Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Anmerkungen und Vorsichtshinweise

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

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

Dezember 2009

Zurück zum Inhaltsverzeichnis

Übersicht der RACADM-Unterbefehle

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Dieser Abschnitt enthält Beschreibungen der Unterbefehle, die in der RACADM-Befehlszeilenoberfläche verfügbar sind.

VORSICHT: RACADM legt den Wert von Objekten fest, ohne sie einer Funktionsprüfung zu unterziehen. Mit RACADM ist es beispielsweise möglich, das Zertifikatvalidierungsobjekt auf 1 zu setzen, während das Active Directory-Objekt auf 0 gesetzt ist, obgleich die Zertifikatvalidierung nur dann erfolgt, wenn Active Directory® aktiviert wird. Genauso kann auch das cfgADSSOEnable-Objekt auf 0 oder 1 gesetzt werden, wenn das cfgADEnable-Objekt 0 ist. Der Wert tritt jedoch erst in Kraft, wenn Active Directory aktiviert wird.

---

help

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Am iDRAC anmelden** verfügen.

Tabelle A-1 beschreibt den Befehl **help**.

Tabelle A-1. Befehl help

Befehl	Definition
help	Führt alle verfügbaren Unterbefehle auf, die mit **RACADM** verwendet werden können, und enthält eine kurze Beschreibung der einzelnen Befehle.

Übersicht

```
racadm help

racadm help <Unterbefehl>
```

Beschreibung

Der Unterbefehl **help** führt alle Unterbefehle, die unter dem Befehl **racadm** verfügbar sind, zusammen mit einer einzeiligen Beschreibung auf. Es kann auch ein Unterbefehl nach **help** eingegeben werden, um die Syntax für einen bestimmten Unterbefehl zu erhalten.

Ausgabe

Der Befehl **racadm help** zeigt eine vollständige Liste aller Unterbefehle an.

Der Befehl **racadm help** <*Unterbefehl*> zeigt nur Informationen für den angegebenen Unterbefehl an.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

arp

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Diagnosebefehle ausführen** verfügen.

Tabelle A-2 beschreibt den Befehl **arp**.

Tabelle A-2. Befehl arp

Befehl	Definition
arp	Zeigt den Inhalt der ARP-Tabelle an. Es dürfen keine ARP-Tabelleneinträge hinzugefügt oder gelöscht werden.

Übersicht

```
racadm arp
```

Unterstützte Schnittstellen

- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

clearasrscreen

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Protokolle löschen** verfügen.

Tabelle A-3 beschreibt den Unterbefehl **clearasrscreen**.

Tabelle A-3. clearasrscreen

Unterbefehl	Definition
clearasrscreen	Löscht den letzten Absturzbildschirm, der sich im Speicher befindet.

Übersicht

```
racadm clearasrscreen
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

config

ANMERKUNG: Um den Befehl **getconfig** zu verwenden, müssen Sie über die Berechtigung **Am iDRAC anmelden** verfügen.

Tabelle A-4 beschreibt die Unterbefehle **config** und **getconfig**.

Tabelle A-4. config/getconfig

Unterbefehl	Definition
config	Konfiguriert den iDRAC6.
getconfig	Ruft die iDRAC6-Konfigurationsdaten ab.

Übersicht

```
racadm config [-c|-p] -f <Dateiname>

racadm config -g <Gruppenname> -o <Objektname> [-i <Index>] <Wert>
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

Beschreibung

Mit dem Unterbefehl **config** kann der Benutzer die Konfigurationsparameter des iDRAC6 einzeln oder stapelweise als Teil einer Konfigurationsdatei einrichten. Wenn sich die Daten unterscheiden, wird das iDRAC6-Objekt mit dem neuen Wert geschrieben.

ANMERKUNG: Die unter Verwendung von remote racadm und local racadm abgerufenen Konfigurationsdateien sind nicht interoperabel. Die unter Verwendung von remote racadm abgerufene Konfigurationsdatei zeigt die Indexeigenschaft für einige der indizierten Gruppen als Lesen/Schreiben an, z. B. cfgSSADRoleGroupIndex. Verwenden Sie für den Befehl "config -f <Dateiname>" die über dieselbe Schnittstelle abgerufene Konfigurationsdatei. Beispiel: Verwenden Sie für local racadm "config -f <Dateiname>" die aus dem lokalen racadm-Befehl "getconfig -f <Dateiname>" erstellte Datei.

Eingabe

Tabelle A-5 beschreibt die Optionen des Unterbefehls **config**.

ANMERKUNG: Die Optionen **-f** und **-p** werden für die serielle/Telnet/ssh-Konsole nicht unterstützt.

Tabelle A-5. Optionen und Beschreibungen des Unterbefehls config

Option	Beschreibung
-f	Über die Option **-f** <***Dateiname***> liest **config** den Inhalt der durch <***Dateiname***> festgelegten Datei und konfiguriert den iDRAC6. Die Datei muss Daten enthalten, die dem unter "Parsing-Regeln" festgelegten Format entsprechen.
-p	Die Option **-p** bzw. die Kennwortoption weist **config** an, die Kennworteinträge in der config-Datei **-f <*Dateiname*>** zu löschen, sobald die Konfiguration abgeschlossen wurde.
-g	Die Option **-g <*Gruppenname*>** bzw. die Gruppenoption muss zusammen mit der Option **-o** verwendet werden. Der <*Gruppenname*> gibt die Gruppe an, in der das einzustellende Objekt enthalten ist.
-o	Die Option **-o <*Objektname*> <*Wert*>** bzw. die Objektoption muss zusammen mit der Option **-g** verwendet werden. Diese Option legt den Objektnamen fest, der mit der Zeichenkette <*Wert*> geschrieben wird.
-i	Die Option **-i <*Index*>** bzw. die Indexoption ist nur für indizierte Gruppen gültig und kann zur Bestimmung einer eindeutigen Gruppe verwendet werden. Der <*Index*> ist eine ganze Dezimalzahl von 1 bis 16. Der Index wird hier durch den Indexwert bestimmt und nicht durch einen "benannten" Wert.
-c	Die Option **-c** bzw. die Überprüfungsoption wird zusammen mit dem Unterbefehl **config** verwendet und ermöglicht es dem Benutzer, die **.cfg**-Datei auf Syntaxfehler zu analysieren. Falls Fehler gefunden werden, wird die Zeilennummer zusammen mit einer kurzen Beschreibung des Fehlers angezeigt. Es finden keine Schreibvorgänge auf dem iDRAC6 statt. Diese Option ist nur eine Kontrolle.

Ausgabe

Dieser Unterbefehl erzeugt eine Fehlerausgabe, wenn einer der folgenden Umstände eintritt:

- Ungültige Syntax, ungültiger Gruppenname, Objektname, Index oder andere ungültige Datenbankmitglieder
- RACADM-CLI-Fehler

Dieser Unterbefehl zeigt an, wie viele Konfigurationsobjekte im Verhältnis zu den Gesamtobjekten in der **.cfg**-Datei geschrieben wurden.

Beispiele

- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100`

  Stellt den **cfgNicIpAddress**-Konfigurationsparameter (Objekt) auf den Wert 10.35.10.110 ein. Dieses IP-Adressen-Objekt befindet sich in der Gruppe **cfgLanNetworking**.

- `racadm config -f myrac.cfg`

  Konfiguriert oder neukonfiguriert den iDRAC6. Die Datei **myrac.cfg** kann aus dem Befehl **getconfig** erstellt werden. Die Datei **myrac.cfg** kann auch manuell bearbeitet werden, solange die Analyserichtlinien befolgt werden.

ANMERKUNG: Die Datei **myrac.cfg** enthält keine Kennwortinformationen. Um diese Informationen in der Datei zu speichern, müssen sie manuell eingegeben werden. Wenn Sie während der Konfiguration Kennwortinformationen aus der Datei **myrac.cfg** entfernen möchten, verwenden Sie die Option **-p** .

ANMERKUNG: Um PEF-Maßnahmen für den informativen Assertionsfilter der SD-Karte zu konfigurieren, können Sie nicht den lokalen racadm-Befehl verwenden. Verwenden Sie stattdessen den Befehl `remote racadm: racadm -r <iDRAC6-IP-Adresse> -u <Benutzername> -p <calvin> config -g cfgIpmipef -i 20 -o cfgIpmipefaction [0-3]`.

---

getconfig

Beschreibung des Unterbefehls getconfig

Mit dem Unterbefehl **getconfig** kann der Benutzer iDRAC6-Konfigurationsparameter einzeln abrufen oder alle iDRAC6-Konfigurationsgruppen abrufen und in einer Datei speichern.

Eingabe

Tabelle A-6 beschreibt die Optionen des Unterbefehls **getconfig**.

ANMERKUNG: Die Option **-f** ohne Dateiangabe gibt den Dateiinhalt auf den Terminal-Bildschirm aus.

Tabelle A-6. Optionen des Unterbefehls getconfig

Option	Beschreibung
-f	Die Option -f <*Dateiname*> weist getconfig an, die gesamte iDRAC6-Konfiguration in eine Konfigurationsdatei zu schreiben. Diese Datei kann für Stapelverarbeitungs-Konfigurationsvorgänge verwendet werden, die den Unterbefehl **config** verwenden. **ANMERKUNG:** Die Option **-f** erstellt keine Einträge für die Gruppen **cfgIpmiPet** und **cfgIpmiPef**. Sie müssen mindestens ein Trap-Ziel festlegen, um die **cfgIpmiPet**-Gruppe in die Datei zu erfassen.
-g	Die Option -g <*Gruppenname*> bzw. Gruppenoption kann zur Anzeige der Konfiguration einer einzelnen Gruppe verwendet werden. Der **Gruppenname** ist der Name der Gruppe, die in den **racadm.cfg**-Dateien verwendet wird. Wenn es sich bei der Gruppe um eine indizierte Gruppe handelt, verwenden Sie die Option **-i**.
-h	Die Option **-h** bzw. die **Hilfe**option zeigt eine Liste aller vorhandenen Konfigurationsgruppen an, die Sie verwenden können. Diese Option ist nützlich, wenn die genauen Gruppennamen nicht bekannt sind.
-i	Die Option -i <*Index*> bzw. die Indexoption ist nur für indizierte Gruppen gültig und kann zur Bestimmung einer eindeutigen Gruppe verwendet werden. Der <*Index*> ist eine ganze Dezimalzahl von 1 bis 16. Wenn die Option **-i <***Index***>** nicht angegeben wird, wird ein Wert von 1 für Gruppen angenommen, bei denen es sich um Tabellen mit mehreren Einträgen handelt. Der Index wird durch den Indexwert bestimmt und nicht durch einen "benannten" Wert.
-o	Die Option -o <*Objektname*> bzw. die Objektoption bestimmt den Objektnamen, der in der Abfrage verwendet wird. Diese Option ist optional und kann mit der Option -g verwendet werden.
-u	Die Option -u <*Benutzername*> bzw. die Benutzerna**me**nsoption kann verwendet werden, um die Konfiguration für den festgelegten Benutzer anzuzeigen. Die Option **<***Benutzername***>** ist der Anmeldename des Benutzers.
-v	Die Option **-v** zeigt zusätzliche Details durch Anzeige der Eigenschaften an und wird mit der Option **-g** verwendet.

Ausgabe

Dieser Unterbefehl erzeugt eine Fehlerausgabe, wenn einer der folgenden Umstände eintritt:

- Ungültige Syntax, ungültiger Gruppenname, Objektname, Index oder andere ungültige Datenbankmitglieder
- RACADM-CLI-Übertragungsfehler

Wenn keine Fehler festgestellt werden, zeigt dieser Unterbefehl den Inhalt der angegebenen Konfiguration an.

Beispiele

- `racadm getconfig -g cfgLanNetworking`

  Zeigt alle Konfigurationseigenschaften (Objekte) an, die in der Gruppe **cfgLanNetworking** enthalten sind.

- `racadm getconfig -f myrac.cfg`

  Speichert alle Gruppenkonfigurationsobjekte vom iDRAC6 in **myrac.cfg**.

- `racadm getconfig -h`

  Zeigt eine Liste der verfügbaren Konfigurationsgruppen auf dem iDRAC6 an.

- `racadm getconfig -u root`

  Zeigt die Konfigurationseigenschaften für den Benutzer mit dem Namen root an.

- `racadm getconfig -g cfgUserAdmin -i 2 -v`

  Zeigt die Benutzergruppen-Instanz bei Index 2 mit ausführlichen Informationen für die Eigenschaftswerte an.

Übersicht

```
racadm getconfig -f <Dateiname>

racadm getconfig -g <Gruppenname> [-i <Index>]

racadm getconfig -u <Benutzername>

racadm getconfig -h
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

coredump

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Debug-Befehle ausführen** verfügen.

Tabelle A-7 beschreibt den Unterbefehl **coredump**.

Tabelle A-7. coredump

Unterbefehl	Definition
coredump	Zeigt den letzten Core Dump des iDRAC6 an.

Übersicht

```
racadm coredump
```

Beschreibung

Mit dem Unterbefehl **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 Betriebszyklen des iDRAC6 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 Unterbefehl **coredumpdelete** enthält weitere Informationen über das Löschen des **coredump**.

Unterstützte Schnittstellen

- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

coredumpdelete

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Protokolle löschen** oder **Debug-Befehle ausführen** verfügen.

Tabelle A-8 beschreibt den Unterbefehl **coredumpdelete**.

Tabelle A-8. coredumpdelete

Unterbefehl	Definition
coredumpdelete	Löscht den im iDRAC6 gespeicherten Core Dump.

Übersicht

```
racadm coredumpdelete
```

Beschreibung

Der Unterbefehl **coredumpdelete** kann zum Löschen aller gegenwärtig vorhandenen, im RAC gespeicherten **coredump**-Daten verwendet werden.

ANMERKUNG: Wenn der Befehl **coredumpdelete** abgegeben wird und gegenwärtig kein Core Dump im RAC gespeichert ist, wird für den Befehl eine Erfolgsmeldung angezeigt. Dieses Verhalten wird erwartet.

Weitere Information zum Anzeigen eines Core Dump finden Sie beim Unterbefehl **coredump**.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

fwupdate

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC6 konfigurieren** verfügen.

ANMERKUNG: Lesen Sie die zusätzlichen Informationen unter "Erweiterte iDRAC6-Konfiguration", bevor Sie mit der Firmware-Aktualisierung beginnen.

Tabelle A-9 beschreibt den Unterbefehl **fwupdate**.

Tabelle A-9. fwupdate

Unterbefehl	Definition
fwupdate	Aktualisiert die Firmware auf dem iDRAC6.

Übersicht

```
racadm fwupdate -s
```

```
racadm fwupdate -g -u -a <TFTP_Server-IP-Adresse> [-d <Pfad>]

racadm fwupdate -r
```

Beschreibung

Mit dem Unterbefehl **fwupdate** können Benutzer die Firmware auf dem iDRAC6 aktualisieren. Der Benutzer kann:

- Den Status des Firmware-Aktualisierungsverfahrens prüfen
- Die iDRAC6-Firmware von einem TFTP-Server durch Angabe einer IP-Adresse und eines optionalen Pfads aktualisieren.
- Die iDRAC6-Firmware vom lokalen Dateisystem mittels lokalem RACADM aktualisieren.
- Auf die Standby-Firmware zurücksetzen.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM (Die Option **-p** wird bei der seriellen/Telnet/ssh-Konsole nicht unterstützt)

Eingabe

Tabelle A-10 beschreibt die Optionen des Unterbefehls **fwupdate**.

ANMERKUNG: Die Option **-p** wird auf lokalem und Remote-RACADM unterstützt. Bei der seriellen/Telnet/ssh-Konsole wird sie jedoch nicht unterstützt. Die Option **-p** wird außerdem auch auf Linux-Betriebssystemen nicht unterstützt.

Tabelle A-10. Optionen des Unterbefehls fwupdate

Option	Beschreibung
-u	Die Option **Aktualisierung** führt einen Prüfsummentest der Firmware-Aktualisierungsdatei durch und startet das eigentliche Aktualisierungsverfahren. Diese Option kann zusammen mit den Optionen **-g** oder **-p** verwendet werden. Nach der Aktualisierung führt der iDRAC6 einen Software-Neustart durch.
-s	Die Option **Status** gibt Informationen zum derzeitigen Status des Aktualisierungsverfahrens aus. Diese Option wird immer allein verwendet.
-g	Die Option **get** weist die Firmware an, die Firmware-Aktualisierungsdatei vom TFTP-Server abzurufen. Der Benutzer muss auch die Optionen **-a** und **-d** angeben. Wenn die Option **-a** nicht zur Verfügung steht, werden die Standardeinstellungen in den Eigenschaften der Gruppe **cfgRemoteHosts** gelesen, wobei die Eigenschaften **cfgRhostsFwUpdateIpAddr** und **cfgRhostsFwUpdatePath** verwendet werden.
-a	Die Option **IP-Adresse** gibt die IP-Adresse des TFTP-Servers an.
-d	Die Option **-d** bzw. **directory** bestimmt das Verzeichnis auf dem TFTP-Server oder auf dem Hostserver des iDRAC6, in dem sich die Firmware-Aktualisierungsdatei befindet.
-p	Die Option **-p** bzw. **put** wird zum Aktualisieren der Firmware-Datei vom verwalteten System zum iDRAC6 verwendet. Die Option **-u** muss zusammen mit der Option **-p** verwendet werden.
-r	Die Option **rollback** wird zum Zurücksetzen der Standby-Firmware verwendet.

Ausgabe

Zeigt durch eine Meldung an, welcher Vorgang ausgeführt wird.

Beispiele

- `racadm fwupdate -g -u - a 143.166.154.143 -d <Pfad>`

  In diesem Beispiel wird die Firmware durch die Option **-g** angewiesen, die Firmware-Aktualisierungsdatei von einem Speicherort (durch die Option **-d a**ngegeben) auf dem TFTP-Server unter einer bestimmten IP-Adresse (durch die Option **-a** angegeben) herunterzuladen. Nachdem die Imagedatei vom TFTP-Server heruntergeladen wurde, beginnt der Aktualisierungsvorgang. Wenn dieser abgeschlossen ist, wird der iDRAC6 zurückgesetzt.

- `racadm fwupdate -s`

  Diese Option liest den derzeitigen Status der Firmware-Aktualisierung.

ANMERKUNG: Die Firmware-Aktualisierung mit Remote-RACADM über den lokalen Pfad wird auf Linux-Betriebssystemen nicht unterstützt.

getssninfo

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Am iDRAC anmelden** verfügen.

Tabelle A-11 beschreibt den Unterbefehl **getssninfo**.

Tabelle A-11. Unterbefehl getssninfo

Unterbefehl	Definition
getssninfo	Sitzungsinformationen für eine oder mehrere derzeit aktive oder ausstehende Sitzungen der Sitzungstabelle des Sitzungs-Managers abrufen.

Übersicht

