitzt demzufolge den Berechtigungssatz: am iDRAC anmelden, virtuelle Datenträger, Protokolle löschen, iDRAC konfigurieren und Testwarnungen (kombinierter Berechtigungssatz von Priv1 und Priv2).

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 einer verschachtelten Gruppe angehören kann.

Erweitertes Schema des Active Directory für den Zugriff auf den iDRAC6 konfigurieren

Konfigurieren Sie die Active Directory-Software und den iDRAC6, bevor Sie Active Directory für den Zugriff auf den iDRAC6 verwenden, indem Sie die folgenden Schritte ausführen:

1. Erweitern Sie das Active Directory-Schema (siehe „Erweitern des Active Directory-Schemas“ auf Seite 167).
2. Erweitern Sie das Snap-In von Active Directory-Benutzern und -Computern (siehe „Dell-Erweiterung zu Microsoft Active Directory Benutzer- und Computer-Snap-In installieren“ auf Seite 174).
3. Fügen Sie iDRAC6-Benutzer und deren Berechtigungen zum Active Directory hinzu (siehe „iDRAC-Benutzer und -Berechtigungen zum Microsoft Active Directory hinzufügen“ auf Seite 175).
4. Konfigurieren Sie die iDRAC6 Active Directory-Eigenschaften entweder über die webbasierte iDRAC6-Schnittstelle oder über RACADM (siehe „Konfiguration des Microsoft Active Directory mit erweitertem Schema unter Verwendung der webbasierten iDRAC6-Schnittstelle“ auf Seite 177 oder „Konfiguration des Microsoft Active Directory mit erweitertem Schema unter Verwendung von RACADM“ auf Seite 180.)

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 Snap-In für die Active Directory-Benutzer und -Computer-MMC (Microsoft-Verwaltungskonsole) 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 hat keine Auswirkung auf die Vorgängerversionen des Produktes.

Der Schema Extender und die Erweiterung für das Benutzer- und Computer-MMC-Snap-In von Active Directory stehen auf der DVD *Dell Systems Management Tools and Documentation* zur Verfügung. Informationen zu deren Installation finden Sie unter „Dell-Erweiterung zu Microsoft Active Directory Benutzer- und Computer-Snap-In installieren“ auf Seite 174. 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 **dell.com/support/manuals** zur Verfügung steht.

ANMERKUNG: Beim Erstellen von iDRAC-Zuordnungsobjekten oder iDRAC-Geräteobjekten müssen Sie sicherstellen, dass **Dell Remote Management Object Advanced** ausgewählt ist.

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**

ANMERKUNG: Der Ordner **Remote_Management** dient zur Erweiterung des Schemas auf älteren Remote-Zugriff-Produkten wie DRAC 4 und DRAC 5, und der Ordner **Remote_Management_Advanced** dient zur Erweiterung des Schemas auf iDRAC6.

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 168.

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

Dell Schema Extender verwenden

ANMERKUNG: 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 7-2 bis Tabelle 7-7)
- Attribute (Tabelle 7-8)

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

Tabelle 7-2. 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 7-3. dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Beschreibung	Repräsentiert das Dell iDRAC-Gerät. Das iDRAC-Gerät muss im Active Directory als delliDRACDevice konfiguriert sein. Anhand dieser Konfiguration kann der iDRAC LDAP-Abfragen (Lightweight Directory Access Protocol) an das Active Directory senden.
Klassentyp	Strukturklasse
SuperClasses	dellProduct
Attribute	dellSchemaVersion dellRacType

Tabelle 7-4. delliDRACAssociationObject Class

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

Tabelle 7-5. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Beschreibung	Wird verwendet, um die Berechtigungen (Autorisierungsrechte) für das iDRAC-Gerät zu definieren.
Klassentyp	Erweiterungsklasse
SuperClasses	NONE
Attribute	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Tabelle 7-6. 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 7-7. 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 7-8. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden

Attributname/Beschreibung	Zugewiesener OID/ Syntax-Objektkennzeichner	Einzelbe-wertung
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

Tabelle 7-8. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden *(fortgesetzt)*

Attributname/Beschreibung	Zugewiesener OID/ Syntax-Objektkennzeichner	Einzelbe-wertung
dellIsLoginUser	1.2.840.113556.1.8000.1280.1.1.2.3	TRUE
TRUE, wenn der Benutzer Anmeldungsrechte auf dem Gerät hat.	Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsCardConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.4	TRUE
TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat.	Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsUserConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.5	TRUE
TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat.	Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsLogClearAdmin	1.2.840.113556.1.8000.1280.1.1.2.6	TRUE
TRUE, wenn der Benutzer Protokolllöschungsrechte auf dem Gerät hat.	Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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)	

Tabelle 7-8. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden *(fortgesetzt)*

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

Dell-Erweiterung zu Microsoft Active Directory Benutzer- und Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch das Active Directory-Benutzer- und -Computer-Snap-In erweitern, so dass der Administrator iDRAC-Geräte, Benutzer und Benutzergruppen, iDRAC-Zuordnungen und iDRAC-Berechtigungen verwalten kann.

Wenn Sie die Systems Management-Software mit der DVD *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In installieren, indem Sie während des Installationsverfahrens die Option **Active Directory-Benutzer und -Computer-Snap-in** auswählen. Das *Schnellinstallationshandbuch zu Dell OpenManage-Software* enthält zusätzliche Anleitungen zur Installation von Systemverwaltungssoftware. Für x64-Bit-Windows-Betriebssysteme befindet sich das Snap-In-Installationsprogramm 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

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

Weitere Informationen finden Sie unter „Öffnen des Microsoft Active Directory-Benutzer- und -Computer-Snap-In“ auf Seite 174.

Öffnen des Microsoft 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 Verwaltungstools→ 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. Um dieses Administratorpaket zu installieren, klicken Sie auf **Start→ Ausführen**, geben Sie `MMC` ein und drücken Sie 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**.

iDRAC-Benutzer und -Berechtigungen zum Microsoft Active Directory hinzufügen

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

- Erstellen eines iDRAC-Geräteobjekts
- Erstellen eines Berechtigungsobjekts
- Erstellen eines Zuordnungsobjekts
- Zuordnungsobjekt konfigurieren

iDRAC-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 iDRAC-Namen übereinstimmen, den Sie in Schritt A von „Konfiguration des Microsoft Active Directory mit erweitertem Schema unter Verwendung der webbasierten iDRAC6-Schnittstelle“ auf Seite 177 eingeben werden.

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 das Register **Remote-Management-Berechtigungen** und wählen Sie die Berechtigungen aus, die der Benutzer haben soll.

Erstellen von Zuordnungsobjekten

ANMERKUNG: Das iDRAC-Verbindungsobjekt wird von der Gruppe abgeleitet und sein Wirkungsbereich ist auf "Lokale Domäne" festgelegt.

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. Klicken Sie auf **OK**.

Zuordnungsobjekt konfigurieren

Mithilfe des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und iDRAC-Geräte zuordnen.

Sie können Gruppen von Benutzern 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**.

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

Berechtigungen hinzufügen

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

Wählen Sie das Register **Produkte** und fügen Sie ein iDRAC-Gerät hinzu, das mit dem Netzwerk verbunden ist, das den definierten Benutzern oder Benutzergruppen zur Verfügung steht. Mehrere iDRAC-Geräte können einem Zuordnungsobjekt hinzugefügt werden.

iDRAC-Geräte hinzufügen

So fügen Sie iDRAC-Geräte hinzu:

1. Wählen Sie das Register **Produkte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den iDRAC-Gerätenamen ein und klicken Sie auf **OK**.
3. Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.

Konfiguration des Microsoft Active Directory mit erweitertem Schema unter Verwendung der webbasierten iDRAC6-Schnittstelle

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
3. Wechseln Sie zu **iDRAC-Einstellungen**→ Register **Netzwerk/Sicherheit**→ Register **Verzeichnisdienst**→ **Microsoft Active Directory**.

4 Verwenden Sie den Bildlauf, um an den unteren Rand der Seite **Active Directory-Konfiguration und -Verwaltung** zu gelangen, und klicken Sie auf **Active Directory konfigurieren**.

Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 1 von 4** wird angezeigt.

5 Wählen Sie unter **Zertifikateinstellungen** die Option **Überprüfung des Zertifikats aktivieren** aus, falls Sie das SSL-Zertifikat der Active Directory-Server überprüfen möchten; fahren Sie andernfalls mit Schritt 9 fort.

6 Geben Sie unter **Active Directory-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**.

Die Zertifikatsinformationen für das Active Directory-CA-Zertifikat, das Sie hochgeladen haben, wird angezeigt.

8 **(Optional: Bei AD-Authentifizierung)** Geben Sie unter **Kerberos-Keytab hochladen** den Pfad der Keytab-Datei ein, oder suchen Sie die Datei mit der Durchsuchen-Funktion. Klicken Sie auf **Hochladen**. Das Kerberos-Keytab wird in den iDRAC6 hochgeladen.

9 Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 2 von 4** wird angezeigt.

10 Wählen Sie **Active Directory aktivieren**.

VORSICHTSHINWEIS: 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.

11 Klicken Sie auf **Hinzufügen**, um den Benutzer-Domänennamen einzugeben.

12 Geben Sie den Namen der Benutzerdomäne in die Eingabeaufforderung ein und klicken Sie **OK**.

ANMERKUNG: Dieser Schritt ist optional. Wenn Sie eine Liste von Benutzerdomänen konfigurieren, ist diese Liste auf dem Anmeldebildschirm der Webschnittstelle verfügbar. Sie können eine Auswahl treffen, sodass Sie anschließend nur noch den Benutzernamen eingeben müssen.

13 Geben Sie in das Feld **Zeitüberschreitung** die Zeit in Sekunden ein, wie lange iDRAC auf eine Antwort des Active Directory warten soll. Der Standardwert beträgt 120 Sekunden.

14 Wählen Sie eine der folgenden Optionen:

a **Domänen-Controller mit DNS suchen**, um die Active Directory-Domänen-Controller über eine DNS-Suche abzurufen. Die Domänen-Controller-Serveradressen 1-3 werden ignoriert. Wählen Sie **Benutzerdomäne der Anmeldung** aus, um die DNS-Suche mit dem Domänennamen des Anmeldebenutzers durchzuführen. Alternativ dazu können Sie **Domäne angeben** auswählen und den Domänennamen eingeben, der bei der DNS-Anfrage 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. Für **Erweitertes Schema** befinden sich die Domänen-Controller dort, wo sich das iDRAC6-Geräteobjekt und die Zuordnungsobjekte befinden.

b Option **Domänen-Controller-Adressen angeben**, um iDRAC6 zu ermöglichen, die Serveradressen des Active Directory-Domänen-Controllers zu verwenden, die festgelegt wurden. DNS-Suche wird nicht durchgeführt. Geben Sie die IP-Adresse oder den vollständigen qualifizierten Domänennamen (FQDN) des Domänen-Controllers ein. Wenn die Option **Domänen-Controller-Adressen angeben** ausgewählt wird, muss mindestens eine der drei Adressen konfiguriert werden. 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, an denen sich das iDRAC6-Geräteobjekt und die Zuordnungsobjekte befinden.

ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie im Feld **Domänen-Controller-Serveradresse** angeben, muss mit dem Feld „Servername" oder „Alternativer Servername" des Domänen-Controller-Zertifikats übereinstimmen, wenn die Zertifikatsüberprüfung aktiviert ist.

15 Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 3 von 4** wird angezeigt.

16 Wählen Sie unter **Schemaauswahl** die Option **Erweitertes Schema** aus.

17 Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 4 von 4** wird angezeigt.

18 Geben Sie unter **Erweiterte Schemaeinstellungen** den **iDRAC-Namen** und den **iDRAC-Domänennamen** ein, um das iDRAC-Geräteobjekt zu konfigurieren. Der iDRAC-Domänenname ist die Domäne, in der das iDRAC-Objekt erstellt wird.

19 Klicken Sie auf **Fertig stellen**, um die Einstellungen des Active Directory mit erweitertem Schema zu speichern.

Der iDRAC6-Web Server kehrt automatisch zur Seite **Active Directory-Konfiguration und Verwaltung** zurück.

20 Klicken Sie auf **Einstellungen überprüfen**, um die Einstellungen des Active Directory mit erweitertem Schema zu prüfen.

21 Geben Sie Ihren Active Directory-Benutzernamen und das Kennwort ein.

Die Testergebnisse und das Testprotokoll werden angezeigt. Weitere Informationen finden Sie unter „Einstellungen testen“ auf Seite 194.

ANMERKUNG: Um die Anmeldung beim Active Directory zu unterstützen, müssen Sie einen DNS-Server korrekt im iDRAC-Programm konfiguriert haben. Klicken Sie auf die Seite **iDRAC-Einstellungen→ Netzwerk/ Sicherheit→ Netzwerk**, um 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 Microsoft Active Directory mit erweitertem Schema unter Verwendung von RACADM

Verwenden Sie die folgenden Befehle, um die iDRAC6-Microsoft Active Directory-Funktion mit erweitertem Schema zu konfigurieren, indem Sie das RACADM-CLI-Hilfsprogramm anstelle der webbasierten Schnittstelle verwenden.

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: Mindestens eine der drei Adressen muss konfiguriert werden. iDRAC versucht so lange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte. Wenn die Option für das erweiterte Schema ausgewählt ist, sind dies die FQDN bzw. IP-Adressen des Domänen-Controllers, auf dem sich das iDRAC-Gerät befindet. Global Catalog Server werden im Modus „Erweitertes Schema" nicht verwendet.

ANMERKUNG: Der FQDN oder die IP-Adresse, den/die Sie in diesem Feld angeben, sollte mit dem Feld „Servername" oder „Alternativer Servername" des Zertifikats Ihres Domänen-Controllers übereinstimmen, wenn Sie die Überprüfung des Zertifikats aktiviert haben.

VORSICHTSHINWEIS: 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.

Wenn Sie die DNS-Suche zum Abrufen der Serveradresse des Active Directory-Domänen-Controllers verwenden möchten, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgActiveDirectory -o
cfgADDcSRVLookupEnable=1
```

- Zum Ausführen der DNS-Suche mit dem Domänennamen des Anmeldebenutzers:

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupbyUserdomain=1
  ```

- Zur Angabe des Domänennamens zur Verwendung der DNS-Suche:

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <Domänenname zur
  Verwendung bei der DNS-Suche>
  ```

Wenn Sie für den SSL-Handshake die Überprüfung des Zertifikats 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 für den SSL-Handshake die Überprüfung des Zertifikats erzwingen 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 config -g cfgActiveDirectory -o
cfgADCertValidationEnable 1
```

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

Die Verwendung des folgenden RACADM-Befehls kann optional sein. Weitere Informationen hierzu finden Sie unter „SSL-Zertifikat der iDRAC6-Firmware importieren“ auf Seite 160.

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

2 Wenn Sie die Zeit in Sekunden angeben möchten, die abgewartet werden soll, bis Active Directory-Abfragen abgeschlossen werden, bevor eine Zeitüberschreitung eintritt, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgActiveDirectory -o
cfgADAuthTimeout <Zeit in Sekunden>
```

3 Wenn DHCP auf dem iDRAC 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
```

4 Wenn DHCP auf dem iDRAC deaktiviert ist, oder Sie möchten Ihre DNS-IP-Adresse manuell eingeben, geben Sie folgende RACADM-Befehle ein:

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

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

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

5 Wenn Sie eine Liste von Benutzerdomänen erstellen möchten, so dass für die Anmeldung bei der iDRAC6-Webschnittstelle nur der Benutzername eingegeben werden muss, verwenden Sie den folgenden Befehl:

```
racadm config -g cfgUserDomain -o
cfgUserDomainName -i <Index>
```

Sie können bis zu 40 Benutzerdomänen mit Indexzahlen zwischen 1 und 40 konfigurieren.

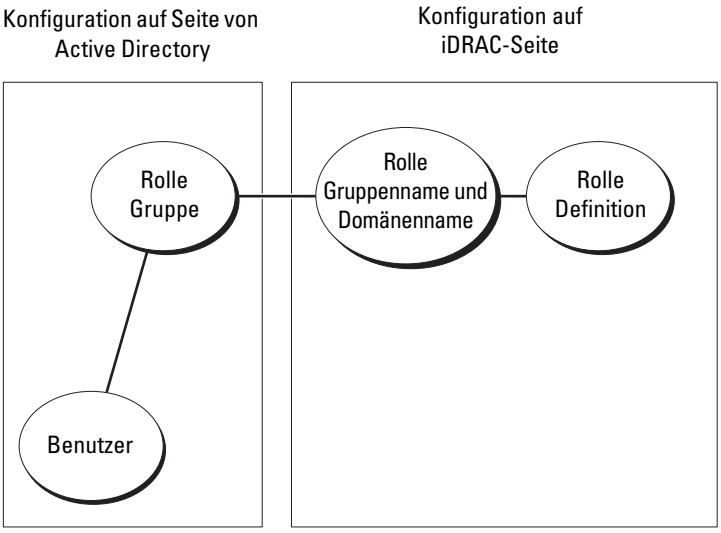
Details zu Benutzerdomänen finden Sie unter „Allgemeiner LDAP-Verzeichnisdienst“ auf Seite 195.

6 Drücken Sie die **Eingabetaste**, um die Konfiguration des Active Directory mit erweitertem Schema abzuschließen.

Übersicht des Standardschema-Active Directory

Wie in Abbildung 7-3 dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration unter Active Directory und unter iDRAC6.

Abbildung 7-3. Konfiguration des iDRAC 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 einen bestimmten iDRAC6 zu gewähren, muss der Rollengruppenname und dessen Domänenname auf dem jeweiligen iDRAC6 konfiguriert werden. Im Gegensatz zur Lösung des erweiterten Schemas wird die Rolle und die Berechtigungsebene auf jedem iDRAC6 und nicht im Active Directory definiert. Auf jedem iDRAC können bis zu fünf Rollengruppen konfiguriert und definiert werden. Tabelle 7-9 zeigt die Standard-Rollengruppen-Berechtigungen.

ANMERKUNG: Die Standardeinstellung der Berechtigungsstufe der Rollengruppe ist für alle fünf Rollengruppen **Keine**. Sie müssen eine der Standardrollengruppenberechtigungen aus dem Drop-Down-Feld auswählen.

Tabelle 7-9. Standardeinstellungsberechtigungen der Rollengruppe

Berechtigungsstufe	Gewährte Berechtigungen	Bitmaske
Administrator	Am iDRAC anmelden, iDRAC konfigurieren, Benutzer konfigurieren, Protokolle löschen, Serversteuerungsbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen	0x000001ff
Operator	Am iDRAC anmelden, iDRAC konfigurieren, Serversteuerungsbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen	0x000000f9
Schreibgeschützt	Am iDRAC anmelden	0x00000001
Keine	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bitmasken-Werte werden nur verwendet, wenn das Standardschema unter Verwendung des RACADM eingerichtet wird.

Einfache Domänen (Single Domains) und mehrfache Domänen (Multiple Domains)

Wenn sich alle Anmeldebenutzer und Rollengruppen sowie die verschachtelten Gruppen in derselben Domäne befinden, müssen lediglich die Adressen der Domänen-Controller auf dem iDRAC6 konfiguriert werden. In diesem Muster einer einfachen Domäne wird jede Art von Gruppe unterstützt.

Wenn alle Anmeldebenutzer und Rollengruppen oder beliebige der verschachtelten Gruppen mehreren Domänen angehören, müssen Server-Adressen des Globalen Katalogs auf dem iDRAC6 konfiguriert werden. In diesem Muster mehrfacher Domänen müssen alle Rollengruppen und, falls vorhanden, alle verschachtelten Gruppen einer Universalgruppe angehören.

Konfiguration des Microsoft Active Directory mit Standardschema für den Zugriff auf 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 Gruppennamen und den Domänennamen auf iDRAC6, indem Sie entweder die webbasierte Schnittstelle oder RACADM verwenden. Weitere Informationen finden Sie unter „Konfiguration des Microsoft Active Directory mit Standardschema unter Verwendung der webbasierten iDRAC6-Schnittstelle“ auf Seite 186 und „Konfiguration des Microsoft Active Directory mit Standardschema unter Verwendung von RACADM“ auf Seite 190.

Konfiguration des Microsoft Active Directory mit Standardschema unter Verwendung der webbasierten iDRAC6-Schnittstelle

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
3. Wechseln Sie zu **iDRAC-Einstellungen**→ Register **Netzwerk/ Sicherheit**→ Register **Verzeichnisdienst**→ **Microsoft Active Directory**.
4. Verwenden Sie den Bildlauf, um an den unteren Rand der Seite **Active Directory-Konfiguration und -Verwaltung** zu gelangen, und klicken Sie auf **Active Directory konfigurieren**.

   Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 1 von 4** wird angezeigt.
5. Wählen Sie unter **Zertifikateinstellungen** die Option **Überprüfung des Zertifikats aktivieren** aus, falls Sie das SSL-Zertifikat der Active Directory-Server überprüfen möchten; fahren Sie andernfalls mit Schritt 9 fort.
6. Wechseln Sie unter **Active Directory-CA-Zertifikat hochladen** zur Zertifikatsdatei.

7 Klicken Sie auf **Hochladen**.

Die Zertifikatsinformationen für das gültige Active Directory-CA-Zertifikat werden angezeigt.

8 **(Optional: Bei AD-Authentifizierung)** Geben Sie unter **Kerberos-Keytab hochladen** den Pfad der Keytab-Datei ein, oder suchen Sie die Datei mit der Durchsuchen-Funktion. Klicken Sie auf **Hochladen**. Das Kerberos-Keytab wird in den iDRAC6 hochgeladen.

9 Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 2 von 4** wird angezeigt.

10 Wählen Sie **Active Directory aktivieren**.

11 Wählen Sie **Einfache Anmeldung aktivieren**, wenn Sie sich bei iDRAC6 anmelden möchten, ohne Ihre Benutzeranmeldeinformationen für die Domäne, z. B. Benutzername und Kennwort, einzugeben.

12 Klicken Sie auf **Hinzufügen**, um den Benutzer-Domänennamen einzugeben.

13 Geben Sie den Namen der Benutzerdomäne in die Eingabeaufforderung ein und klicken Sie **OK**.

14 Geben Sie in die **Zeitüberschreitungs**-Felder die Zeit in Sekunden ein, wie lange iDRAC auf Antworten des Active Directory warten soll. Der Standardwert beträgt 120 Sekunden.

15 Wählen Sie eine der folgenden Optionen:

a **Domänen-Controller mit DNS suchen**, um die Active Directory-Domänen-Controller über eine DNS-Suche abzurufen. Die Domänen-Controller-Serveradressen 1-3 werden ignoriert. Wählen Sie **Benutzerdomäne der Anmeldung** aus, um die DNS-Suche mit dem Domänennamen des Anmeldebenutzers durchzuführen. Alternativ dazu können Sie **Domäne angeben** auswählen und den Domänennamen eingeben, der bei der DNS-Anfrage 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 das **Standardschema** ausgewählt ist, befinden sich die Domänen-Controller dort, wo sich die Benutzerkonten und Rollengruppen befinden.

b Wählen Sie die Option **Domänen-Controller-Adressen angeben** aus, um iDRAC6 zu ermöglichen, die Serveradressen des Active Directory-Domänen-Controllers zu verwenden, die festgelegt wurden. DNS-Suche wird nicht durchgeführt. Geben Sie die IP-Adresse oder den vollständigen qualifizierten Domänennamen (FQDN) des Domänen-Controllers ein. Wenn die Option **Domänen-Controller-Adressen angeben** ausgewählt wird, muss mindestens eine der drei Adressen 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.

ANMERKUNG: Der FQDN oder die IP-Adresse, den/die Sie in diesem Feld angeben, sollte mit dem Feld „Servername" oder „Alternativer Servername" des Zertifikats Ihres Domänen-Controllers übereinstimmen, wenn Sie die Überprüfung des Zertifikats aktiviert haben.

16 Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 3 von 4** wird angezeigt.

17 Wählen Sie unter **Schemaauswahl** die Option **Standardschema** aus.

18 Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 4a von 4** wird angezeigt.

19 Wählen Sie eine der folgenden Optionen:

- 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. Serveradressen 1-3 des Globalen Katalogs werden 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 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 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.

ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie im Feld **Global Catalog-Serveradresse** angeben, muss mit dem Feld „Servername" oder „Alternativer Servername" des Domänen-Controller-Zertifikats übereinstimmen, wenn die Zertifikatsüberprüfung aktiviert ist.

ANMERKUNG: Der Server des Globalen Katalogs ist nur dann für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen in verschiedenen Domänen befinden. Im Falle mehrerer Domänen wie hier kann nur die Universalgruppe verwendet werden.

20 Klicken Sie unter **Rollengruppen** auf eine **Rollengruppe**.

Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 4b von 4** wird angezeigt.

21 Geben Sie den **Rollengruppennamen** an.

Der **Rollengruppenname** identifiziert die Rollengruppe im Active Directory, das dem iDRAC zugeordnet ist.

22 Geben Sie die **Rollengruppendomäne** an, d. h. die Domäne der Rollengruppe.

23 Geben Sie die **Rollengruppenberechtigungen** an, indem Sie die **Rollengruppenberechtigungsebene** auswählen. Wenn Sie zum Beispiel **Administrator** auswählen, werden alle Berechtigungen für diese Berechtigungsebene ausgewählt.

24 Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern.

Der iDRAC6-Web Server kehrt automatisch zur Seite **Schritt 4a von 4 Active Directory-Konfiguration und -Verwaltung** zurück, auf der Ihre Einstellungen angezeigt werden.

25 Konfigurieren Sie, falls erforderlich, weitere Rollengruppen.

26 Klicken Sie auf **Fertig stellen**, um zur Seite **Active Directory-Konfiguration und -Verwaltung** zurückzukehren.

27 Klicken Sie auf **Einstellungen überprüfen**, um die Einstellungen des Active Directory-Standardschemas zu prüfen.

28 Geben Sie Ihren iDRAC6-Benutzernamen und das Kennwort ein.

Die Testergebnisse und das Testprotokoll werden angezeigt. Weitere Informationen finden Sie unter „Einstellungen testen“ auf Seite 194.

ANMERKUNG: Um die Anmeldung beim Active Directory zu unterstützen, müssen Sie einen DNS-Server korrekt im iDRAC-Programm konfiguriert haben. Klicken Sie auf die Seite **iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Netzwerk**, um DNS-Server manuell zu konfigurieren, oder verwenden Sie DHCP, um DNS-Server abzurufen.

Die Konfiguration des Active Directory mit Standardschema ist nun abgeschlossen.

Konfiguration des Microsoft Active Directory mit Standardschema unter Verwendung von RACADM

Verwenden Sie die folgenden Befehle zum Konfigurieren der Active Directory-Funktion von iDRAC mit Standardschema unter Verwendung der RACADM-CLI anstelle 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 <allgemeiner Name der
Rollengruppe>

racadm config -g cfgStandardSchema -i <Index> -o
cfgSSADRoleGroupDomain <vollständig qualifizierter
Domänenname>

racadm config -g cfgStandardSchema -i <Index> -o
cfgSSADRoleGroupPrivilege <Bitmasken-Zahlenwert
für spezifische Benutzerberechtigungen>
```

ANMERKUNG: Informationen zu den Bitmasken-Zahlenwerten finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

```
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: Der FQDN oder die IP-Adresse, den/die Sie in diesem Feld angeben, sollte mit dem Feld „Servername" oder „Alternativer Servername" des Zertifikats Ihres Domänen-Controllers übereinstimmen, wenn Sie die Überprüfung des Zertifikats aktiviert haben.

ANMERKUNG: Geben Sie den FQDN des Domänen-Controllers ein, *nicht* nur den FQDN der Domäne. 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.

Wenn Sie die DNS-Suche zum Abrufen der Serveradresse des Active Directory-Domänen-Controllers verwenden möchten, geben Sie den folgenden Befehl ein:

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

- Zum Ausführen der DNS-Suche mit dem Domänennamen des Anmeldebenutzers:

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

- Zur Angabe des Domänennamens zur Verwendung der DNS-Suche:

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <Domänenname zur
  Verwendung bei der DNS-Suche>
  ```

Um die Adresse des Global Catalog-Servers anzugeben, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog1 <vollständig qualifizierter Domänenname
oder IP-Adresse des Domänen-Controllers>
```

```
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog2 <vollständig qualifizierter Domänenname
oder IP-Adresse des Domänen-Controllers>
```

```
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog3 <vollständig qualifizierter Domänenname
oder IP-Adresse des Domänen-Controllers>
```

ANMERKUNG: Der Server des Globalen Katalogs ist nur dann 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.

ANMERKUNG: Der FQDN oder die IP-Adresse, den/die Sie in diesem Feld angeben, sollte mit dem Feld „Servername" oder „Alternativer Servername" des Zertifikats Ihres Domänen-Controllers übereinstimmen, wenn Sie die Überprüfung des Zertifikats aktiviert haben.

Wenn Sie die DNS-Suche zum Abrufen der Serveradresse des globalen Active Directory-Katalogs verwenden möchten, geben Sie den folgenden Befehl ein:

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

```
racadm config -g cfgActiveDirectory -o
cfgADGcRootDomain <Domänenname>
```

Wenn Sie für den SSL-Handshake die Überprüfung des Zertifikats 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 für den SSL-Handshake die Überprüfung des Zertifikats erzwingen 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-
Zertifikat>
```

Die Verwendung des folgenden RACADM-Befehls kann optional sein. Weitere Informationen hierzu finden Sie unter „SSL-Zertifikat der iDRAC6-Firmware importieren“ auf Seite 160.

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

2 Wenn Sie die Zeit in Sekunden angeben möchten, die abgewartet werden soll, bis Active Directory-Abfragen abgeschlossen werden, bevor eine Zeitüberschreitung eintritt, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgActiveDirectory -o
cfgADAuthTimeout <Zeit in Sekunden>
```

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

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

4 Wenn DHCP auf dem iDRAC6 deaktiviert ist, oder Sie möchten Ihre DNS-IP-Adresse manuell eingeben, geben Sie die folgenden RACADM-Befehle ein:

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

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

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

5 Wenn Sie eine Liste von Benutzerdomänen erstellen möchten, so dass für die Anmeldung bei der Webschnittstelle nur der Benutzername eingegeben werden muss, verwenden Sie den folgenden Befehl:

```
racadm config -g cfgUserDomain -o
cfgUserDomainName -i <Index>
```

Sie können bis zu 40 Benutzerdomänen mit Indexzahlen zwischen 1 and 40 konfigurieren. Weitere Informationen zu Benutzerdomänen finden Sie unter „Allgemeiner LDAP-Verzeichnisdienst“ auf Seite 195.

Einstellungen testen

Wenn Sie überprüfen möchten, ob die Konfiguration korrekt funktioniert, oder eine Problemanalyse wegen der Fehlermeldung bei der Anmeldung zum Active Directory durchführen möchten, können Sie die Einstellungen von der iDRAC6-Webschnittstelle aus testen.

Nach Abschluss der Konfiguration in der iDRAC6-Webschnittstelle klicken Sie am unteren Rand der Seite 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 unteren Rand der Ergebnisseite 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 zu Active Directory“ auf Seite 201.

Wenn Sie Ihre Einstellungen ändern müssen, wählen Sie die Registerkarte **Active Directory** und ändern Sie die Konfiguration Schritt für Schritt.

Allgemeiner LDAP-Verzeichnisdienst

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 allgemein zu gestalten, werden die Übereinstimmungen zwischen unterschiedlichen Verzeichnisdiensten verwendet, um Benutzer zu gruppieren und dann die Benutzergruppenbeziehung zuzuordnen. 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 anmeldende Benutzer gibt nur den Benutzernamen ein und lässt den Domänennamen aus. 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 das allgemeine LDAP aktiviert ist, zeigt die GUI-Anmeldeseite im Dropdown-Menü nur „Dieser iDRAC“ an.

ANMERKUNG: Die Zeichen „<“ und „>“ sind im Benutzernamen für openLDAP- und OpenDS-basierte Verzeichnisdienste nicht zulässig.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes unter Verwendung der webbasierten iDRAC6-Schnittstelle

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
3. Wechseln Sie zu **iDRAC-Einstellungen**→ Register **Netzwerk/Sicherheit**→ Register **Verzeichnisdienst**→ **Allgemeiner LDAP-Verzeichnisdienst**.

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 **Allgemeines LDAP – Konfiguration und Verwaltung Schritt 1 von 3** 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.

4 Markieren Sie unter **Zertifikatseinstellungen** die Option **Zertifikatsüberprüfung aktivieren**, um die Zertifikatsüberprüfung 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. Das LDAP-Serveradressfeld in iDRAC6 muss so eingestellt werden, dass es mit der FQDN-Adresse übereinstimmt, damit die Zertifikatsüberprüfung funktionieren kann.

5 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.

6 Klicken Sie auf **Hochladen.**

Das Zertifikat der Stamm-Zertifizierungsstelle, die alle SSL-Serverzertifikate (Security Socket Layer) des Domänen-Controllers unterzeichnet, wird hochgeladen.

7 Klicken Sie auf **Weiter**. Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung Schritt 2 von 3** wird angezeigt. Auf dieser Seite können Sie Informationen über die Speicherorte generischer LDAP-Server und Benutzerkonten konfigurieren.

ANMERKUNG: In dieser Version werden Smart Card-basierte Zweifaktor-Authentifizierung (TFA) und einfache Anmeldung (SSO) nicht für den allgemeinen LDAP-Verzeichnisdienst unterstützt.

8 Geben Sie die folgenden Informationen ein:

- 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.

- 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.
- Geben Sie in das Feld **LDAP-Serveradresse** den vollständigen qualifizierten Domänennamen (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.
- Geben Sie den Anschluss, der für LDAP über SSL verwendet wird, in das Feld **LDAP-Serveranschluss** ein. Die Standardeinstellung ist 636.

- 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.
- Geben Sie das **Bindungskennwort** ein, das zusammen mit dem **Bindungs-DN** verwendet werden soll. Dies ist erforderlich, wenn keine anonyme Bindung zugelassen ist.
- Geben Sie in das Feld **Basis-DN zur Suche** den DN des Verzeichnisasts ein, bei dem alle Suchen starten sollen.
- 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.
- 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*.
- 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.

9 Klicken Sie auf **Weiter**. Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung Schritt 3a von 3** wird angezeigt. Auf dieser Seite können Sie die Berechtigungsgruppen für Benutzerbefugnisse konfigurieren. Wenn das allgemeine LDAP aktiviert ist, werden eine oder mehrere Rollengruppen verwendet, um die Befugnisrichtlinie für iDRAC6-Benutzer festzulegen.

ANMERKUNG: Anders als bei AD ist es in dieser Version nicht erforderlich, Sonderzeichen zu verwenden („@“, „\“ und „/“), um einen LDAP-Benutzer von einem lokalen Benutzer zu unterscheiden. Verwenden Sie zum Anmelden ausschließlich Ihren Benutzernamen und nicht den Domänennamen.

10 Klicken Sie unter **Rollengruppen** auf eine **Rollengruppe**.

Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung Schritt 3b von 3** wird angezeigt. Auf dieser Seite können Sie jede zur Kontrolle der Benutzerbefugnisse verwendete Rollengruppe konfigurieren.

11 Geben Sie in das Feld **Gruppen-DN** den abgegrenzten Gruppennamen ein, der die Rollengruppe im allgemeinen LDAP-Verzeichnisdienst identifiziert, der mit dem iDRAC6 verbunden ist.

12 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.

13 Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern.

Der iDRAC6-Web Server führt Sie automatisch zur Seite **Allgemeines LDAP – Konfiguration und Verwaltung: Schritt 3a von 3** zurück, wo Ihre Rollengruppeneinstellungen angezeigt werden.

14 Konfigurieren Sie bei Bedarf weitere Rollengruppen.

15 Klicken Sie auf **Fertig stellen**, um zur Zusammenfassungsseite **Allgemeines LDAP – Konfiguration und Verwaltung** zurückzuwechseln.

16 Klicken Sie auf **Einstellungen überprüfen,** um die Einstellungen für das generische LDAP zu überprüfen.

17 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.

Die Testergebnisse und das Testprotokoll werden angezeigt. Sie haben die Konfiguration des allgemeinen LDAP-Verzeichnisdiensts abgeschlossen.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM

```
racadm config -g cfgldap -o cfgLdapEnable 1
```

```
racadm config -g cfgldap -o cfgLdapServer <FQDN oder
IP-Adresse>
```

```
racadm config -g cfgldap -o cfgLdapPort
<Schnittstellennummer>
```

```
racadm config -g cfgldap -o cfgLdapBaseDN dc=
common,dc=com
```

```
racadm config -g cfgldap -o
cfgLdapCertValidationenable 0
```

```
racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupDN 'cn=everyone,ou=groups,dc=
common,dc=com'
```

```
racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupPrivilege 0x0001
```

Zeigen Sie die Einstellungen unter Verwendung der folgenden Befehle an:

```
racadm getconfig -g cfgldap
```

```
racadm getconfig -g cfgldaprolegroup -i 1
```

Verwenden Sie RACADM, um zu prüfen, ob die Anmeldung möglich ist

```
racadm -r <iDRAC6-IP> -u user.1 -p password getractime
```

Zusätzliche Einstellungen zum Testen der Option BindDN

```
racadm config -g cfgldap -o cfgLdapBindDN "cn=
idrac_admin, ou=iDRAC_admins, ou=People, dc=common,
dc=com"
```

```
racadm config -g cfgldap -o cfgLdapBindPassword
password
```

ANMERKUNG: Konfigurieren Sie iDRAC6 zur Verwendung eines Domänennamenservers, wodurch der LDAP-Server-Host-Name aufgelöst wird, für dessen Verwendung in der LDAP-Serveradresse der iDRAC6 konfiguriert ist. Der Host-Name muss mit dem „CN“ oder „Subjekt“ im Zertifikat des LDAP-Servers übereinstimmen.

Häufig gestellte Fragen zu Active Directory

Meine Active Directory-Anmeldung ist gescheitert. Wie kann ich dieses Problem beheben?

iDRAC6 bietet über die Webschnittstelle ein Diagnoseprogramm an. Melden Sie sich auf der Webschnittstelle als lokaler Benutzer mit Administratorrechten an. Klicken Sie auf **iDRAC-Einstellungen**→ Register **Netzwerk/Sicherheit**→ **Verzeichnisdienst**→ **Microsoft Active Directory**. Verwenden Sie den Bildlauf, um an den unteren Rand der Seite **Active Directory-Konfiguration und Verwaltung**zu gelangen, und klicken Sie auf **Einstellungen überprüfen**. 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. Ein detaillierter Testbericht zur Unterstützung beim Lösen von Problemen wird ebenfalls aufgezeichnet. Wechseln Sie zur Seite **Active Directory-Konfiguration und -Verwaltung** zurück. Verwenden Sie den Bildlauf, um an den unteren Rand der Seite zu gelangen, und klicken Sie auf **Active Directory konfigurieren**, um Ihre Konfiguration zu ändern, und führen Sie den Test erneut durch, bis der Testbenutzer die Autorisierung erhält.

Ich habe die Überprüfung des Zertifikats aktiviert, meine Active Directory-Anmeldung ist aber trotzdem gescheitert. Ich habe die Diagnose von der GUI aus durchgeführt und die Testergebnisse zeigen die folgende Fehlermeldung an:

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.

Wo könnte das Problem liegen, und wie kann ich es beheben?

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:

1. Das Gültigkeitsdatum des iDRAC6 liegt über dem des Server-Zertifikats oder des CA-Zertifikats. Überprüfen Sie die aktuelle iDRAC6-Zeit und die Gültigkeitsdauer Ihres Zertifikats.

2 Die in iDRAC6 konfigurierten Domänen-Controller-Adressen stimmen nicht mit dem Servernamen oder alternativen Servernamen im Directory-Server-Zertifikat überein. Falls Sie eine IP-Adresse verwenden, lesen Sie bitte die folgende Frage und Antwort. Wenn Sie einen FQDN verwenden, stellen Sie bitte sicher, dass Sie den FQDN des Domänen-Controllers verwenden und nicht den der Domäne selbst, zum Beispiel `servername.example.com` anstelle von `example.com`.

Ich verwende eine IP-Adresse als Adresse des Domänen-Controllers und erhalte keine Genehmigung für mein Zertifikat. Wo liegt das Problem?

Prüfen Sie das Feld Servername oder alternativer Servername Ihres Domänen-Controller-Zertifikats. Normalerweise verwendet Active Directory den Host-Namen und nicht die IP-Adresse des Domänen-Controllers im Feld Servername oder alternativer Servername des Domänen-Controller-Zertifikats. Das Problem lässt sich auf verschiedene Weisen beheben.

1 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.

2 Erstellen Sie das Server-Zertifikat erneut, damit im Feld „Servername“ oder „Alternativer Servername“ eine IP-Adresse verwendet wird, die auf dem iDRAC6 konfiguriert ist.

3 Deaktivieren Sie die Überprüfung des Zertifikats, wenn Sie dem Domänen-Controller beim SSL-Handshake ohne diese Überprüfung vertrauen.

Ich verwende das erweiterte Schema in einer Umgebung mit mehreren Domänen. Wie kann ich die Adresse(n) des Domänen-Controllers konfigurieren?

Es sollte der Host-Name (FQDN) oder die IP-Adresse des Domänen-Controllers sein, der die Domäne bedient, in der sich das iDRAC6-Objekt befindet.

Muss ich Adressen des globalen Katalogs konfigurieren?

Wenn Sie ein erweitertes Schema verwenden, wird die Adresse des globalen Katalogs nicht verwendet.

Wenn Sie das Standardschema verwenden und Benutzer und Rollengruppen verschiedenen Domänen angehören, sind Adressen des globalen Katalogs erforderlich. In diesem Fall kann nur die Universalgruppe verwendet werden.

Wenn Sie das Standardschema verwenden und alle Benutzer und alle Rollengruppen derselben Domäne angehören, sind keine Adressen des globalen Katalogs erforderlich.

Wie funktioniert die Abfrage im Standardschema?

iDRAC6 verbindet sich zuerst mit den konfigurierten Domänen-Controller-Adressen, wenn sich die Benutzer und Rollengruppen in dieser Domäne befinden. Die Berechtigungen werden gespeichert.

Wenn Adressen des globalen Katalogs konfiguriert sind, fragt iDRAC6 weiterhin den globalen Katalog ab. Wenn zusätzliche Berechtigungen vom globalen Katalog abgerufen werden, werden diese Berechtigungen angesammelt.

Verwendet iDRAC6 immer LDAP über SSL?

Ja Der gesamte Transfer erfolgt über den geschützten Anschluss 636 und/oder 3269.

Unter *Einstellungen testen* führt iDRAC6 einen LDAP CONNECT durch, um das Problem zu isolieren, er führt jedoch keinen LDAP BIND auf einer unsicheren Verbindung aus.

Warum ist in der Standardkonfiguration des 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.

Unterstützt iDRAC6 den NetBIOS-Namen?

Nicht in dieser Version.

Was sollte ich überprüfen, wenn ich mich nicht über Active Directory beim iDRAC6 anmelden kann?

Sie können das Problem diagnostizieren, indem Sie in der webbasierten iDRAC6-Schnittstelle am unteren Rand der Seite **Active Directory-Konfiguration und -Verwaltung** auf **Einstellungen testen** klicken. Anschließend können Sie das Problem mithilfe der durch die Testergebnisse angezeigten Lösung beheben. Weitere Informationen finden Sie unter „Einstellungen testen“ auf Seite 194.

Die meisten der häufig vorkommenden Probleme werden in diesem Abschnitt erklärt. Grundsätzlich sollte jedoch Folgendes überprüft werden:

1. Stellen Sie sicher, dass Sie während einer Anmeldung den korrekten Benutzerdomänennamen und nicht den NetBIOS-Namen verwenden.
2. Wenn Sie ein lokales iDRAC6-Benutzerkonto besitzen, melden Sie sich mit den lokalen Anmeldeinformationen am iDRAC6 an.

   Wenn Sie angemeldet sind:

   a. Stellen Sie sicher, dass die Option **Active Directory aktivieren** auf der iDRAC6-Seite **Active Directory-Konfiguration und -Verwaltung** markiert ist.

   b. Stellen Sie sicher, dass die DNS-Einstellung auf der iDRAC6-Netzwerkkonfigurationsseite korrekt ist.

   c. Stellen Sie sicher, dass Sie das richtige Stamm-CA-Zertifikat des Active Directory auf den iDRAC6 hochgeladen haben, falls Überprüfung des Zertifikats aktiviert ist. Überprüfen Sie, ob die Gültigkeitsdauer des iDRAC6-Zertifikats mit der des CA-Zertifikats übereinstimmt.

   d. Wenn Sie mit dem erweiterten Schema arbeiten, prüfen Sie, ob die **iDRAC6-Namen** und **iDRAC6-Domänennamen** mit der Umgebungskonfiguration in Ihrem Active Directory übereinstimmen.

      Wenn Sie mit dem Standardschema arbeiten, ist sicherzustellen, dass der **Gruppenname** und der **Gruppendomänenname** mit der Konfiguration in Ihrem Active Directory übereinstimmen.

3. Überprüfen Sie die SSL-Zertifikate des Domänen-Controllers, um sicherzustellen, dass die iDRAC6-Zeit innerhalb der Gültigkeitsdauer des Zertifikats liegt.

8

iDRAC6 für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren

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 Kerberos-basierte Active Directory-Authentifizierung zum Unterstützen von Active Directory-Smart Card- und -SSO-Anmeldungen.

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 -SSO-Anmeldungen.

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista und Windows Server 2008 verwenden Kerberos standardmäßig als Authentifizierungsmethode.

iDRAC6 verwendet Kerberos, um zwei Typen von Authentifizierungsmechanismen zu unterstützen: Active Directory-SSO- und Active Directory-Smart Card-Anmeldungen. Bei der Active Directory-SSO-Anmeldung verwendet iDRAC6 die Anmeldeinformationen des Benutzers, die im Betriebssystem zwischengespeichert werden, nachdem sich dieser 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. Dies ist die Nachfolgefunktion zur lokalen Smart Card-Authentifizierung.

Die Kerberos-Authentifizierung am iDRAC6 schlägt fehl, wenn die iDRAC6-Zeit von der Zeit des Domänen-Controllers abweicht. Es ist ein maximaler Unterschied von 5 Minuten zulässig. Um eine erfolgreiche Authentifizierung zu ermöglichen, müssen Sie die Serverzeit mit der Zeit des Domänen-Controllers synchronisieren und dann den iDRAC6 **zurücksetzen**.

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„iDRAC6-Verzeichnisdienst verwenden“ auf Seite 155.
- Registrieren Sie den iDRAC6 als Computer in der Active Directory-Root-Domäne. Führen Sie dazu folgende Schritte durch:
  - **a** Klicken Sie auf **iDRAC-Einstellungen**→ Register **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 **iDRAC auf DNS registrieren** aus.
  - **d** Geben Sie einen gültigen **DNS-Domänennamen an**.

    Weitere Informationen finden Sie in der *iDRAC6-Online-Hilfe*.
- 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.

Das vom Dienstprogramm "ktpass" abgerufene Keytab wird dem iDRAC6 als Datei-Upload 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 -princ
HOST/dracname.domainname.com@DOMAINNAME.COM -
mapuser dracname -crypto DES-CBC-MD5 -ptype
KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

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: Es wird empfohlen, das neueste **ktpass**-Dienstprogramm zum Erstellen der Keytab-Datei zu verwenden.

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://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true

- Die iDRAC6-Zeit muss mit dem Active Directory-Domänen-Controller synchronisiert sein. Sie können auch den folgenden RACADM-Zeitzonenabweichungsbefehl verwenden, um die Zeit zu synchronisieren:

  ```
  racadm config -g cfgRacTuning -o

  cfgRacTuneTimeZoneOffset <Abweichungswert>
  ```

- Beim Aktivieren der einfachen Anmeldung für das erweiterte Schema ist sicherzustellen, dass die Option **Diesem Benutzer bzgl. der Delegierung zu beliebigen Diensten vertrauen (nur Kerberos)** auf dem Register **Delegierung** für den Keytab-Benutzer ausgewählt ist. Dieses Register ist erst nach dem Erstellen der Keytab-Datei unter Verwendung des Dienstprogramms **ktpass** verfügbar.

Browser-Einstellungen zum Aktivieren der Active Directory-SSO

So konfigurieren Sie die Browser-Einstellungen für Internet Explorer:

1. Öffnen Sie den Webbrowser 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 relativen Domänennamen hinzu, die für Weblogic-Serverinstanzen verwendet werden, die Teil der SSO-Konfiguration sind (z. B. meinhost.beispiel.com).

7 Klicken Sie auf **Close** (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 Hängen Sie den iDRAC-Namen an network.negotiate-auth.trusted-uris an (unter Verwendung einer Liste mit Kommas als Trennzeichen).

5 Hängen Sie den iDRAC-Namen an network.negotiate-auth.delegation-uris an (unter Verwendung einer Liste mit Kommas als Trennzeichen).

Microsoft Active Directory SSO verwenden

Mit der SSO-Funktion können Sie sich direkt nach der Anmeldung an der Workstation am iDRAC6 anmelden, ohne die Benutzerauthentifizierungs-Anmeldeinformationen für die Domäne (z. B. Benutzername und Kennwort) eingeben zu müssen. Zum Anmelden beim iDRAC6 mit dieser Funktion sollten Sie sich bereits mit einem gültigen Active Directory-Benutzerkonto beim System angemeldet haben. Außerdem sollten Sie das Benutzerkonto konfiguriert haben, um sich unter Verwendung der Active Directory-Anmeldeinformationen am iDRAC6 anzumelden. Der iDRAC6 verwendet die zwischengespeicherten Active Directory-Anmeldeinformationen, um Sie anzumelden.

Sie können iDRAC6 aktivieren, um mithilfe von Kerberos, einem Netzwerk-Authentifizierungsprotokoll, SSO zu aktivieren. Weitere Informationen finden Sie unter„Informationen zur Kerberos-Authentifizierung“ auf Seite 205. Stellen Sie sicher, dass Sie die im Abschnitt „Voraussetzungen für die Active Directory-SSO- und -Smart Card-Authentifizierung“ auf Seite 206 aufgeführten Schritte ausgeführt haben, bevor Sie iDRAC6 für die SSO-Anmeldung konfigurieren.

iDRAC6 für die Verwendung von SSO konfigurieren

Führen Sie die folgenden Schritte aus, um iDRAC6 unter Verwendung der iDRAC-Webschnittstelle für SSO zu konfigurieren:

1. Melden Sie sich an der iDRAC-Webschnittstelle an.
2. Wechseln Sie zu **iDRAC-Einstellungen**→ Register **Netzwerk/ Sicherheit**→ Register **Verzeichnisdienst**→ **Microsoft Active Directory**.
3. Klicken Sie auf **Active Directory konfigurieren**. Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 1 von 4** wird angezeigt.
4. Laden Sie das aus der Active Directory-Root-Domäne abgerufene Keytab auf den iDRAC6 hoch. Geben Sie hierzu unter **Kerberos-Keytab hochladen** den Pfad der Keytab-Datei ein, oder klicken Sie auf **Durchsuchen**, um die Datei ausfindig zu machen. Klicken Sie auf **Hochladen**. Das Kerberos-Keytab wird in den iDRAC6 hochgeladen. Das Keytab ist dieselbe Datei, die Sie erstellt haben, während Sie die unter „Voraussetzungen für die Active Directory-SSO- und -Smart Card-Authentifizierung“ auf Seite 206 aufgeführten Tasks ausgeführt haben.
5. Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 2 von 4** wird angezeigt.
6. Wählen Sie **Einfache Anmeldung aktivieren** aus, um die SSO-Anmeldung zu aktivieren.
7. Klicken Sie auf **Weiter**, bis die letzte Seite angezeigt wird. Wenn Active Directory zur Verwendung des Standardschemas konfiguriert ist, wird die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 4a von 4** angezeigt. Wenn Active Directory zur Verwendung des erweiterten Schemas konfiguriert ist, wird die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 4 von 4** angezeigt.
8. Klicken Sie auf **Fertigstellen**, um die Einstellungen zu übernehmen.

RACADM verwenden:

Sie können die Keytab-Datei unter Verwendung des folgenden CLI-racadm-Befehls auf den iDRAC6 hochladen.

```
racadm krbkeytabupload -f <Dateiname>
```

wobei <Dateiname> der Name der Keytab-Datei ist. Der racadm-Befehl wird sowohl vom lokalen als auch vom Remote-racadm unterstützt.

Zum Aktivieren der einfachen Anmeldung über die CLI führen Sie den RACADM-Befehl aus:

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

Unter Verwendung der SSO am iDRAC6 anmelden

1. Melden Sie sich unter Verwendung eines gültigen Active Directory-Kontos am System an.
2. Geben Sie Folgendes ein, um die iDRAC6-Webseite abzurufen:

   `https://<FQDN-Adresse>`

   Wurde die Standard-HTTPS-Portnummer (443) geändert, geben Sie Folgendes ein:

   `https://<FQDN-Adresse>:<Anschlussnummer>`

   Hierbei ist *FQDN-Adresse* der iDRAC-FQDN (idracdnsname.domänenname) und *Schnittstellennummer* die Nummer der HTTPS-Schnittstelle.

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

   Der iDRAC6 meldet Sie an und verwendet dabei die Anmeldeinformationen, die im Betriebssystem zwischengespeichert wurden, als Sie sich unter Verwendung Ihres gültigen Active Directory-Kontos angemeldet haben.

   Sie sind am iDRAC6 mit den entsprechenden Microsoft Active Directory-Berechtigungen angemeldet, wenn:

   - Sie ein Microsoft Active Directory-Benutzer sind.
   - Sie im iDRAC6 für die Active Directory-Anmeldung konfiguriert sind.
   - Der iDRAC6 für die Kerberos Active Directory-Authentifizierung aktiviert ist.

Smart Card-Authentifizierung konfigurieren

iDRAC6 unterstützt die Zweifaktor-Authentifizierungsfunktion (TFA) durch die Aktivierung 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, wie ein Kennwort oder eine PIN.

Für die Zweifaktor-Authentifizierung ist es erforderlich, dass Benutzer ihre Identität durch die Angabe *beider* Faktoren bestätigen.

Lokale iDRAC6-Benutzer für Smart Card-Anmeldung konfigurieren

Sie können die lokalen iDRAC6-Benutzer zum Anmelden am iDRAC6 mittels Smart Card konfigurieren. Klicken Sie auf **iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Benutzer**.

Bevor sich der Benutzer jedoch mittels der Smart Card am iDRAC6 anmelden kann, müssen Sie das Smart Card-Zertifikat des Benutzers sowie das Zertifikat der vertrauenswürdigen Zertifizierungsstelle (CA) auf den iDRAC6 hochladen.

ANMERKUNG: Stellen Sie sicher, dass die Überprüfung des Zertifizierungsstellenzertifikats aktiviert ist, bevor Sie die Smart Card konfigurieren.

Smart Card-Zertifikat exportieren

Das Benutzerzertifikat kann abgerufen werden, indem Sie das Smart Card-Zertifikat mithilfe der Kartenverwaltungssoftware (CMS) von der Smart Card in eine Datei mit Base64-kodiertem Format exportieren. Die CMS ist normalerweise vom Anbieter der Smart Card erhältlich. Diese kodierte Datei muss als Benutzerzertifikat auf den iDRAC6 hochgeladen werden.
Die vertrauenswürdige Zertifizierungsstelle, welche die Smart Card-Benutzerzertifikate ausstellt, sollte auch das CA-Zertifikat in eine Datei in Base64-kodiertem Format exportieren. Laden Sie diese Datei als vertrauenswürdiges CA-Zertifikat für den Benutzer hoch. Konfigurieren Sie den Benutzer mit dem Benutzernamen, der den Benutzerprinzipalnamen (UPN) des Benutzers im Smart Card-Zertifikat bildet.

ANMERKUNG: Achten Sie beim Anmelden am iDRAC6 darauf, dass der im iDRAC6 konfigurierte Benutzername in Bezug auf Groß-/Kleinschreibung mit dem Benutzerprinzipalnamen (UPN) im Smart Card-Zertifikat übereinstimmt.

Beispiel: Wenn das Smart Card-Zertifikat an den Benutzer ausgegeben wurde, muss der Benutzername „Beispielbenutzer@Domäne.com" als „Beispielbenutzer" konfiguriert werden.

Active Directory-Benutzer für Smart Card-Anmeldung konfigurieren

Bevor Sie die Active Directory Smart Card-Anmeldung verwenden, stellen Sie sicher, dass der iDRAC6 bereits für die Active Directory-Anmeldung konfiguriert ist und das Benutzerkonto, dem die Smart Card zugeordnet wurde, für iDRAC6 Active Directory-Anmeldung aktiviert wurde.

Stellen Sie außerdem sicher, dass Sie die Einstellung für die Active Directory-Anmeldung aktiviert haben. Weitere Informationen zum Einrichten von Active Directory-Benutzern finden Sie unter „iDRAC6-Verzeichnisdienst verwenden" auf Seite 155. Sie müssen den iDRAC6 außerdem als Kerberos-Dienst aktivieren, indem Sie eine gültige *Keytab*-Datei aus der Active Directory-Root-Domäne auf den iDRAC6 hochladen.

Um die Active Directory-Benutzer so zu konfigurieren, dass sie sich mittels Smart Card am iDRAC6 anmelden müssen, muss der iDRAC6-Administrator den DNS-Server konfigurieren, das Active Directory-CA-Zertifikat auf den iDRAC6 hochladen und die Active Directory-Anmeldung aktivieren. Weitere Informationen zum Einrichten von Active Directory-Benutzern finden Sie unter „iDRAC6-Verzeichnisdienst verwenden" auf Seite 155.

Sie können das Active Directory über **iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Verzeichnisdienst→ Microsoft Active Directory** konfigurieren.

ANMERKUNG: Stellen Sie sicher, dass die Überprüfung des Zertifizierungsstellenzertifikats aktiviert ist, bevor Sie die Smart Card konfigurieren.

Smart Card unter Verwendung von iDRAC6 konfigurieren

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

1. Wechseln Sie in der iDRAC6-Webschnittstelle zu **iDRAC-Einstellungen→ Netzwerk/Sicherheit→** Register **Smart Card**.
2. Konfigurieren Sie die Einstellungen für die Smart Card-Anmeldung.

   Tabelle 8-1 enthält Informationen über die Einstellungen der Seite **Smart Card**.
3. Klicken Sie auf **Anwenden**.

Tabelle 8-1. Smart Card-Einstellungen

Einstellung	Beschreibung
Smart Card-Anmeldung konfigurieren	• **Deaktiviert** - Deaktiviert die Smart Card-Anmeldung. Bei nachfolgenden Anmeldungen über die grafische Benutzeroberfläche (GUI) wird die reguläre Anmeldungsseite angezeigt. Alle bandexternen Befehlszeilenoberflächen einschließlich Secure Shell (SSH), Telnet, Seriell- und Remote-RACADM behalten ihren Zustand. • **Aktiviert** – Aktiviert die Smart Card-Anmeldung. Melden Sie sich nach Übernahme der Änderungen ab, legen Sie die Smart Card ein, und klicken Sie dann auf **Anmeldung**, um Ihre Smart Card-PIN einzugeben. Durch die Aktivierung der Smart Card-Anmeldung werden alle bandexternen CLI-Schnittstellen einschließlich SSH, Telnet, Seriell, Remote-RACADM und IPMI-über-LAN deaktiviert, da diese Dienste nur die Einzelfaktor-Authentifizierung unterstützen. • **Mit Remote-Racadm aktiviert** - Aktiviert die Smart Card-Anmeldung zusammen mit Remote-RACADM. Alle anderen bandexternen CLI-Schnittstellen werden deaktiviert. Wenn Sie **Aktiviert** oder **Mit Remote-Racadm aktiviert** auswählen, werden Sie bei allen nachfolgenden Anmeldeversuchen über die webbasierte Schnittstelle zu einer Smart Card-Anmeldung aufgefordert. Es wird empfohlen, dass der iDRAC6-Administrator die Einstellung **Mit Remote-Racadm aktivieren** nur dazu verwendet, um zur Ausführung von Skripts unter Verwendung der Remote-RACADM-Befehle auf die webbasierte iDRAC6-Schnittstelle zuzugreifen. Wenn es für einen Administrator nicht erforderlich ist, Remote-RACADM zu verwenden, wird empfohlen, die Einstellung **Aktiviert** für die Smart Card-Anmeldung zu verwenden. Stellen Sie vor Aktivierung der Smart Card-Anmeldung sicher, dass die Konfiguration des lokalen iDRAC6-Benutzers und/oder die Konfiguration des Active Directory abgeschlossen wurden. **ANMERKUNG:** Für die Smart Card-Anmeldung ist die Konfiguration der lokalen iDRAC6-Benutzer mit den entsprechenden Zertifikaten erforderlich. Wenn die Smart Card-Anmeldung zur Anmeldung eines Microsoft Active Directory-Benutzers verwendet wird, ist sicherzustellen, dass das Active Directory-Benutzerzertifikat für diesen Benutzer konfiguriert wird. Das Benutzerzertifikat kann auf der Seite **Benutzer→ Benutzerhauptmenü** konfiguriert werden.

Tabelle 8-1. Smart Card-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
CRL-Prüfung für Smart Card-Anmeldung aktivieren	Diese Prüfung ist nur für lokale Smart Card-Benutzer verfügbar. Wählen Sie diese Option aus, wenn der iDRAC6 die Zertifikatsperrliste (CRL) auf Widerrufung des Smart Card-Zertifikats des Benutzers prüfen soll. Das iDRAC-Zertifikat des Benutzers, das vom CRL-Verteilungsserver (Certificate Revocation List, Zertifikatsperrliste) heruntergeladen wird, wird in der CRL auf Widerrufung überprüft. Die CRL-Verteilungsserver werden in den Smart Card-Zertifikaten der Benutzer aufgeführt. Damit die CRL-Funktion funktioniert, muss der iDRAC6 über eine gültige DNS-IP-Adresse verfügen, die als Teil der Netzwerkkonfiguration konfiguriert ist. Sie können die DNS-IP-Adresse in iDRAC6 unter **iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Netzwerk** konfigurieren. Der Benutzer wird nicht in der Lage sein, sich anzumelden, wenn eine der folgenden Bedingungen erfüllt ist: • Das Benutzerzertifikat wird in der CRL-Datei als widerrufen aufgeführt. • Der iDRAC6 ist nicht in der Lage, mit dem CRL-Verteilungsserver zu kommunizieren. • Der iDRAC6 ist nicht in der Lage, die CRL herunterzuladen. **ANMERKUNG:** Damit diese Prüfung erfolgreich ausgeführt werden kann, müssen Sie die IP-Adresse des DNS-Servers auf der Seite Netzwerk/Sicherheit→ Netzwerk korrekt konfigurieren.

Anmeldung am iDRAC6 über die Smart Card

Die iDRAC6-Webschnittstelle zeigt die Smart Card-Anmeldeseite für alle Benutzer an, die zur Verwendung der Smart Card konfiguriert wurden.

ANMERKUNG: Stellen Sie vor der Aktivierung der Smart Card-Anmeldung für den Benutzer sicher, dass die Konfiguration des lokalen iDRAC6-Benutzers und/oder die Konfiguration des Active Directory abgeschlossen wurden.

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

1 Greifen Sie über https auf die iDRAC6-Website zu.

`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-Anmeldeseite wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

2 Legen Sie die Smart Card in das Laufwerk ein und klicken Sie auf **Anmeldung**.

Der iDRAC6 fordert Sie zur Eingabe der Smart Card-PIN auf.

3 Geben Sie die Smart Card-PIN für lokale Smart Card-Benutzer ein. Wenn der Benutzer nicht lokal erstellt wurde, fordert der iDRAC6 Sie zur Eingabe des Kennworts für das Active Directory-Benutzerkonto auf.

ANMERKUNG: Wenn Sie ein Active Directory-Benutzer sind, für den die Option **CRL-Prüfung für Smart Card-Anmeldung aktivieren** ausgewählt wurde, versucht der iDRAC6, die CRL herunterzuladen, und sucht in der CRL nach dem Benutzerzertifikat. Die Anmeldung durch das Active Directory schlägt fehl, wenn das Zertifikat als widerrufen aufgeführt ist, oder wenn die CRL aus einem bestimmten Grund nicht heruntergeladen werden kann.

Sie werden am iDRAC6 angemeldet.

Anmeldung am iDRAC6 unter Verwendung der Active Directory-Smart Card-Authentifizierung

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 address>:<port number>`, wobei *IP address* für die IP-Adresse des iDRAC6 und *port number* für die HTTPS-Schnittstellennummer steht.

Die iDRAC6-Anmeldeseite wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

2 Legen Sie die Smart Card ein und klicken Sie auf **Anmeldung**.

Das PIN-Popup-Dialogfeld wird angezeigt.

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

Sie werden über Ihre in Active Directory festgelegten Anmeldeinformationen beim iDRAC6 angemeldet.

Fehler bei der Smart-Card-Anmeldung am iDRAC6 beheben

Wenden Sie die folgenden Tipps an, die beim Debuggen einer Smart Card behilflich sein können, auf die nicht zugegriffen werden kann:

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 lokalen iDRAC6 nicht möglich.

Wenn ein lokaler iDRAC6-Benutzer nicht in der Lage ist, sich anzumelden, überprüfen Sie, ob der Benutzername und die auf den iDRAC6 hochgeladenen Benutzerzertifikate abgelaufen sind. Die iDRAC6-Ablaufverfolgungsprotokolle enthalten eventuell wichtige Protokollmeldungen, die sich auf die Fehler beziehen. Hierbei ist jedoch zu beachten, dass Fehlermeldungen aus Sicherheitsgründen manchmal absichtlich unklar formuliert sind.

Anmeldung am iDRAC6 als Active Directory-Benutzer nicht möglich.

- Wenn Sie sich als Active Directory-Benutzer nicht am iDRAC6 anmelden können, versuchen Sie sich anzumelden, ohne die Smart Card-Anmeldung zu aktivieren. Wenn Sie die CRL-Prüfung aktiviert haben, versuchen Sie die Active Directory-Anmeldung ohne Aktivierung der CRL-Prüfung. Das iDRAC6-Ablaufverfolgungsprotokoll sollte im Falle eines CRL-Fehlers wichtige Meldungen enthalten.
- Sie haben auch die Möglichkeit, die Smart Card-Anmeldung unter Verwendung des folgenden Befehls über den lokalen racadm zu deaktivieren: `racadm config -g cfgSmartCard -o cfgSmartCardLogonEnable 0`
- Bei 64–Bit-Windows-Plattformen wird das iDRAC6-Authentifizierungs-Active–X-Plugin nicht installiert, wenn eine 64-Bit-Version des Microsoft Visual C++ 2005 Redistributable Package bereitgestellt wird. Stellen Sie zum ordnungsgemäßen Installieren und Ausführen des Active–X-Plugin die 32–Bit-Version des Microsoft Visual C++ 2005 SP1 Redistributable Package (x86) bereit. Dieses Paket ist erforderlich, um die Sitzung der virtuellen Konsole auf einem Internet Explorer-Browser zu starten.
- 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-Plugin konnte nicht geladen werden. Überprüfen Sie bitte Ihre IE-Einstellungen, oder Sie haben möglicherweise ungenügende Berechtigungen zur Verwendung des Smart Card-Plugin.“) eingeblendet wird, installieren Sie bitte das Microsoft Visual C++ 2005 SP1 Redistributable Package (x86). 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-Plugin geladen wird. Weitere Informationen finden Sie unter Tabelle 8-2.

Tabelle 8-2. 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 auf dem Domänen-Controller-Server nicht mehr als 5 Minuten voneinander abweichen. Sie können die **RAC-Zeit** auf der Seite **System→ iDRAC-Einstellungen→ Eigenschaften→** Seite **iDRAC-Informationen** nachprüfen und die Domänen-Controller-Zeit können Sie nachprüfen, indem Sie mit der rechten Maustaste in der unteren rechten Ecke des Bildschirms auf die Uhrzeit 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-Zeitzonenunterschied, um die iDRAC6-Zeit zu synchronisieren (über 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 „360“ in den oben aufgeführten Befehl für die Abweichung eingeben müssen. Sie können auch *cfgRacTuneDaylightoffset* verwenden, um die Sommerzeitdifferenz zu berücksichtigen. Hierdurch können Sie vermeiden, jedes Jahr zu diesen beiden Anlässen die Zeit umstellen zu müssen, wenn die Zeitumstellung vorgenommen wird, oder berücksichtigen Sie sie bei der Differenz des oben aufgeführten Beispiels einfach, indem Sie „300“ wählen.

Häufig gestellte Fragen zur SSO

Die SSO-Anmeldung schlägt auf Windows Server 2008 R2 x64 fehl. Was muss ich tun, damit SSO mit Windows Server 2008 R2 x64 funktioniert?

1. Führen Sie **http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** für den Domänen-Controller und die Domänenregel aus. Konfigurieren Sie Ihre Computer zur Verwendung der DES-CBC-MD5-Cipher-Suite. Diese Einstellungen haben möglicherweise Einfluss auf die Kompatibilität mit Client-Computern oder -Diensten und Anwendungen in Ihrer Umgebung. Die Regeleinstellung **Für Kerberos zulässige Verschlüsselungstypen konfigurieren** ist unter **Computer Configuration\Security Settings\Local Policies\Security Options** gespeichert.
2. Die Domänen-Clients müssen über das aktualisierte GPO verfügen. Geben Sie in der Befehlszeile den Befehl `gpupdate /force` ein und löschen Sie die alte Keytab mit `klist purge` cmd.
3. Sobald das GPO aktualisiert wurde, erstellen Sie die neue Keytab.
4. Laden Sie die Keytab zu iDRAC6 hoch.

Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Die SSO-Anmeldung schlägt bei AD-Benutzern auf Windows 7 und Windows Server 2008 R2 fehl. Was muss ich tun, um dieses Problem zu beheben?

Sie müssen die Verschlüsselungstypen für Windows 7 und Windows Server 2008 R2 aktivieren. So aktivieren Sie die Verschlüsselungstypen:

1. Melden Sie sich als Administrator oder als Benutzer mit Administratorrechten an.
2. Wechseln Sie zu **Start** und führen Sie **gpedit.msc** aus. Das Fenster **Editor für lokale Gruppenrichtlinien** wird angezeigt.
3. Navigieren Sie zu **Einstellungen des lokalen Computers→ Windows-Einstellungen→ Sicherheitseinstellungen→ Lokale Richtlinien→ Sicherheitsoptionen**.
4. Klicken Sie mit der rechten Maustaste auf **Netzwerksicherheit: Für Kerberos genehmigte Verschlüsselungstypen konfigurieren** und wählen Sie **Eigenschaften** aus.

5. Aktivieren Sie alle Optionen.
6. Klicken Sie auf **OK**. Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Führen Sie die folgenden zusätzlichen Einstellungen für das erweiterte Schema aus:

1. Navigieren Sie im Fenster **Editor für lokale Gruppenrichtlinien** zu **Einstellungen des lokalen Computers→ Windows-Einstellungen→ Sicherheitseinstellungen→ Lokale Richtlinien→ Sicherheitsoptionen**.
2. Klicken Sie mit der rechten Maustaste auf **Netzwerksicherheit: NTLM einschränken: Ausgehender NTLM-Verkehr zu Remote-Server** und wählen Sie **Eigenschaften** aus.
3. Wählen Sie **Alle zulassen** aus.
4. Klicken Sie auf **OK** und schließen Sie dann das Fenster **Editor für lokale Gruppenrichtlinien**.
5. Wechseln Sie zu **Start** und führen Sie **cmd** aus. Das **Befehlszeilen**fenster wird angezeigt.
6. Führen Sie den Befehl `gpupdate /force` aus. Die Gruppenrichtlinien werden aktualisiert. Schließen Sie das **Befehlszeilen**fenster.
7. Wechseln Sie zu **Start** und führen Sie **regedit** aus. Das Fenster **Registrierungseditor** wird angezeigt.
8. Navigieren Sie zu **HKEY_LOCAL_MACHINE→ System→ CurrentControlSet→ Control→ LSA**.
9. Klicken Sie mit der rechten Maustaste in den rechten Fensterbereich und wählen Sie **Neu→ DWORD (32-Bit) Wert** aus.
10. Geben Sie dem neuen Schlüssel den Namen **SuppressExtendedProtection**.
11. Klicken Sie mit der rechten Maustaste auf **SuppressExtendedProtection** und klicken Sie dann auf **Verwalten.**
12. Geben Sie in das Feld **Wertdaten** die Zahl 1 ein und klicken Sie auf **OK**.
13. Schließen Sie das Fenster **Registrierungseditor**. Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Wenn Sie die SSO für iDRAC aktiviert haben und Internet Explorer zum Anmelden an iDRAC verwenden, schlägt die SSO fehl, und Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben. Wie kann ich dieses Problem lösen?

Stellen Sie sicher, dass die iDRAC-IP-Adresse unter **Extras→ Internetoptionen→ Sicherheit→ Vertrauenswürdige Sites** aufgelistet ist. Wenn sie nicht aufgelistet ist, schlägt die SSO fehl, und Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben. Klicken Sie auf **Abbrechen** und fahren Sie fort.

9

Virtuelle GUI-Konsole verwenden

Dieser Abschnitt enthält Informationen über die Verwendung der Funktion der virtuellen iDRAC6-Konsole.

Übersicht

Mit der Funktion der virtuellen iDRAC6-Konsole können Sie im Remote-Zugriff im graphischen Modus oder im Textmodus auf die lokale Konsole zugreifen. Unter Verwendung der virtuellen Konsole können Sie ein oder mehrere iDRAC6-aktivierte Systeme von einem einzelnen Standort aus steuern.

Es ist nicht notwendig, vor jedem Server zu sitzen, um alle routinemäßigen Wartungsvorgänge auszuführen. Sie können die Server stattdessen auf Ihrem Desktop- oder Laptop-Computer von einem beliebigen Standort aus verwalten. Sie können auch die Informationen für Andere freigeben - im Remote-Zugriff und sofort.

Virtuelle Konsole verwenden

ANMERKUNG: Wenn Sie die Sitzung einer virtuellen Konsole öffnen, zeigt der verwaltete Server nicht an, dass die Konsole umgeleitet wurde.

ANMERKUNG: Wenn in einer Management Station bereits eine Sitzung der virtuellen Konsole zu einem bestimmten iDRAC6 geöffnet ist, kann über diese Management Station keine weitere Sitzung zu demselben iDRAC6 geöffnet werden.

ANMERKUNG: Von einer einzelnen Management Station aus können mehrere Sitzungen der virtuellen Konsole zu mehreren iDRAC6-Controllern gleichzeitig geöffnet werden.

Die Seite **Virtuelle Konsole** ermöglicht Ihnen, das Remote-System zu verwalten, indem Sie Tastatur, Video und Maus auf der lokalen Management Station verwenden, um die entsprechenden Geräte auf einem verwalteten Remote-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:

- Es können maximal vier gleichzeitige Sitzungen einer virtuellen Konsole unterstützt werden. Alle Sitzungen zeigen dieselbe verwaltete Serverkonsole gleichzeitig an.
- Ab Version 1.5 sind mehrere Sitzungen zu mehreren Remote-Servern über denselben Client möglich, basierend auf der Reihenfolge, in der sie geöffnet werden. Wenn eine Sitzung der virtuellen Konsole, bei der das Java-Plugin verwendet wird, geöffnet ist, können Sie unter Verwendung des ActiveX-Plugins eine weitere Sitzung der virtuellen Konsole öffnen. Wenn jedoch eine ActiveX-basierte Sitzung der virtuellen Konsole geöffnet ist, kann keine weitere Sitzung der virtuellen Konsole unter Verwendung des Java-Plugins geöffnet werden. Um eine zweite Sitzung der virtuellen Konsole öffnen zu können, müssen Sie zuerst die erste Sitzung der virtuellen Konsole schließen.
- 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.
- Die erste Sitzung einer virtuellen Konsole zum iDRAC6 ist eine Sitzung mit vollem Zugriff. Wenn ein zweiter Benutzer eine Sitzung der virtuellen Konsole anfordert, wird der erste Benutzer benachrichtigt und erhält die Option (genehmigen, ablehnen oder als Nur-Lesen zulassen), eine Freigabe-Aufforderung an den zweiten Benutzer zu senden. Der zweite Benutzer wird benachrichtigt, dass ein anderer Benutzer die Steuerung übernommen hat. Wenn der erste Benutzer auf die Freigabe-Aufforderung jedes nachfolgenden Benutzers nicht innerhalb eines Zeitraums von 30 Sekunden reagiert hat, wird der Zugriff auf die virtuelle Konsole basierend auf dem Wertsatz für das Objekt `cfgRacTuneVirtualConsoleAuthorizeMultipleSessions` gewährt. Dieses Objekt ist unabhängig vom Plugin-Typ (ActiveX oder Java), der zur Verwendung in der zweiten/dritten/vierten Sitzung festgelegt wird. Weitere Informationen zu diesem Objekt finden Sie im *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

  ANMERKUNG: Diese Regel gilt nur für den Remote- oder Firmware-RACADM (SSH oder Telnet) und nicht für den lokalen RACADM.