```
racadm getssninfo [-A] [-u <Benutzername> | *]
```

Beschreibung

Über den Befehl **getssninfo** wird eine Liste der Benutzer ausgegeben, die mit dem iDRAC6 verbunden sind. Die zusammenfassenden Informationen geben die folgende Auskunft:

- Benutzername
- IP-Adresse (falls zutreffend)
- Sitzungstyp (Beispiel: seriell oder Telnet)
- Konsolen in Gebrauch (zum Beispiel: virtueller Datenträger oder virtuelle KVM)

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

Eingabe

Tabelle A-12 beschreibt die Optionen des Unterbefehls **getssninfo**.

Tabelle A-12. Optionen des Unterbefehls getssninfo

Option	Beschreibung
-A	Die Option **-A** unterdrückt das Drucken von Datenkopfzeilen.
-u	Die Benutzernamenoption **-u <***Benutzername***>** begrenzt die ausgedruckte Ausgabe auf detaillierte Sitzungseinträge für den angegebenen Benutzernamen. Wenn das Zeichen "*" als Benutzername angegeben wird, werden alle Benutzer aufgelistet. Es werden keine zusammenfassenden Informationen gedruckt, wenn diese Option angegeben wird.

Beispiele

- `racadm getssninfo`

Tabelle A-13 enthält ein Ausgabebeispiel des Befehls **racadm getssninfo**.

Tabelle A-13. Ausgabebeispiel des Unterbefehls getssninfo

Benutzer	IP-Adresse	Typ	Konsolen
root	192.168.0.10	Telnet	Virtuelle KVM

- `racadm getssninfo -A`

  ```
  "root" "143.166.174.19" "Telnet" "NONE"
  ```

- `racadm getssninfo -A -u *`

  `"root" "143.166.174.19" "Telnet" "NONE"`

  `"bob" "143.166.174.19" "GUI" "NONE"`

---

getsysinfo

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Am iDRAC anmelden** verfügen.

Tabelle A-14 beschreibt den Unterbefehl **racadm getsysinfo**.

Tabelle A-14. getsysinfo

Befehl	Definition
getsysinfo	Zeigt Informationen zum iDRAC6, System und Watchdog-Status an.

Übersicht

```
racadm getsysinfo [-d] [-s] [-w] [-A] [-c] [-4] [-6] [-r]
```

Beschreibung

Mit dem Unterbefehl **getsysinfo** werden Informationen im Zusammenhang mit der Konfiguration des RAC, verwalteten Systems und Watchdogs angezeigt.

ANMERKUNG: Der lokale racadm-Unterbefehl *getsysinfo* auf Linux zeigt die *PrefixLength (Präfixlänge)* in separaten Zeilen für IPv6-Adresse 2 - IPv6-Adresse 15 und die Link-Local-Adresse an.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

Eingabe

Tabelle A-15 beschreibt die Optionen des Unterbefehls **getsysinfo**.

Tabelle A-15. Optionen des Unterbefehls getsysinfo

Option	Beschreibung
-4	Zeigt IPv4-Einstellungen an.
-6	Zeigt IPv6-Einstellungen an.
-c	Zeigt allgemeine Einstellungen an.
-d	Zeigt iDRAC6-Informationen an.
-s	Zeigt Systeminformationen an
-w	Zeigt Watchdog-Informationen an
-A	Unterdrückt das Drucken von Kopfzeilen und Kennzeichnungen.

Wenn die Option **-w** nicht angegeben wird, werden die anderen Optionen als Standardeinstellungen verwendet.

Ausgabe

Mit dem Unterbefehl **getsysinfo** werden Informationen im Zusammenhang mit der Konfiguration des RAC, verwalteten Systems und Watchdogs angezeigt.

Beispielausgabe

```
RAC Information:

RAC Date/Time = 10/27/2009 14:38:00

Firmware Version = 1.30

Firmware Build = 20

Last Firmware Update = 10/26/2009 16:55:08

Hardware Version = 0.01

MAC Address = 00:24:e8:2e:c5:d3

Common settings:

Register DNS RAC Name = 1

DNS RAC Name = eval710-08-r

Current DNS Domain = blr.amer.dell.com

Domain Name from DHCP = 1

IPv4 settings:

Enabled = 1

Current IP Address = 10.94.20.134

Current IP Gateway = 10.94.20.1

Current IP Netmask = 255.255.254.0

DHCP Enabled = 1

Current DNS Server 1 = 163.244.180.39

Current DNS Server 2 = 163.244.180.40

DNS Servers from DHCP = 1

IPv6 settings:

Enabled = 1

Current IP Address 1 = ::

Current IP Gateway = ::

Autoconfig = 1

Link Local IP Address = fe80::224:e8ff:fe2e:c5d3/255

Current IP Address 2 = ::

Current IP Address 3 = ::

Current IP Address 4 = ::

Current IP Address 5 = ::

Current IP Address 6 = ::

Current IP Address 7 = ::

Current IP Address 8 = ::

Current IP Address 9 = ::

Current IP Address 10 = ::

Current IP Address 11 = ::

Current IP Address 12 = ::

Current IP Address 13 = ::

Current IP Address 14 = ::

Current IP Address 15 = ::
```

```
DNS Servers from DHCPv6 = 0

Current DNS Server 1 = ::

Current DNS Server 2 = ::

System Information:

System Model = PowerEdge R710

System BIOS Version = 1.0.4

Service Tag = 2X2Q12S

Host Name = WIN-IHF5D2BF5SN

OS Name =

Power Status = ON

Embedded NIC MAC Addresses:

NIC1 Ethernet = 00:24:e8:2e:c5:cb

iSCSI = 00:24:e8:2e:c5:cc

NIC2 Ethernet = 00:24:e8:2e:c5:cd

iSCSI = 00:24:e8:2e:c5:ce

NIC3 Ethernet = 00:24:e8:2e:c5:cf

iSCSI = 00:24:e8:2e:c5:d0

NIC4 Ethernet = 00:24:e8:2e:c5:d1

iSCSI = 00:24:e8:2e:c5:d2

Watchdog Information:

Recovery Action = None

Present countdown value = 15 seconds

Initial countdown value = 15 seconds
```

Beispiele

- `racadm getsysinfo -A -s`

  `"System Information:" "PowerEdge 2900" "A08" "1.0" "EF23VQ-0023" "Hostname"`

  `"Microsoft Windows 2000 version 5.0, Build Number 2195, Service Pack 2" "ON"`

- `racadm getsysinfo -w -s`

```
System Information:
System Model             = PowerEdge 2900
System BIOS Version      = 0.2.3
BMC Firmware Version     = 0.17
Service Tag              = 48192
Host Name                = racdev103
OS Name                  = Microsoft Windows Server 2003
Power Status            = OFF


Watchdog Information:
Recovery Action          = None
Present countdown value  = 0 seconds
Initial countdown value = 0 seconds
```

Einschränkungen

Die Felder Hostname (Host-Name) und OS Name (BS-Name) in der **getsysinfo**-Ausgabe zeigen nur dann genaue Informationen an, wenn Dell™ OpenManage™ Server Administrator auf dem verwalteten System installiert ist. Wenn er nicht installiert ist, sind diese Felder eventuell leer oder enthalten falsche Angaben.

getractime

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Am iDRAC anmelden** verfügen.

Tabelle A-16 beschreibt den Unterbefehl **getractime**.

Tabelle A-16. getractime

Unterbefehl	Definition
getractime	Zeigt die aktuelle Uhrzeit vom Remote Access Controller an.

Übersicht

```
racadm getractime [-d]
```

Beschreibung

Ohne Optionen zeigt der Unterbefehl **getractime** die Zeit in einem allgemein lesbaren Format an.

Mit der Option **-d** zeigt **getractime** die Zeit im Format *yyyymmddhhmmss.mmmmmms* an. Dieses Format wird auch vom UNIX-Befehl **date** zurückgegeben.

Ausgabe

Der Unterbefehl **getractime** zeigt die Ausgabe auf einer Zeile an.

Beispielausgabe

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20051208201542.000000
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

ifconfig

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Diagnosebefehle ausführen** oder **iDRAC konfigurieren** verfügen.

Tabelle A-17 beschreibt den Unterbefehl **ifconfig**.

Tabelle A-17. ifconfig

Unterbefehl	Definition
ifconfig	Zeigt den Inhalt der Netzwerkschnittstellentabelle an.

Übersicht

```
racadm ifconfig
```

netstat

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Diagnosebefehle ausführen** verfügen.

Tabelle A-18 beschreibt den Unterbefehl **netstat**.

Tabelle A-18. netstat

Unterbefehl	Definition
netstat	Zeigt die Routingtabelle und die aktuellen Verbindungen an.

Übersicht

```
racadm netstat
```

Unterstützte Schnittstellen

- Remote-RACADM
- Telnet/ssh/serieller RACADM

ping

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Diagnosebefehle ausführen** oder **iDRAC konfigurieren** verfügen.

Tabelle A-19 beschreibt den Unterbefehl **ping**.

Tabelle A-19. ping

Unterbefehl	Definition
ping	Überprüft, ob die Ziel-IP-Adresse unter Verwendung des Inhalts der aktuellen Routingtabelle vom iDRAC6 aus erreichbar ist. Eine Ziel-IP-Adresse ist erforderlich. Ein ICMP-Echo-Paket wird zur Ziel-IP-Adresse gesendet, basierend auf dem Inhalt der aktuellen Routingtabelle.

Übersicht

```
racadm ping <IP-Adresse>
```

Unterstützte Schnittstellen

- Remote-RACADM
- Telnet/ssh/serieller RACADM

setniccfg

ANMERKUNG: Um den Befehl **setniccfg** zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-20 beschreibt den Unterbefehl **setniccfg**.

Tabelle A-20. setniccfg

Unterbefehl	Definition
setniccfg	Stellt die IP-Konfiguration für den Controller ein.

ANMERKUNG: Die Begriffe NIC und Ethernet-Verwaltungsanschluss können synonym verwendet werden.

Übersicht

```
racadm setniccfg -d

racadm setniccfg -d6

racadm setniccfg -s <IPv4-Adresse> <Netzmaske> <IPv4-Gateway>

racadm setniccfg -s6 <IPv6-Adresse> <IPv6-Präfixlänge> <IPv6-Gateway>

racadm setniccfg -o
```

Beschreibung

Der Unterbefehl **setniccfg** stellt die IP-Adresse des Controllers ein.

- Die Option **-d** aktiviert DHCP für den Ethernet-Verwaltungsanschluss (standardmäßig ist DHCP deaktiviert).
- Die Option **-d6** aktiviert die automatische Konfiguration für den Ethernet-Verwaltungsanschluss. Sie ist standardmäßig aktiviert.
- Die Option **-s** aktiviert statische IP-Einstellungen. IPv4-Adresse, Netzmaske und Gateway können angegeben werden. Ansonsten werden die vorhandenen statischen Einstellungen verwendet. *<IPv4-Adresse>*, *<Netzmaske>* und *<Gateway>* müssen als durch Punkte getrennte Zeichenketten eingegeben werden.
- Die Option **-s6** aktiviert die statischen IPv6-Einstellungen. IPv6-Adresse, Präfixlänge und IPv6-Gateway können angegeben werden.
- Die Option **-o** deaktiviert den Ethernet-Verwaltungsanschluss vollständig.

Ausgabe

Mit dem Unterbefehl **setniccfg** wird eine entsprechende Fehlermeldung angezeigt, wenn der Vorgang nicht erfolgreich ist. Wenn erfolgreich, wird eine Meldung angezeigt.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

getniccfg

ANMERKUNG: Um den Befehl **getniccfg** zu verwenden, müssen Sie über die Berechtigung **Am iDRAC anmelden** verfügen.

Tabelle A-21 beschreibt die Unterbefehle **setniccfg** und **getniccfg**.

Tabelle A-21. setniccfg/getniccfg

Unterbefehl	Definition
getniccfg	Zeigt die derzeitige IP-Konfiguration für den Controller an.

Übersicht

```
racadm getniccfg
```

Beschreibung

Der Unterbefehl **getniccfg** zeigt die aktuellen Einstellungen des Ethernet-Verwaltungsanschlusses an.

Beispielausgabe

Mit dem Unterbefehl **getniccfg** wird eine entsprechende Fehlermeldung angezeigt, wenn der Vorgang nicht erfolgreich ist. Andernfalls wird bei erfolgreicher Ausführung die Ausgabe in folgendem Format angezeigt:

```
NIC Enabled     = 1

DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

getsvctag

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Am iDRAC anmelden** verfügen.

Tabelle A-22 beschreibt den Unterbefehl **getsvctag**.

Tabelle A-22. getsvctag

Unterbefehl	Definition
getsvctag	Zeigt eine Service-Tag-Nummer an.

Übersicht

```
racadm getsvctag
```

Beschreibung

Der Unterbefehl **getsvctag** wird verwendet, um die Service-Tag-Nummer für das Hostsystem anzuzeigen.

Beispiel

Geben Sie an der Eingabeaufforderung `getsvctag` ein. Die Ausgabe wird folgendermaßen angezeigt:

```
Y76TP0G
```

Der Befehl gibt `0` bei Erfolg und einen anderen Wert als Null bei Fehlern aus.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

racdump

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Debug** verfügen.

Tabelle A-23 beschreibt den Unterbefehl **racdump**.

Tabelle A-23. racdump

Unterbefehl	Definition
racdump	Zeigt den Status und allgemeine Informationen zum iDRAC6 an.

Übersicht

```
racadm racdump
```

Beschreibung

Der Unterbefehl **racdump** bietet einen Einzelbefehl, mit dem ein Speicherabbild, der Status und allgemeine iDRAC6-Platineninformationen abgefragt werden können.

Die folgenden Informationen werden angezeigt, wenn der Unterbefehl **racdump** verarbeitet wird:

- Allgemeine System-/RAC-Informationen
- Coredump
- Sitzungsinformationen
- Verfahrensinformationen
- Firmware-Build-Informationen

Unterstützte Schnittstellen

- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

racreset

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-24 beschreibt den Unterbefehl **racreset**.

Tabelle A-24. racreset

Unterbefehl	Definition
racreset	Setzt den iDRAC6 zurück.

ANMERKUNG: Wenn Sie einen racreset-Unterbefehl abgeben, kann der iDRAC6 bis zu einer Minute in Anspruch nehmen, um in einen einsatzfähigen Zustand zurückzukehren.

Übersicht

```
racadm racreset [hard | soft]
```

Beschreibung

Der Unterbefehl **racreset** sendet einen Reset an den iDRAC6. Das Reset-Ereignis wird in das iDRAC6-Protokoll eingetragen.

Ein Hardware-Reset führt einen tiefen Reset-Vorgang auf dem RAC aus. Ein Hardware-Reset sollte nur als letztes Mittel ausgeführt werden, um den RAC wiederherzustellen.

ANMERKUNG: Das System muss nach einem Hardware-Reset des iDRAC6 neu gestartet werden, siehe Tabelle A-25.

Tabelle A-25 beschreibt die Optionen des Unterbefehls **racreset**.

Tabelle A-25. Optionen des Unterbefehls racreset

Option	Beschreibung
hard	Ein *Hardware*-Reset führt einen tiefen Reset-Vorgang auf dem Remote Access Controller aus. Ein Hardware-Reset sollte nur als letztes Mittel ausgeführt werden, um den iDRAC6-Controller zu Wiederherstellungszwecken zurückzusetzen.
soft	Ein *Software*-Reset führt einen sanften Neustart auf dem RAC aus.