Management Station konfigurieren

Führen Sie zur Verwendung der virtuellen Konsole auf der Management Station die folgenden Maßnahmen durch:

1. Installieren und konfigurieren Sie einen unterstützten Internet-Browser. Weitere Informationen finden Sie in den folgenden Abschnitten:
   - „Unterstützte Webbrowser“ auf Seite 28
   - „Konfigurieren eines unterstützten Webbrowsers“ auf Seite 44
2. Wenn Sie Firefox verwenden oder den Java Viewer mit Internet Explorer verwenden möchten, installieren Sie eine Java-Laufzeitumgebung (JRE). Wenn Sie Internet Explorer als Browser verwenden, ist für den Konsolen-Viewer bereits eine ActiveX-Steuerung bereitgestellt. Sie können den Java-Konsolen-Viewer auch mit Firefox verwenden, wenn Sie eine JRE installieren und den Konsolen-Viewer in der iDRAC6-Webschnittstelle konfigurieren, bevor Sie den Viewer starten.
3. Wenn Sie Internet Explorer (IE) verwenden, stellen Sie wie folgt sicher, dass der Browser für das Herunterladen von verschlüsselten Inhalten aktiviert ist:
   - Gehen Sie zu den Optionen oder Einstellungen von Internet Explorer und wählen Sie **Extras→ Internetoptionen→ Erweitert** aus.
   - Scrollen Sie zu **Sicherheit** und heben Sie die Markierung dieser Option auf:

     `Speichern Sie keine verschlüsselten Seiten auf das Laufwerk.`
4. Wenn Sie Internet Explorer zum Starten einer Sitzung der virtuellen Konsole mit Active-X-Plugin verwenden, müssen Sie sicherstellen, dass Sie die iDRAC6-IP oder den Host-Namen der Liste **Vertrauenswürdige Sites** hinzugefügt haben. Sie sollten außerdem die benutzerdefinierten Einstellungen auf **Mittel-niedrig** einstellen oder die Einstellungen so ändern, dass die Installation signierter Active-X-Plugins zugelassen wird. Weitere Informationen finden Sie unter„Internet Explorer-Konfigurationen für ActiveX-basierte Anwendungen der virtuellen Konsole und des virtuellen Datenträgers“ auf Seite 227.

ANMERKUNG: 64-Bit-ActiveX-Plugin wird nicht zum Starten einer Sitzung der virtuellen Konsole unter Verwendung von Internet Explorer unterstützt.

5 Es wird empfohlen, die Bildschirmauflösung auf 1280x1024 Pixel oder höher einzustellen.

ANMERKUNG: Wenn das System ein Linux-Betriebssystem ausführt, kann eine X11-Konsole auf dem lokalen Monitor u. U. nicht angezeigt werden. Drücken Sie in der virtuellen iDRAC6-Konsole <Strg><Alt><F1>, um Linux auf eine Textkonsole umzuschalten.

ANMERKUNG: Gelegentlich kann es zu folgendem Java Script-Kompilierungsfehler kommen: "`Expected: ;`". Um dieses Problem zu beheben, ändern Sie die Netzwerkeinstellungen zur Verwendung der **direkten Verbindung** in JavaWebStart: **Bearbeiten**→ **Einstellungen**→ **Allgemein**→ **Netzwerkeinstellungen** und wählen Sie **Direktverbindung** anstelle von **Browser-Einstellungen verwenden** aus.

Löschen Sie den Cache des Browsers

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

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

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 aus dem Dropdown-Menü **Anzeigen** die Option **Von Internet Explorer verwendete Add-ons** aus.

4 Löschen Sie das Add-On *Video Viewer*.

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 aus dem Dropdown-Menü **Anzeigen** die Option **Alle Add-ons** aus.

4 Wählen Sie das Add-On *Video Viewer* aus und klicken Sie auf den Link **Weitere Informationen**.

5 Wählen Sie im Fenster **Weitere Informationen Entfernen** aus.

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 bei der Eingabeaufforderung `javaws-viewer` oder `javaws-uninstall` aus.

2 Der **Java Cache-Viewer** wird angezeigt.

3 Löschen Sie die Elemente mit der Bezeichnung *Client der virtuellen iDRAC6-Konsole*.

Internet Explorer-Konfigurationen für ActiveX-basierte Anwendungen der virtuellen Konsole und des virtuellen Datenträgers

Dieser Abschnitt bietet Informationen über die Internet Explorer-Einstellungen, die zum Starten und Ausführen der ActiveX-basierten Anwendungen der virtuellen Konsole und des virtuellen Datenträgers erforderlich sind.

ANMERKUNG: Löschen Sie den Browser-Cache und führen Sie dann die Konfigurationseinstellungen des Browsers aus. Weitere Informationen finden Sie unter„Löschen Sie den Cache des Browsers“ auf Seite 226.

Allgemeine Einstellungen für Microsoft Windows-Betriebssysteme

1 Wechseln Sie in Internet Explorer zu **Extras→ Internetoptionen→ Sicherheit**.

2 Wählen Sie die Zone aus, die Sie zum Ausführen der Anwendung verwenden möchten.

3 Klicken Sie auf **Benutzerdefiniert**. Wenn Sie Internet Explorer 8 verwenden, klicken Sie auf **Stufe anpassen**. Das Fenster **Sicherheitseinstellungen** wird angezeigt.

4 Unter **ActiveX-Steuerelemente und -Plugins**:

- Wählen Sie die Option **Auffordern** für **Signierte ActiveX-Steuerelemente herunterladen** aus.
- Wählen Sie die Option **Aktivieren** oder **Auffordern** für **ActiveX-Steuerelemente und -Plugins ausführen** aus.

- Wählen Sie die Option **Aktivieren** oder **Auffordern** für **Script-ActiveX-Steuerelemente, die für das Scripting als sicher gekennzeichnet wurden** aus.
- Klicken Sie auf **OK** und dann noch einmal auf **OK**.

Zusätzliche Einstellungen für Windows Vista oder neuere Microsoft-Betriebssysteme

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

Sie können ActiveX-Anwendungen in Internet Explorer-Browsern mit dem „Schutzmodus“ auf eine der folgenden Arten starten und ausführen:

- Wechseln Sie zu **Programme→ Internet Explorer**. Klicken Sie mit der rechten Maustaste auf **iexplore.exe** und klicken Sie dann auf **Als Administrator ausführen**.
- Fügen Sie die iDRAC-IP-Adresse der Liste vertrauenswürdiger Sites hinzu. Führen Sie dazu folgende Schritte durch:

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

Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

Tabelle 9-1 listet die unterstützten Bildschirmauflösungen und entsprechenden Bildwiederholfrequenzen für die Sitzung einer virtuellen Konsole auf, die auf dem verwalteten Server ausgeführt wird.

Tabelle 9-1. 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

Virtuelle Konsole auf der iDRAC6-Webschnittstelle konfigurieren

Um die virtuelle Konsole auf der iDRAC6-Webschnittstelle zu konfigurieren, führen Sie folgende Schritte aus:

1. Klicken Sie auf **System→ Konsole/Datenträger→ Konfiguration**, um die Einstellungen der virtuellen iDRAC6-Konsole zu konfigurieren.
2. Konfigurieren Sie die Eigenschaften der virtuellen Konsole. Tabelle 9-2 beschreibt die Eigenschaften der virtuellen Konsole.
3. Wenn Sie fertig sind, klicken Sie auf **Anwenden**, um die neuen Einstellungen zu speichern.

Tabelle 9-2. Konfigurationseigenschaften der virtuellen Konsole

Eigenschaft	Beschreibung
Enabled (Aktiviert)	Klicken Sie, um die virtuelle Konsole zu aktivieren oder zu deaktivieren. Wenn diese Option markiert ist, zeigt dies an, dass die virtuelle Konsole aktiviert ist. Die Standardoption ist **Aktiviert**. **ANMERKUNG:** Das Aktivieren oder Löschen der Option **Aktiviert** nach dem Start der virtuellen Konsole kann zur Unterbrechung aller vorhandenen Sitzungen der virtuellen Konsole führen.

Tabelle 9-2. Konfigurationseigenschaften der virtuellen Konsole *(fortgesetzt)*

Eigenschaft	Beschreibung
Max. Sitzungen	Wählen Sie die maximale Anzahl von zulässigen Sitzungen der virtuellen Konsole aus: 1 bis 4. Die Standardeinstellung ist **2**.
Aktive Sitzungen	Zeigt die Anzahl der Sitzungen aktiver Konsolen an. Dieses Feld ist schreibgeschützt.
Remote-Präsenz-Anschluss	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.** **ANMERKUNG:** Das Ändern des Werts **Remote-Präsenz-Anschluss** nach dem Start der virtuellen Konsole kann zur Unterbrechung aller vorhandenen Sitzungen der virtuellen Konsole führen.
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. **ANMERKUNG:** Das Aktivieren oder Deaktivieren der Option **Videoverschlüsselung aktiviert** nach dem Start der virtuellen Konsole kann zur Unterbrechung aller vorhandenen Sitzungen der virtuellen Konsole führen.
Lokales Servervideo aktiviert	Die Markierung weist darauf hin, dass die Ausgabe an den Monitor der virtuellen iDRAC6-Konsole während der virtuellen Konsole deaktiviert wird. Hierdurch wird sichergestellt, dass die unter Verwendung der **Virtuellen Konsole** ausgeführten Tasks auf dem lokalen Monitor des verwalteten Servers nicht sichtbar sind.

Tabelle 9-2. Konfigurationseigenschaften der virtuellen Konsole *(fortgesetzt)*

Eigenschaft	Beschreibung
Plugin-Typ	Der Typ des zu konfigurierenden Plugins. • **Systemeigen** (ActiveX für Windows und Java-Plugin für Linux) – ActiveX Viewer funktioniert nur auf Internet Explorer. • **Java** - Ein Java-Viewer wird gestartet.

ANMERKUNG: Informationen zur Verwendung des virtuellen Datenträgers mit der virtuellen Konsole finden Sie unter „Virtuellen Datenträger konfigurieren und verwenden“ auf Seite 283.

Sitzung einer virtuellen Konsole öffnen

Wenn Sie eine Sitzung einer virtuellen Konsole öffnen, startet die Dell Virtual Console Viewer-Anwendung, und der Desktop des Remote-Systems wird im Viewer eingeblendet. Unter Verwendung der Virtual Console Viewer-Anwendung können die Maus- und Tastaturfunktionen des Remote-Systems von der lokalen Management Station aus gesteuert werden.

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→ Konsole/Datenträger→ Virtuelle Konsole und Virtueller Datenträger**.
2. Verwenden Sie die Informationen in Tabelle 9-3, um sicherzustellen, dass eine Sitzung einer virtuellen Konsole verfügbar ist.

   Falls Sie einige der angezeigten Eigenschaftswerte neu konfigurieren möchten, finden Sie entsprechende Informationen unter „Virtuelle Konsole auf der iDRAC6-Webschnittstelle konfigurieren“ auf Seite 229.

Tabelle 9-3. Virtuelle Konsole

Eigenschaft	Beschreibung
Virtuelle Konsole aktiviert	Ja/Nein (markiert\unmarkiert)
Videoverschlüsselung aktiviert	Ja/Nein (markiert\unmarkiert)
Max. Sitzungen	Zeigt die maximale Anzahl unterstützter Sitzungen der virtuellen Konsole an.
Aktive Sitzungen	Zeigt die aktuelle Anzahl aktiver Sitzungen der virtuellen Konsole an.
Lokales Servervideo aktiviert	Ja = Aktiviert; Nein = Deaktiviert.
Remote-Präsenz-Anschluss	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.
Plugin-Typ	Zeigt den Typ des auf der Seite **Konfiguration** ausgewählten Plugins an. **ANMERKUNG:** Auf 64–Bit-Windows-Plattformen wird das iDRAC6-Authentifizierungs-Active–X-Plugin nicht korrekt installiert, wenn eine 64-Bit-Version des Microsoft Visual C++ 2005 Redistributable Package bereitgestellt ist. Stellen Sie zum ordnungsgemäßen Installieren und Ausführen des Active–X-Plugin die 32–Bit-Version des Microsoft Visual C++ 2005 SP1 Redistributable Package (x86) bereit. Dieses Paket ist erforderlich, um die Sitzung der virtuellen Konsole auf Internet Explorer zu starten.

ANMERKUNG: Informationen zur Verwendung des virtuellen Datenträgers mit der virtuellen Konsole finden Sie unter „Virtuellen Datenträger konfigurieren und verwenden“ auf Seite 283.

3 Wenn eine Sitzung der virtuellen Konsole verfügbar ist, klicken Sie auf der Seite **Virtuelle Konsole und Virtueller Datenträger** 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 diese Dialogfelder innerhalb von drei Minuten 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 der Viewer-Anwendung der virtuellen iDRAC6-Konsole angezeigt.

4 Zwei Mauszeiger erscheinen im Viewer-Fenster: einer für das Remote-System und einer für das lokale System. Sie können im Menü der virtuellen iDRAC6-Konsole unter **Extras** die Option **Einzel-Cursor** auswählen, um auf einen Einzel-Cursor umschalten.

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 Image der virtuellen Konsole ist nur dann verfügbar, wenn Sie die virtuelle Konsole aktiviert haben und wenn die iDRAC6 Enterprise-Karte vorhanden ist.

Tabelle 9-4 enthält Informationen über die verfügbaren Optionen.

Tabelle 9-4. Vorschau der virtuellen Konsole – Optionen

Option	Beschreibung
Starten	Klicken Sie auf diesen Link, 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. Dieser Link wird nicht angezeigt, wenn Sie keine Berechtigungen für die virtuelle Konsole besitzen oder wenn sowohl die virtuelle Konsole als auch der virtuelle Datenträger deaktiviert sind.
Einstellungen	Klicken Sie auf diesen Link, um die Konfigurationseinstellungen der virtuellen Konsole auf der Seite **Konsolen-/ Datenträgerkonfiguration** anzuzeigen oder zu bearbeiten. **ANMERKUNG:** Sie müssen über die Berechtigung zum Konfigurieren von iDRAC verfügen, um die Konfigurationseinstellungen der virtuellen Konsole bearbeiten zu können.
Refresh (Aktualisieren)	Klicken Sie auf diesen Link, um das angezeigte Image der virtuellen Konsole zu aktualisieren.

Virtuelle iDRAC6-Konsole verwenden (Video Viewer)

Die virtuelle iDRAC6-Konsole (Video Viewer) bietet eine Benutzerschnittstelle zwischen der Management Station und dem verwalteten Server, die Ihnen ermöglicht, den Desktop des verwalteten Servers zu sehen und dessen Maus- und Tastaturfunktionen von Ihrer Management Station aus zu steuern. Wenn Sie eine Verbindung zum Remote-System herstellen, wird die virtuelle iDRAC6-Konsole in einem separaten Fenster gestartet.

ANMERKUNG: Sie müssen über Administratorrechte verfügen, um eine virtuelle iDRAC6-Konsole (Video Viewer) starten zu können.

ANMERKUNG: Wird der Remote-Server ausgeschaltet, wird die Meldung Kein Signal angezeigt.

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>, Benutzer: <Benutzername>, <fps>
```

Die virtuelle iDRAC6-Konsole bietet die Möglichkeit verschiedener Steuerungseinstellungen, z. B. Maussynchronisierung, Snapshots, Tastaturmakros und Zugriff auf virtuelle Datenträger. Um weitere Informationen zu diesen Funktionen einzusehen, klicken Sie auf **System→ Konsole/Datenträger** und dann auf der GUI-Seite **Virtuelle Konsole und Virtueller Datenträger** auf **Hilfe**.

Wenn Sie eine Sitzung der virtuellen Konsole starten und die virtuelle iDRAC6-Konsole angezeigt wird, ist es eventuell notwendig, die Mauszeiger zu synchronisieren.

Tabelle 9-5 beschreibt die Menüoptionen, die im Viewer zum Gebrauch verfügbar sind.

Tabelle 9-5. Auswahlmöglichkeiten auf der Viewer-Menüleiste

Menüelement	Element	Beschreibung
„Reißzwecken“-Symbol	–	Klicken Sie auf das „Reißzwecken“-Symbol, um die Menüleiste der virtuellen iDRAC6-Konsole zu sperren. Hierdurch wird verhindert, dass die Symbolleiste automatisch ausgeblendet wird. **ANMERKUNG:** Dies gilt nur für den Active-X Viewer und nicht für das Java-Plugin.
Virtueller Datenträger	**Virtuellen Datenträger starten**	Die **Sitzung des virtuellen Datenträgers** wird angezeigt und führt im Hauptfenster die Geräte auf, die zur Zuordnung bereitstehen. Um ein ISO- oder IMG-Image zu virtualisieren, klicken Sie auf **Hinzufügen** und wählen die Imagedatei aus. Im Hauptfenster wird die ausgewählte Imagedatei zusammen mit der Liste der Geräte, die für die Zuweisung verfügbar sind, angezeigt. Sie können ein Gerät oder ein Image virtualisieren, indem Sie die Option in der Spalte **Zugeordnet** der Tabelle markieren. Das Gerät oder das Image wird jetzt dem Server zugeordnet. Die Zuordnung kann rückgängig gemacht werden, indem Sie die Markierung des Kontrollkästchens aufheben. Klicken Sie auf **Details**, um eine Übersicht anzuzeigen, die die virtuellen Geräte und Images auflistet. Sie zeigt auch die Lese-/Schreibaktivität für jedes Gerät oder Image an.

Tabelle 9-5. Auswahlmöglichkeiten auf der Viewer-Menüleiste *(fortgesetzt)*

Menüelement	Element	Beschreibung
Datei	In Datei erfassen	Erfasst den aktuellen Remote-Systembildschirm in einer BMP-Datei auf Windows oder in einer PNG-Datei auf Linux. Ein Dialogfeld wird angezeigt, in dem Sie die Datei zu einem angegebenen Standort speichern können. **ANMERKUNG:** Das BMP-Dateiformat auf Windows oder das PNG-Dateiformat auf Linux gelten nur für das systemeigene Plugin. Das Java-Plugin unterstützt nur die Dateiformate JPG und JPEG.
	Beenden	Wenn Sie die Konsole nicht mehr verwenden und sich abgemeldet haben (hierzu den Abmeldevorgang des Remote-Systems verwenden), wählen Sie im Menü **Datei** die Option **Beenden** aus, um das Fenster **Virtuelle iDRAC6-Konsole** zu schließen.
Ansicht	Refresh (Aktualisieren)	Aktualisiert die Ansicht der virtuellen Videokonsole. Die virtuelle Konsole fordert ein Referenz-Video-Frame vom Server an.
	Vollbildschirm/Mit Fenstern	Zeigen Sie die virtuelle Videokonsole im Vollbildschirmmodus an. Um den Vollbildschirmmodus zu beenden, klicken Sie auf **Mit Fenstern**.
	Anpassen	Ändert die Größe des Fensters der virtuellen Videokonsole zur minimalen Größe, die zum Anzeigen des Servervideos erforderlich ist. Dieses Menüelement steht nicht im Vollbildschirmmodus zur Verfügung.

Tabelle 9-5. Auswahlmöglichkeiten auf der Viewer-Menüleiste *(fortgesetzt)*

Menüelement	Element	Beschreibung
Makros	• Alt+Strg+Entf • Alt+Tab • Alt+Esc • Strg+Esc • Alt+Leertaste • Alt+Eingabe • Alt+Bindestrich • Alt+F4 • Druck • Alt+Druck • F1 • Pause (Anhalten) • Tabulatortaste • Strg+Eingabe • SysRq • Alt+LUmsch+R Umsch+Esc • Strg+Alt+ Rücktaste • Alt+F? (Wobei F? für die Tasten F1-F12 steht) • Strg+Alt+F? (Wobei F? für die Tasten F1-F12 steht)	Wenn Sie ein Makro auswählen oder die für das Makro angegebenen Schnelltaste eingeben, wird die Maßnahme auf dem Remote-System ausgeführt.

Tabelle 9-5. Auswahlmöglichkeiten auf der Viewer-Menüleiste *(fortgesetzt)*

Menüelement	Element	Beschreibung
Extras	Sitzungsoptionen	Das Fenster „Sitzungsoptionen“ bietet zusätzliche Steuerungseinstellungen für den Session Viewer. Dieses Fenster enthält die Register **Allgemein** and **Maus**. Sie können den **Modus Tastaturdurchgang** über das Register Allgemein steuern. Wählen Sie **Alle Tastenanschläge ans Ziel durchreichen** aus, um die Tastenanschläge der Management Station an das Remote-System durchzureichen. Das Maus-Register enthält zwei Abschnitte: **Einzel-Cursor** und **Mausbeschleunigung**. Die Funktion **Einzel-Cursor** wird bereitgestellt, um Mausausrichtungsprobleme auf einigen Remote-Betriebssystemen auszugleichen. Sobald der Viewer in den Modus **Einzel-Cursor** übergeht, ist der Mauszeiger im Viewer-Fenster blockiert. Drücken Sie die Terminierungstaste, um diesen Modus zu beenden. Wählen Sie diese Steuerung aus, um die Taste auszuwählen, die den Einzel-Cursor-Modus beenden wird. **Mausbeschleunigung** optimiert die Mausleistung je nach Betriebssystem.
	Einzel-Cursor	Ermöglicht den Einzel-Cursor-Modus im Viewer. In diesem Modus ist der Client-Cursor ausgeblendet, so dass nur der Server-Cursor sichtbar ist. Der Client-Cursor ist ebenso im Viewer-Frame blockiert. Der Benutzer wird nicht in der Lage sein, den Cursor außerhalb des Viewer-Fensters zu verwenden, bis er die **Terminierungstaste** drückt, wie im Register **Sitzungsoptionen - Maus** angegeben.
	Stats (Statistik)	Diese Menüoption startet einen Dialog, der Leistungsstatistiken für den Viewer anzeigt. Die angezeigten Werte sind: • Frame-Rate • Bandbreite • Komprimierung • Paketrate

Tabelle 9-5. Auswahlmöglichkeiten auf der Viewer-Menüleiste *(fortgesetzt)*

Menüelement	Element	Beschreibung
Strom	System EINschalten	Schaltet das System ein.
	System AUSschalten	Schaltet das System aus.
	Ordentliches Herunterfahren	Fährt das System herunter. **ANMERKUNG:** Stellen Sie sicher, dass die Option zum Herunterfahren für das Betriebssystem konfiguriert ist, bevor Sie unter Verwendung dieser Option das System ordentlich herunterfahren. Wenn Sie diese Option verwenden, ohne sie auf dem Betriebssystem zu konfigurieren, startet es das verwaltete System neu anstatt den Vorgang zum Herunterfahren auszuführen.
	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.
Hilfe	Inhalt und Index	Bietet Anleitungen dazu, wie die Onlinehilfe anzuwenden ist.
	Informationen über die virtuelle iDRAC6-Konsole	Zeigt die Version der **virtuellen iDRAC6-Konsole** an.

Lokales Server-Video deaktivieren oder aktivieren

Sie können den iDRAC6 so konfigurieren, dass Verbindungen der virtuellen iDRAC6-Konsole über die iDRAC6-Webschnittstelle nicht zulässig sind.

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 **Konfiguration der virtuellen Konsole** auf `1` neu konfigurieren.

ANMERKUNG: Beim Deaktivieren (Ausschalten) des lokalen Videos auf dem Server sind der Monitor, die Tastatur und die Maus, die an die virtuelle iDRAC6-Konsole angeschlossen sind, weiterhin aktiviert.

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.
2. Klicken Sie auf **System→ Konsole/Datenträger→ Konfiguration**.
3. Um das lokale Video auf dem Server zu deaktivieren (auszuschalten), deaktivieren Sie das Kontrollkästchen **Lokales Servervideo aktiviert** auf der Seite **Konfiguration,** und klicken Sie dann auf **Anwenden**. Der Standardwert ist AUS.

   ANMERKUNG: Wenn das lokale Servervideo EINGESCHALTET ist, dauert es 15 Sekunden, um es AUSZUSCHALTEN.
4. Um das lokale Video auf dem Server zu aktivieren (einzuschalten), wählen Sie das Kontrollkästchen **Lokales Servervideo aktiviert** auf der Seite **Konfiguration** aus, und klicken Sie dann auf **Anwenden**.

Virtuelle Konsole und virtuellen Datenträger im Remote-Zugriff starten

Sie können die virtuelle Konsole/den virtuellen Datenträger starten, indem Sie auf einem unterstützten Browser eine einzige URL eingeben, statt diese über die iDRAC6-Web-GUI zu starten. Je nach Systemkonfiguration durchlaufen Sie entweder den manuellen Authentifizierungsprozess (Anmeldeseite) oder werden automatisch an den Viewer der virtuellen Konsole/des virtuellen Datenträgers weitergeleitet.

Wenn SSO bereits auf dem System konfiguriert ist, können Sie mit dem URL-Format die virtuelle Konsole/den virtuellen Datenträger nicht starten.

Sie können die virtuelle Konsole über ein lokal in iDRAC6, LDAP oder Active Directory erstelltes Benutzerkonto starten.

ANMERKUNG: Internet Explorer unterstützt lokale Anmeldungen, Active Directory (AD)- und Smart Card (SC)-Anmeldungen sowie Einzelanmeldungen (SSO). Firefox unterstützt nur lokale, AD- und SSO-Anmeldungen auf Windows-basierten Betriebssystemen. SC-Anmeldungen werden von Firefox nicht unterstützt.

Konsole über das URL-Format starten

Wenn Sie `link<IP>/console` im Browser eingeben, melden Sie sich über das normale manuelle Anmeldeverfahren, je nach Anmeldekonfiguration, an. Wenn die Anmeldung erfolgreich verläuft, wird die Ansicht der virtuellen Konsole/des virtuellen Datenträgers gestartet. Anderenfalls werden Sie auf die iDRAC6-GUI-Startseite umgeleitet.

Die iDRAC-Web-GUI-Sitzung wird im Hintergrund auf der vKVM-Seite angezeigt.

Sie können immer nur eine Sitzung der virtuellen Konsole gleichzeitig starten.

Wenn Sie über Leserechte verfügen, verwenden Sie das URL-Format, um nur die Seite Virtuelle Konsole und nicht die Seite Virtueller Datenträger zu starten.

Ist die virtuelle Konsole in iDRAC6 deaktiviert, kann der Benutzer oder Administrator die Seite Virtueller Datenträger trotzdem starten, vorausgesetzt, er verfügt über ausreichende Berechtigungen.
Weitere Informationen zu ausreichenden Berechtigungen finden Sie unter „Virtuelle Konsole und virtuellen Datenträger im Remote-Zugriff starten“ auf Seite 240.

Allgemeine Fehlerszenarien

Tabelle 9-6 listet allgemeine Fehlerszenarien auf, sowie die Gründe für diese Fehler und das iDRAC6-Verhalten.

Tabelle 9-6. Fehlerszenarien

Fehlerszenarien	Ursache	Funktionsweise
Anmeldung ist fehlgeschlagen	Sie haben entweder einen unzulässigen Benutzernamen oder ein falsches Kennwort eingegeben.	Gleiches Verhalten, wenn *https://<IP>* festgelegt ist und die Anmeldung fehlschlägt.
iDRAC6-Enterprise-Karte nicht vorhanden	Die iDRAC6-Enterprise-Karte ist nicht vorhanden. Die Funktion Virtuelle Konsole/Virtueller Datenträger ist nicht verfügbar.	Der Viewer der virtuellen iDRAC6-Konsole wird nicht gestartet. Leitet zur iDRAC6-GUI-Startseite um.

Tabelle 9-6. Fehlerszenarien *(fortgesetzt)*

Fehlerszenarien	Ursache	Funktionsweise
Unzureichende Berechtigungen	Sie haben keine Berechtigung für Virtuelle Konsole und Virtueller Datenträger.	Der Viewer der virtuellen iDRAC6-Konsole wurde nicht gestartet und Sie werden zur GUI-Seite der Konsolen-/ Datenträgerkonfiguration umgeleitet.
Virtuelle Konsole deaktiviert	Die virtuelle Konsole ist auf Ihrem System deaktiviert.	Der Viewer der virtuellen iDRAC6-Konsole wurde nicht gestartet und Sie werden zur GUI-Seite der Konsolen-/ Datenträgerkonfiguration umgeleitet.
Unbekannte URL-Parameter festgestellt	Die von Ihnen eingegebene URL enthält undefinierte Parameter.	Die Nachricht „Seite nicht gefunden (404)“ wird angezeigt.

Häufig gestellte Fragen zur virtuellen Konsole

Tabelle 9-7 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 9-7. 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 9-7. 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 Anforderung zum **Einschalten** des lokalen Videos erhält, wird das Video sofort eingeschaltet.
Kann der lokale Benutzer das Video auch ausschalten?	Wenn die lokale Konsole deaktiviert ist, kann der lokale Benutzer das Video nicht ausschalten.
Kann der lokale Benutzer das Video auch einschalten?	Wenn die lokale Konsole deaktiviert ist, kann der lokale Benutzer das Video nicht einschalten.
Werden beim Ausschalten des lokalen Videos auch die lokale Tastatur und Maus ausgeschaltet?	Nein.
Wird durch das Ausschalten der lokalen Konsole auch das Video der Remote-Konsolensitzung ausgeschaltet?	Nein, das Ein- oder Ausschalten des lokalen Videos ist von der Remote-Konsolensitzung unabhängig.
Welche Berechtigungen sind für einen iDRAC6-Benutzer erforderlich, um das lokale Servervideo ein- oder auszuschalten?	Jeder Benutzer mit iDRAC6-Konfigurationsberechtigungen kann die lokale Konsole ein- oder ausschalten.
Wie kann ich den aktuellen Status des lokalen Servervideos abrufen?	Der Status wird auf der Seite **Konfiguration der virtuellen Konsole** der iDRAC6-Webschnittstelle angezeigt. Der RACADM-CLI-Befehl `racadm getconfig -g cfgRacTuning` zeigt den Status im Objekt **cfgRacTuneLocalServerVideo** an.

Tabelle 9-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
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. Versuchen Sie, die Bildlaufleisten auch beim Client der virtuellen iDRAC6-Konsole zu verwenden.
Das Konsolenfenster wird nicht richtig dargestellt.	Für den Konsolen-Viewer auf Linux ist ein UTF-8-Zeichensatz erforderlich. Überprüfen Sie Ihren lokalen Zeichensatz und setzen Sie diesen zurück, wenn notwendig.
Warum kann die Maus unter der Linux-Textkonsole nicht synchronisiert werden (entweder in Dell Unified Server Configurator (USC), Dell Lifecycle Controller 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.
Ich habe immer noch Probleme mit der Maussynchronisierung.	Stellen Sie sicher, dass vor dem Beginn einer Sitzung der virtuellen Konsole die richtige Maus für das Betriebssystem ausgewählt ist. Stellen Sie sicher, dass im Menü der virtuellen iDRAC6-Konsole unter **Extras** die Option **Einzel-Cursor** auf dem Client der virtuellen iDRAC6-Konsole ausgewählt ist. Der Standard ist der Doppel-Cursor-Modus.

Tabelle 9-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
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.
Warum zeigt die Num-Tasten-Anzeige auf meiner Management Station nicht den Status der Num-Taste auf dem Remote-Server an?	Bei Zugriff über den iDRAC6 stimmt die Num-Tasten-Anzeige 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 beide Kontrolle über das System.

Tabelle 9-7. Virtuelle Konsole verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Welche Bandbreite benötige ich, um eine Sitzung der virtuellen Konsole auszuführen?	Zum Erzielen einer guten Leistung wird eine Verbindungsgeschwindigkeit 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.
Warum wird die Meldung **Kein Signal** im Video Viewer der virtuellen iDRAC6-Konsole angezeigt?	Sie sehen diese Meldung möglicherweise, da das Plugin der virtuellen iDRAC6-Konsole das Desktop-Video des Remote-Servers nicht empfängt. Dieses Verhalten kann auftreten, wenn der Remote-Server ausgeschaltet wird. Manchmal wird diese Meldung auf Grund einer Empfangsfehlfunktion des Remote-Server-Desktop-Videos angezeigt.
Warum wird die Meldung **Außerhalb des Bereichs** im Video Viewer der virtuellen iDRAC6-Konsole angezeigt?	Diese Meldung wird möglicherweise angezeigt, weil sich ein Parameter, der für die Videoerfassung erforderlich ist, außerhalb des Bereichs befindet, für den der iDRAC6 das Video erfassen kann. Wenn Parameter wie Auflösung oder Bildwiederholfrequenz zu hoch sind, kann dieser Zustand verursacht werden. Normalerweise wird der Maximalbereich der Parameter durch physische Begrenzungen wie Videospeichergröße oder Bandbreite bestimmt.

10

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 über WS-MAN verfügbaren Daten werden von der iDRAC6-Instrumentationsschnittstelle bereitgestellt und auf die folgenden DMTF-Profile und Dell-Erweiterungsprofile aufgeteilt:

Unterstützte CIM-Profile

Tabelle 10-1. Standard-DMTF

Standard-DMTF
1 Basisserver Bestimmt CIM-Klassen zum Darstellen des Hostservers.
2 Serviceprozessor: Enthält die Definition von CIM-Klassen zur Darstellung des iDRAC6.
3 Physische Anlagen: Bestimmt CIM-Klassen zum Darstellen der physischen Aspekte der verwalteten Elemente. iDRAC6 verwendet dieses Profil, um die FRU-Informationen des Host-Servers darzustellen.

Tabelle 10-1. Standard-DMTF *(fortgesetzt)*

Standard-DMTF
4 SM-CLP-Administrator-Domäne Bestimmt CIM-Klassen zum Darstellen der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für die Implementierung von CLP.
5 Stromzustandsverwaltung Bestimmt CIM-Klassen für Stromsteuerungsvorgänge. iDRAC6 verwendet dieses Profil für die Stromsteuerungsvorgänge des Hostservers.
6 Netzteil (Version 1.1) Definiert CIM-Klassen zur Darstellung von Netzteilen. iDRAC6 verwendet dieses Profil zur Darstellung der Netzteile des Hostservers, um den Stromverbrauch, z. B. Wasserzeichen eines hohen und niedrigen Stromverbrauchs, zu beschreiben.
7 CLP-Dienst Bestimmt CIM-Klassen zum Darstellen der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für die Implementierung von CLP.
8 IP-Schnittstelle
9 DHCP-Client
10 DNS-Client
11 Ethernet-Anschluss Die zuvor erwähnten Profile bestimmen CIM-Klassen zur Darstellung von Netzwerkstapeln. iDRAC6 verwendet diese Profile, um die Konfiguration des iDRAC6-NIC darzustellen.
12 Datensatzprotokoll Bestimmt CIM-Klassen zum Darstellen unterschiedlicher Protokolltypen. iDRAC6 verwendet dieses Profil, um das Systemereignisprotokoll (SEL) und das iDRAC6-RAC-Protokoll darzustellen.
13 Software-Bestandsaufnahme Definiert CIM-Klassen zur Bestandsaufnahme von installierter oder verfügbarer Software. iDRAC6 verwendet dieses Profil zur Bestandsaufnahme derzeit installierter iDRAC6-Firmwareversionen über das TFTP-Protokoll.
14 Rollenbasierte Authentifizierung Bestimmt CIM-Klassen zum Darstellen von Rollen. iDRAC6 verwendet dieses Profil zum Konfigurieren von iDRAC6-Kontoberechtigungen.

Tabelle 10-1. Standard-DMTF *(fortgesetzt)*

Standard-DMTF
15 Software-Aktualisierung Definiert CIM-Klassen zur Bestandsaufnahme von verfügbaren Software-Aktualisierungen. iDRAC6 verwendet dieses Profil zur Bestandsaufnahme von Firmware-Aktualisierungen über das TFTP-Protokoll.
16 SMASH-Sammlung Bestimmt CIM-Klassen zum Darstellen der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für die Implementierung von CLP.
17 Profilregistrierung Bestimmt CIM-Klassen zur Ankündigung der Profil-Implementierungen. iDRAC6 verwendet dieses Profil, um die eigenen implementierten Profile, wie in dieser Tabelle dargestellt, anzukündigen.
18 Basismetrik Definiert CIM-Klassen zur Darstellung der Metrik. iDRAC6 verwendet dieses Profil zur Darstellung der Metrik des Hostservers, um den Stromverbrauch, z. B. Wasserzeichen eines hohen und niedrigen Stromverbrauchs, zu beschreiben.
19 Einfache Identitätsverwaltung Bestimmt CIM-Klassen zum Darstellen der Identitäten. iDRAC6 verwendet dieses Profil zum Konfigurieren von iDRAC6-Konten.
20 USB-Umleitung Definiert CIM-Klassen zur Darstellung der Remote-Umleitung von lokalen USB-Anschlüssen. iDRAC6 verwendet dieses Profil in Verbindung mit dem virtuellen Datenträgerprofil, um den virtuellen Datenträger zu konfigurieren.

Tabelle 10-1. Standard-DMTF *(fortgesetzt)*

Dell-Erweiterungen
1 Dell Active Directory Client Version 2.0.0 Bestimmt CIM- und Dell-Erweiterungsklassen zum Konfigurieren des iDRAC6 Active Directory-Clients und der lokalen Berechtigungen für Active Directory-Gruppen.
2 Dells virtueller Datenträger Bestimmt CIM- und Dell-Erweiterungsklassen zum Konfigurieren des virtuellen iDRAC6-Datenträgers. Erweitert das USB-Umleitungsprofil.
3 Dell Ethernet-Anschluss Definiert CIM- und Dell-Erweiterungsklassen zur Konfiguration der NIC-Seitenband-Schnittstelle für den iDRAC6-NIC. Erweitert Ethernet-Anschlussprofile.
4 Dells Energienutzungsverwaltung Definiert CIM- und Dell-Erweiterungsklassen zur Darstellung, Konfiguration und Überwachung des Strombudgets des Hostservers.
5 Dell-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.
6 Dell-Auftragssteuerung Bestimmt CIM- und Dell-Erweiterungsklassen zum Verwalten von Konfigurationsaufträgen.
7 Dell-LC-Verwaltungsprofil Bestimmt CIM- und Dell-Erweiterungsklassen für die Konfigurationsattribute des Dell Lifecycle Controllers, wie z. B. automatische Ermittlung. Dieses Profil ermöglicht außerdem die Verwaltung für die Teileersetzung, die Hauptplatinenersetzung und den Export und Import des Systemprofils, das Starten von einer Netzwerkfreigabe und die Verwaltung von Verschlüsselungszertifikaten.
8 Beständiger Dell-Speicher Bestimmt CIM- und Dell-Erweiterungsklassen für die Verwaltung der Partitionen auf der vFlash-SD-Karte von Dell-Plattformen.
9 Einfacher Dell-NIC Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der Konfiguration von NIC-Netzwerk-Controllern

Tabelle 10-1. Standard-DMTF *(fortgesetzt)*

Dell-Erweiterungen
10 Dell-BIOS- und Startverwaltungsprofil Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen von Dell-BIOS-Attributen und zum Konfigurieren der Startsequenz des Hosts.
11 Dell-RAID-Profil Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der Konfiguration des RAID-Speichers des Hosts.
12 Profil zur Dell-Stromversorgung Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der Netzteil-Bestandsinformationen des Hosts.
13 Profil der Dell-iDRAC-Karte Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der iDRAC6-Bestandsinformationen. Dieses Profil ermöglicht ferner die Darstellung und Methoden zum Konfigurieren von iDRAC-Attributen und Benutzerkonten.
14 Dell-Lüfterprofil Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der Lüfter-Bestandsinformationen des Hosts.
15 Dell-Speicherprofil Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der DIMM-Bestandsinformationen des Hosts.
16 Dell-CPU-Profil Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der CPU-Bestandsinformationen des Hosts.
17 Dell-Systeminfoprofil Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der Plattform-Bestandsinformationen des Hosts.
18 Profil des Dell-PCI-Geräts Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen der PCI-Geräte-Bestandsinformationen des Hosts.
19 Dell-Videoprofil 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 und die Digest-Authentifizierung. Webdiensteschnittstellen können durch wirksame Nutzung von Client-Infrastruktur, z. B. Windows WinRM und Powershell CLI sowie Open Source-Dienstprogramme wie WSMANCLI und Anwendungsprogrammierumgebungen wie Microsoft .NET, eingesetzt werden.

Weitere Informationen zu den Remote-Diensten von Dell Lifecycle Controller finden Sie in den folgenden Dokumenten:

- Benutzerhandbuch
- Versionshinweise
- Liste der Fehlermeldungen und Fehlerbehebungen

So können Sie auf diese Dokumente zugreifen:

1. Rufen Sie die Website **dell.com/support/manuals** auf.
2. Klicken Sie auf **Software→ Systemverwaltung→ Dell Unified Server Configurator und Lifecycle Controller**.
3. Klicken Sie auf die relevante Version, um alle Dokumente zu einer bestimmten Version anzuzeigen.

Handbücher für die Webdienstschnittstelle (Windows und Linux), Profilunterlagen, Beispielcode, Informationsberichte und andere nützliche Informationen finden Sie unter **OpenManage Systems Management→ Lifecycle Controller** auf der Website **www.delltechcenter.com**.

Weitere Informationen stehen zur Verfügung unter:

- DMTF-Website unter **www.dmtf.org/standards/profiles/**
- WS–MAN, Anmerkungen zur Version oder Infodatei.

11

iDRAC6-SM-CLP-Befehlszeilenoberfläche verwenden

Dieser Abschnitt enthält Informationen zum im iDRAC6 integrierten Serververwaltungs-Befehlszeilenprotokoll (Server Management-Command Line Protocol, SM-CLP) der verteilten Management Task Force (Distributed Management Task Force, DMTF).

ANMERKUNG: Für diesen Abschnitt wird angenommen, dass Sie mit der SMASH-Initiative (Systemverwaltungsarchitektur für Serverhardware) und den SM-CLP-Spezifikationen vertraut sind. Weitere Informationen zu diesen Spezifikationen finden Sie auf der Website der Distributed Management Task Force (DMTF) unter **www.dmtf.org**.

Das iDRAC6-SM-CLP ist ein Protokoll, das Standards für CLI-Implementierungen der Systemverwaltung bietet. Das SM-CLP ist eine Unterkomponente der DMTF SMASH-Initiative zum Rationalisieren der Serververwaltung über mehrere Plattformen. In Verbindung mit der Spezifikation für verwaltete Elementadressierung und zahlreichen Profilen zu SM-CLP-Zuordnungsspezifikationen beschreibt die SM-CLP-Spezifikation die standardisierten Verben und Ziele zum Ausführen verschiedener Verwaltungsaufgaben.

Support für iDRAC6-SM-CLP

Das SM-CLP wird von der iDRAC6-Controller-Firmware aus gehostet und unterstützt Telnet, SSH und seriell-basierte Schnittstellen. Die iDRAC6-SM-CLP-Schnittstelle basiert auf der SM-CLP-Spezifikation Version 1.0, bereitgestellt von der DMTF-Organisation. iDRAC6 SM-CLP unterstützt alle unter Tabelle 10-1 beschriebenen Profile.

Die folgenden Abschnitte enthalten eine Übersicht über die SM-CLP-Funktion, die vom iDRAC6 gehostet wird.

SM-CLP-Funktionen

Das SM-CLP fördert das Konzept von Verben und Zielen und stellt Systemverwaltungsfunktionen über die CLI bereit. Das Verb gibt den auszuführenden Vorgang an, und das Ziel bestimmt die Einheit (oder das Objekt), die den Vorgang ausführt.

Beispiel für eine SM-CLP-Befehlszeilensyntax:

```
<Verb> [<Optionen>] [<Ziel>] [<Eigenschaften>]
```

Während einer typischen SM-CLP-Sitzung können Sie Vorgänge mittels der in Tabelle 11-1 aufgeführten Verben ausführen.

Tabelle 11-1. Unterstützte CLI-Verben für System

Verb	Definition
CD	Navigiert durch den MAP mittels der Shell.
set	Stellt eine Eigenschaft auf einen bestimmten Wert ein.
Hilfe	Zeigt die Hilfe für ein bestimmtes Ziel an.
reset	Setzt das Ziel zurück.
Anzeigen	Zeigt die Zieleigenschaften, Verben und Unterziele an.
start	Schaltet ein Ziel ein.
stop	Fährt ein Ziel herunter.
Beenden	Beendet die SM-CLP-Shell-Sitzung.
Version	Zeigt die Versionsattribute eines Ziels an.
load	Lädt ein Binärbild von einer URL zu einer bestimmten Zieladresse.

SM-CLP verwenden

SSH (oder Telnet) zum iDRAC6 mit den richtigen Anmeldeinformationen.

Die SMCLP-Eingabeaufforderung (/admin1->) wird angezeigt.

SM-CLP-Ziele

Tabelle 11-2 enthält eine Liste von Zielen, die über das SM-CLP bereitgestellt werden, um die in Tabelle 11-1 beschriebenen Vorgänge zu unterstützen.

Tabelle 11-2. SM-CLP-Ziele

Ziel	Definitionen
admin1	admin domain
admin1/profiles1	Im iDRAC6 registrierte Profile
admin1/hdwr1	Hardware
admin1/system1	Ziel des verwalteten Systems
admin1/system1/redundancyset1	Netzteil
admin1/system1/redundancyset1/pwrsupply*	Netzteil des verwalteten Systems
admin1/system1/sensors1	Sensoren des verwalteten Systems
admin1/system1/capabilities1	SMASH-Erfassungsfunktionen des verwalteten Systems
admin1/system1/capabilities1/pwrcap1	Funktionen zur Energienutzung des verwalteten Systems
admin1/system1/capabilities1/elecap1	Zielfunktionen des verwalteten Systems
admin1/system1/logs1	Datensatzprotokoll-Erfassungsziel
admin1/system1/logs1/log1	Systemereignisprotokoll (SEL) Datensatzeintrag
admin1/system1/logs1/log1/Datensatz*	Eine einzelne SEL-Datensatzinstanz auf dem verwalteten System
admin1/system1/settings1	SMASH-Erfassungseinstellungen des verwalteten Systems
admin1/system1/settings1/pwrmaxsetting1	Einstellungen zur maximalen Stromzuteilung des verwalteten Systems
admin1/system1/settings1/pwrminsetting1	Einstellungen zur minimalen Stromzuteilung des verwalteten Systems

Tabelle 11-2. SM-CLP-Ziele *(fortgesetzt)*

Ziel	Definitionen
admin1/system1/capacities1	SMASH-Erfassung der verwalteten Systemkapazitäten
admin1/system1/consoles1	SMASH-Erfassung der verwalteten Systemkonsolen
admin1/system1/usbredirectsap1	USB-Umleitungs-SAP des virtuellen Datenträgers
admin1/system1/usbredirectsap1/remotesap1	Ziel-USB-Umleitungs-SAP des virtuellen Datenträgers
admin1/system1/sp1	Serviceprozessor
admin1/system1/sp1/timesvc1	Zeitansage des Serviceprozessors
admin1/system1/sp1/capabilities1	SMASH-Erfassung der Serviceprozessorfunktionen
admin1/system1/sp1/capabilities1/clpcap1	CLP-Dienstfunktionen
admin1/system1/sp1/capabilities1/pwrmgtcap1	Dienstfunktionen der Stromzustandsverwaltung auf dem System
admin1/system1/sp1/capabilities1/ipcap1	IP-Schnittstellenfunktionen
admin1/system1/sp1/capabilities1/dhcpcap1	DHCP-Clientfunktionen
admin1/system1/sp1/capabilities1/NetPortCfgcap1	Konfigurationsfunktionen des Netzwerkanschlusses
admin1/system1/sp1/capabilities1/usbredirectcap1	USB-Umleitungs-SAP der virtuellen Datenträgerfunktionen
admin1/system1/sp1/capabilities1/vmsapcap1	SAP-Funktionen des virtuellen Datenträgers
admin1/system1/sp1/capabilities1/swinstallsvccap1	Dienstfunktionen der Softwareinstallation
admin1/system1/sp1/capabilities1/acctmgtcap*	Dienstfunktionen der Kontoverwaltung

Tabelle 11-2. SM-CLP-Ziele *(fortgesetzt)*

Ziel	Definitionen
admin1/system1/sp1/capabilities1/adcap1	Active Directory-Funktionen
admin1/system1/sp1/capabilities1/rolemgtcap*	Lokale rollenbasierte Verwaltungsfunktionen
admin1/system1/sp1/capabilities/PwrutilmgtCap1	Energienutzung-Verwaltungsfunktionen
admin1/system1/sp1/capabilities/metriccap1	Funktionen des metrischen Dienstes
admin1/system1/sp1/capabilities1/elecap1	Funktionen der Multi-Faktor-Authentifizierung
admin1/system1/sp1/capabilities1/lanendptcap1	LAN (Ethernet-Anschluss)-Endpunkt-Funktionen
admin1/system1/sp1/logs1	Sammlung von Serviceprozessorprotokollen
admin1/system1/sp1/logs1/log1	Systemdatensatzprotokoll
admin1/system1/sp1/logs1/log1/record*	Systemprotokolleintrag
admin1/system1/sp1/settings1	Sammlung von Serviceprozessoreinstellungen
admin1/system1/sp1/settings1/clpsetting1	CLP-Dienst-Einstellungsdaten
admin1/system1/sp1/settings1/ipsettings1	IP-Schnittstellenzuweisungs-Einstellungsdaten (statisch)
admin1/system1/sp1/settings1/ipsettings1/staticipsettings1	Statische IP-Schnittstellenzuweisungs-Einstellungsdaten
admin1/system1/sp1/settings1/ipsettings1/dnssettings1	DNS-Client-Einstellungsdaten
admin1/system1/sp1/settings1/ipsettings2	IP-Schnittstellenzuweisungs-Einstellungsdaten (DHCP)
admin1/system1/sp1/settings1/ipsettings2/dhcpsettings1	DHCP-Client-Einstellungsdaten

Tabelle 11-2. SM-CLP-Ziele *(fortgesetzt)*

Ziel	Definitionen
admin1/system1/sp1/clpsvc1	CLP-Dienst-Protokolldienst
admin1/system1/sp1/clpsvc1/ clpendpt*	CLP-Dienst-Protokollendpunkt
admin1/system1/sp1/clpsvc1/ tcpendpt*	CLP-Dienst-Protokoll-TCP-Endpunkt
admin1/system1/sp1/jobq1	Auftragswarteschlange des CLP-Dienst-Protokolls
admin1/system1/sp1/jobq1/job*	CLP-Dienst-Protokollaufgabe
admin1/system1/sp1/pwrmgtsvc1	Stromzustandsverwaltungsdienst
admin1/system1/sp1/ipcfgsvc1	IP-Schnittstellenkonfigurationsdienst
admin1/system1/sp1/ipendpt1	IP-Schnittstellen-Protokollendpunkt
admin1/system1/sp1/ ipendpt1/gateway1	IP-Schnittstellen-Gateway
admin1/system1/sp1/ ipendpt1/dhcpendpt1	DHCP-Client-Protokollendpunkt
admin1/system1/sp1/ ipendpt1/dnsendpt1	DNS-Client-Protokollendpunkt
admin1/system1/sp1/ipendpt1/ dnsendpt1/dnsserver*	DNS-Clientserver
admin1/system1/sp1/ NetPortCfgsvc1	Konfigurationsdienst des Netzwerkanschlusses
admin1/system1/sp1/lanendpt1	LAN-Endpunkt
admin1/system1/sp1/ lanendpt1/enetport1	Ethernet-Anschluss
admin1/system1/sp1/VMediaSvc1	Virtueller Datenträger-Dienst
admin1/system1/sp1/ VMediaSvc1/tcpendpt1	TCP-Protokollendpunkt des virtuellen Datenträgers
admin1/system1/sp1/swid1	Softwareidentität
admin1/system1/sp1/ swinstallsvc1	Softwareinstallationsdienst

Tabelle 11-2. SM-CLP-Ziele *(fortgesetzt)*

Ziel	Definitionen
admin1/system1/sp1/ account1-16	Multi-Faktor-Authentifizierungskonto (MFA)
admin1/sysetm1/sp1/ account1-16/identity1	Identitätskonto des lokalen Benutzers
admin1/sysetm1/sp1/ account1-16/identity2	IPMI-Identitätskonto (LAN)
admin1/sysetm1/sp1/ account1-16/identity3	IPMI-Identitätskonto (seriell)
admin1/sysetm1/sp1/ account1-16/identity4	CLP-Identitätskonto
admin1/system1/sp1/acctsvc1	MFA-Kontoverwaltungsdienst
admin1/system1/sp1/acctsvc2	IPMI-Kontoverwaltungsdienst
admin1/system1/sp1/acctsvc3	CLP-Kontoverwaltungsdienst
admin1/system1/sp1/group1-5	Active Directory-Gruppe
admin1/system1/sp1/ group1-5/identity1	Active Directory-Identität
admin1/system1/sp1/ADSvc1	Active Directory-Dienst
admin1/system1/sp1/rolesvc1	Lokaler rollenbasierter Authentifizierungsdienst (RBA)
admin1/system1/sp1/rolesvc1/ Role1-16	Lokale Rolle
admin1/system1/sp1/rolesvc1/ Role1-16/privilege1	Lokale Rollenberechtigung
admin1/system1/sp1/rolesvc1/ Role17-21/	Active Directory-Rolle
admin1/system1/sp1/rolesvc1/ Role17-21/privilege1	Active Directory-Berechtigung
admin1/system1/sp1/rolesvc2	IPMI-RBA-Dienst
admin1/system1/sp1/rolesvc2/ Role1-3	IPMI-Rolle

Tabelle 11-2. SM-CLP-Ziele *(fortgesetzt)*

Ziel	Definitionen
admin1/system1/sp1/rolesvc2/ Role4	IPMI Seriell-über-LAN-Rolle (SOL)
admin1/system1/sp1/rolesvc3	CLP-RBA-Dienst
admin1/system1/sp1/rolesvc3/ Role1-3	CLP-Rolle
admin1/system1/sp1/rolesvc3/ Role1-3/privilege1	CLP-Rollenberechtigung
admin1/system1/sp1/ pwrutilmgtsvc1	Energienutzungs-Verwaltungsdienst
admin1/system1/sp1/ pwrutilmgtsvc1/pwrcurr1	Einstellungsdaten der aktuellen Stromzuweisung für den Energienutzungs-Verwaltungsdienst
admin1/system1/sp1/metricsvc1	Metrischer Dienst
/admin1/system1/sp1/metricsvc1/ cumbmd1	Kumulative Basismetrikdefinition
/admin1/system1/sp1/metricsvc1/ cumbmd1/cumbmv1	Kumulativer Basismetrikwert
/admin1/system1/sp1/metricsvc1/ cumwattamd1	Kumulative Metrikdefinition der Watt-Aggregation
/admin1/system1/sp1/metricsvc1/ cumwattamd1/cumwattamv1	Kumulativer Metrikwert der Watt-Aggregation
/admin1/system1/sp1/metricsvc1/ cumampamd1	Kumulative Metrikdefinition der Ampere-Aggregation
/admin1/system1/sp1/metricsvc1/ cumampamd1/cumampamv1	Kumulativer Metrikwert der Ampere-Aggregation
/admin1/system1/sp1/metricsvc1/ loamd1	Metrikdefinition der geringen Aggregation
/admin1/system1/sp1/metricsvc1/ loamd1/loamv*	Metrikwert der geringen Aggregation
/admin1/system1/sp1/metricsvc1/ hiamd1	Metrikdefinition der hohen Aggregation

Tabelle 11-2. SM-CLP-Ziele *(fortgesetzt)*

Ziel	Definitionen
`/admin1/system1/sp1/metricsvc1/hiamd1/hiamv*`	Metrikwert der hohen Aggregation
`/admin1/system1/sp1/metricsvc1/avgamd1`	Metrikdefinition der Durchschnittsaggregation
`/admin1/system1/sp1/metricsvc1/avgamd1/avgamv*`	Metrikwert der Durchschnittsaggregation

12

Betriebssystem mittels VMCLI bereitstellen

Das VMCLI-Dienstprogramm (Befehlszeilenoberfläche des virtuellen Datenträgers) ist eine Befehlszeilenoberfläche, welche die Funktionen des virtuellen Datenträgers über die Management Station zum iDRAC6 im Remote-System bereitstellt. Mit VMCLI und Skriptmethoden können Sie das Betriebssystem auf mehreren Remote-Systemen im Netzwerk bereitstellen.

Dieser Abschnitt bietet Informationen zum Einbinden des VMCLI-Dienstprogramms in das Unternehmensnetzwerk.

Bevor Sie beginnen

Stellen Sie vor Verwendung des VMCLI-Dienstprogramms sicher, dass die gewünschten Remote-Systeme und das Unternehmensnetzwerk den in den folgenden Abschnitten aufgeführten Anforderungen entsprechen.

Remote-System-Anforderungen

Der iDRAC6 ist auf 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 Imagedatei zu prüfen, übertragen Sie sie mithilfe der webbasierten iDRAC6-Benutzeroberfläche auf ein Testsystem und führen Sie dann einen Neustart des Systems durch.

Die folgenden Abschnitte enthalten spezifische Informationen über das Erstellen von Imagedateien für Linux- und Microsoft Windows-Systeme.

Imagedatei für Linux-Systeme erstellen

Verwenden Sie das Datenvervielfältigungs-Dienstprogramm (dd), um eine startfähige Imagedatei 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. das Windows-Betriebssystem bereitzustellen, kann die Imagedatei 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 netzwerkbasierte Standardinstallationsverfahren.
- Markieren Sie das Bereitstellungsimage als *schreibgeschützt*, um sicherzustellen, dass jedes Zielsystem dasselbe Bereitstellungsverfahren startet und ausführt.

4 Führen Sie eines der folgenden Verfahren aus:

- Integrieren Sie **IPMItool** und die Befehlszeilenoberfläche des virtuellen Datenträgers (VMCLI) in die vorhandene Betriebssystem-Bereitstellungsanwendung. Verwenden Sie das Beispielskript **vm6deploy** als Orientierungshilfe beim Verwenden des Dienstprogramms.
- Verwenden Sie das vorhandene **vm6deploy**-Skript, um das Betriebssystem bereitzustellen.

Betriebssystem bereitstellen

Verwenden Sie das VMCLI-Dienstprogramm und das im Dienstprogramm enthaltene Skript **vm6deploy**, um das Betriebssystem auf den Remote-Systemen bereitzustellen.

Prüfen Sie, bevor Sie beginnen, das Beispielskript **vm6deploy**, das im VMCLI-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 Geben Sie die iDRAC6-IPv4- oder IPv6-Adressen der Remote-Systeme an, die in der Textdatei **ip.txt** bereitgestellt werden (eine IPv4- oder IPv6-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 **vm6deploy** aus.

Geben Sie zum Ausführen des **vm6deploy**-Skripts den folgenden Befehl in die Befehlszeile ein:

```
vm6deploy -r ip.txt -u <idrac-Benutzer> -p <idrac-
Benutzerkennwort> -c {<iso9660-Abbild> | <Pfad>} -f
{<Diskettengerät> oder <Diskettenimage>}
```

wobei

- *<idrac-Benutzer>* ist der iDRAC6-Benutzername, z. B. **root**
- *<idrac-Benutzerkennwort>* ist das Kennwort für den iDRAC6-Benutzer, z. B. **calvin**
- *<iso9660-Img>* ist der Pfad zu einem ISO9660-Image der Betriebssystem-Installations-CD-ROM oder -DVD
- -f {*<Diskettengerät>*} ist der Pfad zu dem Gerät, das die Installations-CD, -DVD oder -Diskette des Betriebssystems enthält
- *<Diskettenimage>* ist der Pfad zu einem gültigen Diskettenimage

Das Skript **vm6deploy** leitet seine Befehlszeilenoptionen an das Dienstprogramm **VMCLI** weiter. Einzelheiten zu diesen Optionen finden Sie unter „Befehlszeilenoptionen“. Das Skript verarbeitet die Option **-r** auf leicht unterschiedliche Weise als die Option **vmcli -r**. Wenn das Argument der Option **-r** der Name einer vorhandenen Datei ist, liest das Skript iDRAC6-IPv4- oder IPv6-Adressen aus der festgelegten Datei und führt das Dienstprogramm **VMCLI** 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 **VMCLI** beschrieben.

VMCLI-Dienstprogramm verwenden

Das VMCLI-Dienstprogramm ist eine skriptfähige Befehlszeilenoberfläche, welche die Funktionen des virtuellen Datenträgers über die Management Station zum iDRAC6 bereitstellt.

Das VMCLI-Dienstprogramm 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
- Automatische Terminierung, wenn die Einmalstart-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 Start des VMCLI-Befehlszeilendienstprogramms die interaktive Flag-Option '-i' zu verwenden. Dies gewährleistet höhere Sicherheit, indem der Benutzername und das Kennwort privat bleiben. Auf vielen Windows- und Linux-Betriebssystemen sind der Benutzername und das Kennwort sichtbar, wenn Verfahren durch andere Benutzer untersucht werden.

Wenn das Betriebssystem Administratorberechtigungen oder eine betriebssystemspezifische Berechtigung oder Gruppenmitgliedschaft unterstützt, sind auch Administratorberechtigungen zum Ausführen des VMCLI-Befehls erforderlich.

Der Administrator des Client-Systems steuert Benutzergruppen und -berechtigungen und dadurch auch die Benutzer, die das Dienstprogramm ausführen können.

Auf Windows-Systemen müssen Sie über Hauptbenutzerberechtigungen verfügen, um das VMCLI-Dienstprogramm auszuführen.

Auf Linux-Systemen können Sie ohne Administratorberechtigungen auf das VMCLI-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 VMCLI-Gruppe hinzuzufügen oder zu bearbeiten, verwendet der Administrator den Befehl **visudo**. Benutzer ohne Administratorberechtigungen können den Befehl **sudo** als Präfix zur VMCLI-Befehlszeile (oder zum VMCLI-Skript) hinzufügen, um Zugriff auf den iDRAC6 im Remote-System zu erhalten und das Dienstprogramm auszuführen.

VMCLI-Dienstprogramm installieren

Das VMCLI-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 *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk des Systems ein und befolgen Sie die Anleitungen auf dem Bildschirm.

Die DVD *Dell Systems Management Tools and Documentation* enthält die neuesten Systems Management Software-Produkte einschließlich Speicherverwaltung, RAS-Dienst und des IPMItool-Dienstprogramms. 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 **vm6deploy**, das illustriert, wie die VMCLI- und IPMItool-Dienstprogramme zur Bereitstellung von Software an mehrere Remote-Systeme verwendet werden.

ANMERKUNG: Das vm6deploy-Skript hängt bei der Installation von den anderen Dateien ab, die im gleichen Verzeichnis vorhanden sind. Wenn Sie das Skript von einem anderen Verzeichnis aus ausführen möchten, müssen Sie alle Dateien mitkopieren. Ist das IPMItool-Dienstprogramm nicht installiert, muss zusätzlich zu den anderen Dateien auch das Dienstprogramm kopiert werden.

Befehlszeilenoptionen

Die VMCLI-Schnittstelle ist auf Windows- und Linux-Systemen identisch.

Das VMCLI-Befehlsformat sieht wie folgt aus:

`VMCLI [Parameter] [Betriebssystem_Shell-Optionen]`

Bei der Befehlszeilensyntax wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter „VMCLI-Parameter“ auf Seite 269.

Wenn das Remote-System die Befehle akzeptiert und der iDRAC6 die Verbindung genehmigt, wird der Befehl weiter ausgeführt, bis einer der folgenden Zustände eintritt:

- Die VMCLI-Verbindung wird aus einem bestimmten Grund abgebrochen.
- Der Prozess wird mit einer Betriebssystemsteuerung manuell abgebrochen. Beispiel: In Windows können Sie den Task Manager verwenden, um den Prozess abzubrechen.

VMCLI-Parameter

iDRAC6-IP-Adresse

`-r <iDRAC-IP-Adresse[:iDRAC-SSL-Anschluss]>`

Dieser Parameter gibt die iDRAC6-IPv4- oder IPv6-Adresse und den SSL-Anschluss an. Das Dienstprogramm benötigt diese Angaben zum Herstellen einer Verbindung des virtuellen Datenträgers zum Ziel-iDRAC6. Wenn Sie eine ungültige IPv4- oder IPv6-Adresse oder einen ungültigen DDNS-Namen eingeben, wird eine Fehlermeldung angezeigt und der Befehl wird abgebrochen.

<iDRAC-IP-Adresse> ist eine gültige, eindeutige IPv4- oder IPv6-Adresse oder der iDRAC6-DDNS-Name (Dynamic Domain Naming System), falls unterstützt. Wenn *<iDRAC-SSL-Anschluss>* ausgelassen wird, wird der Anschluss 443 (Standardanschluss) verwendet. Solange der iDRAC6-Standard-SSL-Anschluss nicht geändert wird, ist der optionale SSL-Anschluss nicht erforderlich.

iDRAC6-Benutzername

`-u <iDRAC-Benutzer>`

Dieser Parameter gibt den iDRAC6-Benutzernamen an, der den virtuellen Datenträger ausführt.

Der *<iDRAC-Benutzer>* 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 bricht ab.

Disketten-/Festplattengerät oder Imagedatei

`-f {<Diskettengerät> oder <Diskettenimage>}` und/oder

`-c {<CD-DVD-Gerät> oder <CD-DVD-Image>}`

wobei `<Diskettengerät>` oder `<CD-DVD-Gerät>` ein gültiger Laufwerkbuchstabe (für Windows-Systeme) oder ein gültiger Gerätedateiname (für Linux-Systeme) und `<Diskettenimage>` oder `<CD-DVD-Image>` der Dateiname und Pfad einer gültigen Imagedatei sind.

ANMERKUNG: Bereitstellungspunkte für das VMCLI-Dienstprogramm werden nicht unterstützt.

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)

ANMERKUNG: Red Hat Enterprise Linux Version 4 bietet keine Unterstützung für mehrere LUNs. Der Kernel unterstützt diese Funktionalität jedoch. Aktivieren Sie Red Hat Enterprise Linux Version 4 zum Erkennen eines SCSI-Geräts mit mehreren LUNs, indem Sie die nachstehenden Schritte befolgen:

1. Bearbeiten Sie **/etc/modprobe.conf** und fügen Sie folgende Zeile hinzu:
   `options scsi_mod max_luns=8`
   (Sie können 8 LUNs oder eine beliebige Anzahl größer als 1 angeben.)
2. Um den Namen für das Kernel-Image zu erhalten, geben Sie den folgenden Befehl in die Befehlszeile ein:

   `uname -r`

3 Gehen Sie zum Verzeichnis **/boot** und löschen Sie die Kernel-Imagedatei, deren Namen Sie in Schritt 2 ermittelt haben:

```
mkinitrd /boot/initrd-'uname -r'.img 'uname -r'
```

4 Starten Sie den Server neu.

5 Führen Sie folgenden Befehl aus, um die Unterstützung für die ergänzten LUNS aus Schritt 1 zu überprüfen:

```
cat /sys/modules/scsi_mod/max_luns
```

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 ermittelt wird, wird eine Fehlermeldung angezeigt und der Befehl bricht ab.

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 bestimmt das Gerät oder die Datei, das/die die virtuellen CD/DVD-ROM-Datenträger liefert:

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:\` (Microsoft 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 ermittelt 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.

Versionsanzeige

`-v`

Dieser Parameter wird zur Anzeige der Version des VMCLI-Dienstprogramms verwendet. Wenn keine anderen Nicht-Switch-Optionen bereitgestellt werden, bricht der Befehl ohne Fehlermeldung ab.

Hilfeanzeige

`-h`

Dieser Parameter zeigt eine Zusammenfassung der VMCLI-Dienstprogrammparameter an. Wenn keine anderen Nicht-Switch-Optionen bereitgestellt werden, wird der Befehl ohne Fehlermeldung abgebrochen.

Verschlüsselte Daten

`-e`

Wenn dieser Parameter in der Befehlszeile enthalten ist, verwendet die VMCLI 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.

ANMERKUNG: Wird diese Option verwendet, ändert das den angezeigten Verschlüsselungsstatus des virtuellen Datenträgerstatus in anderen iDRAC6-Konfigurationsschnittstellen, z. B. RACADM- oder Webschnittstelle, nicht in *aktiviert*.

VMCLI: Betriebssystem-Shell-Optionen

Die folgenden Betriebssystemfunktionen können in der VMCLI-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 die angegebene Datei mit der gedruckten Ausgabe des VMCLI-Dienstprogramms überschrieben.

  ANMERKUNG: Das VMCLI-Dienstprogramm liest nicht von der Standardeingabe (**stdin**). Infolgedessen ist keine **stdin**-Umleitung erforderlich.

- Ausführung im Hintergrund - standardmäßig wird das VMCLI-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 VMCLI-Befehl ermöglicht wird, fortzufahren (andernfalls würde das Skript blockieren, bis das VMCLI-Programm beendet ist). Wenn auf diese Weise mehrere VMCLI-Instanzen gestartet werden und eine oder mehrere Befehlsinstanzen manuell beendet werden müssen, sind die betriebssystemspezifischen Einrichtungen zum Auflisten und Beenden von Prozessen zu verwenden.

VMCLI-Rückgabecodes

Immer wenn Fehler auftreten, werden neben der Standardfehlerausgabe auch Textmeldungen auf Englisch ausgegeben.

13

Intelligente Plattform-Verwaltungsschnittstelle konfigurieren

Dieser Abschnitt enthält Informationen zum Konfigurieren und Verwenden der iDRAC6-IPMI-Schnittstelle. Die Schnittstelle enthält Folgendes:

- IPMI über LAN
- IPMI-über-seriell
- Seriell-über-LAN

Der iDRAC6 ist uneingeschränkt IPMI 2.0-konform. Die iDRAC6-IPMI kann mit folgenden Hilfsmitteln konfiguriert werden:

- iDRAC6-GUI über Ihren Browser.
- Open Source-Dienstprogramm, z. B. *IPMItool*.
- Dell OpenManage-IPMI-Shell, *ipmish*
- RACADM

Weitere Informationen zur Verwendung von IPMI-Shell und ipmish finden Sie im *Benutzerhandbuch für Dienstprogramme des Dell OpenManage Baseboard-Verwaltungs-Controllers* unter **support.dell.com\manuals**.

Weitere Informationen über die Verwendung von RACADM finden Sie unter „RACADM im Remote-Zugriff verwenden“ auf Seite 121.

IPMI unter Verwendung der webbasierten Schnittstelle konfigurieren

Ausführliche Informationen finden Sie unter „IPMI unter Verwendung der Webschnittstelle konfigurieren“ auf Seite 63.

IPMI mittels RACADM-CLI konfigurieren

1. Melden Sie sich über eine der RACADM-Schnittstellen am Remote-System an. Siehe „RACADM im Remote-Zugriff verwenden“ auf Seite 121.
2. Konfigurieren Sie IPMI-über-LAN.

   Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

   ```
   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.

      Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

      ```
      racadm config -g cfgIpmiLan -o
      cfgIpmiLanPrivilegeLimit <Stufe>
      ```

      wobei *<Stufe>* eine der folgenden Optionen 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 den IPMI-LAN-Kanalverschlüsselungsschlüssel ein, falls erforderlich.

   ANMERKUNG: Die iDRAC6-IPMI unterstützt das RMCP+-Protokoll. Die IPMI 2.0-Spezifikationen enthalten weitere Informationen.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiLan -o
cfgIpmiEncryptionKey <Schlüssel>
```

wobei *<Schlüssel>* ein aus 20 Zeichen bestehender Verschlüsselungsschlüssel in einem gültigen Hexadezimalformat ist.

3 IPMI Seriell über LAN (SOL) konfigurieren.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a Aktualisieren Sie die IPMI-SOL-Mindestberechtigungsebene.

ANMERKUNG: Die IPMI-SOL-Mindestberechtigungsstufe bestimmt die Mindestberechtigung, die zum Aktivieren von IPMI SOL erforderlich ist. Weitere Informationen enthält die IPMI 2.0-Spezifikation.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
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 auf 2 (Benutzer) zu konfigurieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege 2
```

b Aktualisieren Sie die IPMI-SOL-Baudrate.

ANMERKUNG: Um die serielle Konsole über LAN umzuleiten, stellen Sie sicher, dass die SOL-Baudrate mit der Baudrate des verwalteten Systems übereinstimmt.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate <Baudrate>
```

wobei *<Baudrate>* 9600, 19200, 57600 oder 115200 Bits pro Sekunde ist.

Zum Beispiel:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate 57600
```

c Aktivieren Sie SOL für einen einzelnen Benutzer.

ANMERKUNG: SOL kann für jeden einzelnen Benutzer aktiviert oder deaktiviert werden.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgUserAdmin -o
cfgUserAdminSolEnable -i <ID> 2
```

wobei *<ID>* die eindeutige Benutzer-ID ist.

4 Konfigurieren Sie IPMI-Seriell.

a Ändern Sie den Modus der seriellen IPMI-Verbindung auf die entsprechende Einstellung.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgSerial -o
cfgSerialConsoleEnable 0
```

b Stellen Sie die IPMI-Seriell-Baudrate ein.

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialBaudRate <Baudrate>
```

wobei *<Baudrate>* 9600, 19200, 57600 oder 115200 Bits pro Sekunde ist.

Zum Beispiel:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialBaudRate 57600
```

c Aktivieren Sie die Hardware-Datenflusssteuerung auf der seriellen IPMI.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialFlowControl 1
```

d Stellen Sie die Mindestberechtigungsebene auf dem seriellen IPMI-Kanal ein.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialChanPrivLimit <Ebene>
```

wobei *<Stufe>* eine der folgenden Optionen ist:

- `2` (Benutzer)
- `3` (Operator)
- `4` (Administrator)

Beispiel: Um die Berechtigungen auf dem seriellen IPMI-Kanal auf 2 (Benutzer) einzustellen, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialChanPrivLimit 2
```

e Stellen Sie sicher, dass der serielle MUX im BIOS-Setup-Programm ordnungsgemäß eingestellt ist.

- Starten Sie das System neu.
- Drücken Sie während des POST <F2>, um das BIOS-Setup-Programm zu öffnen.
- Klicken Sie auf **Serial Communication** (Serielle Kommunikation).

- Stellen Sie im Menü **Serial Connection** (Serielle Verbindung) sicher, dass **External Serial Connector** (Externe serielle Schnittstelle) auf **Remote Access Device** (Remote-Zugriffsgerät) gesetzt ist.
- Speichern und beenden Sie das BIOS-Setup-Programm.
- Starten Sie das System neu.

Die IPMI- Konfiguration ist abgeschlossen.

Wenn sich die serielle IPMI im Terminalmodus befindet, können Sie die folgenden zusätzlichen Einstellungen mittels der Befehle **racadm config cfgIpmiSerial** konfigurieren:

- Löschsteuerung
- Echosteuerung
- Zeilenbearbeitung
- Neue Zeilenfolgen
- Neue Zeilenfolgen eingeben

Weitere Informationen über diese Eigenschaften finden Sie in der IPMI 2.0-Spezifikation.

Serielle IPMI-Remote-Zugriffsschnittstelle verwenden

In der seriellen IPMI-Schnittstelle sind die folgenden Modi verfügbar:

- **IPMI-Terminalmodus** - Unterstützt ASCII-Befehle, die von einem seriellen Terminal gesendet werden. Der Befehlssatz ist auf eine bestimmte Anzahl von Befehlen (einschließlich der Stromsteuerung) begrenzt und unterstützt Raw-IPMI-Befehle, die als hexadezimale ASCII-Zeichen eingegeben werden.
- **Grundlegender IPMI-Modus** - Unterstützt eine binäre Schnittstelle für Programmzugriff, z. B. die IPMI-Shell (IPMISH), die zum Lieferumfang des Baseboard-Verwaltungsdienstprogramms (BMU) gehört.

So konfigurieren Sie den IPMI-Modus mittels RACADM:

1. Deaktivieren Sie die serielle RAC-Schnittstelle.

   Geben Sie Folgendes in die Befehlszeile ein:

   ```
   racadm config -g cfgSerial -o
   cfgSerialConsoleEnable 0
   ```

2. Aktivieren Sie den entsprechenden IPMI-Modus.

   Beispiel: Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   racadm config -g cfgIpmiSerial -o
   cfgIpmiSerialConnectionMode <0 oder 1>
   ```

Weitere Informationen finden Sie unter Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Seriell-über-LAN mittels webbasierter Schnittstelle konfigurieren

Ausführliche Informationen finden Sie unter „IPMI unter Verwendung der Webschnittstelle konfigurieren“ auf Seite 63.

ANMERKUNG: Seriell-über-LAN kann mit den folgenden Dell OpenManage-Hilfsprogrammen verwendet werden: SOLProxy und IPMItool. Weitere Informationen hierzu finden Sie im *Benutzerhandbuch für Dienstprogramme des Dell OpenManage Baseboard-Verwaltungs-Controllers* unter **support.dell.com\manuals**.

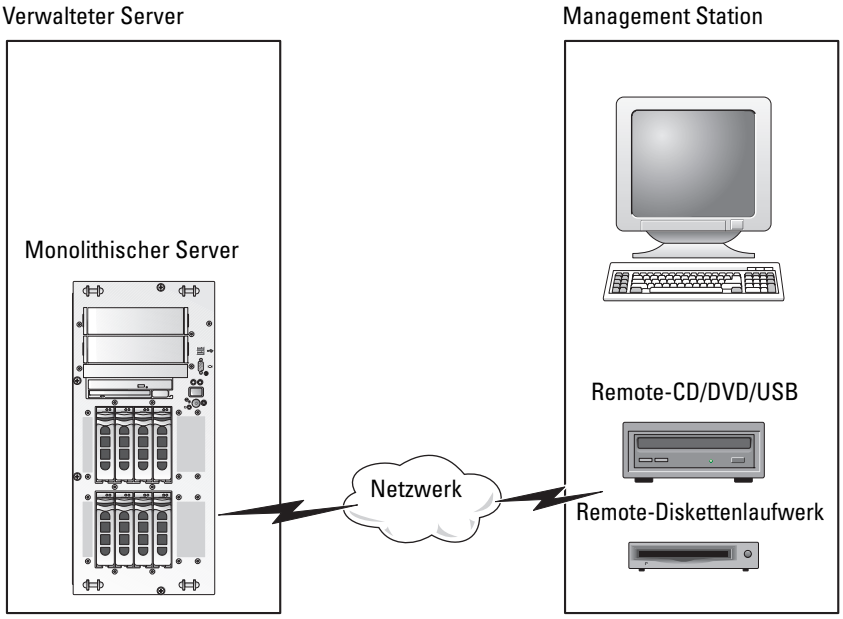
14

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 14-1 zeigt die gesamte Architektur des **virtuellen Datenträgers**.