Beispiele

- `racadm racreset`

  Starten Sie die Software-Reset-Sequenz für den iDRAC6.

- `racadm racreset hard`

  Starten Sie die Hard-Reset-Sequenz für den iDRAC 6.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

racresetcfg

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-26 beschreibt den Unterbefehl **racresetcfg**.

Tabelle A-26. racresetcfg

Unterbefehl	Definition
racresetcfg	Setzt die gesamte iDRAC6-Konfiguration auf die werkseitigen Standardwerte zurück.

Übersicht

```
racadm racresetcfg
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

Beschreibung

Der Befehl **racresetcfg** entfernt alle vom Benutzer konfigurierten Einträge der Datenbankeigenschaften. Die Datenbank besitzt Standardeigenschaften für alle Einträge, die zur Wiederherstellung der ursprünglichen Standardeinstellungen des Controllers verwendet werden. Nach dem Zurücksetzen der Datenbankeigenschaften wird der iDRAC6 automatisch zurückgesetzt.

ANMERKUNG: Mit diesem Befehl wird die aktuelle iDRAC6-Konfiguration gelöscht und der iDRAC6 und die serielle Konfiguration werden auf die ursprünglichen Standardeinstellungen zurückgesetzt. Nach dem Reset sind der Standardname bzw. das Standardkennwort **root** bzw. **calvin**, und die IP-Adresse lautet 192.168.0.120. Wenn Sie den Befehl **racresetcfg** von einem Netzwerk-Client (z. B. einem unterstützten Webbrowser, Telnet/ssh oder Remote-RACADM) senden, müssen Sie die Standard-IP-Adresse verwenden.

ANMERKUNG: Bestimmte iDRAC6-Firmware-Prozesse müssen zum Zurücksetzen auf die Standardeinstellungen angehalten und neu gestartet werden, um den Vorgang abzuschließen. Der iDRAC6 ist für ca. 30 Sekunden nicht ansprechbar, während dieser Vorgang abgeschlossen wird.

---

serveraction

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Serversteuerungsbefehle ausführen** verfügen.

Tabelle A-27 beschreibt den Unterbefehl **serveraction**.

Tabelle A-27. serveraction

Unterbefehl	Definition
serveraction	Führt einen Reset des verwalteten Systems oder einen Einschalt-/Ausschaltzyklus durch.

Übersicht

```
racadm serveraction <Maßnahme>
```

Beschreibung

Der Unterbefehl serveraction ermöglicht Benutzern, Stromverwaltungsvorgänge auf dem Host-System auszuführen. Tabelle A-28 beschreibt die Stromregelungsoptionen von **serveraction**.

Tabelle A-28. Optionen des Unterbefehls serveraction

Zeichenkette	Definition
<Maßnahme>	Bestimmt die 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 gleicht dem Drücken des Netzschalters an der Systemvorderseite, 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.

Ausgabe

Mit dem Unterbefehl **serveraction** wird eine Fehlermeldung angezeigt, wenn der angeforderte Vorgang nicht durchgeführt werden konnte, bzw. eine Erfolgsmeldung, wenn der Vorgang erfolgreich beendet wurde.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

getraclog

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Am iDRAC anmelden** verfügen.

Tabelle A-29 beschreibt den Befehl **racadm getraclog**.

Tabelle A-29. getraclog

Befehl	Definition
getraclog -i	Zeigt die Anzahl der Einträge im iDRAC6-Protokoll an.
getraclog	Zeigt die iDRAC6-Protokolleinträge an.

Übersicht

```
racadm getraclog -i

racadm getraclog [-A] [-o] [-c Zählwert] [-s Start-Datensatz] [-m]
```

Beschreibung

Der Befehl **getraclog -i** zeigt die Anzahl der Einträge im iDRAC6-Protokoll an.

Anhand der folgenden Optionen kann der Befehl **getraclog** Einträge lesen:

- **-A** - Zeigt die Ausgabe ohne Kopfzeilen oder Kennzeichnungen an.
- **-c** - Zeigt die Höchstanzahl der zurückzugebenden Einträge an.
- **-m** - Zeigt jeweils einen Bildschirm mit Informationen an und fordert den Benutzer auf, fortzufahren (ähnlich wie der UNIX-Befehl **more**).
- **-o** - Zeigt die Ausgabe auf einer Zeile an.
- **-s** - Gibt den für die Anzeige verwendeten Startdatensatz an.

ANMERKUNG: Wenn keine Optionen angegeben werden, wird das gesamte Protokoll angezeigt.

Ausgabe

Die Standardausgabe zeigt Folgendes an: Datensatznummer, Zeitstempel, Quelle und Beschreibung. Der Zeitstempel beginnt am 1. Januar um Mitternacht und nimmt so lange zu, bis das System startet. Nachdem das System gestartet wurde, wird der Zeitstempel des Systems verwendet.

Beispielausgabe

```
Record:       1
Date/Time:    Dec 8 08:10:11
Source:       login[433]
Description:  root login from 143.166.157.103
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

clrraclog

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Protokolle löschen** verfügen.

Übersicht

```
racadm clrraclog
```

Beschreibung

Mit dem Unterbefehl **clrraclog** werden alle vorhandenen Einträge aus dem iDRAC6-Protokoll entfernt. Ein neuer Einzeldatensatz wird erstellt, um Datum und Uhrzeit des Löschens des Protokolls aufzuzeichnen.

---

getsel

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Am iDRAC anmelden** verfügen.

Tabelle A-30 beschreibt den Befehl **getsel**.

Tabelle A-30. getsel

Befehl	Definition
getsel -i	Zeigt die Anzahl der Einträge im Systemereignisprotokoll an.
getsel	Zeigt die Einträge im Systemereignisprotokoll an.

Übersicht

```
racadm getsel-i

racadm getsel [-E] [-R] [-A] [-o] [-c Zählwert] [-s Zählwert] [-m]
```

Beschreibung

Der Befehl **getsel -i** zeigt die Anzahl der Einträge im Systemereignisprotokoll an.

Die folgenden Optionen für den Befehl **getsel** (ohne die Option **-i**) werden für das Lesen von Einträgen verwendet.

-A - Legt die Ausgabe ohne Kopfzeilen oder Kennzeichnungen fest.

-c - Zeigt die Höchstanzahl der zurückzugebenden Einträge an.

-o - Zeigt die Ausgabe auf einer Zeile an.

-s - Gibt den für die Anzeige verwendeten Startdatensatz an.

-E - Platziert die 16 Byte des unformatierten Systemereignisprotokolls am Ende jeder Ausgabezeile als Sequenz von Hexadezimalwerten.

-R - Es werden nur die unformatierten Daten gedruckt.

-m - Zeigt jeweils einen Bildschirm an und fordert den Benutzer auf, fortzufahren (ähnlich wie der UNIX-Befehl **more**).

ANMERKUNG: Wenn keine Argumente vorgegeben werden, wird das gesamte Protokoll angezeigt.

Ausgabe

Die Standardausgabe zeigt Folgendes an: Datensatznummer, Zeitstempel, Schweregrad und Beschreibung.

Beispiel:

```
Record:      1
Date/Time:   11/16/2005 22:40:43
Severity:    Ok
Description: System Board SEL: event log sensor for System Board, log cleared was asserted
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

clrsel

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Protokolle löschen** verfügen.

Übersicht

```
racadm clrsel
```

Beschreibung

Mit dem Befehl **clrsel** werden alle vorhandenen Datensätze aus dem Systemereignisprotokoll (SEL) entfernt.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

gettracelog

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Am iDRAC anmelden** verfügen.

Tabelle A-31 beschreibt den Unterbefehl **gettracelog**.

Tabelle A-31. gettracelog

Befehl	Definition
gettracelog -i	Zeigt die Anzahl der Einträge im iDRAC6-Ablaufverfolgungsprotokoll an.
gettracelog	Zeigt das iDRAC6-Ablaufverfolgungsprotokoll an.

Übersicht

```
racadm gettracelog -i

racadm gettracelog [-A] [-o] [-c Zählwert] [-s Startdatensatz] [-m]
```

Beschreibung

Mit dem Befehl **gettracelog** (ohne die Option **-i**) können Einträge gelesen werden. Mit den folgenden **gettracelog**-Optionen werden Einträge gelesen:

-i - Zeigt die Anzahl der Einträge im iDRAC6-Ablaufverfolgungsprotokoll an.

-m - Zeigt jeweils einen Bildschirm an und fordert den Benutzer auf, fortzufahren (ähnlich wie der UNIX-Befehl **more**).

-o - Zeigt die Ausgabe auf einer Zeile an.

-c - Gibt die Anzahl der anzuzeigenden Datensätze an.

-s - Gibt den anzuzeigenden Startdatensatz an.

-A - Zeigt Kopfzeilen oder Kennzeichnungen nicht an.

Ausgabe

Die Standardausgabe zeigt Folgendes an: Datensatznummer, Zeitstempel, Quelle und Beschreibung. Der Zeitstempel beginnt am 1. Januar um Mitternacht und nimmt so lange zu, bis das System startet. Nachdem das System gestartet wurde, wird der Zeitstempel des Systems verwendet.

Beispiel:

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

Description: root from 143.166.157.103: session timeout sid 0be0aef4
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

sslcsrgen

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-32 beschreibt den Unterbefehl **sslcsrgen**.

Tabelle A-32. sslcsrgen

Unterbefehl	Beschreibung
sslcsrgen	Erstellt eine SSL-Zertifikatsignierungsanforderung (CSR) und lädt sie vom RAC herunter.

Übersicht

```
racadm sslcsrgen [-g] [-f <Dateiname>]

racadm sslcsrgen -s
```

Beschreibung

Der Unterbefehl **sslcsrgen** kann verwendet werden, um eine CSR zu erstellen und die Datei auf das lokale Dateisystem des Clients herunterzuladen. Die CSR kann zum Erstellen eines benutzerdefinierten SSL-Zertifikats verwendet werden, das für SSL-Transaktionen auf dem RAC eingesetzt werden kann.

Optionen

ANMERKUNG: Die Option **-f** wird für die serielle/Telnet/SSH-Konsole nicht unterstützt.

Tabelle A-33 beschreibt die Optionen des Unterbefehls **sslcsrgen**.

Tabelle A-33. Optionen des Unterbefehls sslcsrgen

Option	Beschreibung
-g	Erstellt eine neue CSR.
-s	Gibt den Status eines CSR-Erstellungsverfahrens zurück (Erstellung läuft, aktiv oder keine).
-f	Gibt den Dateinamen des Speicherortes an (<*Dateiname*>), auf den die CSR heruntergeladen wird.

ANMERKUNG: Wenn die Option **-f** nicht angegeben wird, lautet der Dateiname im aktuellen Verzeichnis automatisch **sslcsr**.

Wenn keine Optionen angegeben werden, wird eine CSR erstellt und standardmäßig als **sslcsr** auf das lokale Dateisystem heruntergeladen. Die Option **-g** darf nicht mit der Option **-s** verwendet werden, und die Option **-f** kann nur mit der Option **-g** verwendet werden.

Der Unterbefehl **sslcsrgen -s** gibt einen der folgenden Statuscodes zurück:

- CSR erfolgreich erstellt.
- CSR existiert nicht.
- CSR-Erstellung wird durchgeführt.

Einschränkungen

Der Unterbefehl **sslcsrgen** kann nur von einem lokalen oder einem Remote-RACADM-Client aus ausgeführt werden und kann nicht in der seriellen, Telnet- oder SSH-Schnittstelle verwendet werden.

ANMERKUNG: Bevor eine CSR erstellt werden kann, müssen die CSR-Felder in der RACADM-Gruppe **cfgRacSecurity** konfiguriert werden. Beispiel: racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName MyCompany

Beispiele

```
racadm sslcsrgen -s

oder
```

```
racadm sslcsrgen -g -f c:\csr\csrtest.txt
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet-/ssh-/serieller RACADM (Die Option **-f** wird bei der seriellen/Telnet/ssh-Konsole nicht unterstützt)

---

sslcertupload

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-34 beschreibt den Unterbefehl **sslcertupload**.

Tabelle A-34. sslcertupload

Unterbefehl	Beschreibung
sslcertupload	Lädt einen benutzerdefinierten SSL-Server oder ein Zertifizierungsstellenzertifikat für den Verzeichnisdienst vom Client zum RAC hoch.

Übersicht

```
racadm sslcertupload -t <Typ> [-f <Dateiname>]
```

Optionen

Tabelle A-35 beschreibt die Optionen des Unterbefehls **sslcertupload**.

Tabelle A-35. Optionen des Unterbefehls sslcertupload

Option	Beschreibung
-t	Gibt den Typ des hochzuladenden Zertifikats an, entweder das Zertifizierungsstellenzertifikat für den Verzeichnisdienst oder das Serverzertifikat. 1 = Serverzertifikat 2 = Zertifizierungsstellenzertifikat für den Verzeichnisdienst
-f	Gibt den Dateinamen des hochzuladenden Zertifikats an. Wenn die Datei nicht angegeben wird, wird die Datei **sslcert** im aktuellen Verzeichnis ausgewählt.

Der Befehl **sslcertupload** gibt bei Erfolg `0` und bei Fehlern einen Wert ungleich Null zurück.

Einschränkungen

Der Unterbefehl **sslcertupload** kann nur von einem lokalen oder einem Remote-RACADM-Client aus ausgeführt werden. Der Unterbefehl **sslcsrgen** kann nicht auf der seriellen, Telnet- oder SSH-Schnittstelle verwendet werden.

Beispiel

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

sslcertdownload

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-36 beschreibt den Unterbefehl **sslcertdownload**.

Tabelle A-36. sslcertdownload

Unterbefehl	Beschreibung
sslcertupload	Lädt ein SSL-Zertifikat vom iDRAC6 auf das Dateisystem des Clients herunter.

Übersicht

```
racadm sslcertdownload -t <Typ> [-f <Dateiname>]
```

Optionen

Tabelle A-37 beschreibt die Optionen des Unterbefehls **sslcertdownload**.

Tabelle A-37. Optionen des Unterbefehls sslcertdownload

Option	Beschreibung
-t	Gibt den Typ des herunterzuladenden Zertifiks an, entweder das Zertifizierungsstellenzertifikat für den Verzeichnisdienst oder das Serverzertifikat. 1 = Serverzertifikat 2 = Zertifizierungsstellenzertifikat für den Verzeichnisdienst
-f	Gibt den Dateinamen des hochzuladenden Zertifikats an. Wenn die Option **-f** oder der Dateiname nicht angegeben werden, wird die **sslcert**-Datei im aktuellen Verzeichnis ausgewählt.

Der Befehl **sslcertdownload** gibt bei Erfolg `0` und bei Fehlern einen Wert ungleich Null zurück.

Einschränkungen

Der Unterbefehl **sslcertdownload** kann nur von einem lokalen oder einem Remote-RACADM-Client aus ausgeführt werden. Der Unterbefehl **sslcsrgen** kann nicht auf der seriellen, Telnet- oder SSH-Schnittstelle verwendet werden.

Beispiel

```
racadm sslcertdownload -t 1 -f c:\cert\cert.txt
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

sslcertview

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-38 beschreibt den Unterbefehl **sslcertview**.

Tabelle A-38. sslcertview

Unterbefehl	Beschreibung
sslcertview	Zeigt den SSL-Server- oder das CA-Zertifikat an, das auf dem RAC vorhanden ist.

Übersicht

```
racadm sslcertview -t <Typ> [-A]
```

Optionen

Tabelle A-39 beschreibt die Optionen des Unterbefehls **sslcertview**.

Tabelle A-39. Optionen des Unterbefehls sslcertview

Option	Beschreibung
-t	Gibt den Typ des anzuzeigenden Zertifikats an, entweder ein Zertifizierungsstellenzertifikat oder ein Serverzertifikat. 1 = Serverzertifikat 2 = Zertifizierungsstellenzertifikat für den Verzeichnisdienst
-A	Unterdrückt das Drucken von Kopfzeilen/Kennzeichnungen.

Ausgabebeispiel

```
racadm sslcertview -t 1

Serial Number             : 00

Subject Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organization (O)          : Dell Inc.
Organizational Unit (OU)  : Remote Access Group
Common Name (CN)          : iDRAC6 default certificate

Issuer Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organization (O)          : Dell Inc.
Organizational Unit (OU)  : Remote Access Group
Common Name (CN)          : iDRAC6 default certificate

Valid From                : Jul 8 16:21:56 2005 GMT
Valid To                  : Jul 7 16:21:56 2010 GMT

racadm sslcertview -t 1 -A

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

sslkeyupload

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-40 beschreibt den Unterbefehl **sslkeyupload**.

Tabelle A-40. sslkeyupload

Unterbefehl	Beschreibung
sslkeyupload	Lädt den SSL-Schlüssel vom Client auf den iDRAC6 hoch.

Übersicht

```
racadm sslkeyupload -t <Typ> -f <Dateiname>
```

Optionen

Tabelle A-41 beschreibt die Optionen des Unterbefehls **sslkeyupload**.

Tabelle A-41. Optionen des Unterbefehls sslkeyupload

Option	Beschreibung
-t	Gibt den hochzuladenden Schlüssel an. 1 = Der zum Erstellen des Serverzertifikats verwendete SSL-Schlüssel.
-f	Gibt den Dateinamen des hochzuladenden SSL-Schlüssels an.

Der Befehl **sslkeyupload** gibt bei Erfolg `0` und bei Fehlern einen Wert ungleich Null zurück.

Einschränkungen

Der Unterbefehl **sslkeyupload** kann nur von einem lokalen oder einem Remote-RACADM-Client aus ausgeführt werden. Er kann nicht auf der seriellen, Telnet- oder SSH-Schnittstelle verwendet werden.

Beispiel

```
racadm sslkeyupload -t 1 -f c:\sslkey.txt
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

testemail

Tabelle A-42 beschreibt den Unterbefehl **testemail**.

Tabelle A-42. testemail-Konfiguration

Unterbefehl	Beschreibung
testemail	Testet die E-Mail-Warnungsfunktion für den RAC

Übersicht

```
racadm testemail -i <Index>
```

Beschreibung

Sendet eine Test-E-Mail vom iDRAC6 an ein festgelegtes Ziel.

Stellen Sie vor der Durchführung des Test-E-Mail-Befehls sicher, dass der angegebene Index in der RACADM-Gruppe **cfgEmailAlert** aktiviert und ordnungsgemäß konfiguriert ist. Tabelle A-43 enthält eine Liste und zugehörige Befehle für die **cfgEmailAlert**-Gruppe.

Tabelle A-43. testemail-Konfiguration

Maßnahme	Befehl
Aktivieren Sie die Warnung.	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
Legen Sie die Ziel-E-Mail-Adresse fest.	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 benutzer1@meinefirma.com
Legen Sie die benutzerdefinierte Nachricht fest, die zur Ziel-E-Mail-Adresse gesendet werden soll.	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "Dies ist ein Test!"
Stellen Sie sicher, dass die SMTP-IP-Adresse korrekt konfiguriert ist.	racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr 192.168.0.152
Zeigen Sie die aktuellen E-Mail-Warnungseinstellungen an.	racadm getconfig -g cfgEmailAlert -i <*Index*> wobei <*Index*> eine Zahl von 1 bis 4 ist

Optionen

Tabelle A-44 beschreibt die Optionen des Unterbefehls **testemail**.

Tabelle A-44. testemail-Unterbefehle

Option	Beschreibung
-i	Gibt den Index der zu testenden E-Mail-Warnung an.

Ausgabe

Keine.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

testtrap

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Testwarnungen** verfügen.

Tabelle A-45 beschreibt den Unterbefehl **testtrap**.

Tabelle A-45. testtrap

Unterbefehl	Beschreibung
testtrap	Testet die Trap-Warnungsfunktion des RAC-SNMP.

Übersicht

```
racadm testtrap -i <Index>
```

Beschreibung

Mit dem Unterbefehl **testtrap** wird die Trap-Warnungsfunktion des RAC-SNMP getestet, indem ein Test-Trap vom iDRAC6 an einen festgelegten Ziel-Trap-Listener im Netzwerk gesendet wird.

Stellen Sie vor der Durchführung des Unterbefehls **testtrap** sicher, dass der angegebene Index in der RACADM-Gruppe **cfgIpmiPet** ordnungsgemäß konfiguriert ist.

Tabelle A-46 enthält eine Liste und zugehörige Befehle für die Gruppe **cfgIpmiPet**.

Tabelle A-46. cfgEmailAlert-Befehle

Maßnahme	Befehl
Aktivieren Sie die Warnung.	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
Legen Sie die Ziel-E-Mail-IP-Adresse fest.	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110
Zeigen Sie die aktuellen Test-Trap-Einstellungen an.	racadm getconfig -g cfgIpmiPet -i <*Index*> wobei <*Index*> eine Zahl von 1 bis 4 ist

Eingabe

Tabelle A-47 beschreibt die Optionen des Unterbefehls **testtrap**.

Tabelle A-47. Optionen des Unterbefehls testtrap

Option	Beschreibung
-i	Gibt den Index der Trap-Konfiguration an, die für den Test verwendet werden soll. Gültige Werte liegen im Bereich von 1 bis 4.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

vmdisconnect

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Zugriff auf virtuellen Datenträger** verfügen.

Tabelle A-48 beschreibt den Unterbefehl **vmdisconnect**.

Tabelle A-48. vmdisconnect

Unterbefehl	Beschreibung
vmdisconnect	Schließt alle offenen iDRAC6-Verbindungen des virtuellen Datenträgers von Remote-Clients aus.

Übersicht

```
racadm vmdisconnect
```

Beschreibung

Mit dem Unterbefehl **vmdisconnect** kann ein Benutzer die Sitzung des virtuellen Datenträgers eines anderen Benutzers unterbrechen. Wenn unterbrochen, spiegelt die webbasierte Schnittstelle den korrekten Verbindungsstatus wider. Diese Möglichkeit steht nur bei Verwendung von lokalem oder Remote-RACADM zur Verfügung.

Mit dem Unterbefehl **vmdisconnect** wird einem iDRAC6-Benutzer ermöglicht, alle aktiven Sitzungen des virtuellen Datenträgers zu unterbrechen. Die aktiven Sitzungen des virtuellen Datenträgers können auf der webbasierten iDRAC6-Schnittstelle oder durch Verwendung des RACADM-Unterbefehls **getsysinfo** angezeigt werden.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

vmkey

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **Zugriff auf virtuellen Datenträger** verfügen.

Tabelle A-49 beschreibt den Unterbefehl **vmkey**.

Tabelle A-49. vmkey

Unterbefehl	Beschreibung
vmkey	Führt schlüsselbezogene Vorgänge des virtuellen Datenträgers aus.

Übersicht

```
racadm vmkey <Maßnahme>
```

Wenn *<Maßnahme>* auf Reset konfiguriert ist, wird der virtuelle Flash-Speicher auf die Standardgröße von 256 MB zurückgesetzt.

Beschreibung

Wenn ein benutzerdefiniertes Schlüsselimage des virtuellen Datenträgers zum RAC hochgeladen wird, wird die Schlüsselgröße zur Imagegröße. Der vmkey-Unterbefehl kann verwendet werden, um den Schlüssel auf seine ursprüngliche Standardgröße zurückzusetzen, d. h. 256 MB auf dem iDRAC6.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

usercertupload

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-50 beschreibt den Unterbefehl **usercertupload**.

Tabelle A-50. usercertupload

Unterbefehl	Beschreibung
usercertupload	Lädt ein Benutzerzertifikat oder ein Benutzer-Zertifizierungsstellenzertifikat vom Client auf den iDRAC6 hoch.

Übersicht

```
racadm usercertupload -t <Typ> [-f <Dateiname>] -i <Index>
```

Optionen

Tabelle A-51 beschreibt die Optionen des Unterbefehls **usercertupload**.

Tabelle A-51. Optionen des Unterbefehls usercertupload

Option	Beschreibung
-t	Gibt den hochzuladenden Zertifikatstyp an, entweder ein Zertifizierungsstellenzertifikat oder ein Serverzertifikat. 1 = Benutzerzertifikat 2 = Benutzer-Zertifizierungsstellenzertifikat
-f	Gibt den Dateinamen des hochzuladenden Zertifikats an. Wenn die Datei nicht angegeben wird, wird die Datei **sslcert** im aktuellen Verzeichnis ausgewählt.
-i	Indexnummer des Benutzers. Gültige Werte 1 - 16.

Der Befehl **usercertupload** gibt bei Erfolg `0` und bei Fehlern einen Wert ungleich Null zurück.

Einschränkungen

Der Unterbefehl **usercertupload** kann nur von einem lokalen oder einem Remote-RACADM-Client aus ausgeführt werden.

Beispiel

```
racadm usercertupload -t 1 -f c:\cert\cert.txt -i 6
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

usercertview

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-52 beschreibt den Unterbefehl **usercertview**.

Tabelle A-52. usercertview

Unterbefehl	Beschreibung
usercertview	Zeigt das Benutzerzertifikat oder das Benutzer-Zertifizierungsstellenzertifikat an, das auf dem iDRAC6 vorhanden ist.

Übersicht

```
racadm sslcertview -t <Typ> [-A] -i <Index>
```

Optionen

Tabelle A-53 beschreibt die Optionen des Unterbefehls **sslcertview**.

Tabelle A-53. Optionen des Unterbefehls sslcertview

Option	Beschreibung
-t	Gibt den Typ des anzuzeigenden Zertifikats an, entweder das Benutzerzertifikat oder das Benutzer-Zertifizierungsstellenzertifikat. 1 = Benutzerzertifikat

	2 = Benutzer-Zertifizierungsstellenzertifikat
-A	Unterdrückt das Drucken von Kopfzeilen/Kennzeichnungen.
-i	Indexnummer des Benutzers. Gültige Werte sind 1 - 16.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

---

localConRedirDisable

ANMERKUNG: Dieser Befehl kann nur von einem lokalen RACADM-Benutzer ausgeführt werden.

Tabelle A-54 beschreibt den Unterbefehl **localConRedirDisable**.

Tabelle A-54. localConRedirDisable

Unterbefehl	Beschreibung
localConRedirDisable	Deaktiviert die Konsolenumleitung auf die Management Station.

Übersicht

`racadm localConRedirDisable <Option>`

Wenn <*Option*> auf 1 gesetzt ist, ist die Konsolenumleitung deaktiviert.

Wenn <*Option*> auf 0 gesetzt ist, ist die Konsolenumleitung aktiviert.

Unterstützte Schnittstellen

- Lokaler RACADM

---

krbkeytabupload

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Tabelle A-55 beschreibt den Unterbefehl **krbkeytabupload**.

Tabelle A-55. kerbkeytabupload

Unterbefehl	Beschreibung
krbkeytabupload	Eine Kerberos-Keytab-Datei hochladen.

Übersicht

`racadm krbkeytabupload [-f <Dateiname>]`

<Dateiname> ist der Name der Datei, einschließlich des Pfads.

Optionen

Tabelle A-56 beschreibt die Optionen des Unterbefehls **krbkeytabupload**.

Tabelle A-56. Optionen des Unterbefehls kerbkeytabupload

Option	Beschreibung
-f	Gibt den Dateinamen des hochzuladenden Keytabs an. Wenn die Datei nicht angegeben wird, wird die Keytab-Datei im aktuellen Verzeichnis ausgewählt.

Der Befehl **krbkeytabupload** gibt bei Erfolg `0` und bei Fehlern einen Wert ungleich Null zurück.

Einschränkungen

Der Unterbefehl **krbkeytabupload** kann nur von einem lokalen oder einem Remote-RACADM-Client ausgeführt werden.

Beispiel

`racadm krbkeytabupload -f c:\keytab\krbkeytab.tab`

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

sshpkauth

Übersicht

`racadm sshpkauth`

Hochladen

Der Hochlademodus ermöglicht Ihnen, eine Schlüsseldatei hochzuladen oder den Schlüsseltext auf der Befehlszeile zu kopieren. Sie können einen Schlüssel nicht gleichzeitig hochladen und kopieren.

Lokaler und *Remote*-RACADM:

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

Telnet-/ssh-/serieller RACADM:

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

<Schlüsseltext>
```

Ansicht

Der Ansichtsmodus ermöglicht dem Benutzer, einen vom Benutzer festgelegten Schlüssel oder alle Schlüssel anzuzeigen.

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

racadm sshpkauth -i <2 bis 16> -v -k alle
```

Löschen

Der Löschmodus ermöglicht dem Benutzer, einen vom Benutzer festgelegten 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
```

Beschreibung

Ermöglicht Ihnen, bis zu 4 verschiedene öffentliche SSH-Schlüssel hochzuladen und zu verwalten. Sie können entweder eine Schlüsseldatei hochladen, einen vom Benutzer festgelegten Schlüssel oder alle Schlüssel anzeigen oder einen vom Benutzer festgelegten Schlüssel oder alle Schlüssel löschen. Dieser Befehl hat drei einander ausschließende Modi - Hochladen, Anzeigen und Löschen - die durch die Optionen festgelegt werden (siehe Tabelle A-57), die für den Befehl bereitgestellt werden.

Optionen

Tabelle A-57. Optionen des Unterbefehls sshpkauth

Option	Beschreibung
-i <Benutzerindex>	Index für den Benutzer. <Benutzerindex> muss auf dem iDRAC6 zwischen 2 und 16 sein
-k [<Schlüsselindex> | all]	Index zum Zuweisen des PK-Schlüssels, der hochgeladen wird. "**all**" funktioniert nur mit den Optionen -v oder -d. <Schlüsselindex> muss auf dem iDRAC6 zwischen 1 und 4 oder "**all**" (alle) sein.
-t <PK-Schlüsseltext>	Schlüsseltext for the öffentlichen SSH-Schlüssel.
-f <Dateiname>	Datei, die den hochzuladenden Schlüsseltext enthält. Die Option **-f** wird für Telnet/ssh/seriellen RACADM nicht unterstützt.
-v	Anzeige des Schlüsseltexts für den bereitgestellten Index.
-d	Löschen des Schlüssels für den bereitgestellten Index.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/ssh/serieller RACADM

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Die iDRAC6-Eigenschaftendatenbank enthält die Konfigurationsinformationen für den iDRAC6. Daten werden nach assoziiertem Objekt organisiert und Objekte werden nach der Objektgruppe organisiert. Die IDs für die Gruppen und Objekte, die von der Eigenschaftendatenbank unterstützt werden, werden in diesem Abschnitt aufgeführt.

Verwenden Sie die Gruppen- und Objekt-IDs mit dem RACADM-Dienstprogramm, um den iDRAC6 zu konfigurieren. Die folgenden Abschnitte beschreiben jedes Objekt und zeigen an, ob das Objekt schreibbar oder lesbar oder beides ist.

△ **VORSICHT: RACADM legt den Wert von Objekten fest, ohne sie einer Funktionsprüfung zu unterziehen. Mit RACADM ist es beispielsweise möglich, das Zertifikatvalidierungsobjekt auf 1 zu setzen, während das Active Directory-Objekt auf 0 gesetzt ist, obgleich die Zertifikatvalidierung nur dann erfolgen kann, wenn Active Directory® aktiviert wird. Genauso kann auch das cfgADSSOEnable-Objekt auf 0 oder 1 gesetzt werden, wenn das cfgADEnable-Objekt 0 ist. Der Wert tritt jedoch erst in Kraft, wenn Active Directory aktiviert wird.**

Alle Zeichenkettenwerte sind auf anzeigbare ASCII-Zeichen beschränkt, wenn nicht anderweitig vermerkt.

Anzeigbare Zeichen

Anzeigbare Zeichen umfassen den folgenden Satz:

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789~`!@#$%^&*()_+-={}[]|\:";'<>,.?/
```

---

idRacInfo

Diese Gruppe enthält Anzeigeparameter für Informationen zu den Einzelheiten des abgefragten iDRAC6.

Es ist eine Instanz der Gruppe zulässig. In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben.

idRacProductInfo (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 63 ASCII-Zeichen.

Standardeinstellung

Integrierter Dell Remote Access Controller

Beschreibung

Eine Textzeichenkette, die das Produkt identifiziert.

idRacDescriptionInfo (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 255 ASCII-Zeichen.

Standardeinstellung

Diese Systemkomponente bietet einen vollständigen Satz von Remote-Verwaltungsfunktionen für Dell PowerEdge-Server.

Beschreibung

Eine Textbeschreibung des iDRAC-Typs.

idRacVersionInfo (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 63 ASCII-Zeichen.

Standardeinstellung

<aktuelle Versionsnummer>

Beschreibung

Eine Zeichenkette, die die aktuelle Firmware-Version des Produkts enthält.

idRacBuildInfo (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 16 ASCII-Zeichen.

Standardeinstellung

Die aktuelle Build-Version der iDRAC6-Firmware.

Beschreibung

Eine Zeichenkette mit der aktuellen Build-Version des Produkts.

idRacName (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 15 ASCII-Zeichen.

Standardeinstellung

iDRAC

Beschreibung

Ein vom Benutzer vergebener Name zur Identifizierung dieses Controllers.

idRacType (Nur-Lesen)

Zulässige Werte

Product ID (Produkt-ID)

Standardeinstellung

10

Beschreibung

Identifiziert den Remote Access Controller-Typ als den iDRAC6.

---

cfgLanNetworking

Diese Gruppe enthält Parameter zum Konfigurieren des iDRAC6-NIC.

Es ist eine Instanz der Gruppe zulässig. Für einige Objekte in dieser Gruppe ist u. U. ein Reset des iDRAC6-NIC erforderlich, wodurch ein kurzzeitiger Verlust der Verbindungen auftreten kann. Objekte, die die iDRAC6-NIC-IP-Adresseneinstellungen ändern, schließen alle aktiven Benutzersitzungen und erfordern, dass Benutzer mit den aktualisierten IP-Adresseneinstellungen eine neue Verbindung herstellen.

cfgNicIPv4Enable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert den iDRAC6-IPv4-Stack.

cfgNicSelection (Lesen/Schreiben)

Zulässige Werte

0 = Freigegeben

1 = Freigegeben für Failover: LOM2

2 = Dediziert

3 = Freigegeben für Failover: Alle LOMs (nur iDRAC6 Enterprise)

Standardeinstellung

0 (iDRAC6 Express)

2 (iDRAC6 Enterprise)

Beschreibung

Legt den aktuellen Verfahrensmodus für den RAC-NIC (Netzwerkschnittstellen-Controller) fest. Tabelle B-1 beschreibt die unterstützten Modi.