Abbildung 14-1. 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 Floppy-Laufwerken installieren.

ANMERKUNG: Virtuelle Datenträger erfordern eine verfügbare Netzwerkbandbreite von mindestens 128 Kbit/s.

Virtueller Datenträger definiert zwei Geräte für das Betriebssystem und BIOS des verwalteten Servers: ein Floppy-Laufwerk und ein optisches Laufwerk.

Die Management Station stellt den physischen Datenträger oder die Imagedatei über das Netzwerk bereit. Wenn ein **virtueller Datenträger** angeschlossen ist oder automatisch angeschlossen wird, werden alle Zugriffsanforderungen virtueller CD-/Floppy-Laufwerke des verwalteten Servers über das Netzwerk an die Management Station geleitet. Verbinden/Anschließen 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 14-1 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 14-1. 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	

Windows-basierte Management Station

Um die Funktion des **virtuellen Datenträgers** auf einer Management Station mit dem Betriebssystem Microsoft Windows auszuführen, installieren Sie eine unterstützte Internet Explorer- oder Firefox-Version mit Java-Laufzeitumgebung (JRE).

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 Plugins der virtuellen Konsole ist eine 32-Bit-Java-Laufzeitumgebung (JRE) erforderlich. Sie können eine JRE von **java.sun.com** herunterladen.

VORSICHTSHINWEIS: Damit Sie den virtuellen Datenträger erfolgreich starten können, müssen Sie sicherstellen, dass auf einem 64-Bit-Betriebssystem eine 32-Bit- oder 64-Bit-JRE-Version installiert ist oder auf einem 32-Bit-Betriebssystem eine 32-Bit-JRE-Version. iDRAC6 unterstützt *nicht* 64-Bit-ActiveX-Versionen. Stellen Sie außerdem sicher, dass für Linux das mit „compat-libstdc++-33-3.2.3-61" in Beziehung stehende Paket installiert ist, damit der virtuelle Datenträger gestartet werden kann. Auf Windows ist das Paket eventuell im .NET-Framework-Paket enthalten.

Virtuellen Datenträger konfigurieren

1. Melden Sie sich an der iDRAC6-Webschnittstelle an.
2. Wählen Sie **System**→ Register **Konsole/Datenträger**→ **Konfiguration**→ **Virtueller Datenträger** aus, um die Einstellungen des virtuellen Datenträgers zu konfigurieren.

   Tabelle 14-2 beschreibt die Konfigurationswerte des **virtuellen Datenträgers**.
3. Wenn Sie mit den Einstellungen fertig sind, klicken Sie auf **Anwenden**.

Tabelle 14-2. Konfigurationseigenschaften für virtuelle Datenträger

Attribut	Wert
Status	**Verbinden** - Schließt den **virtuellen Datenträger** umgehend an den Server an. **Abtrennen** - Trennt den **virtuellen Datenträger** umgehend vom Server ab. **Automatisch Verbinden** – Verbindet den **virtuellen Datenträger** nur dann mit dem Server, wenn eine Sitzung des virtuellen Datenträgers gestartet wird.
Max. Sitzungen	Zeigt die maximale Anzahl zulässiger **virtueller Datenträger**-Sitzungen an. Der Wert ist stets 1.
Aktive Sitzungen	Zeigt die aktuelle Anzahl von Sitzungen des virtuellen Datenträgers an.
Virtuelle Datenträgerverschlüsselung aktiviert	Wählen Sie das Kontrollkästchen aus oder ab, um die Verschlüsselung auf Verbindungen des **virtuellen Datenträgers** zu aktivieren bzw. zu deaktivieren. Wenn ausgewählt, ist die Verschlüsselung aktiviert, wenn abgewählt, ist sie deaktiviert.
Diskettenemulation	Zeigt an, ob der **virtuelle Datenträger** dem Server als Floppy-Laufwerk oder USB-Schlüssel angezeigt wird. Wenn **Diskettenemulation** markiert ist, wird das **virtuelle Datenträger**-Gerät auf dem Server als Floppy-Gerät angezeigt. Wenn es nicht ausgewählt ist, wird es als USB-Schlüssellaufwerk angezeigt. **ANMERKUNG:** In bestimmten Windows Vista- und Red Hat-Umgebungen werden Sie eventuell nicht in der Lage sein, einen USB bei aktivierter **Diskettenemulation** zu virtualisieren.
Verbindungsstatus	**Verbunden** – Es wird derzeit eine Sitzung des virtuellen Datenträgers durchgeführt. **Nicht verbunden** – Es wird derzeit keine Sitzung des virtuellen Datenträgers durchgeführt.

Tabelle 14-2. Konfigurationseigenschaften für virtuelle Datenträger *(fortgesetzt)*

Attribut	Wert
„Einmal Starten“ aktivieren	Wählen Sie dieses Kästchen aus, um die Option **Einmal starten** zu aktivieren. Verwenden Sie dieses Attribut, um vom virtuellen Datenträger aus zu starten. Wählen Sie beim nächsten Startvorgang das Startgerät aus dem BIOS-Startmenü aus. Diese Option trennt die **virtuellen Datenträger**-Geräte automatisch, nachdem das System einmal gestartet wurde.

Virtuellen Datenträger ausführen

VORSICHTSHINWEIS: Geben Sie keinen racreset-Befehl aus, wenn eine Virtueller Datenträger-Sitzung ausgeführt wird. Andernfalls könnten unerwünschte Ergebnisse einschließlich Datenverlust auftreten.

ANMERKUNG: Die Anwendung des Konsolen-Viewer-Fensters muss während des Zugriffs auf den virtuellen Datenträger aktiviert bleiben.

ANMERKUNG: Führen Sie die folgenden Schritte aus, um Red Hat Enterprise Linux (Version 4) für die Erkennung eines SCSI-Geräts mit mehreren logischen Einheiten (LUNs) einzustellen:

1. Fügen Sie die folgende Zeile zu **/ect/modprobe** hinzu:

   ```
   options scsi_mod max_luns=256

   cd /boot

   mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp
   ```

2. Starten Sie den Server neu.
3. Führen Sie die folgenden Befehle aus, um die virtuelle CD/DVD und/oder das virtuelle Diskettenlaufwerk anzuzeigen:

   ```
   cat /proc/scsi/scsi
   ```

ANMERKUNG: Mit „Virtueller Datenträger“ können Sie nur ein Floppy-/USB-Laufwerk oder ein Abbild oder einen Schlüssel und ein optisches Laufwerk von Ihrer Management Station virtualisieren und als virtuelles Laufwerk auf dem verwalteten Server bereitstellen.

Unterstützte Konfigurationen des virtuellen Datenträgers

Sie können den virtuellen Datenträger für ein Floppy-Laufwerk und ein optisches Laufwerk aktivieren. Es kann für jeden Datenträgertyp jeweils nur ein einziges Laufwerk virtualisiert werden.

Unterstützte Floppy-Laufwerke umfassen ein Floppy-Image oder ein verfügbares Floppy-Laufwerk. Unterstützte optische Laufwerke umfassen maximal ein verfügbares optisches Laufwerk oder eine einzige ISO-Imagedatei.

Virtuellen Datenträger verbinden

Führen Sie die folgenden Schritte aus, um „Virtueller Datenträger" auszuführen:

1. Öffnen Sie einen unterstützten Internet-Browser auf der Management Station.
2. Starten Sie die iDRAC6-Webschnittstelle. Weitere Informationen finden Sie unter „Zugriff auf die Webschnittstelle" auf Seite 48.
3. Wählen Sie **System→ Konsole/Datenträger→ Virtuelle Konsole** und **Virtueller Datenträger** aus.
4. Die Seite **Virtuelle Konsole** und **Virtueller Datenträger** wird angezeigt. Wenn Sie die Werte angezeigter Attribute ändern möchten, finden Sie entsprechende Informationen unter „Virtuellen Datenträger konfigurieren" auf Seite 285.

   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 ein Floppy-/USB-Flash-Laufwerk gleichzeitig zur Virtualisierung 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 lösen, schlagen Sie in der Dokumentation zu Ihrem Microsoft-Betriebssystem nach oder wenden Sie sich an Ihren Systemadministrator.

5 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 **Virtuelle iDRAC6-Konsole** wird in einem separaten Fenster gestartet.

6 Klicken Sie auf **Virtueller Datenträger→ Virtuellen Datenträger starten**.

Der Assistent für**Sitzungen des virtuellen Datenträgers** wird angezeigt.

ANMERKUNG: Schließen Sie diesen Assistenten nur, wenn Sie die Sitzung des virtuellen Datenträgers beenden möchten.

7 Wenn eine Datenträgerverbindung besteht, muss diese vor dem Verbinden mit einer anderen Datenträgerquelle zuerst abgetrennt werden. Deaktivieren Sie das Kästchen links neben dem Datenträger, der getrennt werden soll.

8 Wählen Sie die Datenträgertypen aus, zu denen Sie eine Verbindung herstellen möchten.

Wenn Sie eine Verbindung zu einem Diskettenabbild-Image oder ISO-Image herstellen möchten, geben Sie (auf Ihrem lokalen Computer) den Pfad zum Image ein oder klicken Sie auf die Schaltfläche **Abbild hinzufügen**, um zum Image zu navigieren.

Die Verbindung zum Datenträger wird hergestellt und das Fenster **Status** aktualisiert.

Verbindung des virtuellen Datenträgers trennen

1 Klicken Sie auf **Extras→ Virtuellen Datenträger starten**.

2 Deaktivieren Sie das Kästchen neben dem Datenträger, den Sie trennen möchten.

Die Verbindung zum Datenträger wird getrennt und das Fenster **Status** aktualisiert.

3 Klicken Sie auf **Beenden**, um den Assistenten für **Sitzungen des virtuellen Datenträgers** zu beenden.

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.

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 unter Verwendung des **virtuellen Datenträgers** kann weniger als 15 Minuten beanspruchen. Weitere Informationen finden Sie unter „Betriebssystem bereitstellen“ auf Seite 265.

1. Überprüfen Sie folgende Punkte:
   - Die Installations-CD des Betriebssystems ist in das CD-Laufwerk der Management Station eingelegt.
   - Das lokale CD-Laufwerk ist ausgewählt.
   - Sie sind mit den virtuellen Laufwerken verbunden.
2. Befolgen Sie die Schritte zum Starten über den virtuellen Datenträger im Abschnitt „Starten vom virtuellen Datenträger“ auf Seite 290, um sicherzustellen, dass das BIOS so eingestellt ist, dass es vom CD-Laufwerk startet, von dem aus Sie die Installation vornehmen.
3. Folgen Sie den Bildschirmanleitungen, um die Installation abzuschließen.

Es ist wichtig, diese Schritte für die Installation von mehreren Disketten zu befolgen:

1. Heben Sie die Zuordnung der virtualisierten (umgeleiteten) CD/DVD von der Konsole des virtuellen Datenträgers auf.
2. Legen Sie die nächste CD/DVD in das optische Remote-Laufwerk ein.
3. Ordnen Sie diese CD/DVD von der Konsole des virtuellen Datenträgers zu (umleiten).

   Das Einlegen einer neuen CD/DVD in das optische Remote-Laufwerk ohne erneutes Zuordnen funktioniert u. U. nicht.

Einmalstart-Funktion

Mit der Einmalstart-Funktion können Sie die Startreihenfolge vorübergehend ändern, um von einem virtuellen Remote-Datenträgergerät aus zu starten. Diese Funktion wird normalerweise in Verbindung mit Virtueller Datenträger beim Installieren von Betriebssystemen verwendet.

ANMERKUNG: Sie benötigen die Berechtigung **iDRAC6 konfigurieren**, um diese Funktion zu nutzen.

ANMERKUNG: Remote-Geräte müssen mit Virtueller Datenträger umgeleitet werden, um diese Funktion zu nutzen.

So verwenden Sie die Einmalstart-Funktion:

1. Melden Sie sich über das Internet beim iDRAC6 an und klicken Sie auf **System→ Konsole/Datenträger→ Konfiguration**.
2. Wählen Sie die Option **Einmal starten aktivieren** unter **Virtueller Datenträger** aus.
3. Schalten Sie den Server ein und rufen Sie den BIOS Boot Manager auf.
4. Ändern Sie die Startreihenfolge zum Starten vom virtuellen Datenträgergerät.
5. Schalten Sie den Server aus und dann wieder ein.

   Der Server startet vom virtuellen Remote-Datenträgergerät. Wenn der Server das nächste Mal neu startet, wird die Verbindung zum virtuellen Datenträger abgetrennt.

   ANMERKUNG: Der virtuelle Datenträger sollte den Status **Verbunden** haben, damit die virtuellen Laufwerke in der Startsequenz angezeigt werden. Stellen Sie, um **Einmal starten** zu aktivieren, sicher, dass der startfähige Datenträger im virtualisierten Laufwerk vorhanden ist.

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 über virtuelle Datenträger

Tabelle 14-3 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 14-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen

Frage	Antwort
Manchmal bemerke ich, dass die Client-Verbindung meines virtuellen Datenträgers unterbrochen ist. Warum?	Wenn bei einem Netzwerk eine Zeitüberschreitung eintritt, verwirft die iDRAC6-Firmware die Verbindung und trennt die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Wenn die Konfigurationseinstellungen des virtuellen Datenträgers über die webbasierte iDRAC6-Schnittstelle oder durch Befehle des lokalen RACADM geändert werden, werden alle verbundenen Datenträger getrennt, wenn die Konfigurationsänderung in Kraft gesetzt wird. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie den virtuellen Datenträger-Assistenten.
Welche Betriebssysteme unterstützen den iDRAC6?	Eine Liste unterstützter Betriebssysteme finden Sie unter „Unterstützte Betriebssysteme“ auf Seite 28.
Welche Webbrowser unterstützen den iDRAC6?	Eine Liste unterstützter Webbrowser finden Sie unter „Unterstützte Webbrowser“ auf Seite 28.

Tabelle 14-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
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 bei einem Netzwerk eine Zeitüberschreitung eintritt, verwirft die iDRAC6-Firmware die Verbindung und trennt die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Es ist auch möglich, dass jemand die Konfigurationseinstellungen des virtuellen Datenträgers über die Webschnittstelle oder durch Eingabe von RACADM-Befehlen verändert hat. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie die Funktion **Virtueller Datenträger**.
Eine Installation des Windows-Betriebssystems über einen virtuellen Datenträger scheint zu lange zu dauern. Warum?	Wenn Sie das Windows-Betriebssystem mithilfe der DVD *Dell Systems Management Tools and Documentation* und 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 14-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Wie konfiguriere ich mein virtuelles Gerät als startfähiges Gerät?	Greifen Sie auf dem verwalteten Server auf das BIOS-Setup zu und klicken Sie auf das Startmenü. Machen Sie die virtuelle CD, die virtuelle Diskette oder vFlash ausfindig und ändern Sie die Geräte-Startreihenfolge nach Bedarf. Machen Sie außerdem den virtuellen Datenträger startfähig, indem Sie im CMOS-Setup während der Startsequenz die Leertaste drücken. Um z. B. von einem CD-Laufwerk aus zu starten, konfigurieren Sie das CD-Laufwerk als erstes Laufwerk in der Startreihenfolge.
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 Wechsellaufwerk erkannt wird • Ein USB-Schlüssel-Image
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. an der DOS-Eingabeaufforderung den folgenden Befehl ein: `sys a: x: /s` wobei *x*: der USB-Schlüssel ist, der startfähig gemacht werden soll.

Tabelle 14-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Ich kann mein virtuelles Disketten-/CD-Laufwerk auf einem System mit dem Betriebssystem Red Hat Enterprise Linux oder SUSE Linux nicht finden. Mein virtueller Datenträger ist angeschlossen und ich bin mit meiner Remote-Diskette verbunden. Was muss ich tun?	Bei einigen Linux-Versionen werden virtuelle Diskettenlaufwerke und virtuelle CD-Laufwerke nicht in gleicher Weise automatisch geladen. Um das virtuelle Diskettenlaufwerk zu laden, machen Sie den Geräteknoten ausfindig, den Linux dem virtuellen Diskettenlaufwerk zuweist. Führen Sie die folgenden Schritte aus, um das virtuelle Diskettenlaufwerk korrekt zu finden 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.

Tabelle 14-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort

Ich kann mein virtuelles Disketten-/CD-Laufwerk auf einem System mit dem Betriebssystem Red Hat Enterprise Linux oder SUSE Linux nicht finden. Mein virtueller Datenträger ist angeschlossen und ich bin mit meiner Remote-Diskette verbunden. Was muss ich tun?	*(Antwort Fortsetzung)*
	Um das virtuelle CD-Laufwerk zu laden, machen Sie den Geräteknoten ausfindig, den Linux dem virtuellen CD-Laufwerk zuweist. Befolgen Sie die nächsten Schritte, um das virtuelle CD-Laufwerk zu finden und zu laden:
	1 Öffnen Sie eine Linux-Eingabeaufforderung und führen Sie den folgenden Befehl aus:
	`grep "Virtual CD" /var/log/messages`
	2 Machen Sie den letzten Eintrag zu dieser Meldung ausfindig und notieren Sie die Zeit.
	3 Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:
	`grep "hh:mm:ss" /var/log/messages`
	wobei
	`hh:mm:ss` der Zeitstempel der Meldung ist, die von `grep` in Schritt 1 zurückgegeben wurde.
	4 Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls und machen Sie den Gerätenamen ausfindig, der der *virtuellen Dell-CD* zugeordnet wurde.
	5 Stellen Sie sicher, dass das virtuelle CD-Laufwerk angeschlossen ist und dass eine Verbindung dazu besteht.
	6 Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:
	`mount /dev/sdx /mnt/CD`
	wobei
	`/dev/sdx` ist der in Schritt 4 gefundene Gerätename.
	`/mnt/floppy` ist der Bereitstellungspunkt.

Tabelle 14-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Als ich im Remote-Zugriff mithilfe der iDRAC6-Webschnittstelle eine Firmware-Aktualisierung ausgeführt habe, wurden meine virtuellen Laufwerke vom Server entfernt. Warum?	Firmware-Aktualisierungen bewirken, dass der iDRAC6 eine Rücksetzung durchführt, die Remote-Verbindung verwirft und die virtuellen Laufwerke aufhebt.
Warum werden nach dem Anschließen eines USB-Geräts alle meine USB-Geräte abgetrennt?	Virtuelle Datenträgergeräte und vFlash-Geräte werden als Verbund-USB-Gerät am Host-USB-BUS angeschlossen und verwenden einen gemeinsamen USB-Anschluss. Immer wenn ein virtuelles Datenträgergerät oder vFlash-USB-Gerät an den Host-USB-BUS angeschlossen oder davon abgetrennt wird, werden alle virtuellen Datenträger- und vFlash-Geräte vorübergehend vom Host-USB-Bus abgetrennt und danach wieder verbunden. Wenn ein virtuelles Datenträgergerät vom Host-Betriebssystem verwendet wird, müssen Sie das Verbinden bzw. Abtrennen eines oder mehrerer virtueller Datenträger- oder vFlash-Geräte vermeiden. Es wird empfohlen, zuerst alle erforderlichen USB-Geräte anzuschließen, bevor Sie sie verwenden.
Welche Funktion hat die **USB-Reset**-Taste?	Sie setzt die Remote- und lokalen USB-Geräte zurück, die an den Server angeschlossen sind.

Tabelle 14-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Wie kann ich mit dem virtuellen Datenträger die Höchstleistung erzielen?	Um die höchste Leistung des virtuellen Datenträgers zu erzielen, starten Sie den virtuellen Datenträger mit deaktivierter virtueller Konsole oder wählen Sie eine der folgenden Verfahrensweisen aus: • Reduzieren Sie die Videoauflösung und Farbtiefe des Bildschirms der virtuellen Konsole auf die kleinstmögliche Einstellung. • Deaktivieren Sie die Verschlüsselung sowohl für den virtuellen Datenträger als auch für die virtuelle Konsole. **ANMERKUNG:** In diesem Fall wird die Datenübertragung zwischen dem verwalteten Server und iDRAC für den virtuellen Datenträger und für die virtuelle Konsole nicht gesichert. • Wenn Sie ein Windows-Server-Betriebssystem verwenden, halten Sie bitte den Windows-Dienst mit der Bezeichnung Windows Event Collector an. Rufen Sie hierzu **Start > Verwaltunghilfsprogramme > Dienste** auf. Klicken Sie mit der rechten Maustaste auf **Windows Event Collector** und klicken Sie auf **Stopp**.

15

vFlash-SD-Karte konfigurieren und vFlash-Partitionen verwalten

Die vFlash-SD-Karte ist eine SD-Karte (Secure Digital), die in den optionalen iDRAC6 Enterprise-Kartensteckplatz an der Rückseite des Systems eingesetzt wird. Sie stellt Speicherplatz bereit und verhält sich wie ein herkömmliches USB Flash Key-Gerät. 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.

Informationen zum Installieren und Entfernen der Karte auf dem bzw. vom System finden Sie im *Hardware-Benutzerhandbuch* des Systems unter **dell.com/support/manuals**.

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. Als *standardmäßige SD-Karte* wird eine gewöhnliche Standard-SD-Karte bezeichnet, die nur eine begrenzte Auswahl an 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. Die einzelnen Partitionen können 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.

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. Zum Ausführen der Partitionsverwaltung muss die vFlash-Funktionalität 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 die Karte im Systemsteckplatz für die iDRAC6 Enterprise-Karte nicht vorhanden ist, wird die 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 15-1 führt die Eigenschaften auf, die für die SD-Karte angezeigt werden.

Tabelle 15-1. Eigenschaften der SD-Karte

Attribut	Beschreibung
Name	Zeigt den Namen der Karte an, die im Server in den Steckplatz für die iDRAC6 Enterprise-Karte eingefügt wird. Wenn die Karte die neuen verbesserten vFlash-Funktionen unterstützt, wird *vFlash-SD-Karte* angezeigt. Wenn sie eingeschränkte vFlash-Funktionen unterstützt, wird *SD-Karte* angezeigt.
Größe	Zeigt die Größe der Karte in Gigabyte (GB) an.
Available Space (Verfügbarer Speicherplatz)	Zeigt den ungenutzten Speicherplatz auf der vFlash-SD-Karte in MB an. Dieser Speicherplatz ist verfügbar, um weitere Partitionen auf der vFlash-SD-Karte zu erstellen. Wenn die eingelegte vFlash-SD-Karte nicht initialisiert ist, wird für den verfügbaren Speicherplatz angezeigt, dass die Karte nicht initialisiert ist. Bei der standardmäßigen SD-Karte wird der verfügbare Speicherplatz nicht angezeigt.
Schreibgeschützt	Zeigt an, ob die Karte schreibgeschützt ist oder nicht.

Tabelle 15-1. Eigenschaften der SD-Karte *(fortgesetzt)*

Attribut	Beschreibung
Seite „Funktionszustand“	Zeigt den allgemeinen Funktionszustand der vFlash-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. Bei der standardmäßigen SD-Karte wird der Funktionszustand nicht angezeigt.
vFlash aktiviert	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, wird nur das Unterregister **Eigenschaften der SD-Karte** angezeigt.

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 gibt eine Meldung darüber Auskunft, dass der Vorgang erfolgreich abgeschlossen worden ist.

ANMERKUNG: **Initialisieren** wird nur aktiviert, wenn Sie die Option **vFlash aktiviert** auswählen.

Wenn eine vFlash-Partition verbunden wird, schlägt der Initialisierungsvorgang fehl, und es wird eine Fehlermeldung angezeigt.

Wenn Sie auf den vFlash-Seiten auf eine beliebige Option klicken, während eine Anwendung wie der WSMAN Provider, das iDRAC6-Konfigurationshilfsprogramm oder RACADM gerade vFlash verwendet, oder wenn Sie zu einer anderen Seite der GUI navigieren, zeigt iDRAC6 möglicherweise die folgende Meldung an:

`vFlash is currently in use by another process. Try again after some time.` (vFlash wird gerade von einem anderen Prozess in Anspruch genommen. Versuchen Sie es nach einiger Zeit erneut.)

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 die folgenden Befehle 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 die folgende Meldung angezeigt: *ERROR: SD Card not present* (FEHLER: SD-Karte nicht vorhanden).

vFlash- oder standardmäßige SD-Karte initialisieren

Öffnen Sie eine Telnet-/SSH-/serielle Konsole zum Server, melden Sie sich an und geben Sie den folgenden Befehl ein, um die Karte zu initialisieren:

```
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 zum Server, melden Sie sich an und geben Sie den folgenden Befehl ein, um den Status des letzten Initialisierungsbefehls abzurufen, der an die vFlash- oder standardmäßige SD-Karte gesendet wurde:

```
racadm vFlashsd status
```

ANMERKUNG: Über diesen Befehl wird nur der Status der Befehle angezeigt, die an die SD-Karte gesendet wurden. Um den Status von Befehlen abzurufen, die an individuelle Partitionen auf der SD-Karte gesendet wurden, verwenden Sie den folgenden Befehl:
`racadm vflashpartition status`

vFlash- oder standardmäßige SD-Karte zurücksetzen

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 *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

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 „vFlash- oder standardmäßige SD-Karte initialisieren“ auf Seite 306.

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 haben die Wahl, eine Partition des Typs *Diskette* oder des Typs *Festplatte* zu erstellen. 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 Erstellen 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 15-2 aufgeführten Informationen ein.
3. Klicken Sie auf **Anwenden**. Es wird eine neue Partition erstellt. Es wird eine Seite eingeblendet, auf der der Fortschritt als Prozentsatz zu sehen ist.

   Es wird eine Fehlermeldung angezeigt, wenn Folgendes zutrifft:

   - Die Karte ist schreibgeschützt.
   - Der Kennzeichnungsname stimmt mit der Kennzeichnung einer vorhandenen Partition überein.
   - Ein nicht ganzzahliger Wert wurde als Partitionsgröße eingegeben, der Wert übersteigt den auf der Karte verfügbaren Speicherplatz oder die Partition ist größer als 4 GB.
   - Auf der Karte wird bereits ein Initialisierungsvorgang ausgeführt.

   ANMERKUNG: Die neue Partition ist unformatiert (RAW).

Tabelle 15-2. 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.
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:** Der Kennzeichnungsname der standardmäßigen SD-Karte lautet standardmäßig VFLASH. Dieser Name kann nicht modifiziert werden.
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 Megabyte (MB) an. Die maximale Partitionsgröße beträgt 4 GB bzw. weniger als der oder gleich dem auf der vFlash-SD-Karte verfügbare(n) Speicherplatz. **ANMERKUNG:** Für die standardmäßige SD-Karte beträgt die Partitionsgröße 256 MB. Diese Größe kann nicht geändert werden.

Partition unter Verwendung einer Imagedatei erstellen

Sie können auf der vFlash- oder standardmäßigen SD-Karte unter Verwendung einer Imagedatei (verfügbar im Format **.img** oder **.iso**) eine neue Partition erstellen. Sie können eine Partition des Typs Diskette, Festplatte oder CD erstellen.

ANMERKUNG: Um Partitionen erstellen zu können, müssen Sie über die Berechtigung 'Zugriff auf virtuellen Datenträger' verfügen.

Wenn eine **ISO**-Imagedatei (für CD) verwendet wird, wird eine schreibgeschützte Partition erstellt. Wenn eine **IMG**-Imagedatei (für Diskette und Festplatte) verwendet wird, wird eine Lese-Schreib-Partition erstellt.

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.

Unter 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 standardmäßige SD-Karte muss die Imagegröße geringer als 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 Image als den festgelegten Imagetyp. 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. Wählen Sie auf der iDRAC6-Webschnittstelle **System→ vFlash→** Unterregister **Über Image erstellen** aus. Die Seite **Partition über Imagedatei erstellen** wird angezeigt.
2. Geben Sie die unter Tabelle 15-3 aufgeführten Informationen ein.
3. Klicken Sie auf **Anwenden**. Es wird eine neue Partition erstellt.

   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 15-3. 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 standardmäßige SD-Karte lautet der Kennzeichnungsname VFLASH und kann nicht modifiziert werden.

Tabelle 15-3. Optionen der Seite 'Partition über Imagedatei erstellen'

Feld	Beschreibung
Emulationstyp	Wählen Sie aus der Drop-Down-Liste den Emulationstyp für die Partition aus. Die verfügbaren Optionen sind **Diskette**, **Festplatte** und **CD**.
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. Das Formatieren von Partitionen des Typs CD 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 **Partition formatieren** wird angezeigt.
2. Geben Sie die unter Tabelle 15-4 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 ausgewählte Partition wird gemäß dem festgelegten Dateisystemtyp formatiert.

Es wird eine Fehlermeldung angezeigt, wenn Folgendes zutrifft:

- Die Karte ist schreibgeschützt.
- Auf der Karte wird bereits ein Initialisierungsvorgang ausgeführt.

Tabelle 15-4. 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.
Formattyp	Wählen Sie den Dateisystemtyp aus, auf den die Partition formatiert werden soll. Die verfügbaren Optionen sind EXT2, EXT3, FAT16 und FAT32.

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. Auf der Seite **Partitionen verwalten** sind die verfügbaren Partitionen aufgeführt.
2. Für jede Partition können Sie die unter Tabelle 15-5 erwähnten Informationen anzeigen.

Tabelle 15-5. 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 Megabyte (MB).
Nur-Lesen	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 315.
Geben Sie Folgendes ein:	Zeigt an, ob der Partitionstyp Diskette, Festplatte oder CD ist.
Status	Status eines sich in Ausführung befindenden Vorgangs oder des letzten auf der Partition ausgeführten Vorgangs mit Fortschrittsprozentsatz. Die Statuswerte lauten: • Leerlauf – Es wird kein Vorgang ausgeführt. • Formatierung – Partition wird gerade formatiert. • Erstellung – Partition wird gerade erstellt.

Partition modifizieren

Stellen Sie sicher, dass die Karte zum Modifizieren der Partition aktiviert ist.

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. Markieren Sie in der Spalte **Nur-Lesen** das Kontrollkästchen für die Partition(en), die Sie zu Nur-Lesen ändern möchten, oder heben Sie die Markierung des Kontrollkästchens für die Partition(en) auf, die Sie zu Lesen-Schreiben ändern möchten.

   ANMERKUNG: Wenn der Typ der Partition "CD" ist, ist der Zustand Nur-Lesen und das Kontrollkästchen wird standardmäßig markiert. Sie können den Zustand nicht zu Lesen-Schreiben ändern.
   Wenn die Partition verbunden ist, ist das Kontrollkästchen grau unterlegt.
   Bei der standardmäßigen SD-Karte ist die Partition Lesen-Schreiben und die Spalte Nur-Lesen 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 virtuelles USB-Massenspeichergerät verbinden, und zwar so, dass sie für das Betriebssystem und das BIOS als USB-Massenspeichergeräte erkennbar sind. Wenn mehrere Partitionen gleichzeitig verbunden werden, werden sie dem Host-Betriebssystem basierend auf dem Index in aufsteigender Reihenfolge dargestellt. Die Zuweisung des entsprechenden Laufwerkbuchstabens wird vom Betriebssystem gesteuert.

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 sich auf beliebige Anwendungen (wie z. B. das Betriebssystem) auswirken, die vFlash verwenden, und trennt die Verbindung zu den Sitzungen des virtuellen iDRAC-Datenträgers.

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 bei verbundenen 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, wie im Host-Betriebssystem erkennbar, nur Lesevorgänge durchführen können.

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 aktiviert.
- Die Karte ist nicht schreibgeschützt.
- Die Partition ist nicht verbunden.
- Es wird nicht bereits ein Initialisierungsvorgang auf der Karte ausgeführt.

So löschen Sie vorhandene Partitionen:

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. Der Remote-Speicherort ist ein Netzwerkspeicherort, der der Management Station zugewiesen ist.

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 85 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.

Optionen, die nur bei der Maßnahme Erstellen gültig sind:

-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, CDDVD oder HDD 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 – Erstellen Sie eine Partition unter Verwendung eines Image, das im Verhältnis zum iDRAC steht. Die folgenden Optionen sind gültig mit dem Imagetyp:
  - -l <Pfad> – Gibt den Remote-Pfad im Verhältnis zum iDRAC an. Der Pfad kann auf einem bereitgestellten Laufwerk sein:
    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.

Optionen, die nur bei der Maßnahme Status gültig sind:

-a

Zeigt den Status von Vorgängen auf allen vorhandenen Partitionen 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: Dieser Befehl unterscheidet bei der Image-Dateinamenerweiterung zwischen Groß- und Kleinschreibung. Wird beispielsweise die Dateinamenerweiterung in Großbuchstaben (FOO.ISO) statt in Kleinbuchstaben (FOO.iso) angegeben, gibt der Befehl einen Syntaxfehler aus.

ANMERKUNG: 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 „vFlash- oder standardmäßige SD-Karte initialisieren“ auf Seite 306.

Status einer Partition abrufen

- So rufen Sie den Status des Vorgangs auf Partition 1 ab:

  ```
  racadm vflashpartition status -i 1
  ```

- So rufen Sie den Status sämtlicher vorhandener Partitionen ab:

  ```
  racadm vflashpartition status -a
  ```

Partitionsinformationen anzeigen

So listen Sie alle vorhandenen Partitionen und deren Eigenschaften auf:

```
racadm vflashpartition list
```

Zu einer Partition starten

- So listen Sie die verfügbaren Geräte in der Startliste auf:

  ```
  racadm getconfig -g cfgServerInfo -o
  cfgServerFirstBootDevice
  ```

  Wenn es sich um eine vFlash-SD-Karte handelt, werden die Kennzeichnungsnamen 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> der Kennzeichnungsname für die vFlash-SD-Karte und VFLASH der Kennzeichnungsname für die standardmäßige SD-Karte ist.

  ANMERKUNG: Wenn Sie diesen Befehl ausführen, wird die Kennzeichnung der vFlash-Partition automatisch für einen einmaligen Start eingestellt, d. h. **cfgserverBootOnce** ist auf 1 eingestellt. 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 über die RACADM-Unterbefehle und die Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 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.

16

Stromüberwachung und -verwaltung

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.

Das Design der Basis-Hardware wurde in Bezug auf den Leistungsaspekt optimiert:

- Es sind jetzt hoch leistungsfähige Netzteile und Spannungsregler eingeschlossen.
- Wo immer möglich, wurden die Komponenten mit dem niedrigsten Energieverbrauch verwendet.
- Das Gehäusedesign hat den Luftstrom durch das System optimiert, um die Leistungsaufnahme des Lüfters zu minimieren.

PowerEdge-Systeme bieten viele Funktionen zur Stromüberwachung und -verwaltung:

- **Strominventar und -budgetierung:** Eine Systembestandsaufnahme ermöglicht beim Start die Kalkulation eines Systemstrombudgets für die aktuelle Konfiguration.
- **Strombegrenzung:** Die Systeme können gedrosselt werden, um einen bestimmten Stromgrenzwert einzuhalten.
- **Stromüberwachung:** Der iDRAC6 fragt die Netzteile ab, um Leistungsaufnahmewerte zu erfassen. Der iDRAC6 dokumentiert den Verlauf von Energiemesswerten und berechnet Durchschnitts- und Spitzenwerte. Mithilfe der webbasierten iDRAC6-Schnittstelle können Sie die Informationen auf der Seite **Stromüberwachung** einsehen.

Strominventar, -budgetierung und -begrenzung

Aus der Verbrauchsperspektive kann die Kühlung auf Rack-Ebene begrenzt sein. Mit einer benutzerdefinierten Strombegrenzung können Sie Strom je nach Bedarf zur Erfüllung Ihrer Leistungsanforderungen zuordnen.

Der iDRAC6 überwacht den Stromverbrauch und drosselt die Prozessoren dynamisch, um die von Ihnen definierte Strombegrenzung einzuhalten. Als Folge wird die Leistung maximiert und Ihre Leistungsanforderungen werden erfüllt.

Stromüberwachung

Der iDRAC6 überwacht kontinuierlich den Stromverbrauch in PowerEdge-Servern. Der iDRAC6 berechnet folgende Stromwerte und zeigt die Informationen auf der webbasierten Schnittstelle oder der RACADM-CLI an:

- Gesamtstrom
- Durchschnittliche, minimale und maximale Leistungsaufnahme
- Strom-Aussteuerungsreservewerte
- Stromverbrauch (wird auch grafisch auf der Webschnittstelle angezeigt)

Strom konfigurieren und verwalten

Sie können die webbasierte iDRAC6-Schnittstelle und die RACADM-Befehlszeilenoberfläche (CLI) zur Verwaltung und Konfiguration der Stromsteuerungen im PowerEdge-System verwenden. Genauer gesagt können Sie:

- Stromstatus des Servers anzeigen
- Stromsteuerungsmaßnahmen auf dem Server (z. B. Strom EIN, Strom AUS, System-Reset, Aus- und Einschalten) ausführen
- Strombudgetinformationen für den Server und die installierten Netzteile, z. B. die minimale und die maximale Leistungsaufnahme, anzeigen
- Schwellenwert für das Strombudget des Servers anzeigen

Funktionszustand der Netzteile anzeigen

Die Seite **Netzteile** zeigt den Status und die Nennleistung der Netzteile an, die im Server installiert sind.

Auf die webbasierte Schnittstelle zugreifen

So zeigen Sie den Funktionszustand der Netzteile an:

1. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
2. Wählen Sie in der Systemstruktur **Netzteile** aus. Die Seite **Netzteile** wird angezeigt und liefert die folgenden Informationen:
   - **Redundanzstatus der Netzteile**: Mögliche Werte sind:
   - **Voll**: Die auf dem System installierten Netzteile sind vom gleichen Typ und funktionieren ordnungsgemäß.
   - **Verloren**: Auf Systemen mit zwei Netzteileinheiten sind die auf dem System installierten Netzteile von unterschiedlichen Typen, oder eines davon ist defekt oder wurde entfernt. Auf Systemen mit vier Netzteileinheiten sind die auf dem System installierten Netzteile von unterschiedlichen Typen, oder zwei oder drei Einheiten sind defekt oder wurden entfernt.
   - **Deaktiviert**: Nur eines der Netzteile steht zur Verfügung. Keine Redundanz.
   - **Herabgesetzt** (nur auf Systemen mit vier Netzteileinheiten): Vier Netzteileinheiten sind auf dem System installiert, allerdings ist eine davon defekt oder wurde entfernt.
   - **Einzelne Netzteilelemente**: Mögliche Werte sind:
   - **Status** zeigt Folgendes an:
     - **OK** zeigt an, dass das Netzteil vorhanden ist und mit dem Server kommuniziert.
     - **Warnung** zeigt an, dass nur Warnmeldungen ausgegeben wurden und der Administrator Korrekturmaßnahmen ergreifen muss. Wenn keine Korrekturmaßnahmen ergriffen werden, könnte dies zu kritischen oder schwerwiegenden Stromausfällen und somit zu einer Beeinträchtigung der Integrität des Servers führen.

- **Schwerwiegend** zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Der Fehlerstatus zeigt einen Stromausfall des Servers an. Es müssen umgehend Korrekturmaßnahmen getroffen werden.

– **Standort** zeigt den Namen des Netzteils an: PS-n, wobei n die Nummer des Netzteils ist.

– **Typ** zeigt den Netzteiltyp an, z. B. AC oder DC (AC-DC- oder DC-DC-Spannungswandlung).

– **Eingangsleistung in Watt** zeigt die Eingangsleistung des Netzteils in Watt an, d. h. die höchste Wechselstromlast, die das System dem Datencenter auferlegen kann.

– **Max. Wattleistung** zeigt die maximale Leistung des Netzteils in Watt an, d. h. die dem System zur Verfügung stehende Gleichstromversorgung. Dieser Wert dient zur Bestätigung, dass ausreichend Stromkapazität für die Konfiguration des Systems verfügbar ist.

– **Online-Status** zeigt den Stromstatus der Netzteile an; vorhanden und OK, Eingang ausgefallen, fehlt oder absehbares Versagen.

– **FW-Version** zeigt die Firmware-Version des Netzteils an.

ANMERKUNG: Aufgrund der Netzteileffizienz entspricht die **Max. Wattleistung** nicht der **Eingangsleistung in Watt**. Beispiel: Wenn die Effizienz des Netzteils 89 % beträgt und die **Max. Wattleistung** 717 W, liegt die **Eingangsleistung in Watt** bei ungefähr 797 W.

RACADM verwenden

Öffnen Sie eine Telnet/SSH-Textkonsole für den iDRAC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm getconfig -g cfgServerPower
```

Strombudget anzeigen

Der Server enthält auf der Seite **Informationen zum Strombudget** Übersichten zum Status des Strombudgets für das Stromsubsystem.