Tabelle B-1. cfgNicSelection, unterstützte Modi

Modus	Beschreibung
Freigegeben	Wird verwendet, wenn der integrierte Host-Server-NIC an den RAC auf dem Host-Server freigegeben wird. Dieser Modus ermöglicht, dass Konfigurationen zum Zweck der allgemeinen Zugänglichkeit im Netzwerk dieselbe IP-Adresse auf dem Host-Server und dem RAC verwenden.
Freigegeben für Failover: LOM 2	Aktiviert Teaming-Fähigkeiten zwischen LOM2 auf den integrierten Netzwerkschnittstellen-Controllern des Host-Servers.
Dediziert	Legt fest, dass der RAC-NIC zum Zweck der Remote-Zugänglichkeit als dedizierter NIC verwendet wird.
Freigegeben für Failover: Alle LOMs	Aktiviert Teaming-Fähigkeiten zwischen allen LOMs auf den integrierten Netzwerkschnittstellen-Controllern des Host-Servers. 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. Failover tritt vom NIC 2 zum NIC 3 und dann zum NIC 4 auf. Wenn der NIC 4 fehlerhaft ist, schaltet das Remote-Zugriffsgerät für alle Datenübertragungen zum NIC 1 zurück. Dies geschieht jedoch nur, wenn der ursprüngliche NIC 1-Fehler korrigiert wurde.

cfgNicVLanEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die VLAN-Funktionen des RAC/BMC.

cfgNicVLanId (Lesen/Schreiben)

Zulässige Werte

1 - 4094

Standardeinstellung

1

Beschreibung

Gibt die VLAN-ID für die Netzwerk-VLAN-Konfiguration an. Diese Eigenschaft ist nur gültig, wenn **cfgNicVLanEnable** auf **1** (aktiviert) eingestellt ist.

cfgNicVLanPriority (Lesen/Schreiben)

Zulässige Werte

0 - 7

Standardeinstellung

0

Beschreibung

Gibt die VLAN-Priorität für die Netzwerk-VLAN-Konfiguration an. Diese Eigenschaft ist nur gültig, wenn cfgNicVLanEnable auf 1 (aktiviert) eingestellt ist.

cfgDNSDomainNameFromDHCP (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Legt fest, dass der iDRAC6-DNS-Domänenname vom Netzwerk-DHCP-Server aus zugewiesen werden muss.

cfgDNSDomainName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 ASCII-Zeichen Mindestens ein Zeichen muss ein alphabetisches Zeichen sein. Zeichen sind auf die alphanumerischen Zeichen, "-" und "." beschränkt.

ANMERKUNG: Microsoft® Active Directory® unterstützt nur vollständig qualifizierte Domänennamen (FQDN) von bis zu 64 Byte.

Standardeinstellung

<leer>

Beschreibung

Dies ist der DNS-Domänenname.

cfgDNSRacName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 63 ASCII-Zeichen. Mindestens ein Zeichen muss alphabetisch sein.

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

Standardeinstellung

idrac-<Service-Tag-Nummer>

Beschreibung

Zeigt den iDRAC6-Namen an, der standardmäßig der RAC-*Service-Tag-Nummer* entspricht. Dieser Parameter ist nur gültig, wenn **cfgDNSRegisterRac** auf 1 (TRUE) eingestellt ist.

cfgDNSRegisterRac (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Registriert den iDRAC6-Namen auf dem DNS-Server.

cfgDNSServersFromDHCP (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Bestimmt, dass die DNS-Server-IPv4-Adressen über den DHCP-Server auf dem Netzwerk zugewiesen werden sollen.

cfgDNSServer1 (Lesen/Schreiben)

Zulässige Werte

Zeichenkette, die eine gültige IPv4-Adresse repräsentiert. Beispiel: 192.168.0.20.

Standardeinstellung

0.0.0.0

Beschreibung

Gibt die IPv4-Adresse für den DNS-Server 1 an.

cfgDNSServer2 (Lesen/Schreiben)

Zulässige Werte

Zeichenkette, die eine gültige IPv4-Adresse repräsentiert. Beispiel: 192.168.0.20.

Standardeinstellung

0.0.0.0

Beschreibung

Ruft die für den DNS-Server 2 verwendete IPv4-Adresse ab.

cfgNicEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert den iDRAC6-Netzwerkschnittstellen-Controller (NIC). Wenn der NIC deaktiviert ist, kann nicht mehr auf die Remote-Netzwerkschnittstellen über den iDRAC6 zugegriffen werden.

cfgNicIpAddress (Lesen/Schreiben)

ANMERKUNG: Dieser Parameter kann nur konfiguriert werden, wenn der Parameter **cfgNicUseDhcp** auf 0 (FALSE) eingestellt ist.

Zulässige Werte

Zeichenkette, die eine gültige IPv4-Adresse repräsentiert. Beispiel: 192.168.0.20.

Standardeinstellung

192.168.0.120

Beschreibung

Gibt die dem iDRAC6 zugewiesene IPv4-Adresse an.

cfgNicNetmask (Lesen/Schreiben)

ANMERKUNG: Dieser Parameter kann nur konfiguriert werden, wenn der Parameter **cfgNicUseDhcp** auf 0 (FALSE) eingestellt ist.

Zulässige Werte

Eine Zeichenkette, die eine gültige Subnetzmaske repräsentiert. Beispiel: 255.255.255.0.

Standardeinstellung

255.255.255.0

Beschreibung

Die für die iDRAC6-IP-Adresse verwendete Subnetzmaske.

cfgNicGateway (Lesen/Schreiben)

ANMERKUNG: Dieser Parameter kann nur konfiguriert werden, wenn der Parameter **cfgNicUseDhcp** auf 0 (FALSE) eingestellt ist.

Zulässige Werte

Zeichenkette, die eine gültige Gateway-IPv4-Adresse repräsentiert. Beispiel: 192.168.0.1.

Standardeinstellung

192.168.0.1

Beschreibung

Die iDRAC6-Gateway-IPv4-Adresse.

cfgNicUseDhcp (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Gibt an, ob DHCP zum Zuweisen der iDRAC6-IPv4-Adresse verwendet wird. Wenn diese Eigenschaft auf 1 (TRUE) eingestellt ist, werden die iDRAC6-IPv4-Adresse, die Subnetzmaske sowie der Gateway vom DHCP-Server im Netzwerk zugewiesen. Wenn diese Eigenschaft auf **0** (FALSE) eingestellt ist, kann der Benutzer die Eigenschaften von **cfgNicIpAddress**, **cfgNicNetmask** und **cfgNicGateway** konfigurieren.

cfgNicMacAddress (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette, welche die iDRAC6-NIC-MAC-Adresse repräsentiert.

Standardeinstellung

Die aktuelle MAC-Adresse des iDRAC6-NIC. Beispiel: 00:12:67:52:51:A3.

Beschreibung

Die iDRAC6-NIC-MAC-Adresse.

---

cfgRemoteHosts

Diese Gruppe enthält Eigenschaften, welche die Konfiguration des SMTP-Servers für E-Mail-Warnungen zulassen.

cfgRhostsFwUpdateTftpEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die iDRAC6-Firmware-Aktualisierung über einen Netzwerk-TFTP-Server.

cfgRhostsFwUpdateIpAddr (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die eine gültige IPv4-Adresse repräsentiert. Beispiel: 192.168.0.61

Standardeinstellung

0.0.0.0

Beschreibung

Gibt die IPv4-Adresse des Netzwerk-TFTP-Servers an, die für TFTP-iDRAC6-Firmware-Aktualisierungsvorgänge verwendet wird.

cfgRhostsFwUpdatePath (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette mit einer maximalen Länge von 255 ASCII-Zeichen.

Standardeinstellung

<leer>

Beschreibung

Gibt den TFTP-Pfad zum Speicherort der iDRAC6-Firmware-Imagedatei auf dem TFTP-Server an. Der TFTP-Pfad ist relativ zum TFTP-root-Pfad auf dem TFTP-Server.

ANMERKUNG: Der Server erfordert möglicherweise weiterhin die Angabe des Laufwerks (z. B. **C:**).

cfgRhostsSmtpServerIpAddr (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die eine gültige SMTP-Server-IPv4-Adresse repräsentiert. Beispiel: 192.168.0.55

Standardeinstellung

0.0.0.0

Beschreibung

Die IPv4-Adresse des Netzwerk-SMTP-Servers oder TFTP-Servers. Der SMTP-Server überträgt E-Mail-Warnungen vom iDRAC6, wenn die Warnungen konfiguriert und aktiviert sind. Der TFTP-Server überträgt Dateien zum und vom iDRAC6.

cfgRhostsSyslogEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert remote syslog.

cfgRhostsSyslogPort (Lesen/Schreiben)

Zulässige Werte

0 - 65535

Standardeinstellung

514

Beschreibung

Remote-Syslog-Anschlussnummer.

cfgRhostsSyslogServer1 (Lesen/Schreiben)

Zulässige Werte

Zeichenkette von 0 bis 254 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Name des Remote-Syslog-Servers.

cfgRhostsSyslogServer2 (Lesen/Schreiben)

Zulässige Werte

Zeichenkette von 0 bis 254 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Name des Remote-Syslog-Servers.

cfgRhostsSyslogServer3 (Lesen/Schreiben)

Zulässige Werte

Zeichenkette von 0 bis 254 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Name des Remote-Syslog-Servers.

---

cfgUserAdmin

Diese Gruppe bietet Konfigurationsinformationen über die Benutzer, denen erlaubt wird, über die verfügbaren Remote-Schnittstellen auf den iDRAC6 zuzugreifen.

Es sind bis zu 16 Instanzen der Benutzergruppe gestattet. Jede Instanz repräsentiert die Konfiguration für einen einzelnen Benutzer.

cfgUserAdminIndex (Nur-Lesen)

Zulässige Werte

1 - 16

Standardeinstellung

<Instanz>

Beschreibung

Diese Zahl stellt die Benutzerinstanz dar.

cfgUserAdminIpmiLanPrivilege (Lesen/Schreiben)

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

15 (Kein Zugriff)

Standardeinstellung

4 (Benutzer 2)

15 (Alle anderen)

Beschreibung

Die maximale Berechtigung auf dem IPMI-LAN-Kanal.

cfgUserAdminPrivilege (Lesen/Schreiben)

Zulässige Werte

0x00000000 bis 0x000001ff und 0x0

Standardeinstellung

0x00000000

Beschreibung

Diese Eigenschaft legt die für den Benutzer zugelassenen rollenbasierten Autoritätsberechtigungen fest. Der Wert wird als Bitmaske dargestellt, wodurch beliebige Kombinationen von Berechtigungswerten möglich sind. Tabelle B-2 beschreibt die Benutzerberechtigungs-Bitwerte, die zum Erstellen von Bitmasken kombiniert werden können.

Tabelle B-2. Bitmasken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
Am iDRAC anmelden	0x00000001
iDRAC konfigurieren	0x00000002

Benutzer konfigurieren	0x00000004
Protokolle löschen	0x00000008
Serversteuerungsbefehle ausführen	0x00000010
Auf die Konsolenumleitung zugreifen	0x00000020
Zugriff auf virtuelle Datenträger	0x00000040
Testwarnungen	0x00000080
Debug-Befehle ausführen	0x00000100

Beispiele

Tabelle B-3 enthält Beispiele von Berechtigungs-Bitmasken für Benutzer mit einer oder mehreren Berechtigungen.

Tabelle B-3. Beispiel-Bitmasken für Benutzerberechtigungen

Benutzerberechtigung(en)	Berechtigungs-Bitmaske
Ein Benutzerzugriff auf den iDRAC ist nicht zulässig.	0x00000000
Der Benutzer hat nur die Berechtigung, sich am iDRAC anzumelden und iDRAC- und Server-Konfigurationsinformationen anzuzeigen.	0x00000001
Der Benutzer hat die Berechtigung, sich am iDRAC anzumelden und Konfigurationsänderungen vorzunehmen.	0x00000001 + 0x00000002 = 0x00000003
Der Benutzer kann sich am iDRAC anmelden und auf den virtuellen Datenträger sowie auf die Konsolenumleitung zugreifen.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (Lesen/Schreiben)

ANMERKUNG: Dieser Eigenschaftenwert muss auf einen eindeutigen Benutzernamen hinweisen.

Zulässige Werte

Eine Zeichenkette von bis zu 16 ASCII-Zeichen.

Standardeinstellung

root (Benutzer 2)

<leer> (Alle anderen)

Beschreibung

Der Name des Benutzers dieses Indexes. Der Benutzerindex wird durch Schreiben einer Zeichenkette in dieses Namensfeld erzeugt, falls der Index leer ist. Das Schreiben einer Zeichenkette von doppelten Anführungszeichen ("") löscht den Benutzer an diesem Index. Die folgenden Zeichen dürfen nicht in der Zeichenkette enthalten sein: / (Schrägstrich), \ (umgekehrter Schrägstrich), . (Punkt), @ (At-Symbol) oder Anführungszeichen.

ANMERKUNG: Dieser Eigenschaftenwert muss auf einen eindeutigen Benutzernamen hinweisen.

cfgUserAdminPassword (Nur Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 20 ASCII-Zeichen

Standardeinstellung

****

Beschreibung

Das Kennwort für diesen Benutzer. Benutzerkennwörter sind verschlüsselt und nicht sichtbar bzw. können nicht angezeigt werden, nachdem die Eigenschaft geschrieben wurde.

cfgUserAdminEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1 (Benutzer 2)

0 (Alle anderen)

Beschreibung

Aktiviert oder deaktiviert einen einzelnen Benutzer.

cfgUserAdminSolEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert den SOL-Benutzerzugriff (Seriell über LAN) für den Benutzer.

cfgUserAdminIpmiSerialPrivilege (Lesen / Schreiben)

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

15 (Kein Zugriff)

Standardeinstellung

4 (Benutzer 2)

15 (Alle anderen)

Beschreibung

Die maximale Berechtigung auf dem IPMI-LAN-Kanal.

---

cfgEmailAlert

Diese Gruppe enthält Parameter zum Konfigurieren der iDRAC6-E-Mail-Warnmeldungsfunktionen.

In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben. Es sind bis zu vier Instanzen dieser Gruppe gestattet.

cfgEmailAlertIndex (Nur-Lesen)

Zulässige Werte

1 - 4

Standardeinstellung

<Instanz>

Beschreibung

Der eindeutige Index einer Warnungsinstanz.

cfgEmailAlertEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Warnungsinstanz.

cfgEmailAlertAddress (Lesen/Schreiben)

Zulässige Werte

E-Mail-Adressenformat mit einer maximalen Länge von 64 ASCII-Zeichen.

Standardeinstellung

<leer>

Beschreibung

Legt die Ziel-E-Mail-Adresse für E-Mail-Warnungen fest; z. B. benutzer1@company.com

cfgEmailAlertCustomMsg (Lesen / Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<leer>

Beschreibung

Legt eine benutzerdefinierte Nachricht fest, die den Betreff der Warnung bildet.

---

cfgSessionManagement

Diese Gruppe enthält Parameter zum Konfigurieren der Anzahl von Sitzungen, die eine Verbindung zum iDRAC6 herstellen können.

Es ist eine Instanz der Gruppe zulässig. In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben.

cfgSsnMgtRacadmTimeout (Lesen / Schreiben)

Zulässige Werte

10 - 1920

Standardeinstellung

60

Beschreibung

Definiert die Leerlaufzeitüberschreitung in Sekunden für die Remote-RACADM-Schnittstelle. Wenn eine Remote-RACADM-Sitzung länger als die angegebenen Sitzungen inaktiv bleibt, wird die Sitzung geschlossen.

cfgSsnMgtConsRedirMaxSessions (Lesen / Schreiben)

Zulässige Werte

1 - 4

Standardeinstellung

4

Beschreibung

Gibt die maximale Anzahl von Konsolenumleitungssitzungen an, die auf dem iDRAC6 zulässig sind.

cfgSsnMgtWebserverTimeout (Lesen / Schreiben)

Zulässige Werte

60 - 10800

Standardeinstellung

1800

Beschreibung

Definiert die Zeitüberschreitung des Web Servers. Diese Eigenschaft legt die Zeitspanne in Sekunden fest, während der eine Verbindung inaktiv verbleiben darf (keine Benutzereingabe erfolgt). Die Sitzung wird abgebrochen, wenn das durch diese Eigenschaft festgelegte Zeitlimit erreicht wird. Änderungen an dieser Einstellung betreffen die aktuelle Sitzung nicht. Sie müssen sich ab- und wieder anmelden, damit die neuen Einstellungen in Kraft treten.

cfgSsnMgtSshIdleTimeout (Lesen/Schreiben)

Zulässige Werte

0 (Keine Zeitüberschreitung)

60 - 1920

Standardeinstellung

300

Beschreibung

Bestimmt die Leerlaufzeitüberschreitung für Secure Shell. Diese Eigenschaft legt die Zeitspanne in Sekunden fest, während der eine Verbindung inaktiv verbleiben darf (keine Benutzereingabe erfolgt). Die Sitzung wird abgebrochen, wenn das durch diese Eigenschaft festgelegte Zeitlimit erreicht wird. Änderungen an dieser Einstellung betreffen die aktuelle Sitzung nicht. Sie müssen sich ab- und wieder anmelden, damit die neuen Einstellungen in Kraft treten.