Webschnittstelle verwenden

ANMERKUNG: Um Energieverwaltungsmaßnahmen auszuführen, benötigen Sie Administratorberechtigung.

1. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
2. Klicken Sie auf die Registerkarte **Strom**.
3. Wählen Sie die Option **Strombudget** aus.
4. Die Seite **Informationen zum Strombudget** wird angezeigt.

Die erste Tabelle enthält die Minimal- und Maximalgrenzwerte der vom Benutzer spezifizierten Strombegrenzungen für die aktuelle Systemkonfiguration. Diese stellen den Bereich des Netzstromverbrauchs dar, den Sie als Begrenzung für das System festlegen können. Wird die Begrenzung ausgewählt, entspricht sie der maximalen Netzstromlast, die dem Datacenter auferlegt werden kann.

Minimaler Stromverbrauch des Systems zeigt den niedrigsten Standardgrenzwert des Stromverbrauchs an.

Maximaler Stromverbrauch des Systems zeigt den höchsten Standardgrenzwert des Stromverbrauchs an. Dieser Wert ist auch der absolute maximale Stromverbrauch für die aktuelle Systemkonfiguration.

RACADM verwenden

Öffnen Sie eine Telnet/SSH-Textkonsole für den iDRAC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm getconfig -g cfgServerPower
```

ANMERKUNG: Weitere Informationen zu cfgServerPower, einschließlich Ausgabedetails, finden Sie unter cfgServerPower im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Strombudget-Schwellenwert

Wenn aktiviert, ermöglicht der Strombudget-Schwellenwert die Einstellung einer Strombegrenzung für das System. Die Systemleistung wird dynamisch angepasst, um den Stromverbrauch im Bereich des festgelegten Schwellenwerts zu halten. Der tatsächliche Stromverbrauch kann bei niedriger Auslastung geringer sein oder bei höherer Auslastung den Schwellenwert kurzzeitig überschreiten, bis entsprechende Leistungsanpassungen durchgeführt sind.

Wenn Sie **Aktiviert** für den Strombudgetschwellenwert markieren, erzwingt das System den benutzerspezifischen Schwellenwert. Bleibt der Strombudgetschwellenwert **unmarkiert**, begrenzt das System den Strom nicht. Beispiel: Eine gegebene Systemkonfiguration sieht 700 W für den höchsten potenziellen Stromverbrauch und 500 W für den geringsten potenziellen Stromverbrauch vor. Sie können einen Strombudgetschwellenwert festlegen und aktivieren, um den Verbrauch von derzeit 650 W auf 525 W zu senken. Ab diesem Punkt wird die Leistung des Systems dynamisch angepasst, um den Stromverbrauch unter dem benutzerspezifizierten Schwellenwert von 525 W zu halten.

Auf die webbasierte Schnittstelle zugreifen

1. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
2. Klicken Sie auf die Registerkarte **Strom**.
3. Wählen Sie die Option **Strombudget** aus. Die Seite **Informationen zum Strombudget** wird angezeigt.
4. Geben Sie einen Wert in Watt, BTU/h oder einen Prozentwert in die Tabelle **Strombudget** ein. Der von Ihnen angegebene Wert in Watt oder BTU/h stellt dann den Schwellenwert für das Strombudget dar. Wenn Sie einen Prozentwert angeben, ist dies ein Prozentsatz der Maximum-bis-Minimum-Spanne des potenziellen Stromverbrauchs. Beispiel: 100 % Schwellenwert bedeutet einen maximalen potenziellen Stromverbrauch, während 0 % einen minimalen potenziellen Stromverbrauch bedeutet.

   ANMERKUNG: Der Strombudgetschwellenwert kann nicht über dem maximalen potenziellen Stromverbrauch oder unter dem minimalen potenziellen Stromverbrauch liegen.

5 Wählen Sie **Aktiviert**, um den Schwellenwert zu aktivieren. Das System wendet den benutzerdefinierten Schwellenwert an. Wenn Sie die Markierung des Kontrollkästchens aufheben, wird für das System keine Stromgrenze festgelegt.

6 Klicken Sie auf **Änderungen übernehmen**.

RACADM verwenden

```
racadm config -g cfgServerPower -o
cfgServerPowerCapWatts <Strombegrenzungswert in Watt>

racadm config -g cfgServerPower -o
cfgServerPowerCapBTUhr <Strombegrenzungswert in BTU/h>

racadm config -g cfgServerPower -o
cfgServerPowerCapPercent <Strombegrenzungswert in % >

racadm config -g cfgServerPower -o
cfgServerPowerCapEnable <1 zum Aktivieren, 0 zum
Deaktivieren>
```

ANMERKUNG: Bei einem Strombudgetschwellenwert in BTU/h wird bei der Umrechung in Watt auf die nächste Ganzzahl aufgerundet. Bei der Rückumwandlung des Strombudgets von Watt in BTU/h erfolgt die Aufrundung in gleicher Weise. Folglich kann sich der geschriebene Wert nominal vom angezeigten Wert unterscheiden. Beispiel: Ein auf 600 BTU/h eingestellter Schwellenwert wird als 601 BTU/h angezeigt.

Stromüberwachung anzeigen

Webschnittstelle verwenden

So zeigen Sie die Energieüberwachungsdaten an:

1 Melden Sie sich an der iDRAC6-Webschnittstelle an.

2 Wählen Sie in der Systemstruktur **Stromüberwachung** aus. Die Seite **Stromüberwachung** wird angezeigt.

Im folgenden Abschnitt werden die auf der Seite **Stromüberwachung** verfügbaren Informationen beschrieben:

Stromüberwachung

- **Status**: **OK** weist darauf hin, dass Netzteile vorhanden sind und mit dem Server kommunizieren; **Warnung** weist darauf hin, dass eine Warnmeldung ausgegeben wurde, und **Schwerwiegend** weist darauf hin, dass eine Fehlermeldung ausgegeben wurde.
- **Sondenname**: Systemebene der Systemplatine. Diese Beschreibung weist darauf hin, dass die Sonde durch ihren Standort im System überwacht wird.
- **Messwert**: Der aktuelle Stromverbrauch in Watt/BTU/h.
- **Warnungsgrenzwert**: Zeigt den empfohlenen annehmbaren Stromverbrauch (in Watt und BTU/h) für den Systembetrieb an. Wenn der Stromverbrauch diesen Wert überschreitet, werden Warnungsereignisse ausgelöst.
- **Ausfallgrenzwert**: Zeigt den höchsten annehmbaren Stromverbrauch (in Watt und BTU/h) für den Systembetrieb an. Wenn der Stromverbrauch diesen Wert überschreitet, werden kritische Ereignisse/Fehlerereignisse ausgelöst.

Stromstärke (A)

- **Position**: Zeigt den Namen des Netzteils an: PS-n, wobei n die Nummer des Netzteils ist.
- **Messwert**: Der aktuelle Stromverbrauch in Ampere

Stromüberwachungsstatistik

- **Stromverbrauch** zeigt den aktuellen kumulativen Stromverbrauch für den Server an, gemessen von der Eingangsseite der Netzteileinheiten. Der Wert wird in kWh angegeben und ist ein kumulativer Wert, der die gesamte vom System verbrauchte Energie angibt. Dieser Wert kann mit der Schaltfläche **Reset** zurückgesetzt werden.
- **Spitzenstrom des Systems** gibt den maximalen 1-Minuten-Durchschnitt des Stroms für das System seit der Startzeit der Messung an. Dieser Wert kann mit der Schaltfläche **Reset** zurückgesetzt werden.
- **Spitzenstromstärke des Systems** gibt die Spitzenstromstärke innerhalb des Intervalls zwischen Startzeit und Spitzenzeiten an. Dieser Wert kann mit der Schaltfläche **Reset** zurückgesetzt werden.

- **Startzeit der Messung** zeigt das gespeicherte Datum und die gespeicherte Uhrzeit an, zu der die Statistik zuletzt gelöscht wurde und der neue Messzyklus begann. Für **Stromverbrauch** können Sie diesen Wert mit der Schaltfläche **Reset** zurücksetzen. Der Wert bleibt jedoch bei einem System-Reset oder einem Failover-Vorgang erhalten. Für **Spitzenstrom des Systems** und **Spitzenstromstärke des Systems** können Sie diesen Wert mit der Schaltfläche **Reset** zurücksetzen. Der Wert bleibt jedoch bei einem System-Reset oder einem Failover-Vorgang erhalten.
- **Beendigungszeit der Messung** zeigt das aktuelle Datum und die Uhrzeit an, als der Systemstromverbrauch für die Anzeige berechnet wurde. **Spitzenzeit** zeigt die Uhrzeit an, als die Spitze auftrat.

ANMERKUNG: Stromüberwachungsstatistiken bleiben über mehrere System-Resets erhalten und zeigen daher alle Aktivitäten im Intervall zwischen den angegebenen Start- und Endzeiten an. Die Schaltfläche **Reset** setzt das entsprechende Feld auf Null zurück. In der nächsten Tabelle werden die Stromverbrauchsdaten nicht über mehrere System-Resets aufrechterhalten. Sie werden daher bei einem System-Reset auf Null zurückgesetzt. Die angezeigten Stromwerte sind kumulative Durchschnittswerte im jeweiligen Zeitintervall (vorangehende 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)

- Zeigt den durchschnittlichen, maximalen und minimalen Stromverbrauch im System für die letzte Minute, letzte Stunde, den letzten Tag und die letzte Woche an.
- Durchschnittlicher Stromverbrauch: Durchschnitt während der vorhergehenden Minute, der vorhergehenden Stunde, des vorhergehenden Tages und der vorhergehenden Woche.
- Maximaler und minimaler Stromverbrauch: Der maximale und minimale Stromverbrauch, der im gegebenen Zeitintervall gemessen wurde.
- Zeit des maximalen und minimalen Stromverbrauchs: Die Zeit, zu welcher der maximale und minimale Stromverbrauch aufgetreten ist.

Aussteuerungsreserve

- **Momentaner Aussteuerungsreserve des Systems** zeigt den Unterschied zwischen der in den Netzteilen verfügbaren Leistung und dem aktuellen Stromverbrauch des Systems an.
- **Spitzenaussteuerungsreserve des Systems** zeigt den Unterschied zwischen der in den Netzteilen verfügbaren Leistung und dem Spitzenstromverbrauch des Systems an.

Diagramm anzeigen

Klicken Sie auf **Diagramm anzeigen**, um Diagramme anzuzeigen, die den iDRAC6-Stromverbrauch während der vergangenen Stunde in Watt bzw. Ampere veranschaulichen. Der Benutzer kann die Statistiken bis zu einer Woche im Rückblick einsehen, indem er das Dropdown-Menü verwendet, das oberhalb der Diagramme zur Verfügung steht.

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.

RACADM verwenden

Öffnen Sie eine Telnet/SSH-Textkonsole für den iDRAC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm getconfig -g cfgServerPower
```

Weitere Informationen zu **cfgServerPower**, einschließlich Ausgabedetails, finden Sie unter **cfgServerPower** im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Durchführen von Stromsteuerungsmaßnahmen am Server

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchzuführen, müssen Sie über die Berechtigung **Gehäusesteuerungs-Administrator** verfügen.

Mit dem iDRAC6 können im Remote-Zugriff mehrere Stromverwaltungsmaßnahmen durchgeführt werden, z. B. ordnungsgemäßes Herunterfahren.

Webschnittstelle verwenden

1. Melden Sie sich an der iDRAC6-Webschnittstelle an.
2. Klicken Sie auf die Registerkarte **Strom**. Die Seite **Stromsteuerung** wird angezeigt.
3. 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 Server ausgeschaltet ist). Diese Option ist deaktiviert, wenn der Server 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.
   - **Sanftes Herunterfahren** fährt das System herunter.

     ANMERKUNG: Stellen Sie sicher, dass die Option zum Herunterfahren für das Betriebssystem konfiguriert ist, bevor Sie unter Verwendung dieser Option das System ordentlich herunterfahren. Wenn Sie diese Option verwenden, ohne sie auf dem Betriebssystem zu konfigurieren, startet es das verwaltete System neu anstatt den Vorgang zum Herunterfahren auszuführen.
   - **System zurücksetzen (Softwareneustart)** – Führt einen Reset des Systems aus, ohne es auszuschalten. Diese Option ist deaktiviert, wenn das System bereits ausgeschaltet ist.
   - **System aus- und einschalten** [**Hardware-Neustart**]) – Schaltet das System aus und startet es daraufhin neu. Diese Option ist deaktiviert, wenn das System bereits ausgeschaltet ist.
4. Klicken Sie auf **Anwenden**. Daraufhin werden Sie von einem Dialogfeld zur Bestätigung aufgefordert.
5. Klicken Sie auf **OK**, um die gewählte Stromverwaltungsmaßnahme auszuführen (z. B. das System zurückzusetzen).

RACADM verwenden

Öffnen Sie eine Telnet/SSH-Textkonsole zum Server, melden Sie sich an und geben Sie Folgendes ein:

```
racadm serveraction <Maßnahme>
```

`wobei` <Maßnahme> Einschalten, Herunterfahren, Aus-/Einschalten, Hardware-Neustart oder Stromstatus ist.

17

iDRAC6-Konfigurationsdienstprogramm verwenden

Übersicht

Das iDRAC6-Konfigurationsdienstprogramm ist eine Vorstart-Konfigurationsumgebung, die es ermöglicht, Parameter für den iDRAC6 und den verwalteten Server anzuzeigen und einzustellen. Genauer gesagt können Sie:

- Firmware-Revisionsnummern für die Firmware des iDRAC6 und der primären Rückwandplatine anzeigen
- Das lokale Netzwerk des iDRAC6 aktivieren oder deaktivieren
- IPMI über LAN aktivieren oder deaktivieren
- LAN-Parameter konfigurieren
- Autom. Ermittlung aktivieren oder deaktivieren und den Bereitstellungsserver konfigurieren.
- Virtuelle Datenträger konfigurieren
- Smart Card konfigurieren
- Den administrativen Benutzernamen bzw. das administrative Kennwort ändern
- iDRAC6-Konfiguration auf die Werkseinstellungen zurücksetzen
- SEL-Meldungen (Systemereignisprotokoll) anzeigen oder Meldungen aus dem Protokoll löschen
- LCD konfigurieren
- Systemdienste konfigurieren

Die Aufgaben, die Sie mit dem iDRAC6-Konfigurationshilfsprogramm ausführen können, können auch mit anderen Dienstprogrammen der iDRAC6- oder Dell OpenManage-Software ausgeführt werden, einschließlich der webbasierten Schnittstelle, der SM-CLP-Befehlszeilenoberfläche und der lokalen und Remote-RACADM-Befehlszeilenoberfläche.

iDRAC6-Konfigurationsdienstprogramm starten

1. Schalten Sie den Server ein oder starten Sie ihn neu, indem Sie an seiner Vorderseite den Netzschalter drücken.
2. Wenn Sie die Meldung **Für Remote-Zugriffs-Setup innerhalb von 5 Sek. <Strg-E> drücken...** sehen,drücken Sie unverzüglich **<Strg><E>**.

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.

Daraufhin wird das Fenster **iDRAC6-Konfigurationsdienstprogramm** angezeigt. Die ersten beiden Zeilen enthalten Informationen zur iDRAC6-Firmware und zu den 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, die für externe Schnittstellen zuständig ist, z. B. die webbasierte Schnittstelle, 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-Konfigurationsdienstprogramm verwenden

Unterhalb der Firmware-Revisionsmeldungen besteht der Rest des iDRAC6-Konfigurationsdienstprogramms aus einem Menü von Elementen, auf die Sie über <Pfeil nach oben> und <Pfeil nach unten> 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 <Pfeil nach links>, <Pfeil nach rechts> 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-Konfigurationsdienstprogramms fertig sind, drücken Sie auf <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-Konfigurationsdienstprogramms beschrieben.

iDRAC6-LAN

Verwenden Sie <Pfeil nach links> und <Pfeil nach rechts> sowie die Leertaste, um zwischen **Ein** und **Aus** auszuwählen.

Das iDRAC6-LAN ist in der Standardkonfiguration aktiviert. Das LAN muss aktiviert sein, um die Verwendung von iDRAC6-Einrichtungen, wie z. B. webbasierte Schnittstelle, Telnet/SSH, virtuelle Konsole und virtueller Datenträger, zu ermöglichen.

Wenn Sie sich entscheiden, das LAN zu deaktivieren, wird die folgende Warnung angezeigt:

```
iDRAC6-bandexterne Schnittstelle wird deaktiviert,
wenn der LAN-Kanal AUS ist.

Drücken Sie auf eine beliebige Taste, um die Meldung
zu löschen und fortzufahren.
```

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-Schnittstellen zugreifen, der bandexterne Verwaltungsnetzwerkdatenverkehr (z. B. IPMI-Meldungen, die von einer Management Station aus an den iDRAC6 gesendet werden) 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.

IPMI über LAN

Verwenden Sie <Pfeil nach links> und <Pfeil nach rechts> sowie die Leertaste, um zwischen **Ein** und **Aus** zu wählen. Wenn **Aus** ausgewählt ist, akzeptiert der iDRAC6 keine IPMI-Meldungen, die über die LAN-Schnittstelle eingehen.

Wenn Sie **Aus** auswählen, wird die folgende Warnung angezeigt:

```
Die bandexterne iDRAC6-IPMI-Schnittstelle wird
deaktiviert, wenn IPMI-über-LAN AUS ist.
```

Drücken Sie auf eine beliebige Taste, um die Meldung zu löschen und fortzufahren. Unter „iDRAC6-LAN“ auf Seite 339 finden Sie eine Erklärung der Meldung.

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 17-1. LAN-Parameter

Element	Beschreibung
Allgemeine Einstellungen	
NIC-Auswahl	Drücken Sie <Pfeil nach rechts>, <Pfeil nach links> und die Leertaste, um zwischen den Modi umzuschalten. Die verfügbaren Modi sind: **Dediziert**, **Freigegeben**, **Freigegeben für Failover**: **LOM2** und **Freigegeben für Failover**: **Alle LOMs**. Diese Modi ermöglichen dem iDRAC6, die entsprechende Schnittstelle für die Datenübertragung nach außen zu verwenden.
MAC-Adresse	Dies ist die nicht bearbeitbare MAC-Adresse der iDRAC6-Netzwerkschnittstelle.
VLAN aktivieren	Wählen Sie **Ein**, um die virtuelle LAN-Filterung für den iDRAC6 zu verwenden.
VLAN-ID	Wenn **VLAN aktivieren** auf **Ein** gesetzt ist, geben Sie einen beliebigen VLAN ID-Wert zwischen 1 und 4094 ein.
VLAN Priority (VLAN-Priorität)	Wenn **VLAN aktivieren** auf **Ein** gesetzt ist, legen Sie die Priorität des VLAN auf einen Wert zwischen 0 und 7 fest.
iDRAC6-Namen registrieren	Wählen Sie **Ein**, um den iDRAC6-Namen im DNS-Dienst zu registrieren. Wählen Sie **Aus**, wenn Sie nicht möchten, dass Benutzer den iDRAC6-Namen im DNS auffinden.

Tabelle 17-1. LAN-Parameter *(fortgesetzt)*

Element	Beschreibung
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.
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.**

Tabelle 17-1. LAN-Parameter *(fortgesetzt)*

Element	Beschreibung
Verschlüsselungs-schlüssel 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-Adressen-Quelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse ein, die dem iDRAC6 zugewiesen werden soll. Die Standardadresse ist **192.168.0.120**.
Subnetzmaske	Wenn die **IP-Adressenquelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene Subnetzmaskenadresse an. Wenn die **IP-Adressen-Quelle** 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.

Tabelle 17-1. LAN-Parameter *(fortgesetzt)*

Element	Beschreibung
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:	Aktivieren oder deaktivieren Sie die Unterstützung für die IPv6-Verbindung.
IP-Adressen-Quelle	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-Adressen-Quelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse ein, die dem iDRAC6 zugewiesen werden soll.
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	Dies ist die nicht bearbeitbare **IPv6-Adresse 2** der iDRAC6-Netzwerkschnittstelle.
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.

Tabelle 17-1. LAN-Parameter *(fortgesetzt)*

Element	Beschreibung
DNS-Server 2	Wenn **DNS-Server von DHCP** auf **Aus** gesetzt ist, geben Sie die IP-Adresse des ersten DNS-Servers ein.
Erweiterte LAN-Konfigurationen	
Automatische Verhandlung	Wenn **NIC-Auswahl** auf **Dediziert** gesetzt ist, wählen Sie **Aktiviert** bzw. **Deaktiviert** aus. Ist **Aktiviert** ausgewählt, werden **LAN-Taktrateneinstellung** und **LAN-Duplexeinstellung** automatisch konfiguriert.
LAN-Taktrateneinstellung	Wenn **Automatische Verhandlung** auf **Deaktiviert** eingestellt ist, wählen Sie zwischen 10 Mbit/s und 100 Mbit/s.
LAN-Duplexeinstellung	Ist **Automatische Verhandlung** auf **Deaktiviert** eingestellt, wählen Sie **Halb-Duplex oder Voll-Duplex**.

Konfiguration virtueller Laufwerke

Virtueller Datenträger

Drücken Sie die Eingabetaste, um **Abgetrennt, Verbunden** oder **Automatisch verbunden** auszuwählen. Wenn Sie **Verbunden** auswählen, werden die virtuellen Datenträgergeräte mit dem USB-Bus verbunden. Hierdurch werden sie während Sitzungen der **virtuellen Konsole** verfügbar gemacht.

Wenn Sie **Abgetrennt** auswählen, können Benutzer während Sitzungen der **virtuellen Konsole** nicht auf virtuelle Datenträgergeräte zugreifen.

ANMERKUNG: Um ein USB-Flash-Laufwerk mit der Funktion **Virtueller Datenträger** zu verwenden, muss der **Emulationstyp des USB-Flash-Laufwerks** im BIOS-Setup-Dienstprogramm auf **Festplatte** eingestellt sein. Sie können auf das BIOS-Setup-Dienstprogramm zugreifen, indem Sie während des Serverstarts <F2> drücken. Wenn der **Emulationstyp des USB-Flash-Laufwerks** auf **Automatisch** eingestellt ist, erscheint das Flash-Laufwerk dem System als Floppy-Laufwerk.

vFlash

Drücken Sie die Eingabetaste, 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 als 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-Anmeldung

Drücken Sie die Eingabetaste, um **Aktiviert** oder **Deaktiviert** auszuwählen. Mit dieser Option wird die Smart Card-Anmeldung konfiguriert.
Die verfügbaren Optionen sind **Aktiviert**, **Deaktiviert** und **Mit RACADM aktiviert**.

ANMERKUNG: Wenn Sie Aktiviert oder Mit RACADM aktiviert auswählen, wird IPMI-über-LAN ausgeschaltet und für die Bearbeitung gesperrt.

Konfiguration der Systemdienste

System Services (Systemdienste)

Drücken Sie die Eingabetaste, um **Aktiviert** oder **Deaktiviert** auszuwählen. Weitere Informationen finden Sie im *Dell Lifecycle Controller-Benutzerhandbuch*, das auf der Dell Support-Website unter **dell.com/support/manuals** zur Verfügung steht.

ANMERKUNG: Eine Änderung dieser Option bewirkt, dass der Server neu gestartet wird, wenn Sie auf **Speichern** und **Beenden** klicken, um die neuen Einstellungen zu übernehmen.

ANMERKUNG: Wenn Sie wählen, eine Wiederherstellung auf die Werkseinstellungen durchzuführen, ändern sich die Einstellungen für die Systemdienste nicht.

Systemdienste abbrechen

Drücken Sie <Eingabe>, um **Nein** oder **Ja** auszuwählen.

Wenn Sie **Ja** auswählen, werden alle Sitzungen von Unified Server Configurator geschlossen und der Server wird neu gestartet, wenn Sie auf **Speichern** und **Beenden** klicken, um die neuen Einstellungen zu übernehmen.

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** zur Verfügung steht.

ANMERKUNG: Durch das Modifizieren dieser Option wird der Server neu gestartet, nachdem Sie Ihre Einstellungen gespeichert und das iDRAC6-Konfigurationsdienstprogramm beendet haben.

ANMERKUNG: Wenn Sie wählen, eine Wiederherstellung der Werkseinstellungen durchzuführen, ändern sich die Einstellungen für "Systembestandsaufnahmedaten bei Neustart sammeln" nicht.

LCD-Konfiguration

Drücken Sie die Eingabetaste, um das Untermenü der **LAN-Konfiguration** anzuzeigen. Wenn Sie die Konfiguration der LCD-Parameter abgeschlossen haben, drücken Sie <Esc>, um zum vorhergehenden Menü zurückzukehren.

Tabelle 17-2. LCD-Benutzerkonfiguration

LCD-Zeile 1	Drücken Sie <Pfeil nach rechts>, <Pfeil nach links> und die Leertaste, um zwischen den Optionen umzuschalten. Diese Funktion setzt den **Home**-Bildschirm des LCD auf eine der folgenden Optionen: **Umgebungstemp., Systemkennnummer, Host-Name, iDRAC6-IPv4-Adresse, iDRAC6-IPv6-Adresse, iDRAC6-MAC-Adresse, Modellnummer, Keine, Service-Tag-Nummer, Systemstrom, Benutzerdefinierte Zeichenkette**.

Benutzerdefinierte LCD-Zeichenkette	Zeigen Sie die im LCD-Bedienfeld anzuzeigende Zeichenkette an, oder geben Sie sie ein. Die Zeichenkette kann maximal 62 Zeichen aufweisen.
LCD-Systemnetzteileinheiten	Wählen Sie **Watt** oder **BTU/h**, um die im LCD-Bedienfeld anzuzeigende Einheit anzugeben.
LCD-Umgebungstemperatureinheiten	Wählen Sie **Celsius** oder **Fahrenheit**, um die im LCD-Bedienfeld anzuzeigende Einheit anzugeben.
LCD-Fehleranzeige	Wählen Sie **Einfach** oder **SEL** (Systemereignisprotokoll) aus. Diese Funktion ermöglicht die Anzeige von Fehlermeldungen auf dem LCD in einem von zwei Formaten: Das Format „Einfach“ zeigt eine Beschreibung des Ereignisses. Das Format „SEL“ ruft eine Textzeichenkette des Systemereignisprotokolls auf.
LCD-Remote-Indikation der virtuellen Konsole	Wählen Sie **Aktiviert** aus, um den Text *Virtuelle Konsole* immer dann anzuzeigen, wenn auf der Einheit eine virtuelle Konsole aktiv ist.
LCD-Frontblendenzugriff	Drücken Sie <Pfeil nach rechts>, <Pfeil nach links> und die Leertaste, um zwischen den Optionen **Deaktiviert**, **Anzeigen und Ändern** und **Nur anzeigen** zu wechseln. Diese Einstellung definiert die Benutzerberechtigungsebene für das LCD.

LAN-Benutzerkonfiguration

Der LAN-Benutzer ist das iDRAC6-Administratorkonto, das standardmäßig **root** lautet. 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.

Auf Standardeinstellung zurücksetzen

Verwenden Sie das Menü **Auf Standardeinstellung zurücksetzen**, um alle iDRAC6-Konfigurationselemente auf die Werkseinstellungen zurückzusetzen. Dies ist eventuell dann erforderlich, wenn Sie zum Beispiel das Kennwort des administrativen Benutzers vergessen haben oder den iDRAC6 mit den Standardeinstellungen neu konfigurieren möchten.

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 **JA** aus und drücken Sie <Eingabe>, um den iDRAC6 auf die Standardeinstellungen zurückzusetzen.

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 <Eingabe>. Verwenden Sie <Pfeil nach links>, um zur vorhergehenden (früheren) Meldung zu wechseln, und <Pfeil nach rechts>, um zur nächsten (neueren) Meldung zu wechseln. Geben Sie eine Eintragsnummer an, um zu diesem Eintrag zu wechseln. Drücken Sie <Esc>, wenn Sie mit dem Anzeigen von SEL-Meldungen fertig sind.

Wählen Sie zum Löschen des SEL **Systemereignisprotokoll löschen** aus, und drücken Sie <Eingabe>.

Wenn Sie mit der Verwendung des SEL-Menüs fertig sind, drücken Sie <Esc>, um zum vorhergehenden Menü zurückzukehren.

Tabelle 17-3. 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 erstellt wurde, kann eine Remotekonsole mit den im Ermittlungsprozess angegebenen Anmeldeinformationen eine WS-MAN-Datenverbindung mit dem iDRAC6 herstellen und dann die sicheren Anweisungen 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 • IPv4 aktivieren • 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 Autom. Ermittlung 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 17-3. LAN-Benutzerkonfiguration *(fortgesetzt)*

Element	Beschreibung
Autom. Ermittlung *(fortgesetzt...)*	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 von IPv4-Adressen oder ein Host-Name sein und darf nicht mehr als 255 Zeichen betragen. Jede Adresse ist durch ein Komma zu trennen. Falls die Funktion Autom. Ermittlung aktiviert ist und nachdem dieser Prozess erfolgreich abgeschlossen wurde, werden die Benutzeranmeldeinformationen vom konfigurierten Bereitstellungsserver abgerufen, um zukünftige Remote-Bereitstellungen zu ermöglichen. Weitere Informationen finden Sie im *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 die Autom. Ermittlung aktiviert ist.
Kontoberechtigung	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 nicht auf der Anzeige wiedergegeben, während Sie sie eingeben.
Kennwort bestätigen	Geben Sie das neue Kennwort für das Administratorkonto erneut ein. Wenn die eingegeben Zeichen nicht mit den im Feld **Kennwort eingeben** eingegebenen Zeichen übereinstimmen, wird eine Meldung angezeigt und das Kennwort muss erneut eingegeben werden.

iDRAC6-Konfigurationsdienstprogramm beenden

Wenn Sie mit den Änderungen der iDRAC6-Konfiguration fertig sind, drücken Sie <Esc>, um das Menü „Beenden“ anzuzeigen.

- Wählen Sie **Änderungen speichern und beenden** aus und drücken Sie <Eingabe>, um Ihre Änderungen beizubehalten. Wenn dieser Vorgang fehlschlägt, wird eine der folgenden Meldungen angezeigt:
  - iDRAC6-Kommunikationsfehler – wird angezeigt, wenn nicht auf den iDRAC zugegriffen werden kann.
  - Einige der Einstellungen können nicht übernommen werden – wird angezeigt, wenn einige Einstellungen nicht übernommen werden können.
- Wählen Sie **Änderungen ablehnen und beenden** aus und drücken Sie <Eingabe>, um alle vorgenommenen Änderungen zu ignorieren.
- Wählen Sie **Zum Setup zurückkehren** aus und drücken Sie <Eingabe>, um zum iDRAC6-Konfigurationsdienstprogramm zurückzukehren.

18

Überwachungs- und Warnungsverwaltung

Dieser Abschnitt erklärt, wie der iDRAC6 überwacht wird, und enthält Verfahren zur Konfiguration des Systems und des iDRAC6 für den Empfang von Warnungen.

Das verwaltete System zur Erfassung des Bildschirms „Letzter Absturz“ konfigurieren

Bevor der iDRAC6 den Bildschirm „Letzter Absturz“ erfassen kann, müssen Sie die folgenden Voraussetzungen auf dem verwalteten System konfigurieren.

1. Installieren Sie die Managed System-Software. Weitere Informationen über das Installieren der Managed System-Software finden Sie im *Server Administrator-Benutzerhandbuch*.
2. Führen Sie ein unterstütztes Microsoft Windows-Betriebssystem aus, bei dem die Windows-Funktion *Automatisch neustarten* in den **Windows-Start- und Wiederherstellungseinstellungen** deaktiviert ist.
3. Aktivieren Sie den Bildschirm „Letzter Absturz“ (standardmäßig deaktiviert).

   Um die Verwendung des Bildschirms „Letzter Absturz“ mittels lokalem RACADM zu aktivieren, öffnen Sie eine Eingabeaufforderung und geben die folgenden Befehle ein:

   ```
   racadm config -g cfgRacTuning -o
   cfgRacTuneAsrEnable 1
   ```

4. Aktivieren Sie den Zeitgeber für die automatische Wiederherstellung und setzen Sie die Maßnahme **Automatische Wiederherstellung** auf **Reset**, **Herunterfahren** oder **Aus- und Einschaltzyklus**. Zum Konfigurieren des Zeitgebers für **Automatische Wiederherstellung** müssen Sie Server Administrator oder IT Assistant verwenden.

   Informationen zur Konfiguration des Zeitgebers für **Autom. Wiederherstellung** finden Sie im *Server Administrator-Benutzerhandbuch*.

Um sicherzustellen, dass der Bildschirm „Letzter Absturz“ erfasst werden kann, muss der Zeitgeber für **Automatische Wiederherstellung** auf mindestens 60 Sekunden eingestellt werden. Die Standardeinstellung ist 480 Sekunden.

Der Bildschirm „Letzter Absturz“ ist bei einem Absturz des verwalteten Systems nicht verfügbar, wenn die Maßnahme **Automatische Wiederherstellung** auf **Herunterfahren** oder **Aus- und Einschalten** gesetzt ist.

Die Windows-Option "Automatischer Neustart" deaktivieren

Um sicherzustellen, dass die Funktion Bildschirm „Letzter Systemabsturz“ der webbasierten iDRAC6-Schnittstelle richtig funktioniert, deaktivieren Sie die Option **Automatischer Neustart** auf verwalteten Systemen, auf denen die Betriebssysteme Microsoft Windows Server 2008 oder Windows Server 2003 ausgeführt werden.

Die Option „Automatisch Neustart durchführen“ in Windows Server 2008 deaktivieren

1. Öffnen Sie die Windows-**Systemsteuerung** und doppelklicken Sie auf das **System**-Symbol.
2. Klicken Sie unter **Aufgaben** auf der linken Seite auf **Erweiterte Systemeinstellungen**.
3. Klicken Sie auf die Registerkarte **Advanced** (Erweitert).
4. Klicken Sie unter **Autostart und Wiederherstellung** auf **Einstellungen**.
5. Wählen Sie das Kontrollkästchen **Automatisch Neustart durchführen** ab.
6. Klicken Sie zweimal auf **OK**.

Die Option „Automatischer Neustart“ in Windows Server 2003 deaktivieren

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**.

Plattformereignisse konfigurieren

Die Konfiguration von Plattformereignissen bietet eine Möglichkeit, das Remote-Zugriffsgerät so zu konfigurieren, dass ausgewählte Maßnahmen beim Auftreten bestimmter Ereignismeldungen ausgeführt werden. Diese Maßnahmen umfassen Neustart, Aus-/Einschalten, Herunterfahren und Auslösen einer Warnung (Plattformereignis-Trap [PET] und/oder E-Mail).

Die filterbaren Plattformereignisse umfassen:

1 Assertionsfilter Lüfter kritisch

2 Assertionsfilter Batteriewarnung

3 Assertionsfilter Batterie kritisch

4 Assertionsfilter Spannung kritisch

5 Assertionsfilter Temperaturwarnung

6 Assertionsfilter Temperatur kritisch

7 Assertionsfilter Eingriff kritisch

8 Filter Redundanz herabgesetzt

9 Filter Redundanz verloren

10 Assertionsfilter Prozessorwarnung

11 Assertionsfilter Prozessor kritisch

12 Assertionsfilter Prozessor nicht vorhanden/kritisch

13 Assertionsfilter Netzteilwarnung

14 Assertionsfilter Netzteil kritisch

15 Assertionsfilter Netzteil nicht vorhanden/kritisch

16 Assertionsfilter Ereignisprotokoll kritisch

17 Assertionsfilter Watchdog kritisch

18 Assertionsfilter Systemstromwarnung

19 Assertionsfilter Systemstrom kritisch

20 Assertionsfilter wechselbarer Flash-Datenträger nicht vorhanden – Zur Information

21 Assertionsfilter wechselbarer Flash-Datenträger – Kritisch

22 Assertionsfilter wechselbarer Flash-Datenträger – Warnung

Wenn ein Plattformereignis auftritt (z. B. ein Lüftersondenfehler), wird ein Systemereignis erstellt und im Systemereignisprotokoll (SEL) verzeichnet. Wenn dieses Ereignis einem Plattformereignisfilter (PEF) in der Liste der Plattformereignisfilter entspricht und Sie diesen Filter für die Generierung einer Warnung (PET oder E-Mail) konfiguriert haben, dann wird eine PET- oder E-Mail-Warnung an ein konfiguriertes Ziel bzw. an 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

Konfigurieren Sie Ihre Plattformereignisfilter, bevor Sie die Einstellungen für Plattformereignis-Traps oder E-Mail-Warnungen konfigurieren.

PEF mittels webbasierter Schnittstelle konfigurieren

Ausführliche Informationen finden Sie unter „Plattformereignisfilter (PEF) konfigurieren“ auf Seite 60.

PEF mittels RACADM-CLI konfigurieren

1 Aktivieren Sie PEF.

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i
1 1
```

wobei `1` und `1` für den PEF-Index bzw. für die Auswahloption „aktivieren/deaktivieren“ stehen.

Der PEF-Index kann einen Wert zwischen 1 und 22 annehmen. Die Auswahloption „aktivieren/deaktivieren“ kann auf 1 (aktiviert) oder 0 (deaktiviert) eingestellt werden.

Beispiel: Um PEF mit dem Index 5 zu aktivieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i
5 1
```

2 Konfigurieren Sie die PEF-Maßnahmen.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i
1 <Maßnahme>
```

wobei die <*Maßnahme*>-Wertbits wie folgt lauten:

- 0 = Keine Warnungsmaßnahme
- 1 = Server ausschalten
- 2 = Server neu starten
- 3 = Server aus- und einschalten

Beispiel: Um PEF zum Neustarten des Servers zu aktivieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i
1 2
```

wobei `1` der PEF-Index ist und 2 die PEF-Maßnahme für den Neustart.

PET konfigurieren

PET mittels der Internet-Benutzeroberfläche konfigurieren

Ausführliche Informationen finden Sie unter „Plattformereignis-Traps (PET) konfigurieren“ auf Seite 61.

PET mittels RACADM-CLI konfigurieren

1 Aktivieren Sie die globalen Warnungen.

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanAlertEnable 1
```

2 Aktivieren Sie PET.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, und drücken Sie nach jedem Befehl auf die Eingabetaste:

```
IPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 1 1
```

```
IPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIpv6PetAlertEnable -i 1 1
```

wobei `1` und `1` für den PET-Zielindex bzw. für die Auswahloption „aktivieren/deaktivieren“ stehen.

Der PET-Zielindex kann ein Wert von 1 bis 4 sein. Die Auswahloption „aktivieren/deaktivieren“ kann auf 1 (aktiviert) oder 0 (deaktiviert) gesetzt werden.

Beispiel: Um PET mit dem Index 4 zu aktivieren, geben Sie den folgenden Befehl ein:

```
iPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 4 1
```

```
iPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIpv6PetAlertEnable -i 4 1
```

3 Konfigurieren Sie die PET-Regel.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie <Eingabe>:

```
iPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertDestIPAddr -i 1 <IPv4_Adresse>
```

```
iPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIPv6AlertDestIPAddr -i 1 <IPv6_Adresse>
```

wobei `1` der PET-Zielindex und *<IPv4_Adresse>* und *<IPv6_Adresse>* die Ziel-IP-Adressen des Systems sind, das die Plattformereigniswarnungen empfängt.

4 Konfigurieren Sie die Community-Namen-Zeichenkette.

Geben Sie Folgendes in die Befehlszeile ein:

```
racadm config -g cfgIpmiLan -o
cfgIpmiPetCommunityName <Name>
```

E-Mail-Warnungen konfigurieren

E-Mail-Warnungen mittels der Internet-Benutzeroberfläche konfigurieren

Ausführliche Informationen finden Sie unter „Konfiguration von E-Mail-Warnungen“ auf Seite 62.

E-Mail-Warnungen mittels RACADM-CLI konfigurieren„aktivieren/deaktivieren“

1. Aktivieren Sie die globalen Warnungen.

   Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

   ```
   racadm config -g cfgIpmiLan -o
   cfgIpmiLanAlertEnable 1
   ```

2. Aktivieren Sie E-Mail-Warnungen.

   Geben Sie an der Eingabeaufforderung die folgenden Befehle ein und drücken Sie nach jedem Befehl die Eingabetaste:

   ```
   racadm config -g cfgEmailAlert -o
   cfgEmailAlertEnable -i 1 1
   ```

   wobei `1` und `1` für den E-Mail-Zielindex bzw. für die Auswahloption „aktivieren/deaktivieren“ stehen.

   Der E-Mail-Zielindex kann ein Wert von 1 bis 4 sein. Die Auswahloption „aktivieren/deaktivieren“ kann auf 1 (aktiviert) oder 0 (deaktiviert) gesetzt werden.

   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.

   Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie <Eingabe>:

   ```
   racadm config -g cfgEmailAlert -o
   cfgEmailAlertAddress -i 1 <E-Mail-Adresse>
   ```

wobei `1` der E-Mail-Zielindex ist und *<E-Mail-Adresse>* die Ziel-E-Mail-Adresse, die die Plattformereigniswarnungen empfängt.

Um eine kundenspezifische Meldung zu konfigurieren, geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertCustomMsg -i 1
<Kundenspezifische_Meldung>
```

wobei `1` der E-Mail-Zielindex ist und *<Kundenspezifische_Meldung>* die Meldung, die in der E-Mail-Warnung angezeigt wird.

Testen von E-Mail-Warnmeldungen

Mit der RAC-E-Mail-Warnungsfunktion können Benutzer E-Mail-Warnungen erhalten, wenn auf dem verwalteten System ein kritisches Ereignis auftritt. Das folgende Beispiel zeigt, wie man die E-Mail-Warnungsfunktion testet, um sicherzustellen, dass der RAC ordnungsgemäß E-Mail-Warnungen über das Netzwerk versenden kann.

```
racadm testemail -i 2
```

ANMERKUNG: Stellen Sie sicher, dass die SMTP- und E-Mail-Warnungs-Einstellungen konfiguriert sind, bevor die E-Mail-Warnungsfunktion getestet wird. Weitere Informationen finden Sie unter „E-Mail-Warnungen konfigurieren" auf Seite 361.

RAC-SNMP-Trap-Warnungsfunktion testen

Die RAC-SNMP-Trap-Warnungsfunktion ermöglicht SNMP-Trap-Listener-Konfigurationen, Traps für Systemereignisse zu empfangen, die auf dem verwalteten System auftreten.

Das folgende Beispiel veranschaulicht, wie ein Benutzer die SNMP-Trap-Warnungsfunktion des RAC testen kann.

```
racadm testtrap -i 2
```

Stellen Sie vor dem Testen der RAC-SNMP-Trap-Warnungsfunktion sicher, dass die SNMP- und Trap-Einstellungen ordnungsgemäß konfiguriert sind. Informationen zum Konfigurieren dieser Einstellungen finden Sie in den Unterbefehlsbeschreibungen für testtrap und testemail im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

Häufig gestellte Fragen zur SNMP-Authentifizierung

Warum wird die folgende Meldung angezeigt?

`Remote-Zugriff: SNMP-Authentifizierungsfehler`

Als Teil der Ermittlung versucht IT Assistant, die Get- und Set-Community-Namen des Geräts zu überprüfen. In IT Assistant gibt es den Get-**Community-Name = public** und den Set-**Community-Name = private**. Standardmäßig ist der Community-Name für den iDRAC6-Agenten **public**. Wenn IT Assistant eine Set-Anforderung sendet, erstellt der iDRAC6-Agent den SNMP-Authentifizierungsfehler, weil er nur Anforderungen von **Community = public** akzeptiert.

ANMERKUNG: Dies ist der Community-Name des SNMP-Agenten.

Sie können den iDRAC6-Community-Namen mittels RACADM ändern.

Um den iDRAC6-Community-Namen anzuzeigen, geben Sie den folgenden Befehl ein:

```
racadm getconfig -g cfgOobSnmp
```

Um den iDRAC6-Community-Namen festzulegen, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgOobSnmp -o
cfgOobSnmpAgentCommunity <Community-Name>
```

Um auf den Community-Namen des iDRAC6-SNMP-Agenten unter Verwendung der webbasierten Schnittstelle zuzugreifen oder den Community-Namen zu konfigurieren, wechseln Sie zu **iDRAC-Einstellungen→ Netzwerk/ Sicherheit→ Dienste** und klicken Sie auf **SNMP-Agent**.

Um zu verhindern, dass SNMP-Authentifizierungsfehler erstellt werden, müssen Sie Community-Namen eingeben, die vom Agenten akzeptiert werden. Da der iDRAC6 nur einen einzigen Community-Namen zulässt, müssen Sie den gleichen **Get**- und **Set**-Community-Namen für das IT Assistant-Ermittlungs-Setup eingeben.

19

Wiederherstellung und Fehlerbehebung beim verwalteten System

Dieser Abschnitt erklärt, wie man Aufgaben zur Wiederherstellung und Behebung von Störungen bei einem abgestürzten System mit Hilfe der webbasierten iDRAC6-Benutzeroberfläche ausführt.

- „Erste Schritte, um Störungen an einem Remote-System zu beheben“ auf Seite 365.
- „Stromverwaltung auf einem Remote-System“ auf Seite 366.
- „POST-Startprotokolle verwenden“ auf Seite 376.
- „Bildschirm des letzten Systemabsturzes anzeigen“ auf Seite 378.

Erste Schritte, um Störungen an einem Remote-System zu beheben

Die folgenden Fragen werden häufig für die Fehlerbehebung bei Problemen auf hoher Ebene auf dem verwalteten System gestellt:

1. Ist das System ein- oder ausgeschaltet?
2. Wenn eingeschaltet, funktioniert das Betriebssystem, ist es abgestürzt oder nur blockiert?
3. Wenn ausgeschaltet, wurde der Strom unerwartet ausgeschaltet?

Überprüfen Sie für abgestürzte Systeme den Bildschirm des letzten Absturzes (siehe „Bildschirm des letzten Systemabsturzes anzeigen“ auf Seite 378) und verwenden Sie die virtuelle Konsole und die Remote-Stromverwaltung (siehe „Stromverwaltung auf einem Remote-System“ auf Seite 366), um das System neu zu starten und den Neustart zu beobachten.

Stromverwaltung auf einem Remote-System

Der iDRAC6 ermöglicht Ihnen, im Remote-Zugriff mehrere Stromverwaltungsmaßnahmen auf dem verwalteten System auszuführen, damit Sie das System nach einem Systemausfall oder einem anderen Systemereignis wiederherstellen können.

Stromsteuerungsmaßnahmen von der webbasierten iDRAC6-Schnittstelle auswählen

Informationen zum Ausführen von Stromverwaltungsmaßnahmen unter Verwendung der webbasierten Schnittstelle finden Sie unter „Durchführen von Stromsteuerungsmaßnahmen am Server“ auf Seite 334.

Stromsteuerungsmaßnahmen von der iDRAC6-CLI auswählen

Verwenden Sie den Befehl `racadm serveraction`, um Stromverwaltungsvorgänge auf dem Hostsystem auszuführen.

`racadm serveraction <Maßnahme>`

Die Optionen für die Zeichenkette <*Maßnahme*> lauten:

- **powerdown** - Fährt das verwaltete System herunter.
- **powerup** - Fährt das verwaltete System hoch.
- **powercycle** - Löst einen Ein-/Ausschaltvorgang auf dem verwalteten System aus. Diese Maßnahme ist dem Drücken des Netzschalters an der Systemvorderseite ähnlich, um das System aus- und dann wieder einzuschalten.
- **powerstatus** - Zeigt den aktuellen Stromstatus des Servers an („EIN“ oder „AUS“).
- **hardreset** - Führt einen Reset (Neustart) auf dem verwalteten System durch.

Anzeigen von Systeminformationen

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→ Eigenschaften→ Systemzusammenfassung**. Weitere Informationen finden Sie in der *iDRAC6-Online-Hilfe*.

Die Seite **Systemdetails** enthält Informationen über die folgenden Systemkomponenten:

- Hauptsystemgehäuse
- Remote-Access-Controller

Sie können auf die Seite **Systemdetails** zugreifen, indem Sie die Struktur unter **System** erweitern und auf das Register **Eigenschaften→ Systemdetails** klicken.

Hauptsystemgehäuse

ANMERKUNG: Um Informationen zu **Host-Name** und **BS-Name** abzufragen, müssen auf dem verwalteten System iDRAC6-Dienste installiert sein.

Tabelle 19-1. Systeminformationen

Feld	Beschreibung
Beschreibung	Systembeschreibung.
BIOS-Version	BIOS-Version des Systems.
Service Tag (Service-Tag-Nummer)	Service-Tag-Nummer des Systems.
Express-Servicecode:	Servicecode des Systems.
Hostname	Name des Hostsystems.
BS-Name	Betriebssystem, das auf dem System ausgeführt wird.
OS Version (Betriebssystem-Version)	Version des auf dem System ausgeführten Betriebssystems.
Systemrevision	Die Revisionsnummer des Systems.
Lifecycle Controller-Firmware	Version der Lifecycle Controller-Firmware.

Tabelle 19-2. Automatische Wiederherstellung

Feld	Beschreibung
Wiederherstellungsmaßnahme	Wenn ein *Systemhänger* festgestellt wird, kann der iDRAC6 so konfiguriert werden, dass er eine der folgenden Maßnahmen ausführt: Keine Maßnahme, Hardware-Reset, Herunterfahren oder Aus- und einschalten.
Anfänglicher Countdown	Die Anzahl der Sekunden nach Feststellung eines *Systemhängers*, nach denen der iDRAC6 eine Wiederherstellungsmaßnahme ausführt.
Vorhandener Countdown	Der aktuelle Wert des Countdown-Zeitgebers in Sekunden.

Tabelle 19-3. Integrierte NIC-MAC-Adressen

Feld	Beschreibung
Virtuelle MAC	Zeigt virtuelle MAC-Adressen (Media Access Control) an. Die virtuellen MAC-Daten können der Hardware-Bestandsliste entnommen werden, allerdings muss der Hardware-Bestand vor dem Anzeigen der vMAC-Daten einmalig erfasst werden. Klicken Sie auf **Systembestand**. Die Bestandsdaten werden aktualisiert und auf der Seite **Systembestand** angezeigt. Klicken Sie erneut auf **Systemdetails**. Die virtuellen MAC-Adressen für die einzelnen eingebetteten LAN-Netzwerkschnittstellen werden nun auf der Seite **Systemdetails** angezeigt. **ANMERKUNG:** Die Funktion vMAC wird vom erweiterten Infrastrukturmanager von Dell (Dell Advanced Infrastructure Manager, AIM) in zukünftigen Versionen verwendet. Falls Dell AIM den Server derzeit nicht verwaltet, dann sind die Ethernet-MAC-Adresse und die virtuelle MAC-Adresse identisch.

Tabelle 19-3. Integrierte NIC-MAC-Adressen *(fortgesetzt)*

Feld	Beschreibung
NIC 1	Zeigt die Ethernet-, die iSCSI (Internet Small Computer System Interface)- und die virtuelle(n) MAC-Adresse(n) des eingebetteten Netzwerkschnittstellen-Controllers (NIC) 1 an. Ethernet-NICs unterstützen den verkabelten Ethernet-Standard und werden in den Systembus des Servers eingesetzt. Der iSCSI-NIC ist ein Netzwerkschnittstellen-Controller, dessen iSCSI-Stack auf dem Host-Computer ausgeführt wird. MAC-Adressen identifizieren jeden Knoten der Media Access Control-Schicht eindeutig.
NIC 2	Zeigt die Ethernet-, die iSCSI- und die virtuelle(n) MAC-Adresse(n) des eingebetteten Netzwerkschnittstellen-Controllers (NIC) 2 an, die diesen im Netzwerk eindeutig identifizieren.
NIC 3	Zeigt die Ethernet-, die iSCSI- und die virtuelle(n) MAC-Adresse(n) des eingebetteten Netzwerkschnittstellen-Controllers (NIC) 3 an, die diesen im Netzwerk eindeutig identifizieren.
NIC 4	Zeigt die Ethernet-, die iSCSI- und die virtuelle(n) MAC-Adresse(n) des eingebetteten Netzwerkschnittstellen-Controllers (NIC) 4 an, die diesen im Netzwerk eindeutig identifizieren.

Remote-Access-Controller

Tabelle 19-4. RAC-Informationen

Feld	Beschreibung
Name	iDRAC6
Produktinformationen	Integrierter Dell Remote Access Controller 6 – Enterprise
Uhrzeit/Datum	Aktuelle Zeit im Format: Tag Monat TT HH:MM:SS JJJJ Beispiel: Fr Jan 28 16:27:29 2011
Firmware-Version	iDRAC6-Firmware-Version

Tabelle 19-4. RAC-Informationen *(fortgesetzt)*

Feld	Beschreibung
Aktualisierte Firmware	Datum, an dem die Firmware zuletzt aktualisiert wurde im Format: Tag Monat TT HH:MM:SS JJJJ Beispiel: Sa Jan 29 2011 13:31:50
Hardwareversion	Remote Access Controller-Version
MAC-Adresse	Zeigt die MAC-Adresse (Media Access Control) an, die die einzelnen Knoten in einem Netzwerk eindeutig identifiziert.

Tabelle 19-5. IPv4-Information

Feld	Beschreibung
IPv4 aktiviert	**Ja** oder **Nein**
IP-Adresse	Die 32-Bit-Adresse, welche die Netzwerkschnittstellenkarte (NIC) für einen Host identifiziert. Der Wert wird im Punkttrennungs-Format angezeigt, z. B. 143.166.154.127.
Subnetzmaske	Die Subnetzmaske identifiziert die Abschnitte einer IP-Adresse, bei denen es sich um das erweiterte Netzwerkpräfix und die Host-Nummer handelt. Der Wert wird im Punkttrennungs-Format angezeigt, z. B. 255.255.0.0.
Gateway	Die Adresse eines Routers oder Switches. Der Wert wird im Punkttrennungs-Format angezeigt, z. B. 143.166.154.1.
DHCP aktiviert	**Ja** oder **Nein**. Gibt an, ob das dynamische Host-Konfigurationsprotokoll (DHCP) aktiviert ist.
DHCP zum Abrufen von DNS-Serveradressen verwenden	**Ja** oder **Nein**. Gibt an, ob DHCP zum Abrufen von DNS-Serveradressen verwendet werden soll.
Bevorzugter DNS-Server	Gibt die statische IPv4-Adresse des bevorzugten DNS-Servers an.
Alternativer DNS-Server	Gibt die statische IPv4-Adresse des alternativen DNS-Servers an.

Tabelle 19-6. IPv6-Informationsfelder

Feld	Beschreibung
IPv6 aktiviert	Gibt an, ob der IPv6-Stapel aktiviert ist.
IP-Adresse 1	Gibt die IPv6-Adressen-/Präfixlänge für den iDRAC6-NIC an. Die *Präfixlänge* ist mit der IP-Adresse 1 kombiniert. Hierbei handelt es sich um eine ganze Zahl, welche die Präfixlänge der IPv6-Adresse angibt. Diese kann ein Wert im Bereich von 1 bis 128 sein.
IP-Gateway	Gibt das Gateway für den iDRAC6-NIC an.
Lokale Adresse verbinden	Gibt die lokale iDRAC6-NIC-IPv6-Link-Adresse an.
IP-Adresse 2...15	Gibt die zusätzlichen IPv6-Adressen für den iDRAC6-NIC an, falls verfügbar.
Autom. Konfiguration aktiviert	**Ja** oder **Nein**. Autom. Konfiguration gestattet dem Server Administrator die Abfrage der IPv6-Adresse für den iDRAC-NIC vom Server des dynamischen Host-Konfigurationsprotokolls (DHCPv6).
DHCPv6 zum Abrufen von DNS-Serveradressen verwenden	**Ja** oder **Nein**. Gibt an, ob DHCPv6 zum Abrufen von DNS-Serveradressen verwendet werden soll.
Bevorzugter DNS-Server	Gibt die statische IPv6-Adresse des bevorzugten DNS-Servers an.
Alternativer DNS-Server	Gibt die statische IPv6-Adresse des alternativen DNS-Servers an.

Systembestand

Auf der Seite **Systembestand** werden Informationen zu den im System installierten Hardware- und Firmware-Komponenten angezeigt.

Sie können auf die Seite **Systembestand** zugreifen, indem Sie die Struktur unter **System** erweitern und auf **Eigenschaften→ Systembestand** klicken.

Hardware Inventory (Hardware-Bestandsliste)

In diesem Abschnitt werden Informationen zu den derzeit im System vorhandenen Hardware-Komponenten angezeigt. Wenn die Hardware-Bestandsdaten nicht verfügbar sind, wenn Sie auf das Register **Systembestand** klicken, wird folgende Meldung angezeigt:

```
Die Hardware-Bestandsliste ist nicht verfügbar.
```

Aktualisieren Sie die Seite, um die Details anzuzeigen.

Firmware-Bestandsliste

In diesem Abschnitt wird die Firmware-Version der installierten Dell Komponenten angezeigt. Wenn die Firmware-Bestandsdaten nicht verfügbar sind, wenn Sie auf das Register **Systembestand** klicken, wird folgende Meldung angezeigt:

```
Die Hardware-Bestandsliste ist nicht verfügbar.
```

Aktualisieren Sie die Seite, um die Details anzuzeigen.

ANMERKUNG: Wenn die CSIOR-Funktion (Collect System Inventory on Reboot) nicht aktiviert ist, dauert es eine Weile, bis die Daten erfasst sind. Es wird daher empfohlen, zuerst die CSIOR-Funktion auszuführen, um den Systembestand beim Neustart zu erfassen, und dann auf das Register **Systembestand** zu klicken.

Nach dem Hinzufügen neuer Hardware zum System bzw. nach dem Entfernen von Hardware aus dem System wird die Seite **Systembestand** möglicherweise nicht automatisch aktualisiert. Grund dafür ist, dass die während des Herstellungsprozesses erfassten Bestandsdaten möglicherweise nicht mit den neuen Änderungen überschrieben werden.

Um dieses Problem während des BIOS POST zu beheben, wählen Sie die Option **Strg+E**, und aktivieren Sie **Systembestand beim Neustart erfassen**. Speichern Sie Ihre Auswahl, und beenden Sie die Option **Strg+E**.

Das System führt einen Neustart durch, um den neuen Systembestand zu erfassen. Nach Abschluss der Bestandserfassung werden auf der Seite **Systembestand** die richtigen Hardware- und Firmware-Bestandsdaten angezeigt.

Weitere Informationen finden Sie in der *iDRAC6-Online-Hilfe*.

Systemereignisprotokoll (SEL) verwenden

Auf der Seite **SEL** werden systemkritische Ereignisse angezeigt, die auf dem verwalteten System auftreten.

So zeigen Sie das Systemereignisprotokoll an:

1. Klicken Sie in der **System**struktur auf **System**.
2. Klicken Sie auf das Register **Protokolle** und dann auf **Systemereignisprotokoll**.

   Auf der Seite **Systemereignisprotokoll** werden der Ereignis-Schweregrad sowie weitere Informationen angezeigt; siehe Tabelle 19-7.
3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Systemereignisprotokoll**, um fortzufahren. Weitere Informationen finden Sie in der iDRAC6-Online-Hilfe.
4. Klicken Sie auf **Protokoll löschen**, um das SEL zu löschen.

   ANMERKUNG: Die Schaltfläche Protokoll löschen wird nur angezeigt, wenn Sie die Berechtigung Protokolle löschen besitzen.
5. Klicken Sie auf **Speichern unter**, um das SEL in einem Verzeichnis Ihrer Wahl zu speichern.

Tabelle 19-7. Statusanzeigesymbole

Symbol/ Kategorie	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.
Uhrzeit/ Datum	Datum und Uhrzeit des Ereigniseintritts. Wenn das Datumsfeld leer ist, trat das Ereignis während des Systemstarts auf. Das Format lautet <Tag> <Monat> TT JJJJ hh:mm:ss, basierend auf dem 24-Stunden-Zeitsystem.
Beschreibung	Eine kurze Beschreibung des Ereignisses

OEM-Ereignisprotokolle aktivieren/deaktivieren

Die OEM-Ereignisprotokolle werden automatisch auf der Seite **Systemereignisprotokoll** angezeigt. Mithilfe der Schaltfläche **Erweiterte Einstellungen** des Registers **Systeme→ Protokolle** können Sie die Anzeige der OEM-Ereignisprotokolle des verwalteten Systems auf der Seite **Systemereignisprotokoll** aktivieren bzw. deaktivieren.

Um die Anzeige der OEM-Ereignisprotokolle auf der Seite **Systemereignisprotokoll** zu deaktivieren, wählen Sie die Option **OEM-SEL-Ereignisfilter aktiviert** aus.

ANMERKUNG: Die Option **OEM-SEL-Ereignisfilter aktiviert** ist nicht standardmäßig markiert.

Befehlszeile zum Anzeigen des Systemprotokolls verwenden

```
racadm getsel-i
```

Der Befehl **getsel -i** zeigt die Anzahl der Einträge im SEL an.

```
racadm getsel <Optionen>
```

ANMERKUNG: Wenn keine Argumente vorgegeben werden, wird das gesamte Protokoll angezeigt.

ANMERKUNG: Weitere Informationen zu den verfügbaren Optionen finden Sie in der Beschreibung des Unterbefehls getsel im *RACADM-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
```

Arbeitsnotizen verwenden

Arbeitsnotizen sind Notizen oder Kommentare, die vom Benutzer hinzugefügt werden können. Alle iDRAC-Benutzer können Arbeitsnotizen hinzufügen. Arbeitsnotizen können nicht gelöscht werden. Sie können bis zu 1.000 Arbeitsnotizen gleichzeitig anzeigen. Zum schnellen Nachschlagen werden die letzten zehn Arbeitsnotizen auf der iDRAC-Startseite angezeigt.

ANMERKUNG: Wenn mehr als 800 Arbeitsnotizen hinzugefügt wurden, kann es sein, dass die GUI-Seite einige Sekunden länger benötigt, um die Seite zu laden. Das liegt daran, dass eine relativ große Datenmenge zwischen der GUI und dem iDRAC6 übertragen wird. Die neu hinzugefügten Arbeitsnotizen werden möglicherweise nicht angezeigt, nachdem die Seite geladen wurde. Klicken Sie zum Beheben dieses Problems auf **Aktualisieren**.

Auf der Seite **Arbeitsnotizen** können Sie dem Lifecycle-Protokoll Notizen hinzufügen. Der Zeitstempel der einzelnen Notizen wird automatisch erfasst.

Zum Öffnen der Seite **Arbeitsnotizen** erweitern Sie die Struktur unter **System**, und klicken Sie auf **Systeme→ Protokolle→ Arbeitsnotizen**.

Die Seite **Arbeitsnotizen** wird angezeigt und ermöglicht es Ihnen, neue Arbeitsnotizen einzugeben und weitere Informationen anzuzeigen (siehe Tabelle 19-8).

So geben Sie Arbeitsnotizen ein:

1. Geben Sie auf der Seite **Arbeitsnotizen** unter dem Abschnitt **Arbeitsnotizen hinzufügen** eine Arbeitsnotiz in das angezeigte Feld ein.

   ANMERKUNG: Die Arbeitsnotiz darf maximal 50 Zeichen enthalten.

2. Klicken Sie auf **Save** (Speichern).

   Die neue Arbeitsnotiz wird in der Arbeitsnotiztabelle unter dem Abschnitt **Arbeitsnotizen hinzufügen** angezeigt.

Tabelle 19-8. Arbeitsnotizen

Feld	Beschreibung
Uhrzeit/ Datum	Zeigt den Zeitstempel an, der für die einzelnen Arbeitsnotizeinträge erfasst wurde. Das Format lautet JJJJ-MM-TTUhh:mm:ssZ, basierend auf dem 24-Stunden-Zeitsystem, wobei den Kürzeln folgende Bedeutung zukommt: JJJJ: Jahr MM: Monat TT: Tag U: Uhrzeit hh: Stunde mm: Minute ss: Sekunde Z: Zeitzonenkennzeichner **ANMERKUNG:** Wird die Uhrzeit in UTC angegeben, fügen Sie direkt nach der Uhrzeit, ohne Leerzeichen, ein Z hinzu. Z ist der Zonenkennzeichner für die UTC-Nullabweichung. **09:30** UTC kann demnach mit **09:30Z** oder **0930Z** angegeben werden. **14:45:15** UTC kann mit **14:45:15Z** oder **144515Z** angegeben werden.
„Notes" (Anmerkungen)	Zeigt den Inhalt des Arbeitsnotizeintrags an.

POST-Startprotokolle verwenden

ANMERKUNG: Alle Protokolle werden nach dem Neustart des iDRAC6 gelöscht.

Die Seite **Start-Capture** bietet Zugriff auf Aufzeichnungen, die maximal die letzten drei verfügbaren Startzyklen umfassen. Sie sind in der Reihenfolge von neuster zu ältester Aufzeichnung angeordnet. Wenn der Server keine Startzyklen durchlaufen hat, wird die Meldung **Keine Aufzeichnung verfügbar** angezeigt. Klicken Sie auf **Wiedergabe**, nachdem Sie einen verfügbaren Startzyklus ausgewählt haben, um diesen in einem neuen Fenster anzuzeigen.

ANMERKUNG: Das Anzeigen von Systemstartprotokollen wird nur auf Java unterstützt und nicht auf Active-X.

So zeigen Sie die Systemstartprotokolle an:

1. Klicken Sie in der **System**struktur auf **System**.
2. Klicken Sie auf das Register **Protokolle** und dann auf das Register **Start-Capture**.
3. Wählen Sie einen Startzyklus aus und klicken Sie auf **Wiedergabe**.

   Das Video der Protokolle wird auf einem neuen Bildschirm abgespielt.

   ANMERKUNG: Sie müssen ein geöffnetes Systemstartprotokollvideo schließen, um ein anderes abspielen zu können. Sie können nicht zwei Protokolle gleichzeitig ansehen.
4. Klicken Sie auf **Wiedergabe→ Wiedergabe**, um das Systemstartprotokollvideo zu starten.
5. Klicken Sie auf **Wiedergabe→ Datenträgersteuerungen**, um das Video anzuhalten.

ANMERKUNG: Möglicherweise wird eine Nachricht angezeigt, in der Sie gefragt werden, ob eine **data.jnlp**-Datei gespeichert werden soll, anstatt den Viewer zu öffnen. Führen Sie in Internet Explorer die folgenden Schritte aus, um dieses Problem zu beheben: Rufen Sie **Extras→ Internetoptionen→ Erweitert** auf und deaktivieren Sie die Option *Verschlüsselte Seiten nicht auf der Festplatte speichern*.

ANMERKUNG: Wenn iDRAC zurückgesetzt wird, ist das Systemstartvideo nicht mehr verfügbar, da dieses im RAM gespeichert und beim Zurücksetzen von iDRAC gelöscht wird.

Die iDRAC6 Express-Karte wird an iDRAC6 gebunden, wenn Sie die USC-Anwendung (Unified Server Configurator) aufrufen, indem Sie beim Starten **F10** drücken. Wenn die Bindung erfolgreich ist, wird im SEL und LCD die folgende Meldung protokolliert: `iDRAC6-Aktualisierung erfolgreich`. Schlägt die Bindung fehl, wird im SEL und LCD die folgende Meldung protokolliert: `iDRAC6-Aktualisierung fehlgeschlagen`. Wenn eine iDRAC6 Express-Karte mit einer alten oder überholten iDRAC6-Firmware, die die jeweilige Plattform nicht unterstützt, in der Hauptplatine eingesetzt ist und das System gestartet wird, wird außerdem folgendes Protokoll auf dem POST-Bildschirm ausgegeben: `iDRAC-Firmware ist veraltet. Aktualisieren Sie auf die aktuelle Firmware`. Aktualisieren Sie die iDRAC6 Express-Karte mit der aktuellen iDRAC6-Firmware für die jeweilige Plattform. Weitere Informationen finden Sie im *Dell Lifecycle Controller-Benutzerhandbuch*.

Bildschirm des letzten Systemabsturzes anzeigen

ANMERKUNG: Die Funktion „Letzter Absturzbildschirm“ setzt voraus, dass die Funktion **Autom. Wiederherstellung** im Server Administrator auf dem verwalteten System konfiguriert ist. Stellen Sie außerdem sicher, dass die Funktion **Automatisierte Systemwiederherstellung** mittels iDRAC6 aktiviert wird. Wechseln Sie zur Seite **Dienste** unter dem Register **Netzwerk/Sicherheit** im Abschnitt **iDRAC-Einstellungen**, um diese Funktion zu aktivieren.

So zeigen Sie die Seite **Bildschirm Letzter Absturz** an:

1. Klicken Sie in der **System**struktur auf **System**.
2. Klicken Sie auf das Register **Protokolle** und klicken dann auf den **Bildschirm Letzter Absturz**.

   Die Seite **Bildschirm Letzter Absturz** zeigt den Bildschirm des letzten Absturzes an. Die Informationen des letzten Systemabsturzes werden im iDRAC6-Speicher gespeichert und sind im Remote-Zugriff abrufbar.

   Weitere Informationen zu den auf der Seite **Bildschirm Letzter Absturz** angezeigten Schaltflächen finden Sie in der *iDRAC6-Online-Hilfe*.

ANMERKUNG: Aufgrund von Schwankungen des Zeitgebers für automatische Wiederherstellung kann der **Bildschirm Letzter Absturz** nicht erfasst werden, wenn der System-Reset-Zeitgeber auf einen Wert unter 30 Sekunden eingestellt wird. Stellen Sie den System-Reset-Zeitgeber mit dem Server Administrator oder IT Assistant auf mindestens 30 Sekunden ein, und vergewissern Sie sich, dass die Funktionen unter **Bildschirm Letzter Absturz** ordnungsgemäß funktionieren. Weitere Informationen hierzu finden Sie unter „Das verwaltete System zur Erfassung des Bildschirms „Letzter Absturz“ konfigurieren“ auf Seite 355.

20

iDRAC6 wiederherstellen und Fehler beheben

In diesem Abschnitt wird die Durchführung von Aufgaben im Zusammenhang mit der Wiederherstellung und Fehlerbehebung eines abgestürzten iDRAC6 beschrieben.

Die Fehlerbehebung des iDRAC6 kann unter Verwendung eines der folgenden Hilfsprogramme durchgeführt werden:

- RAC-Protokoll
- Diagnosekonsole
- Server identifizieren
- Ablaufverfolgungsprotokoll
- racdump
- coredump

RAC-Protokoll verwenden

Das **RAC-Protokoll** ist ein beständiges Protokoll, das in der iDRAC6-Firmware geführt wird. Das Protokoll enthält eine Liste von Benutzermaßnahmen (z. B. An- und Abmelden, Änderungen der Sicherheitsregeln) und Warnungen, die vom iDRAC6 gesendet werden. Die ältesten Einträge werden überschrieben, wenn der Protokollspeicher erschöpft ist.

So greifen Sie über die iDRAC6-Benutzerschnittstelle (UI) auf das RAC-Protokoll zu:

1. Klicken Sie in der Struktur unter **System** auf **iDRAC-Einstellungen**.
2. Klicken Sie auf das Register **Protokolle** und dann auf **iDRAC-Protokoll**.

Die Seite **iDRAC-Protokoll** zeigt die unter Tabelle 20-1 aufgeführten Informationen an.

Tabelle 20-1. Informationen der iDRAC-Protokollseite

Feld	Beschreibung
Datum/ Uhrzeit	Datum und Uhrzeit (z. B. `19. Dez. 16:55:47`). Wenn der iDRAC6 beim erstmaligen Start nicht in der Lage ist, mit dem verwalteten System zu kommunizieren, wird die Uhrzeit als `Systemstart` angezeigt.
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.

ANMERKUNG: Informationen zum Verwenden der Schaltflächen auf der **iDRAC-Protokollseite** finden Sie in der *iDRAC6-Online-Hilfe*.

Befehlszeile verwenden

Verwenden Sie den Befehl `getraclog`, um die iDRAC6-Protokolleinträge anzuzeigen.

```
racadm getraclog [Optionen]
```

```
racadm getraclog -i
```

Der Befehl **getraclog -i** zeigt die Anzahl der Einträge im iDRAC6-Protokoll an.

ANMERKUNG: 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.

Mithilfe des Befehls `clrraclog` können Sie alle Einträge aus dem iDRAC-Protokoll löschen.

```
racadm clrraclog
```

Diagnosekonsole verwenden

Der iDRAC6 bietet einen Standardsatz von Netzwerkdiagnose-Hilfsprogrammen (siehe Tabelle 20-2), die den mit Microsoft Windows- oder Linux-basierten Systemen gelieferten Hilfsprogrammen ähnlich sind. Mit der webbasierten iDRAC6-Schnittstelle können Sie auf die Hilfsprogramme zum Debuggen des Netzwerks zugreifen.

Klicken Sie auf **iDRAC6 zurücksetzen**, um den iDRAC zurückzusetzen. Auf dem iDRAC wird ein normaler Startvorgang ausgeführt.

So greifen Sie auf die Seite **Diagnosekonsole** zu:

1. Klicken Sie in der Struktur unter **System** auf **iDRAC-Einstellungen**→ Register **Fehlerbehebung**→ **Diagnosekonsole**.
2. Geben Sie einen Befehl ein und klicken Sie auf **Senden**. Tabelle 20-2 beschreibt die Befehle, die verwendet werden können. Die Debug-Ergebnisse werden auf der Seite **Diagnosekonsole** angezeigt.
3. Zum Aktualisieren der Seite **Diagnosekonsole** klicken Sie auf **Aktualisieren**. Um einen anderen Befehl auszuführen, klicken Sie auf **Zurück zur Diagnoseseite**.

Tabelle 20-2. 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. Wenn die optionale Schnittstellenzahl im Textfeld rechts neben der Option **netstat** angegeben wird, druckt netstat zusätzliche Informationen über den Verkehr auf der Schnittstelle, die Pufferauslastung und andere Informationen zur Netzwerkschnittstelle aus.

Tabelle 20-2. 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. In das Feld rechts neben dieser Option muss eine Ziel-IP-Adresse eingegeben werden. Ein ICMP-Echo-Paket (Internetsteuerungs-Meldungsprotokoll) wird basierend auf dem aktuellen Inhalt der Routingtabelle zur Ziel-IP-Adresse gesendet.
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.

Server identifizieren verwenden

Die Seite **Identifizieren** ermöglicht Ihnen, die Systemidentifizierungsfunktion zu aktivieren.

So identifizieren Sie den Server:

1. Klicken Sie auf **System→ iDRAC-Einstellungen→ Fehlerbehebung→ Identifizieren**.
2. Wählen Sie auf dem Bildschirm **Identifizieren** das Kontrollkästchen **Server identifizieren** aus, um das Blinken der LCD und der hinteren Serveridentifizierungs-LED zu aktivieren.
3. Das Feld **Serverzeitüberschreitung identifizieren** zeigt die Anzahl von Sekunden an, während denen die LCD blinkt. Geben Sie den Zeitraum (in Sekunden) an, während dem die LCD blinken soll.
   Der Zeitüberschreitungsbereich beträgt 1 bis 255 Sekunden. Wenn die Zeitüberschreitung auf 0 Sekunden eingestellt ist, blinkt die LCD fortlaufend.
4. Klicken Sie auf **Anwenden**.

Wenn Sie **0** Sekunden eingegeben haben, können Sie diese Einstellung unter Befolgung der nachstehenden Schritte deaktivieren:

1. Klicken Sie auf **System→ iDRAC-Einstellungen→ Fehlerbehebung→ Identifizieren**.
2. Heben Sie im Bildschirm **Identifizieren** die Auswahl der Option **Server identifizieren** auf, und klicken Sie auf **Anwenden**.

Ablaufverfolgungsprotokoll verwenden

Das interne iDRAC6-Ablaufverfolgungsprotokoll wird von Administratoren verwendet, um Warnmeldungen und Netzwerkprobleme des iDRAC6 zu debuggen.

So greifen Sie über die webbasierte iDRAC6-Schnittstelle auf das Ablaufverfolgungsprotokoll zu:

1. Klicken Sie in der Struktur unter **System** auf **iDRAC-Einstellungen**.
2. Klicken Sie auf das Register **Diagnose**.
3. Geben Sie den **gettracelog**-Befehl oder den **racadm gettracelog**-Befehl in das **Befehl**sfeld ein.