Eine abgelaufene Secure Shell-Sitzung zeigt die folgende Fehlermeldung an:

```
Connection timed out (Zeitüberschreitung der Verbindung)
```

Nachdem die Meldung erschienen ist, wechselt das System zu der Shell zurück, die die Secure Shell-Sitzung erstellt hat.

cfgSsnMgtTelnetTimeout (Lesen/Schreiben)

Zulässige Werte

0 (Keine Zeitüberschreitung)

60 - 1920

Standardeinstellung

300

Beschreibung

Definiert die Leerlaufzeitüberschreitung von Telnet. Diese Eigenschaft legt die Zeitspanne in Sekunden fest, während der eine Verbindung inaktiv verbleiben darf (keine Benutzereingabe erfolgt). Die Sitzung wird abgebrochen, wenn das durch diese Eigenschaft festgelegte Zeitlimit erreicht wird. Änderungen an dieser Einstellung haben keine Auswirkung auf die aktuelle Sitzung (Sie müssen sich abmelden und wieder anmelden, damit die neuen Einstellungen in Kraft treten).

Eine abgelaufene Telnet-Sitzung zeigt die folgende Fehlermeldung an:

```
Connection timed out (Zeitüberschreitung der Verbindung)
```

Nachdem die Meldung angezeigt wurde, wechselt das System zu der Shell zurück, die die Telnet-Sitzung erstellt hat.

---

cfgSerial

Diese Gruppe enthält Konfigurationsparameter für die iDRAC6-Dienste.

Es ist eine Instanz der Gruppe zulässig. In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben.

cfgSerialBaudRate (Lesen / Schreiben)

Zulässige Werte

9600, 28800, 57600, 115200

Standardeinstellung

57600

Beschreibung

Legt die Baudrate des seriellen iDRAC6-Anschlusses fest.

cfgSerialConsoleEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die serielle RAC-Konsolenschnittstelle.

cfgSerialConsoleQuitKey (Lesen / Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 4 Zeichen

Standardeinstellung

^\ (<Strg><\>)

ANMERKUNG: Das Symbol "^" ist die Taste <Strg>.

Beschreibung

Diese Taste oder Tastenkombination beendet die Textkonsolenumleitung, wenn der Befehl **connect com2** verwendet wird. Der Wert **cfgSerialConsoleQuitKey** kann auf eine der folgenden Weisen dargestellt werden:

- Dezimalwert - Beispiel: "95"
- Hexadezimalwert - Beispiel: "0x12"
- Oktalwert - Beispiel: "007"
- ASCII-Wert - Beispiel: "^a"

ASCII-Werte können anhand der folgenden Escape-Tastencodes dargestellt werden:

(a) ^ gefolgt von einem beliebigen Buchstaben (a-z, A-Z)

(b) ^ gefolgt von den aufgeführten Sonderzeichen: [ ] \ ^ _

cfgSerialConsoleIdleTimeout (Lesen/Schreiben)

Zulässige Werte

0 = keine Zeitüberschreitung

60 - 1920

Standardeinstellung

300

Beschreibung

Die Höchstanzahl der abzuwartenden Sekunden, bis eine inaktive serielle Sitzung unterbrochen wird.

cfgSerialConsoleNoAuth (Lesen/Schreiben)

Zulässige Werte

0 (aktiviert serielle Anmeldungsauthentifizierung)

1 (deaktiviert serielle Anmeldungsauthentifizierung)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Anmeldungsauthentifizierung der seriellen RAC-Konsole.

cfgSerialConsoleCommand (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 128 Zeichen

Standardeinstellung

<leer>

Beschreibung

Gibt einen seriellen Befehl an, der ausgeführt wird, nachdem sich ein Benutzer an der Schnittstelle der seriellen Konsole angemeldet hat.

cfgSerialHistorySize (Lesen / Schreiben)

Zulässige Werte

0 - 8192

Standardeinstellung

8192

Beschreibung

Gibt die maximale Größe des seriellen Verlaufspuffers an.

cfgSerialCom2RedirEnable (Lesen / Schreiben)

Standardeinstellung

1

Zulässige Werte

1 (TRUE)

0 (FALSE)

Beschreibung

Aktiviert oder deaktiviert die Konsole für COM 2-Anschlussumleitung.

cfgSerialSshEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Secure Shell (SSH)-Schnittstelle auf dem iDRAC6.

cfgSerialTelnetEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Telnet-Konsolenschnittstelle auf dem iDRAC6.

---

cfgOobSnmp

Die Gruppe enthält Parameter zur Konfiguration des SNMP-Agenten und der Trap-Fähigkeiten des iDRAC6.

Es ist eine Instanz der Gruppe zulässig. In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben.

cfgOobSnmpAgentCommunity (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 31 Zeichen

Standardeinstellung

public

Beschreibung

Gibt den für SNMP-Traps verwendeten SNMP-Community-Namen an.

cfgOobSnmpAgentEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert den SNMP-Agenten im iDRAC6.

---

cfgRacTuning

Diese Gruppe wird verwendet, um verschiedene iDRAC6-Konfigurationseigenschaften, z. B. gültige Anschlüsse und Sicherheitsanschlussbeschränkungen zu konfigurieren.

cfgRacTuneConRedirPort(Lesen/Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

5900

Beschreibung

Gibt den Anschluss an, der für Tastatur, Maus, Video und virtuellen Datenträger-Datenverkehr auf dem RAC verwendet werden soll.

cfgRacTuneRemoteRacadmEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Remote-RACADM-Schnittstelle im iDRAC.

cfgRacTuneCtrlEConfigDisable

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Fähigkeit des lokalen Benutzers, den iDRAC über den BIOS-POST-Options-ROM zu konfigurieren.

cfgRacTuneHttpPort (Lesen/Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

80

Beschreibung

Gibt die Anschlussnummer an, die für die HTTP-Netzwerkkommunikation mit dem iDRAC6 zu verwenden ist.

cfgRacTuneHttpsPort (Lesen/Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

443

Beschreibung

Gibt die Anschlussnummer an, die für die HTTPS-Netzwerkkommunikation mit dem iDRAC6 zu verwenden ist.

cfgRacTuneIpRangeEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Funktion zur Überprüfung des iDRAC6-IPv4-Adressenbereichs.

cfgRacTuneIpRangeAddr (Lesen/Schreiben)

Zulässige Werte

Eine als IPv4-Adresse formatierte Zeichenkette, z. B. 192.168.0.44

Standardeinstellung

192.168.1.1

Beschreibung

Legt das annehmbare IPv4-Adressen-Bitmuster in Positionen fest, die durch die Einsen in der Bereichsmaskeneigenschaft (**cfgRacTuneIpRangeMask**) bestimmt werden.

cfgRacTuneIpRangeMask (Lesen/Schreiben)

Zulässige Werte

Eine als IPv4-Adresse formatierte Zeichenkette, z. B. `255.255.255.0`

Standardeinstellung

255.255.255.0

Beschreibung

Standard-IP-Maskenwerte mit linksbündigen Bits. Beispiel: 255.255.255.0.

cfgRacTuneIpBlkEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Funktion zur Blockierung der iDRAC6-IPv4-Adresse.

cfgRacTuneIpBlkFailCount (Lesen/Schreiben)

Zulässige Werte

2 - 16

Standardeinstellung

5

Beschreibung

Die maximale Anzahl von Anmeldefehlern im Fenster (**cfgRacTuneIpBlkFailWindow**), bevor Anmeldeversuche von der IP-Adresse zurückgewiesen werden.

cfgRacTuneIpBlkFailWindow (Lesen/Schreiben)

Zulässige Werte

10 - 65535

Standardeinstellung

60

Beschreibung

Definiert die Zeitspanne in Sekunden, während der die fehlerhaften Versuche gezählt werden. Wenn Fehlversuche diese Grenze überschreiten, werden weitere von der Zählung ausgeschlossen.

cfgRacTuneIpBlkPenaltyTime (Lesen/Schreiben)

Zulässige Werte

10 - 65535

Standardeinstellung

300

Beschreibung

Definiert die Zeitspanne in Sekunden, während der Sitzungsaufforderungen von einer IP-Adresse mit übermäßigen Fehlversuchen zurückgewiesen werden.

cfgRacTuneSshPort (Lesen/Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

22

Beschreibung

Gibt die für die iDRAC6-SSH-Schnittstelle verwendete Anschlussnummer an.

cfgRacTuneTelnetPort (Lesen/Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

23

Beschreibung

Gibt die für die iDRAC6-Telnet-Schnittstelle verwendete Anschlussnummer an

cfgRacTuneConRedirEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert Konsolenumleitung

cfgRacTuneConRedirEncryptEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Verschlüsselt das Video in einer Konsolenumleitungssitzung.

cfgRacTuneAsrEnable (Lesen / Schreiben)

ANMERKUNG: Für dieses Objekt ist ein iDRAC6-Reset erforderlich, bevor es aktiv werden kann.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Erfassungsfunktion für den Bildschirm "Letzter Absturz" des iDRAC6.

cfgRacTuneDaylightOffset (Lesen / Schreiben)

Zulässige Werte

0 - 60

Standardeinstellung

0

Beschreibung

Gibt den Sommerzeit-Offset (in Minuten) an, der für die RAC-Zeit zu verwenden ist.

cfgRacTuneTimezoneOffset (Lesen/Schreiben)

Zulässige Werte

-720 - 780

Standardeinstellung

0

Beschreibung

Gibt den Zeitzonen-Offset (in Minuten) von GMT/UTC an, der für die

RAC-Zeit zu verwenden ist. Zu den gebräuchlichen Zeitzonen-Offsets für Zeitzonen in den Vereinigten

Staaten gehören:

-480 (PST - Pacific Standard Time)

-420 (MST - Mountain Standard Time)

-360 (CST - Central Standard Time)

-300 (EST - Eastern Standard Time)

cfgRacTuneLocalServerVideo (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert das lokale Servervideo (Einblendung) oder deaktiviert es (Ausblendung).

cfgRacTuneLocalConfigDisable (Lesen/Schreiben)

Zulässige Werte

0 (TRUE)

1 (FALSE)

Standardeinstellung

0

Beschreibung

Deaktiviert Schreibzugriff auf die iDRAC6-Konfigurationsdaten durch Einstellung auf 1.

cfgRacTuneWebserverEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert den iDRAC6-Web Server. Wird diese Eigenschaft deaktiviert, ist der Zugriff auf den iDRAC6 über Client-Webbrowser nicht möglich. Diese Eigenschaft hat keinen Einfluss auf die Telnet/SSH- oder RACADM-Schnittstellen.

---

ifcRacManagedNodeOs

Diese Gruppe enthält Eigenschaften, die das Betriebssystem des verwalteten Servers beschreiben.

Es ist eine Instanz der Gruppe zulässig. In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben.

ifcRacMnOsHostname (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 255 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Der Host-Name des verwalteten Servers.

ifcRacMnOsOsName (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 255 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Der Betriebssystemname des verwalteten Servers.

---

cfgRacSecurity

Diese Gruppe wird zum Konfigurieren von Einstellungen verwendet, die mit der iDRAC6-SSL-CSR-Funktion (Zertifikatsignierungsanforderung) in Beziehung stehen. Die Eigenschaften in dieser Gruppe müssen konfiguriert werden, bevor vom iDRAC6 aus eine CSR erstellt wird.

Weitere Informationen über das Erstellen von Zertifikatsignierungsanforderungen befinden sich in den Erläuterungen zum **sslcsrgen** RACADM-Unterbefehl.

cfgRacSecCsrCommonName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Gibt den CSR Common Name (CSR CN) an, der ein IP- oder der iDRAC-Name gemäß Zertifikat sein muss.

cfgRacSecCsrOrganizationName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Gibt den CSR-Organisationsnamen (O) an.

cfgRacSecCsrOrganizationUnit (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Gibt die CSR-Organisationseinheit (OU) an.

cfgRacSecCsrLocalityName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Gibt den CSR-Standort (L) an.

cfgRacSecCsrStateName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Gibt den CSR-Bundesstaatnamen (S) an.

cfgRacSecCsrCountryCode (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 2 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Gibt den CSR-Landescode (CC) an

cfgRacSecCsrEmailAddr (Lesen / Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Legt die CSR-E-Mail-Adresse fest.

cfgRacSecCsrKeySize (Lesen / Schreiben)

Zulässige Werte

1024

2048

4096

Standardeinstellung

1024

Beschreibung

Gibt die asymmetrische SSL-Schlüsselgröße für die CSR an.

---

cfgRacVirtual

Diese Gruppe enthält Parameter zum Konfigurieren der Funktion des virtuellen iDRAC6-Datenträgers. Es ist eine Instanz der Gruppe zulässig. In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben.

cfgRacVirMediaAttached (Lesen / Schreiben)

Zulässige Werte

0 = Trennen

1 = Verbinden

2 = Automatisch verbinden

Standardeinstellung

0

Beschreibung

Dieses Objekt wird verwendet, um virtuelle Geräte über den USB-Bus mit dem System zu verbinden. Wenn die Geräte angeschlossen sind, erkennt der Server gültige, am System angeschlossene USB-Massenspeichergeräte. Dies entspricht dem Anschließen eines lokalen USB-CDROM-/Diskettenlaufwerks am USB-Anschluss eines Systems. Wenn die Geräte angeschlossen sind, können Sie im Remote-Zugriff über die iDRAC 6-Webschnittstelle oder die CLI eine Verbindung zu den virtuellen Geräten herstellen. Durch die Einstellung dieses Objekts auf **0** werden die Geräte veranlasst, die Verbindung zum USB-Bus zu trennen.

cfgVirMediaBootOnce (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Funktion **Virtual Media Boot Once (Einmal-Starten des virtuellen Datenträgers)** auf dem iDRAC6.

cfgVirtualFloppyEmulation (Lesen/Schreiben)

ANMERKUNG: Der virtuelle Datenträger muss neu verbunden werden (mittels cfgRacVirMediaAttached), damit die Änderung in Kraft treten kann.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Bei Einstellung auf 0 wird das virtuelle Diskettenlaufwerk von Windows-Betriebssystemen als Wechselplatte erkannt. Windows-Betriebssysteme weisen während der Aufzählung einen Laufwerkbuchstaben zu, der C: oder höher ist. Bei Einstellung auf 1 wird das virtuelle Diskettenlaufwerk von Windows-Betriebssystemen als Diskettenlaufwerk angesehen. Windows-Betriebssysteme weisen den Laufwerkbuchstaben A: oder B: zu.

cfgVirMediaKeyEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Schlüsselfunktion des virtuellen Datenträgers auf dem RAC.

cfgSDWriteProtect (Nur-Lesen)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

---

cfgServerInfo

Diese Gruppe ermöglicht Ihnen, das erste BIOS-Startlaufwerk auszuwählen und das ausgewählte Laufwerk nur einmal zu starten.

cfgServerFirstBootDevice (Lesen/Schreiben)

Zulässige Werte

No-Override

PXE

HDD

DIAG

CD-DVD

BIOS

vFDD

VCD-DVD

iSCSI

VFLASH

FDD

SD

Standardeinstellung

No-Override

Beschreibung

Stellt das erste Startlaufwerk ein oder zeigt es an.

cfgServerBootOnce (Lesen/Schreiben)

Zulässige Werte

1 = TRUE

0 = FALSE

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Einmal-Starten-Funktion des Servers.

---

cfgActiveDirectory

Diese Gruppe enthält Parameter zum Konfigurieren der iDRAC6-Active Directory-Funktion.

cfgADRacDomain (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette von bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

<leer>

Beschreibung

Active Directory-Domäne, in der sich der iDRAC6 befindet.

cfgADRacName (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette von bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

<leer>

Beschreibung

Name des iDRAC6, wie er in der Active Directory-Gesamtstruktur eingetragen ist.

cfgADEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Active Directory-Benutzerauthentifizierung auf dem iDRAC6. Ist diese Eigenschaft deaktiviert, wird nur die lokale iDRAC6-Authentifizierung für Benutzeranmeldungen verwendet.

cfgADSSOEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die einfache Active Directory-Anmeldungsauthentifizierung auf dem iDRAC6.

cfgADDomainController1 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 ASCII-Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) repräsentiert.

Standardeinstellung

<leer>

Beschreibung

Der iDRAC6 verwendet den von Ihnen festgelegten Wert, um auf dem LDAP-Server nach Benutzernamen zu suchen.

cfgADDomainController2 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 ASCII-Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) repräsentiert.

Standardeinstellung

<leer>

Beschreibung

Der iDRAC6 verwendet den von Ihnen festgelegten Wert, um auf dem LDAP-Server nach Benutzernamen zu suchen.

cfgADDomainController3 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 ASCII-Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) repräsentiert.

Standardeinstellung

<leer>

Beschreibung

Der iDRAC6 verwendet den von Ihnen festgelegten Wert, um auf dem LDAP-Server nach Benutzernamen zu suchen.

cfgADAuthTimeout (Lesen/Schreiben)

Zulässige Werte

15 - 300 Sekunden

Standardeinstellung

120

Beschreibung

Legt die Anzahl von Sekunden fest, während der die Active Directory-Authentifizierungsauffordungen abgeschlossen werden müssen, bevor eine Zeitüberschreitung eintritt.

cfgADType (Lesen/Schreiben)

Zulässige Werte

1 (Erweitertes Schema)

2 (Standardschema)

Standardeinstellung

1

Beschreibung

Bestimmt den Schematyp, der mit dem Active Directory verwendet werden soll.

cfgADGlobalCatalog1 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 ASCII-Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) repräsentiert.

Standardeinstellung

<leer>

Beschreibung

iDRAC6 verwendet den von Ihnen festgelegten Wert, um auf dem globalen Katalogserver nach Benutzernamen zu suchen.

cfgADGlobalCatalog2 (Lesen / Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 ASCII-Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) repräsentiert.

Standardeinstellung

<leer>

Beschreibung

iDRAC6 verwendet den von Ihnen festgelegten Wert, um auf dem globalen Katalogserver nach Benutzernamen zu suchen.

cfgADGlobalCatalog3 (Lesen / Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 ASCII-Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) repräsentiert.

Standardeinstellung

<leer>

Beschreibung

iDRAC6 verwendet den von Ihnen festgelegten Wert, um auf dem globalen Katalogserver nach Benutzernamen zu suchen.

cfgADCertValidationEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Active Directory-Zertifikatvalidierung als Teil des Active Directory-Konfigurationsvorgangs.

cfgADDcSRVLookupEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE) - DNS für die Anfrage von Domänen-Controllern verwenden

0 (FALSE) - vorkonfigurierte Domänen-Controller verwenden

Standardeinstellung

0

Definition

Konfiguriert iDRAC6 zur Verwendung vorkonfigurierter Domänen-Controller oder zur Verwendung von DNS zum Auffinden des Domänen-Controllers. Wenn vorkonfigurierte Domänen-Controller verwendet werden, sind die zu verwendenden Domänen-Controller unter cfgAdDomainController1, cfgAdDomainController2 und cfgAdDomainController3 festgelegt. iDRAC6 führt keinen Failover zu den festgelegten Domänen-Controllern durch, wenn die DNS-Anfrage fehlschlägt oder keiner der Server funktioniert, die von der DNS-Anfrage zurückgegeben wurden.

cfgADDcSRVLookupbyUserdomain (Lesen / Schreiben)

Zulässige Werte

1 (TRUE) - Benutzerdomäne als Suchdomäne für die Anfrage nach DCs verwenden. Die Benutzerdomäne wird aus der Benutzerdomänenliste ausgewählt oder vom Anmeldebenutzer eingegeben.

0 (FALSE) - verwenden Sie die konfigurierte Suchdomäne *cfgADDcSrvLookupDomainName*, um DCs anzufragen.

Standardeinstellung

1

Definition

Wählt die Art und Weise aus, wie die Benutzerdomäne für Active Directory angefragt wird.

cfgADDcSRVLookupDomainName (Lesen / Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254

Standardeinstellung

Null

Definition

Das ist die Active Directory-Domäne, die zu verwenden ist, wenn *cfgAddcSrvLookupbyUserDomain* auf 0 eingestellt ist.

cfgADGcSRVLookupEnable (Lesen / Schreiben)

Zulässige Werte

0(FALSE) - vorkonfigurierte globale Katalogserver (GCS) verwenden

1(TRUE) - DNS für die GCS-Anfrage verwenden

Standardeinstellung

0

Definition

Bestimmt, wie die Anfrage des globalen Katalogservers durchgeführt wird. Wenn vorkonfigurierte globale Katalogserver verwendet werden, verwendet der iDRAC6 die Werte cfgAdGlobalCatalog1, cfgAdGlobalCatalog2 und cfgAdGlobalCatalog3.

cfgADGcRootDomain (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254

Standardeinstellung

Null

Beschreibung

Der Name der Active Directory-Stammdomäne, der für die DNS-Anfrage verwendet wird, um die globalen Katalogserver aufzufinden.

---

cfgLDAP

Diese Gruppe ermöglicht Ihnen, Einstellungen zu konfigurieren, die mit dem Lightweight Directory Access Protocol (LDAP) in Zusammenhang stehen.

cfgLdapEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Schaltet den LDAP-Dienst ein oder aus.

cfgLdapServer (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 1024

Standardeinstellung

Null

Beschreibung

Konfiguriert die Adresse des LDAP-Servers.

cfgLdapPort (Lesen/Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

636

Beschreibung

Anschluss von LDAP über SSL. Nicht-SSL-Anschluss wird nicht unterstützt.

cfgLdapBasedn (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254

Standardeinstellung

Null

Beschreibung

Der Domänenname der Teilstruktur des Verzeichnisses, von dem sämtliche Suchen ausgehen sollten.

cfgLdapUserAttribute (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254

Standardeinstellung

Null.

uid wenn nicht konfiguriert.

Beschreibung

Legt das zu suchende Benutzerattribut fest. Wenn keine Konfiguration vorliegt, lautet die zu verwendende Standardeinstellung uid. Es wird empfohlen, innerhalb des ausgewählten Base-DN eindeutig zu sein, da andernfalls ein Suchfilter konfiguriert werden muss, um die Eindeutigkeit des anmeldenden Benutzers zu gewährleisten. Wenn der Benutzer-DN nicht eindeutig identifiziert werden kann, schlägt die Anmeldung fehl und es wird eine Fehlermeldung angezeigt.

cfgLdapGroupAttribute (Lesen/Schreiben).

Zulässige Werte

Zeichenkette. Maximale Länge = 254

Standardeinstellung

Null

Beschreibung

Legen Sie fest, welches LDAP-Attribut zum Prüfen nach der Gruppenmitgliedschaft verwendet werden soll. Dieses sollte ein Attribut der Gruppenklasse sein. Wenn es nicht festgelegt wird, verwendet iDRAC6 die Attribute des Mitglieds und des eindeutigen Mitglieds.

cfgLdapGroupAttributeIsDN (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Wenn eine Einstellung auf 1 vorliegt, vergleicht iDRAC6 den aus dem Verzeichnis abgerufenen Benutzer-DN, um einen Vergleich mit den Gruppenmitgliedern durchzuführen; wenn eine Einstellung auf 0 vorliegt, wird der vom anmeldenden Benutzer angegebene Benutzername verwendet, um einen Vergleich mit den Gruppenmitgliedern durchzuführen. Dies hat keinen Einfluss auf den Suchalgorithmus für die Bindung. iDRAC6 sucht stets nach dem Benutzer-DN und verwendet den Benutzer-DN zum Binden.

cfgLdapBinddn (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254

Standardeinstellung

Null

Beschreibung

Der abgegrenzte Name eines Benutzers, der bei der Suche nach dem DN des anmeldenden Benutzers zum Binden an den Server verwendet wird. Bei Nichtangabe wird ein anonymer Bind verwendet. Dies ist optional, ist jedoch dann erforderlich, wenn ein anonymer Bind nicht unterstützt wird.

cfgLdapBindpassword (Nur Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254

Standardeinstellung

Null

Beschreibung

Ein Bind-Kennwort, das in Verbindung mit dem Bind-DN zu verwenden ist. Das Bind-Kennwort gilt als vertrauliche Information und ist entsprechend zu schützen. Dies ist optional, ist jedoch dann erforderlich, wenn ein anonymer Bind nicht unterstützt wird.

cfgLdapSearchFilter (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254

Standardeinstellung

(objectclass=*)

Sucht nach allen Objekten in der Struktur.

Beschreibung

Ein gültiger LDAP-Suchfilter. Dieser Filter wird verwendet, wenn das Benutzerattribut den anmeldenden Benutzer innerhalb des ausgewählten Base-DN nicht eindeutig identifizieren kann. Der "Suchfilter" bezieht sich nur auf die Benutzer-DN-Suche und nicht auf die Gruppenmitgliedschaftssuche.

cfgLDAPCertValidationEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Steuert die Zertifikatvalidierung während des SSL-Handshake.

---

cfgLdapRoleGroup

Diese Gruppe ermöglicht dem Benutzer, Rollengruppen für das LDAP zu konfigurieren.

cfgLdapRoleGroupIndex (Nur-Lesen)

Zulässige Werte

Eine ganze Zahl zwischen 1 und 5.

Standardeinstellung

<Instanz>

Beschreibung

Hierbei handelt es sich um den Indexwert des Rollengruppenobjekts.

cfgLdapRoleGroupDN (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 1024

Standardeinstellung

<leer>

Beschreibung

Hierbei handelt es sich um den Domänennamen der Gruppe in diesem Index.

cfgLdapRoleGroupPrivilege (Lesen/Schreiben)

Zulässige Werte

0x00000000 bis 0x000001ff

Standardeinstellung

0x000

Beschreibung

Eine Bit-Maske, welche die Berechtigungen definiert, die mit dieser speziellen Gruppe in Verbindung stehen.

---

cfgStandardSchema

Diese Gruppe enthält Parameter zur Konfiguration der Standardschemaeinstellungen des Active Directory.

cfgSSADRoleGroupIndex (Nur-Lesen)

Zulässige Werte

Eine ganze Zahl zwischen 1 und 5.

Standardeinstellung

<Instanz>

Beschreibung

Index der Rollengruppe, wie im Active Directory verzeichnet.

cfgSSADRoleGroupName (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette von bis zu 254 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Name der Rollengruppe, wie in der Active Directory-Gesamtstruktur verzeichnet.

cfgSSADRoleGroupDomain (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette von bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

<leer>

Beschreibung

Active Directory-Domäne, in der sich die Rollengruppe befindet.

cfgSSADRoleGroupPrivilege (Lesen/Schreiben)

Zulässige Werte

0x00000000 bis **0x000001ff**

Standardeinstellung

<leer>

Beschreibung

Verwenden Sie die Bitmaskenzahlen in Tabelle B-4, um rollenbasierte Autoritätsberechtigungen für eine Rollengruppe festzulegen.

Tabelle B-4. Bitmasken für Berechtigungen der Rollengruppe

Rollengruppenberechtigung	Bitmaske
Am iDRAC anmelden	0x00000001
iDRAC konfigurieren	0x00000002
Benutzer konfigurieren	0x00000004

Protokolle löschen	0x00000008
Serversteuerungsbefehle ausführen	0x00000010
Auf die Konsolenumleitung zugreifen	0x00000020
Zugriff auf virtuelle Datenträger	0x00000040
Testwarnungen	0x00000080
Debug-Befehle ausführen	0x00000100

---

cfgIpmiSol

Diese Gruppe wird zur Konfiguration der SOL-Fähigkeiten (Seriell über LAN) des Systems verwendet.

cfgIpmiSolEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert SOL.

cfgIpmiSolBaudRate (Lesen/Schreiben)

Zulässige Werte

9600, 19200, 57600, 115200

Standardeinstellung

115200

Beschreibung

Die Baudrate für die serielle Datenübertragung über LAN.

cfgIpmiSolMinPrivilege (Lesen/Schreiben)

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

Legt die Mindestberechtigungsebene fest, die für den SOL-Zugriff erforderlich ist.

cfgIpmiSolAccumulateInterval (Lesen/Schreiben)

Zulässige Werte

1 - 255

Standardeinstellung

10

Beschreibung

Gibt die typische Zeitdauer an, in welcher der iDRAC6 vor dem Übertragen eines partiellen SOL-Zeichen-Datenpakets wartet. Dieser Wert besteht aus 1-basierten 5-ms-Schritten.

cfgIpmiSolSendThreshold (Lesen/Schreiben)

Zulässige Werte

1 - 255

Standardeinstellung

255

Beschreibung

Der SOL-Schwellengrenzwert. Legt die Höchstanzahl an Bytes fest, die vor dem Senden eines SOL-Datenpakets zwischengespeichert werden.

---

cfgIpmiLan

Diese Gruppe wird zur Konfiguration der IPMI-über-LAN-Funktionen des Systems verwendet.

cfgIpmiLanEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die IPMI-über-LAN-Schnittstelle.

cfgIpmiLanPrivilegeLimit (Lesen/Schreiben)

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

Gibt die maximal zulässige Berechtigungsebene für den IPMI-über-LAN-Zugriff an.

cfgIpmiLanAlertEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert globale E-Mail-Warnmeldungen. Diese Eigenschaft überschreibt alle individuellen aktivieren/deaktivieren-Eigenschaften für E-Mail-Warnmeldungen.

cfgIpmiEncryptionKey (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von Hexadezimalziffern von 0 bis 40 Zeichen ohne Leerstellen. Es ist nur eine gerade Anzahl von Ziffern zulässig.

Standardeinstellung

00000000000000000000

Beschreibung

IPMI-Verschlüsselungsschlüssel.

cfgIpmiPetCommunityName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 18 Zeichen.

Standardeinstellung

public

Beschreibung

Der SNMP-Community-Name für Traps.

---

cfgIpmiPetIpv6

Diese Gruppe wird zur Konfigurieration von IPv6-Plattformereignis-Traps auf dem verwalteten Server verwendet.

cfgIpmiPetIPv6Index (Nur-Lesen)

Zulässige Werte

1 - 4

Standardeinstellung

<Indexwert>

Beschreibung

Eindeutiger Bezeichner für den Index, der dem Trap entspricht.

cfgIpmiPetIPv6AlertDestIpAddr

Zulässige Werte

IPv6-Adresse

Standardeinstellung

<leer>

Beschreibung

Konfiguriert die IP-Adresse des IPv6-Warnungsziels für den Trap.

cfgIpmiPetIPv6AlertEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert das IPv6-Warnungsziel für den Trap.

---

cfgIpmiPef

Diese Gruppe wird zur Konfiguration der auf dem verwalteten Server verfügbaren Plattformereignisfilter verwendet.

Die Ereignisfilter können zur Kontrolle von Regeln verwendet werden, die mit Maßnahmen in Beziehung stehen, die beim Auftreten kritischer Ereignisse auf dem verwalteten System ausgelöst werden.

Um PEF-Maßnahmen für den informativen Assertionsfilter der SD-Karte zu konfigurieren, können Sie nicht den lokalen racadm-Befehl verwenden. Verwenden Sie stattdessen den Befehl remote racadm:

```
racadm -r <iDRAC6-IP-Adresse> -u <Benutzername> -p <calvin> config -g cfgIpmipef -i 20 -o cfgIpmipefaction [0-3]
```

cfgIpmiPefName (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 255 Zeichen.

Standardeinstellung

Der Name des Indexfilters.

Beschreibung

Gibt den Namen des Plattformereignisfilters an.

cfgIpmiPefIndex (Lesen/Schreiben)

Zulässige Werte

1 - 22

Standardeinstellung

Der Indexwert eines Plattformereignisfilterobjekts.

Beschreibung

Gibt den Index eines spezifischen Plattformereignisfilters an.

cfgIpmiPefAction (Lesen/Schreiben)

Zulässige Werte

0 (Kein)

1 (Herunterfahren)

2 (Rücksetzen)

3 (Aus-/Einschaltzyklus)

Standardeinstellung

0

Beschreibung

Legt die Maßnahme fest, die bei Auslösung der Warnung auf dem verwalteten Server ausgeführt wird.

cfgIpmiPefEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert einen spezifischen Plattformereignisfilter.

---

cfgIpmiPet

Diese Gruppe wird zur Konfiguration von Plattformereignis-Traps auf dem verwalteten Server verwendet.

cfgIpmiPetIndex (Nur-Lesen)

Zulässige Werte

1 - 4

Standardeinstellung

Der Indexwert eines spezifischen Plattformereignis-Traps.

Beschreibung

Eindeutiger Bezeichner für den Index, der dem Trap entspricht.

cfgIpmiPetAlertDestIpAddr (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die eine gültige IPv4-Adresse repräsentiert. Beispiel: `192.168.0.67`.

Standardeinstellung

0.0.0.0

Beschreibung

Gibt die Ziel-IPv4-Adresse für den Trap-Empfänger auf dem Netzwerk an. Der Trap-Empfänger empfängt einen SNMP-Trap, wenn auf dem verwalteten Server ein Ereignis ausgelöst wird.

cfgIpmiPetAlertEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert einen spezifischen Trap.

---

cfgUserDomain

Diese Gruppe wird zur Konfiguration der Active Directory-Benutzerdomänennamen verwendet. Es können jeweils maximal 40 Domänenamen konfiguriert sein.

cfgUserDomainIndex (Nur-Lesen)

Zulässige Werte

1 - 40

Standardeinstellung

Der Indexwert.

Beschreibung

Stellt eine spezifische Domäne dar.

cfgUserDomainName (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 255 ASCII-Zeichen.

Standardeinstellung

<leer>

Beschreibung

Gibt den Active Directory-Benutzerdomänennamen an.