   ANMERKUNG: Sie können diesen Befehl auch über die Befehlszeilenoberfläche verwenden. 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.

Das Ablaufverfolgungsprotokoll verfolgt die folgenden Informationen:

- DHCP – Verfolgt Pakete, die an einen DHCP-Server gesendet und von ihm empfangen werden.
- IP – Verfolgt gesendete und empfangene IP-Pakete.

Das Ablaufverfolgungsprotokoll kann auch spezifische Fehlercodes der iDRAC6-Firmware enthalten, die sich auf die interne iDRAC6-Firmware beziehen und nicht auf das Betriebssystem des verwalteten Systems.

ANMERKUNG: Der iDRAC6 gibt kein Echo auf ein ICMP (Ping) mit einer Paketgröße über 1500 Byte zurück.

racdump verwenden

Der Befehl `racadm racdump` bietet einen Einzelbefehl zum Abrufen von Informationen zu Speicherauszug, Status und iDRAC6-Platine (allgemein).

ANMERKUNG: Dieser Befehl ist nur für Telnet-, SSH- und Remote-RACADM-Schnittstellen verfügbar. Weitere Informationen finden Sie bei der Beschreibung des Befehls racdump im *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

coredump verwenden

Mit dem Befehl `racadm coredump` werden detaillierte Informationen im Zusammenhang mit kritischen Problemen angezeigt, die kürzlich am RAC aufgetreten sind. Die coredump-Informationen können zur Diagnose dieser kritischen Probleme eingesetzt werden.

Wenn verfügbar, sind die Coredump-Informationen über Ein-/Ausschaltzyklen des RAC beständig und bleiben verfügbar, bis eine der folgenden Bedingungen eintritt:

- Die Coredump-Informationen werden mit dem Unterbefehl `coredumpdelete` gelöscht.
- Auf dem RAC tritt ein weiterer kritischer Zustand ein. In diesem Fall beziehen sich die coredump-Informationen auf den zuletzt aufgetretenen kritischen Fehler.

Der Befehl `racadm coredumpdelete` kann zum Löschen aller gegenwärtig vorhandenen, im RAC gespeicherten **Coredump**-Daten verwendet werden. Weitere Informationen finden Sie bei den Beschreibungen der Unterbefehle `coredump` und `ccoredumpdelete` im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist.

21

Sensoren

Hardwaresensoren oder -sonden helfen Ihnen, die Systeme im Netzwerk auf effizientere Weise zu überwachen, indem Sie geeignete Maßnahmen ergreifen können, um Notfallsituationen, wie z. B. eine Instabilität oder Beschädigung des Systems, zu verhindern.

Sie können den iDRAC6 zur Überwachung von Hardwaresensoren für Batterien, Lüftersonden, Gehäuseeingriff, Netzteile, verbrauchtem Strom, Temperatur und Spannung einsetzen.

Batteriesonden

Die Batteriesonden bieten Informationen zu Systemplatinen-CMOS und Speicher-ROMB-Batterien (RAID auf Systemplatine).

ANMERKUNG: Die Einstellungen für Speicher-ROMB-Batterien sind nur verfügbar, wenn das System einen ROMB aufweist.

Lüftersonden

Der Lüftersonden-Sensor bietet Informationen zu Folgendem:

- Lüfterredundanz – die Fähigkeit des sekundären Lüfters, den primären Lüfter zu ersetzen, wenn der primäre Lüfter nicht mehr in der Lage ist, unter einer voreingestellten Geschwindigkeit Wärme abzuleiten.
- Liste der Lüftersonden – bietet Informationen zur Lüftergeschwindigkeit aller Lüfter im System.

Gehäuseeingriffssonden

Die Gehäuseeingriffssonden geben Aufschluss über den Gehäusestatus bzw. darüber, ob das Gehäuse geöffnet oder geschlossen ist.

Netzteilsonden

Die Netzteilsonden bieten Informationen zu Folgendem:

- Status der Stromversorgung
- Netzteilredundanz bzw. die Fähigkeit des redundanten Netzteils, das primäre Netzteil zu ersetzen, falls dieses ausfällt.

ANMERKUNG: Wenn das System nur ein Netzteil aufweist, ist die Netzteilredundanz **deaktiviert**.

Wechselbare Flash-Datenträgersonden

Der wechselbare Flash-Datenträgersensor bietet Informationen über den Status der vFlash-SD-Karte (aktiv oder nicht vorhanden). Weitere Informationen über die vFlash-SD-Karte finden Sie unter „vFlash-SD-Karte konfigurieren und vFlash-Partitionen verwalten“ auf Seite 301.

Stromüberwachungssonden

Die Stromüberwachung liefert Informationen zum Stromverbrauch in *Echtzeit*, in Watt und Ampere.

Sie haben auch die Möglichkeit, eine grafische Darstellung des Stromverbrauchs der letzten Minute, der letzten Stunde, des letzten Tages oder der letzten Woche ab der im iDRAC6 eingestellten aktuellen Uhrzeit anzuzeigen.

Temperatursonde

Der Temperatursensor gibt Auskunft über die Umgebungstemperatur der Systemplatine. Die Temperatursonden zeigen an, ob sich der Status der Sonden innerhalb des voreingestellten Bereichs für Warnungsschwellenwert und kritischen Schwellenwert befindet.

Spannungssonden

Bei den folgenden Sonden handelt es sich um typische Spannungssonden. Es ist möglich, dass diese und/oder andere Sonden auf Ihrem System vorhanden sind.

- CPU [n] VCORE
- Systemplatine 0,9 V PG
- Systemplatine 1,5 V ESB2 PG
- Systemplatine 1,5 V PG
- Systemplatine 1,8 V PG
- Systemplatine 3,3 V PG
- Systemplatine 5 V PG
- Systemplatine Backplane PG
- Systemplatine CPU VTT
- Systemplatine Linear PG

Die Spannungssonden zeigen an, ob sich der Status der Sonden innerhalb des voreingestellten Bereichs für Warnungsschwellenwert und kritischen Schwellenwert befindet.

22

Sicherheitsfunktionen konfigurieren

Der iDRAC6 enthält die folgenden Sicherheitsfunktionen:

- Erweiterte Sicherheitsoptionen für den iDRAC6-Aministrator:
  - Die Option zum Deaktivieren der virtuellen Konsole ermöglicht dem Benutzer des *lokalen* Systems, die virtuelle Konsole unter Verwendung der Funktion für die virtuelle iDRAC6-Konsole zu deaktivieren.
  - Die Deaktivierungsfunktion für die lokale Konfiguration ermöglicht dem *Remote*-iDRAC6-Administrator, die Fähigkeit zur Konfiguration des iDRAC6 selektiv zu deaktivieren, und zwar von:
    - BIOS-POST, Options-ROM
    - dem Betriebssystem unter Verwendung des lokalen RACADM und der Dell OpenManage Server Administrator-Dienstprogramme
- der RACADM-CLI und der webbasierten Schnittstelle aus, die SSL-128-Bit-Verschlüsselung und SSL-40-Bit-Verschlüsselung (für Länder, in denen 128 Bit nicht annehmbar ist) unterstützen

  ANMERKUNG: Telnet unterstützt keine SSL-Verschlüsselung.
- Sitzungszeitüberschreitungs-Konfiguration (in Sekunden) über die webbasierte Schnittstelle oder RACADM-CLI
- 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
- Eingeschränkter IP-Adressenbereich für Clients, die eine Verbindung zum iDRAC6 herstellen

Erweiterte Optionen für den iDRAC6-Aministrator

Lokale iDRAC6-Konfiguration deaktivieren

Administratoren können die lokale Konfiguration über die iDRAC6-GUI (grafische Benutzeroberfläche) deaktivieren, indem sie **iDRAC-Einstellungen→ Netzwerk/Sicherheit→ Dienste** auswählen. Wenn das Kontrollkästchen **Lokale iDRAC-Konfiguration mittels Options-ROM deaktivieren** ausgewählt ist, wird das iDRAC6-Konfigurationsdienstprogramm (auf das Sie durch Drücken von <Strg+E> während des Systemstarts zugreifen können) im schreibgeschützten Modus betrieben, wodurch lokale Benutzer daran gehindert werden, das Gerät zu konfigurieren. Wenn der Administrator das Kontrollkästchen **Lokale iDRAC-Konfiguration mittels RACADM deaktivieren** auswählt, können lokale Benutzer den iDRAC6 nicht über das RACADM-Dienstprogramm oder den Dell OpenManage Server Administrator konfigurieren, obwohl die Konfigurationseinstellungen noch immer abgelesen werden können.

Administratoren können über die webbasierte Schnittstelle eine oder beide dieser Optionen gleichzeitig aktivieren.

Lokale Konfigurationen während des Systemneustarts deaktivieren

Durch diese Funktion wird die Fähigkeit des Benutzers des verwalteten Systems, den iDRAC6 während des Systemneustarts zu konfigurieren, deaktiviert.

```
racadm config -g cfgRacTuning -o
cfgRacTuneCtrlEConfigDisable 1
```

ANMERKUNG: Diese Option wird nur im iDRAC6-Konfigurationsdienstprogramm unterstützt. Um ein Upgrade auf diese Version durchzuführen, müssen Sie ein BIOS-Upgrade durchführen. Das BIOS-Upgrade können Sie mithilfe des BIOS-Aktualisierungspakets durchführen, das auf der Dell Support-Website unter **www.support.dell.com** verfügbar ist.

Lokale Konfiguration über lokalen RACADM deaktivieren

Durch diese Funktion wird die Fähigkeit des Benutzers des verwalteten Systems, den iDRAC6 unter Verwendung des lokalen RACADM oder der Dell OpenManage Server Administrator-Dienstprogramme zu konfigurieren, deaktiviert.

```
racadm config -g cfgRacTuning -o
cfgRacTuneLocalConfigDisable 1
```

VORSICHTSHINWEIS: Durch diese Funktionen wird die Fähigkeit des lokalen Benutzers, den iDRAC6 über das lokale System zu konfigurieren sowie einen Reset auf die Standardeinstellung der Konfiguration vorzunehmen, stark eingeschränkt. Es wird empfohlen, diese Funktionen mit Vorsicht zu verwenden. Deaktivieren Sie nur eine Schnittstelle auf einmal, um zu vermeiden, dass Sie Ihre gesamten Anmeldungsberechtigungen verlieren.

ANMERKUNG: Weitere Informationen finden Sie im Informationsbericht zum Thema *Lokale Konfiguration und virtuelle Remote-KVM im DRAC deaktivieren* auf der Support-Website von Dell unter **support.dell.com**.

Obwohl Administratoren die lokalen Konfigurationsoptionen mithilfe von lokalen RACADM-Befehlen einstellen können, ist es aus Sicherheitsgründen nur möglich, die Optionen über eine bandexterne webbasierte iDRAC6-Schnittstelle oder Befehlszeilenoberfläche zurückzusetzen. Die Option `cfgRacTuneLocalConfigDisable` gilt, sobald der Einschalt-Selbsttest (POST) des Systems abgeschlossen ist und das System in eine Betriebssystemumgebung gestartet wurde. Das Betriebssystem kann Microsoft Windows Server oder Enterprise Linux sein (Betriebssysteme, die Befehle des lokalen RACADM ausführen können) oder ein beschränkt einsetzbares Betriebssystem wie z. B. Microsoft Windows Preinstallation Environment oder vmlinux, die zum Ausführen von Befehlen des lokalen RACADM im Dell OpenManage Deployment Toolkit verwendet werden.

Es gibt verschiedene Situationen, in denen ein Administrator eine lokale Konfiguration u. U. deaktivieren muss. Beispiel: In einem Datenzentrum mit mehreren Administratoren für Server und Remote-Zugriffsgeräte benötigen diejenigen, die für die Wartung von Server-Software-Stacks zuständig sind, eventuell keine Administratorrechte für den Zugriff auf Remote-Zugriffsgeräte. Auf ähnliche Weise haben Techniker während routinemäßigen Systemwartungsarbeiten eventuell direkten Zugriff auf Server und sind dadurch in der Lage, Systeme neu zu starten und auf das kennwortgeschützte BIOS zuzugreifen. Es sollte jedoch nicht möglich sein, dass sie Remote-Zugriffsgeräte konfigurieren. Administratoren von Remote-Zugriffsgeräten sollten in Anbetracht der Möglichkeit solcher Situationen erwägen, die lokale Konfiguration zu deaktivieren.

Administratoren sollten in Betracht ziehen, dass das Deaktivieren lokaler Konfigurationen die Berechtigungen zum Ausführen lokaler Konfigurationen stark einschränkt, was auch das Zurücksetzen des iDRAC6 auf seine ursprüngliche Konfiguration einschließt. Sie sollten entsprechende Optionen daher nur anwenden, wenn dies wirklich notwendig ist und dabei lediglich eine Schnittstelle auf einmal deaktivieren, um einem vollständigen Verlust ihrer Anmeldungsberechtigungen vorzubeugen. Wenn Administratoren z. B. alle lokalen iDRAC6-Benutzer deaktiviert haben und nur Benutzern des Microsoft Active Directory-Verzeichnisdienstes gestatten, sich am iDRAC6 anzumelden, und die Infrastruktur der Active Directory-Authentifizierung daraufhin fehlschlägt, ist es möglich, dass sich die Administratoren nicht mehr anmelden können. Eine vergleichbare Situation tritt auf, wenn Administratoren die gesamte lokale Konfiguration deaktiviert haben und einen iDRAC6 mit statischer IP-Adresse zu einem Netzwerk hinzufügen, das bereits einen DHCP-Server (dynamisches Host-Konfigurationsprotokoll) enthält, und der DHCP-Server die iDRAC6-IP-Adresse daraufhin einem anderen Gerät im Netzwerk zuweist. Durch den sich ergebenden Konflikt kann die bandexterne Konnektivität des DRAC deaktiviert werden, woraufhin Administratoren die Firmware über eine serielle Verbindung auf ihre standardmäßigen Einstellungen zurücksetzen müssen.

Virtuelle iDRAC6-Konsole deaktivieren

Administratoren können die virtuelle iDRAC6-Remote-Konsole selektiv deaktivieren und einem lokalen Benutzer somit eine flexible, sichere Methode zur Verfügung stellen, um auf dem System zu arbeiten, ohne dass eine andere Person über die virtuelle Konsole die Maßnahmen des Benutzers beobachten kann. Damit diese Funktion verwendet werden kann, ist auf dem Server die Installation der iDRAC-Software für den verwalteten Knoten erforderlich. Administratoren können die virtuelle Konsole unter Verwendung des folgenden Befehls deaktivieren:

```
racadm LocalConRedirDisable 1
```

Der Befehl LocalConRedirDisable deaktiviert die vorhandenen Fenster der Sitzung der virtuellen Konsole, wenn er mit dem Argument 1 ausgeführt wird.

Um zu verhindern, dass ein Remote-Benutzer die Einstellungen des lokalen Benutzers überschreibt, steht dieser Befehl nur für den lokalen RACADM zur Verfügung. Administratoren können diesen Befehl auf Betriebssystemen (einschließlich Microsoft Windows Server 2003 und SUSE Linux Enterprise Server 10) verwenden, die RACADM unterstützen. Da dieser Befehl über Systemneustarts hinweg aufrechterhalten bleibt, müssen Administratoren den Befehl ganz spezifisch wieder aufheben, um die virtuelle Konsole erneut zu aktivieren. Die Aufhebung kann durch die Verwendung des Arguments 0 vorgenommen werden:

```
racadm LocalConRedirDisable 0
```

In verschiedenen Situationen ist eventuell die Deaktivierung der virtuellen iDRAC6-Konsole erforderlich. Es ist z. B. möglich, dass Administratoren vermeiden möchten, dass ein Remote-iDRAC6-Benutzer die auf einem System konfigurierten BIOS-Einstellungen anzeigen kann. In diesem Fall können sie die virtuelle Konsole während des System-POST deaktivieren, indem Sie den Befehl `LocalConRedirDisable` anwenden. Es empfiehlt sich eventuell, die Sicherheit zu erhöhen, indem die virtuelle Konsole immer dann automatisch deaktiviert wird, wenn sich ein Administrator am System anmeldet. Hierzu ist der Befehl `LocalConRedirDisable` über die Benutzeranmeldungsskripts auszuführen.

ANMERKUNG: Weitere Informationen finden Sie im Informationsbericht zum Thema *Lokale Konfiguration und virtuelle Remote-KVM im DRAC deaktivieren* auf der Support-Website von Dell unter **support.dell.com**.

Weitere Informationen zu Anmeldungsskripts sind unter **technet2,microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx** zu finden.

iDRAC6-Datenübertragung mit SSL und digitalen Zertifikaten sichern

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

Secure Sockets Layer (SSL)

Der iDRAC6 umfasst einen Web Server, der zur Verwendung des SSL-Sicherheitsprotokolls nach industriellem Standard konfiguriert wurde, um verschlüsselte Daten über das Internet zu übertragen. SSL ist auf einer Verschlüsselungstechnologie mit öffentlichem und privatem Schlüssel aufgebaut. Es handelt sich um eine allgemein akzeptierte Methode, um authentifizierte und verschlüsselte Kommunikationen zwischen Clients und Servern zu ermöglichen und unbefugtes Lauschen in einem Netzwerk zu verhindern.

Merkmale eines SSL-aktivierten Systems:

- Authentifiziert sich selbst an einem SSL-aktivierten Client
- Ermöglicht dem Client, sich am Server selbst zu authentifizieren
- Ermöglicht beiden Systemen, eine verschlüsselte Verbindung herzustellen

Dieses Verschlüsselungsverfahren gewährleistet ein hohes Maß von Datenschutz. Der iDRAC6 verwendet den 128-Bit-SSL-Verschlüsselungsstandard, die sicherste Form von Verschlüsselung, die für Webbrowser in Nordamerika allgemein verfügbar ist.

Der iDRAC6-Web Server enthält ein von Dell selbst signiertes digitales Zertifikat (Server-ID). So stellen Sie eine hohe Sicherheit über das Internet sicher:

1. Ersetzen Sie das standardmäßige SSL-Zertifikat des Web Servers durch ein gültiges Zertifikat einer Zertifizierungsstelle (CA).
2. Generieren Sie eine Zertifikatsignierungsanforderung (CSR), indem Sie eine Anforderung an den iDRAC6 senden.
3. Legen Sie der Zertifizierungsstelle (CA) die CSR vor, um ein gültiges Zertifikat zu erhalten.

Zertifikatsignierungsanforderung (CSR)

Eine CSR ist eine digitale Anforderung eines sicheren Serverzertifikats von einer Zertifizierungsstelle (CA). Sichere Serverzertifikate sind erforderlich, um die Identität eines Remote-Systems zu schützen und um sicherzustellen, dass Informationen, die mit dem Remote-System ausgetauscht werden, von anderen weder gesehen noch geändert werden können. Um die Sicherheit für den iDRAC zu gewährleisten, wird dringend empfohlen, eine CSR zu erstellen, die CSR an eine Zertifizierungsstelle zu senden und das von der Zertifizierungsstelle erhaltene Zertifikat hochzuladen.

Bei einer Zertifizierungsstelle handelt es sich um ein Geschäftsunternehmen, das in der IT-Branche auf Grund seiner hohen Standards bezüglich der zuverlässigen Sicherheitsüberprüfung, Identifizierung und weiterer wichtiger Sicherheitskriterien anerkannt ist. Beispiele für CAs umfassen Thawte und VeriSign. Nachdem die CA die CSR empfangen hat, werden die in der CSR enthaltenen Informationen eingesehen und überprüft. Wenn der Bewerber den Sicherheitsstandards der CA genügt, wird für den Bewerber ein Zertifikat ausgestellt, das den Bewerber bei Übertragungen über Netzwerke oder über das Internet eindeutig identifiziert.

Nachdem die CA die CSR überprüft und ein Zertifikat gesendet hat, muss das Zertifikat zur iDRAC6-Firmware hochgeladen werden. Die auf der iDRAC6-Firmware gespeicherten CSR-Informationen müssen mit den im Zertifikat enthaltenen Informationen übereinstimmen.

Zugriff auf das SSL-Hauptmenü

1. Erweitern Sie die Struktur unter **System**, und klicken Sie auf **iDRAC-Einstellungen**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **SSL**.

Verwenden Sie das **SSL-Hauptmenü** (siehe Tabelle 22-1), um eine CSR zu erstellen, ein bestehendes Serverzertifikat hochzuladen oder ein bestehendes Serverzertifikat anzuzeigen. Die CSR-Informationen werden in der iDRAC6-Firmware gespeichert. Informationen zu den auf der Seite **SSL** verfügbaren Schaltflächen finden Sie in der *iDRAC6-Online-Hilfe*.

Tabelle 22-1. SSL-Hauptmenü

Feld	Beschreibung
Zertifikatsignierungsanforderung (CSR) erstellen	Klicken Sie auf **Weiter**, um die Seite zu öffnen, die es Ihnen ermöglicht, eine CSR zu erstellen, die an eine Zertifizierungsstelle gesendet werden kann, um ein sicheres Webzertifikat anzufordern.

Tabelle 22-1. SSL-Hauptmenü *(fortgesetzt)*

Feld	Beschreibung
Serverzertifikat hochladen	Klicken Sie auf **Weiter**, um ein vorhandenes Zertifikat hochzuladen, das Ihrem Unternehmen gehört und für die Zugriffsteuerung auf den iDRAC6 verwendet wird. **ANMERKUNG:** Der iDRAC6 akzeptiert lediglich X509-Base-64-kodierte Zertifikate. DER-kodierte Zertifikate werden nicht akzeptiert. Das Hochladen eines neuen Zertifikats ersetzt das Standardzertifikat, das Sie mit dem iDRAC6 erhalten haben.
Serverzertifikat anzeigen	Klicken Sie auf **Weiter**, um ein vorhandenes Serverzertifikat anzuzeigen.

Zertifikatsignierungsanforderung erstellen

ANMERKUNG: Jede CSR überschreibt die vorherige CSR der Firmware. Damit iDRAC ein signiertes Zertifikat annehmen kann, muss die CSR in der Firmware mit dem von der Zertifizierungsstelle zurückgesendeten Zertifikat übereinstimmen.

1. Wählen Sie auf der Seite **SSL-Hauptmenü** **Zertifikatsignierungsanforderung (CSR) erstellen** und klicken Sie auf **Weiter.**
2. Geben Sie auf der Seite **Zertifikatsignierungsanforderung (CSR) erstellen** jeweils einen Wert für die einzelnen CSR-Attribute ein.

   Tabelle 22-2 beschreibt die Optionen der Seite **Zertifikatsignierungsanforderung (CSR) erstellen**.
3. Klicken Sie auf **Erstellen**, um die CSR zu speichern.
4. Klicken Sie auf die entsprechende Schaltfläche der Seite **Zertifikatsignierungsanforderung (CSR) erstellen**, um fortzufahren. Weitere Informationen zu den auf der Seite **Zertifikatsignierungsanforderung (CSR) erstellen** verfügbaren Schaltflächen finden Sie in der *iDRAC6-Online-Hilfe*.

Tabelle 22-2. 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**). Gültig sind alphanumerische Zeichen, Bindestriche und Punkte.
Name der Organisation	Der mit dieser Organisation assoziierte Name (zum Beispiel, XYZ GmbH). Gültig sind alphanumerische Zeichen, Bindestriche und Punkte.
Organisationseinheit	Der mit einer organisatorischen Einheit assoziierte Name, z. B. eine Abteilung (zum Beispiel IT). Gültig sind alphanumerische Zeichen, Bindestriche und Punkte.
Ort	Die Stadt oder ein anderer Standort des Unternehmens, das zertifiziert wird (z. B. München). Gültig sind alphanumerische Zeichen, Bindestriche und Punkte.
Zustandsname	Das Bundesland oder der Kanton, in dem sich das Unternehmen, das sich für eine Zertifizierung bewirbt, befindet (z. B. Bayern). Gültig sind alphanumerische Zeichen, Bindestriche und Punkte.
Landescode	Der Name des Landes, in dem sich das Unternehmen befindet, das sich um eine Zertifizierung bewirbt. Verwenden Sie das Dropdown-Menü, um das Land auszuwählen.
E-Mail	Die mit der CSR verbundene E-Mail-Adresse. Sie können die E-Mail-Adresse Ihrer Firma eingeben oder eine E-Mail-Adresse, die mit der CSR in Verbindung stehen soll. Dieses Feld ist optional.

Serverzertifikat anzeigen

1. Wählen Sie auf der Seite **SSL-Hauptmenü** die Option **Serverzertifikat anzeigen** aus, und klicken Sie auf **Weiter.**

   Tabelle 22-3 erläutert die Felder und zugehörigen Beschreibungen, die im Fenster **Zertifikat** aufgeführt werden.

2. Klicken Sie auf der Seite **Serverzertifikat anzeigen** auf die entsprechende Schaltfläche, um fortzufahren.

Tabelle 22-3. Zertifikatinformationen

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

Secure Shell (SSH) verwenden

Weitere Informationen über die Verwendung von SSH finden Sie unter „Secure Shell (SSH) verwenden“ auf Seite 97.

Dienste konfigurieren

ANMERKUNG: Sie müssen die Berechtigung **iDRAC konfigurieren** besitzen, um diese Einstellungen zu ändern. Zusätzlich kann das Remote-RACADM-Befehlszeilen-Dienstprogramm nur aktiviert werden, wenn der Benutzer als **root** angemeldet ist.

1. Erweitern Sie die Struktur unter **System**, und klicken Sie auf **iDRAC-Einstellungen**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Dienste**.
3. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Lokale Konfiguration (Tabelle 22-4)
   - Web Server (Tabelle 22-5)
   - SSH (Tabelle 22-6)
   - Telnet (Tabelle 22-7)
   - Remote-RACADM (Tabelle 22-8)
   - SNMP-Agent (Tabelle 22-9)
   - Automatisierter Systeme-Wiederherstellungsagent (Tabelle 22-10)

Verwenden Sie den **Automatisierten Systeme-Wiederherstellungsagent**, um die Funktion **Bildschirm Letzter Absturz** des iDRAC6 zu aktivieren.

ANMERKUNG: Server Administrator muss mit aktivierter Funktion **Autom. Wiederherstellung** installiert werden, indem die **Maßnahme** entweder auf **System neu starten**, **System ausschalten** oder auf **System aus- und einschalten** eingestellt wird, sodass der **Bildschirm Letzter Absturz** im iDRAC6 funktionieren kann.

4 Klicken Sie auf **Änderungen annehmen**, um die Einstellungen auf der Seite Dienste zu übernehmen.

Tabelle 22-4. Einstellungen der lokalen Konfiguration

Einstellung	Beschreibung
Lokale iDRAC-Konfiguration mittels Options-ROM deaktivieren	Deaktiviert die lokale Konfiguration des iDRAC mithilfe des Options-ROM. Das Options-ROM fordert Sie auf, das Setup-Modul während des Systemneustarts durch Drücken von <Strg+E> zu öffnen.
Lokale iDRAC-Konfiguration mittels RACADM deaktivieren	Deaktiviert die lokale Konfiguration des iDRAC mithilfe von RACADM.

Tabelle 22-5. Web Server-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert den Web Server. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger Sitzungen, die für dieses System zulässig sind.
Aktive Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich **Max. Sitzungen**.

Tabelle 22-5. Web Server-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
Zeitüberschreitung	Die Zeit in Sekunden, für die eine Verbindung ungenutzt bleiben kann. Die Sitzung wird abgebrochen, wenn die Zeitüberschreitung erreicht wird. Änderungen an den Einstellungen der Zeitüberschreitung werden sofort wirksam und beenden die aktuelle Webschnittstellensitzung. Der Web Server wird ebenfalls zurückgesetzt. Bitte warten Sie einige Minuten ab, bevor Sie eine neue Webschnittstellensitzung starten. Der Zeitüberschreitungsbereich beträgt 60 bis 10.800 Sekunden. Der Standardeinstellung ist 1800 Sekunden.
HTTP-Schnittstellennummer	Der vom iDRAC verwendete Anschluss, der auf eine Serververbindung abhört. Die Standardeinstellung ist **80**.
HTTPS-Schnittstellennummer	Der vom iDRAC verwendete Anschluss, der auf eine Serververbindung abhört. Die Standardeinstellung ist **443**.

Tabelle 22-6. SSH-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert SSH. Wenn markiert, ist SSH aktiviert.
Zeitüberschreitung	Die Leerlaufzeitüberschreitung der Secure Shell in Sekunden. Der Zeitüberschreitungsbereich beträgt 60 bis 1920 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitüberschreitungsfunktion zu deaktivieren. Die Standardeinstellung ist **300.**
Port Number (Schnittstellennummer)	Der Anschluss, den der iDRAC6 auf eine Browser-Verbindung abhört. Die Standardeinstellung ist **22.**

Tabelle 22-7. Telnet-Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert Telnet. Wenn markiert, ist Telnet aktiviert.

Tabelle 22-7. Telnet-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
Zeitüberschreitung	Die Leerlaufzeitüberschreitung von Telnet in Sekunden. Der Zeitüberschreitungsbereich beträgt 60 bis 1920 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitüberschreitungsfunktion zu deaktivieren. Die Standardeinstellung ist **300.**
Port Number (Schnittstellennummer)	Der Anschluss, den der iDRAC6 auf eine Telnet-Verbindung abhört. Die Standardeinstellung ist **23.**

Tabelle 22-8. Remote-RACADM- Einstellungen

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert/deaktiviert Remote-RACADM. Wenn markiert, ist Remote-RACADM aktiviert.
Aktive Sitzungen	Die Anzahl der aktuellen Sitzungen auf dem System.

Tabelle 22-9. Einstellungen des SNMP-Agenten

Einstellung	Beschreibung
Enabled (Aktiviert)	Aktiviert oder deaktiviert den SNMP-Agenten. Markiert = Aktiviert; Unmarkiert = Deaktiviert.
Community-Name	Definieren Sie die zu verwendende SNMP-Community-Zeichenkette. Der Community-Name kann bis zu 31 Zeichen (keine Leerzeichen) lang sein. Die Standardeinstellung ist **public**.

Tabelle 22-10. Einstellung des automatisierten System-Wiederherstellungsagenten

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

Zusätzliche iDRAC6-Sicherheitsoptionen aktivieren

Um einen unberechtigten Zugriff auf das Remote-System zu verhindern, enthält der iDRAC6 die folgenden Funktionen:

- IP-Adressenfilter (IPRange) - Definiert einen spezifischen Bereich von IP-Adressen, die auf den iDRAC6 zugreifen können.
- Blockierung von IP-Adressen - Beschränkt die Anzahl von fehlgeschlagenen Anmeldeversuchen von einer spezifischen IP-Adresse

Diese Funktionen sind in der iDRAC6-Standardkonfiguration deaktiviert. Verwenden Sie den folgenden Unterbefehl oder die webbasierte Schnittstelle, um diese Funktionen zu aktivieren.

`racadm config -g cfgRacTuning -o <Objektname> <Wert>`

Verwenden Sie diese Funktionen auch in Verbindung mit den entsprechenden Sitzungszeitüberschreitungswerten und einem festgelegten Sicherheitsplan für Ihr Netzwerk.

Die folgenden Unterabschnitte enthalten zusätzliche Informationen über diese Funktionen.

IP-Filter (IpRange)

Die IP-Adressenfilterung (oder *IP-Bereichsüberprüfung*) gestattet den iDRAC6-Zugriff nur von Clients oder Management-Workstations aus, deren IP-Adressen innerhalb eines benutzerspezifischen Bereichs liegen. Alle anderen Anmeldeversuche werden abgelehnt.

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. Wenn die Ergebnisse von beiden Eigenschaften identisch sind, wird der eingehenden Anmeldeanforderung der Zugriff auf den iDRAC6 gestattet. 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.

Im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist, finden Sie eine vollständige Liste der **cfgRacTuning**-Eigenschaften.

Tabelle 22-11. Eigenschaften der IP-Adressenfilterung (IpRange)

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 mit binärem UND mit **cfgRacTuneIpRangeMask** verbunden, um den oberen Teil der erlaubten IP-Adresse zu bestimmen. Jeder IP-Adresse, die dieses Bitmuster in ihrem oberen Bitbereich enthält, wird erlaubt, eine iDRAC6-Sitzung herzustellen. Anmeldeversuche von IP-Adressen, die sich außerhalb dieses Bereichs befinden, schlagen fehl. Die Standardwerte in jeder Eigenschaft erlauben einem Adressenbereich von 192.168.1.0 bis 192.168.1.255, eine iDRAC6-Sitzung herzustellen.
cfgRacTuneIpRangeMask	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Subnetzmaske sollte in der Form einer Netzmaske sein, wobei die signifikanten Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu Nullen (0) in den niederwertigeren Bits.

IP-Filter aktivieren

Nachfolgend finden Sie einen beispielhaften Befehl zum Einrichten des IP-Filters.

Unter „RACADM im Remote-Zugriff verwenden“ auf Seite 121 finden Sie weitere Informationen zu RACADM- und RACADM-Befehlen.

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

Zur Beschränkung der Anmeldung auf eine einzelne IP-Adresse (z. B. 192.168.0.57) verwenden Sie die volle Maske, wie im folgenden Abschnitt dargestellt:

```
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
```

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 im folgenden Abschnitt dargestellt:

```
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
```

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 signifikanten Bits Einsen (1) sind (was das Subnetz in der Maske definiert), mit einem Übergang zu nur Nullen (0) in den niederwertigeren Bits.
- Verwenden Sie die Basisadresse des Bereichs, die Sie als Wert für **cfgRacTuneIpRangeAddr** bevorzugen. Der binäre 32 Bit-Wert dieser Adresse muss Nullen in allen niederwertigen Bits haben, wo Nullen in der Maske sind.

IP-Blockierung

Die IP-Blockierung stellt dynamisch fest, wenn von einer bestimmten IP-Adresse aus übermäßige Anmeldefehlversuche auftreten, und blockiert (oder hindert) die Adresse während einer zuvor festgelegten Zeitspanne an der Anmeldung am iDRAC6.

Der IP-Blockierungsparameter wendet **cfgRacTuning**-Gruppenfunktionen an, die Folgendes umfassen:

- Anzahl der zulässigen Anmeldefehlversuche
- Zeitrahmen in Sekunden, während dem die Fehlversuche auftreten müssen
- Zeitspanne in Sekunden, während der die *schuldige* IP-Adresse daran gehindert wird, eine Sitzung zu beginnen, nachdem die zulässige Gesamtanzahl von Fehlversuchen überschritten worden ist

Die Anmeldefehlversuche über eine spezifische IP-Adresse werden laufend durch einen internen Zähler *festgehalten*. 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, zeigen einige SSH-Clients u. U. die folgende Meldung an: `ssh exchange identification: Verbindung vom Remote-Host geschlossen`.

Im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*, das auf der Dell Support-Website unter **dell.com/support/manuals** verfügbar ist, finden Sie eine vollständige Liste der **cfgRacTuning**-Eigenschaften.

Tabelle 22-12 führt die vom Benutzer definierten Parameter auf.

Tabelle 22-12. Anmeldungswiederholungs-Beschränkungseigenschaften

Eigenschaft	Definition
cfgRacTuneIpBlkEnable	Aktiviert die IP-Blockierungsfunktion. Wenn aufeinander folgende Fehlversuche (**cfgRacTuneIpBlkFailCount**) von einer spezifischen IP-Adresse innerhalb eines bestimmten Zeitraums festgestellt werden (**cfgRacTuneIpBlkFailWindow**), werden alle weiteren Versuche, von dieser Adresse eine Sitzung herzustellen, während einer bestimmten Zeitspanne 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 Fehlversuche gezählt werden. Wenn die Fehlversuche diese Grenze überschreiten, werden sie aus dem Zähler gelöscht.
cfgRacTuneIpBlkPenaltyTime	Legt die Zeitspanne in Sekunden fest, während der alle Anmeldeversuche von einer IP-Adresse aufgrund übermäßiger Fehlversuche zurückgewiesen werden.

IP-Blockierung aktivieren

Das folgende Beispiel hindert eine Client-IP-Adresse fünf Minuten lang daran, eine Sitzung herzustellen, wenn dieser Client innerhalb einer Minute fünf fehlerhafte Anmeldeversuche durchgeführt hat.

```
racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindows 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
cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 3600
```

Netzwerksicherheitseinstellungen mit der iDRAC6-GUI konfigurieren

ANMERKUNG: Zum Ausführen der nachfolgenden Schritte müssen Sie über die Berechtigung **iDRAC6 konfigurieren** verfügen.

1. Klicken Sie in der Struktur unter **System** auf **iDRAC-Einstellungen**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Netzwerk**.
3. Klicken Sie auf der Seite **Netzwerkkonfiguration** auf **Erweiterte Einstellungen**.
4. Konfigurieren Sie auf der Seite **Netzwerksicherheit** die Attributwerte und klicken Sie dann auf **Änderungen anwenden**.

   Tabelle 22-13 beschreibt die Einstellungen der Seite **Netzwerksicherheit**.
5. Klicken Sie auf der Seite **Netzwerksicherheit** auf die entsprechende Schaltfläche, um fortzufahren. Weitere Informationen zu den auf der Seite **Netzwerksicherheit** verfügbaren Schaltflächen finden Sie in der *iDRAC6-Online-Hilfe*.

Tabelle 22-13. Einstellungen der Seite "Netzwerksicherheit"

Einstellungen	Beschreibung
IP-Bereich aktiviert	Aktiviert die Funktion zur Überprüfung des IP-Bereichs, mit der ein bestimmter Bereich von IP-Adressen definiert wird, die auf den iDRAC6 zugreifen können.

Tabelle 22-13. Einstellungen der Seite "Netzwerksicherheit" *(fortgesetzt)*

Einstellungen	Beschreibung
IP-Bereichs-Adresse	Bestimmt das akzeptable IP-Adressen-Bitmuster, abhängig von den Einsen (1) in der Subnetzmaske. Dieser Wert wird mit binärem UND mit der Subnetzmaske des IP-Bereichs verbunden, um den oberen Teil der zulässigen IP-Adresse zu bestimmen. Jeder IP-Adresse, die dieses Bitmuster in ihrem oberen Bitbereich enthält, wird erlaubt, eine iDRAC6-Sitzung herzustellen. Anmeldeversuche von IP-Adressen, die sich außerhalb dieses Bereichs befinden, schlagen fehl. Die Standardwerte in jeder Eigenschaft erlauben einem Adressenbereich von 192.168.1.0 bis 192.168.1.255, eine iDRAC6-Sitzung herzustellen.
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. Zum Beispiel: **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.
IP-Blockierung, Zählung von Fehlversuchen	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche von dieser Adresse zurückgewiesen werden.
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.
IP-Blockierung, Strafzeit	Die Zeitspanne in Sekunden, während der Anmeldeversuche von einer IP-Adresse aufgrund übermäßiger Fehlversuche zurückgewiesen werden.

Stichwortverzeichnis

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z