---

cfgServerPower

Diese Gruppe enthält verschiedene Energieverwaltungsfunktionen.

cfgServerPowerStatus (Nur-Lesen)

Zulässige Werte

1 (EIN)

0 (AUS)

Standardeinstellung

<aktueller Serverstromzustand>

Beschreibung

Stellt den Serverstromzustand als entweder EIN oder AUS dar.

cfgServerPowerServerAllocation (Nur-Lesen)

ANMERKUNG: Wenn mehr als ein Netzteil verwendet wird, stellt diese Eigenschaft den Netzteil mit minimaler Kapazität dar.

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<leer>

Beschreibung

Stellt die verfügbare zugewiesene Stromversorgung zur Verwendung durch den Server dar.

cfgServerActualPowerConsumption (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<leer>

Beschreibung

Stellt den vom Server derzeit verbrauchten Strom dar.

cfgServerPowerCapEnable (Nur-Lesen)

Zulässige Werte

0

1

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert den benutzerdefinierten Strombudgetschwellenwert

cfgServerMinPowerCapacity (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<leer>

Beschreibung

Stellt die minimale Serverstromkapazität dar.

cfgServerMaxPowerCapacity (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<leer>

Beschreibung

Stellt die maximale Serverstromkapazität dar.

cfgServerPeakPowerConsumption (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<aktueller Spitzenstromverbrauch des Servers>

Beschreibung

Stellt den maximalen vom Server verbrauchten Strom bis zum jetzigen Zeitpunkt dar.

cfgServerPeakPowerConsumptionTimestamp (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

Zeitstempel des maximalen Stromverbrauchs

Beschreibung

Zeitpunkt, zu dem der maximale Stromverbrauch aufgezeichnet wurde.

cfgServerPowerConsumptionClear (Nur-Lesen)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

****

Beschreibung

Setzt die Eigenschaft cfgServerPeakPowerConsumption auf 0 und die Eigenschaft cfgServerPeakPowerConsumptionTimestamp auf die aktuelle iDRAC-Zeit zurück.

cfgServerPowerCapWatts (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

Serverstromschwellenwert in Watt

Beschreibung

Stellt den Serverstromschwellenwert in Watt dar.

cfgServerPowerCapBtuhr (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

Serverstromschwellenwert in BTU/h

Beschreibung

Stellt den Serverstromschwellenwert in BTU/h dar.

cfgServerPowerCapPercent (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

Serverstromschwellenwert in Prozent.

Beschreibung

Stellt den Serverstromschwellenwert in Prozent dar.

---

cfgIPv6LanNetworking

Diese Gruppe wird zur Konfiguration der IPv6-über-LAN-Netzwerkfunktionen verwendet.

cfgIPv6Enable

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert den iDRAC6-IPv6-Stack.

cfgIPv6Address1 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag repräsentiert.

Standardeinstellung

::

Beschreibung

Eine iDRAC6-IPv6-Adresse.

cfgIPv6Gateway (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag repräsentiert.

Standardeinstellung

::

Beschreibung

Die iDRAC6-Gateway-IPv6-Adresse.

cfgIPv6PrefixLength (Lesen/Schreiben)

Zulässige Werte

1 - 128

Standardeinstellung

64

Beschreibung

Die Präfixlänge für die iDRAC6-IPv6-Adresse 1.

cfgIPv6AutoConfig (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die IPv6-Option automatische Konfiguration.

cfgIPv6LinkLocalAddress (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag repräsentiert.

Standardeinstellung

::

Beschreibung

Die lokale iDRAC6-IPv6-Link-Adresse.

cfgIPv6Address2 (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag repräsentiert.

Standardeinstellung

::

Beschreibung

Eine iDRAC6-IPv6-Adresse.

cfgIPv6DNSServersFromDHCP6 (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Gibt an, ob cfgIPv6DNSServer1 und cfgIPv6DNSServer2 statische oder DHCP-IPv6-Adressen sind.

cfgIPv6DNSServer1 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag repräsentiert.

Standardeinstellung

::

Beschreibung

Eine IPv6-DNS-Server-Adresse.

cfgIPv6DNSServer2 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag repräsentiert.

Standardeinstellung

::

Beschreibung

Eine IPv6-DNS-Server-Adresse.

cfgIPv6Addr2PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

Beschreibung

Die Präfixlänge für die iDRAC6-IPv6-Adresse 2.

cfgIPv6LinkLockPrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgTotalnumberofextended IP (Lesen/Schreiben)

Zulässige Werte

1-256

Standardeinstellung

<leer>

cfgIPv6Addr3PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

<leer>

cfgIPv6Addr3Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address3 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr4PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr4Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address4 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr5PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr5Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address5 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr6PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr6Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address6 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr7PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr7Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address7 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr8PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr8Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address8 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr9PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr9Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address9 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr10PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr10Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address10 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr11PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr11Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address11 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr12PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr12Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address12 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr13PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr13Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address13 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr14PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr14Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address14 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

cfgIPv6Addr15PrefixLength (Nur-Lesen)

Zulässige Werte

1 - 128

Standardeinstellung

0

cfgIPv6Addr15Length (Nur-Lesen)

Zulässige Werte

1-40

Standardeinstellung

<leer>

cfgIPv6Address15 (Nur-Lesen)

Zulässige Werte

Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

<leer>

---

cfgIPv6URL

Diese Gruppe legt Eigenschaften fest, die zur Konfiguration der iDRAC6-IPv6-URL verwendet werden.

cfgIPv6URLstring (Nur-Lesen)

Zulässige Werte

Eine Zeichenkette von bis zu 80 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Die iDRAC6-IPv6-URL

---

cfgIpmiSerial

Diese Gruppe legt Eigenschaften fest, die zur Konfiguration der seriellen IPMI-Schnittstelle des BMC verwendet werden.

cfgIpmiSerialConnectionMode (Lesen/Schreiben)

Zulässige Werte

0 (Terminal)

1 (Basic)

Standardeinstellung

1

Beschreibung

Wenn die iDRAC6-Eigenschaft **cfgSerialConsoleEnable** auf 0 (deaktiviert) gesetzt wird, wird der serielle iDRAC6-Anschluss zum seriellen IPMI-Anschluss. Diese Eigenschaft bestimmt den definierten IPMI-Modus des seriellen Anschlusses.

Im Modus Basic verwendet der Anschluss Binärdaten in der Absicht, mit einem Anwendungsprogramm auf dem seriellen Client zu kommunizieren. Im Terminalmodus nimmt der Anschluss an, dass ein nicht-intelligentes ASCII-Terminal angeschlossen ist und ermöglicht die Eingabe sehr einfacher Befehle.

cfgIpmiSerialBaudRate (Lesen/Schreiben)

Zulässige Werte

9600, 19200, 57600, 115200

Standardeinstellung

57600

Beschreibung

Gibt die Baudrate für eine serielle Verbindung über IPMI an.

cfgIpmiSerialChanPrivLimit (Lesen/Schreiben)

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

Gibt die maximale auf dem seriellen IPMI-Kanal zulässige Berechtigungsebene an.

cfgIpmiSerialFlowControl (Lesen/Schreiben)

Zulässige Werte

0 (Kein)

1 (CTS/RTS)

2 (XON/XOFF)

Standardeinstellung

1

Beschreibung

Gibt die Einstellung der Datenflusssteuerung für den seriellen IPMI-Anschluss an.

cfgIpmiSerialHandshakeControl (Lesen/Schreiben)

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Handshake-Steuerung des IPMI-Terminalmodus.

cfgIpmiSerialLineEdit (Lesen/Schreiben)

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Zeilenbearbeitung auf der seriellen IPMI-Schnittstelle.

cfgIpmiSerialEchoControl (Lesen/Schreiben)

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Echosteuerung auf der seriellen IPMI-Schnittstelle.

cfgIpmiSerialDeleteControl (Lesen/Schreiben)

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Löschsteuerung auf der seriellen IPMI-Schnittstelle.

cfgIpmiSerialNewLineSequence (Lesen/Schreiben)

Zulässige Werte

0 (Kein)

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

Standardeinstellung

1

Beschreibung

Spezifiziert die Zeilenumbruchssequenz für die serielle IPMI-Schnittstelle.

cfgIpmiSerialInputNewLineSequence (Lesen/Schreiben)

Zulässige Werte

0 (<EINGABE>)

1 (NULL)

Standardeinstellung

1

Beschreibung

Spezifiziert die Eingabe-Zeilenumbruchssequenz für die serielle IPMI-Schnittstelle.

---

cfgSmartCard

Diese Gruppe legt Eigenschaften fest, die zur Unterstützung des Zugriffs auf den iDRAC6 mithilfe einer Smart Card verwendet werden.

cfgSmartCardLogonEnable (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

2 (Aktiviert mit Remote-RACADM)

Standardeinstellung

0

Beschreibung

Aktiviert, deaktiviert oder aktiviert mit Remote-RACADM-Unterstützung den Zugriff auf den iDRAC6 unter Verwendung einer Smart Card.

cfgSmartCardCRLEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Zertifikatsperrliste (CRL).

---

cfgNetTuning

Diese Gruppe ermöglicht Benutzern, die erweiterten Netzwerkschnittstellen-Parameter für den RAC-NIC zu konfigurieren. Nach der Konfiguration kann es bis zu einer Minute dauern, bis die aktualisierten Einstellungen aktiviert werden.

△ **VORSICHT: Bei der Änderung von Eigenschaften in dieser Gruppe muss mit äußerster Vorsicht vorgegangen werden. Eine unsachgemäße Änderung der Eigenschaften in dieser Gruppe kann dazu führen, dass Ihr RAC-NIC funktionsunfähig wird.**

cfgNetTuningNicAutoneg (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert die automatische Verhandlung für physikalische Verbindungsgeschwindigkeit und Duplex. Wenn aktiviert, hat die automatische Verhandlung Vorrang vor Werten, die in den Objekten **cfgNetTuningNic100MB** und **cfgNetTuningNicFullDuplex** festgelegt wurden.

cfgNetTuningNic100MB (Lesen/Schreiben)

Zulässige Werte

0 (10 MBit)

1 (100 MBit)

Standardeinstellung

1

Beschreibung

Gibt die Geschwindigkeit an, die für den RAC-NIC verwendet werden soll. Diese Eigenschaft wird nicht verwendet, wenn **cfgNetTuningNicAutoNeg** auf **1** (aktiviert) eingestellt ist.

cfgNetTuningNicFullDuplex (Lesen/Schreiben)

Zulässige Werte

0 (Halb-Duplex)

1 (Voll-Duplex)

Standardeinstellung

1

Beschreibung

Gibt die Duplexeinstellung für den RAC-NIC an. Diese Eigenschaft wird nicht verwendet, wenn **cfgNetTuningNicAutoNeg** auf **1** (aktiviert) eingestellt ist.

cfgNetTuningNicMtu (Lesen/Schreiben)

Zulässige Werte

576 - 1500

Standardeinstellung

1500

Beschreibung

Die Größe der maximalen Übertragungseinheit in Bytes, die vom iDRAC6-NIC verwendet wird.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Unterstützte RACADM-Schnittstellen

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Tabelle C-1 enthält eine Übersicht über RACADM-Unterbefehle und deren entsprechende Schnittstellenunterstützung.

Tabelle C-1. Schnittstellenunterstützung für RACADM-Unterbefehle

Unterbefehl	Telnet/SSH/Seriell	Lokaler RACADM	Remote-RACADM
arp	✓	✗	✓
clearasrscreen	✓	✓	✓
clrraclog	✓	✓	✓
clrsel	✓	✓	✓
coredump	✓	✗	✓
coredumpdelete	✓	✓	✓
fwupdate	✓	✓	✓
getconfig	✓	✓	✓
getniccfg	✓	✓	✓
getraclog	✓	✓	✓
getractime	✓	✓	✓
getsel	✓	✓	✓
getssninfo	✓	✓	✓
getsvctag	✓	✓	✓
getsysinfo	✓	✓	✓
gettracelog	✓	✓	✓
help	✓	✓	✓
ifconfig	✓	✗	✓
krbkeytabupload	✗	✓	✓
netstat	✓	✗	✓
ping	✓	✗	✓
racdump	✓	✗	✓
racreset	✓	✓	✓
racresetcfg	✓	✓	✓
serveraction	✓	✓	✓
setniccfg	✓	✓	✓
sshpkauth	✓	✓	✓
sslcertdownload	✗	✓	✓
sslcertupload	✗	✓	✓
sslcertview	✓	✓	✓
sslcsrgen	✗	✓	✓
sslkeyupload	✗	✓	✓
testemail	✓	✓	✓
testtrap	✓	✓	✓
vmdisconnect	✓	✓	✓

vmkey	✓	✓	✓
usercertupload	✗	✓	✓
usercertview	✓	✓	✓
localConRedirDisable	✗	✓	✗
✓ = Unterstützt; ✗ = Nicht unterstützt			

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6-Übersicht

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Der Integrated Dell™ Remote Access Controller 6 (iDRAC6) ist eine Hardware- und Softwarelösung zur Systemverwaltung, die Remote-Verwaltungsfunktionen, 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 koexistieren 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 Netzwerkverwaltungsprotokolls (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.

---

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 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 der LDAP-basierten Authentifizierung (Lightweight Directory Access Protocol). Für diese Funktion ist in Ihren Verzeichnisdiensten keine Schemaerweiterung erforderlich.
- Überwachung - Zugriff auf Systeminformationen und Komponentenstatus
- Zugriff auf Systemprotokolle - Bietet Zugriff auf das Systemereignisprotokoll, das iDRAC6-Protokoll und den Bildschirm "Letzter Absturz" des abgestürzten oder nicht reagierenden Systems, unabhängig vom Zustand des Betriebssystems
- Dell OpenManage™ Software-Integration - Ermöglicht es Ihnen, die iDRAC6-Webschnittstelle vom Dell OpenManage Server Administrator oder Dell OpenManage IT Assistant zu starten
- iDRAC6-Warnungen - Warnt Sie anhand einer E-Mail-Benachrichtigung oder eines SNMP-Traps vor potenziellen Problemen mit verwalteten Knoten
- Remote-Stromverwaltung - Remote-Stromverwaltungsfunktionen wie Herunterfahren und Reset (Zurücksetzen) von einer Verwaltungskonsole aus
- Unterstützung für die intelligente Plattform-Verwaltungsschnittstelle (IPMI)
- SSL-Verschlüsselung (Secure Sockets Layer) - Bietet sichere Remote-Systemverwaltung über die Webschnittstelle
- Sicherheitsverwaltung auf Kennwortebene - Verhindert den unbefugten Zugriff auf ein Remote-System
- Rollenbasierte Autorität - Bietet zuweisbare Berechtigungen für verschiedene Systemverwaltungsaufgaben
- IPv6-Support - 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.
- WS-MAN-Support - Bietet über das Netzwerk zugängliche Verwaltung unter Verwendung des WS-MAN-Protokolls (Webdienste für die Verwaltung).
- SM-CLP-Support - Fügt SM-CLP-Support (Serververwaltungs-Befehlszeilenprotokoll) hinzu, um Standards für SM-CLI-Implementierungen zu bieten.
- Zurücksetzen und Wiederherstellen der Firmware - Ermöglicht Ihnen das Starten (oder Zurücksetzen) von einem Firmware-Image Ihrer Wahl.

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

---

iDRAC6 Enterprise und VFlash- Datenträger

Bietet zusätzliche Unterstützung für RACADM, virtuelle KVM, virtuelle Datenträgerfunktionen, einen dedizierten NIC und Virtual Flash (mit einer optionalen Dell VFlash-Medienkarte). Virtual Flash 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 **support.dell.com/manuals**.

Tabelle 1-1 listet die Funktionen auf, die für BMC, iDRAC6 Express, iDRAC6 Enterprise und VFlash-Datenträger 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	✗	✓	✓	✓
RACADM-Befehlszeile	✗	✗	✓	✓
Verbindungen				
Netzwerkmodi Freigegeben/Failover	✓	✓	✓	✓
IPv4	✓	✓	✓	✓
VLAN-Tagging	✓	✓	✓	✓
IPv6	✗	✓	✓	✓
Dynamisches DNS	✗	✓	✓	✓
Dedizierter NIC	✗	✗	✓	✓
Sicherheit und Authentifizierung				
Rollenbasierte Autorität	✓	✓	✓	✓
Lokale Benutzer	✓	✓	✓	✓
Verzeichnisdienst	✗	✓	✓	✓
Zweifaktor-Authentifizierung	✗	✓	✓	✓
Einfache Anmeldung	✗	✓	✓	✓
SSL-Verschlüsselung	✓	✓	✓	✓
Remote-Verwaltung und Störungsbeseitigung				
Remote-Firmware-Aktualisierung	✓ 1	✓	✓	✓
Remote-Betriebssystem-Installation	✗	✓	✓	✓
Serverstromregelung	✓ 1	✓	✓	✓
Seriell-über-LAN (mit Proxy)	✓	✓	✓	✓
Seriell-über-LAN (ohne Proxy)	✗	✓	✓	✓
Strombegrenzung	✗	✓	✓	✓
Erfassung des Bildschirms "Letzter Absturz"	✗	✓	✓	✓
Start-Capture	✗	✓	✓	✓
Virtueller Datenträger	✗	✗	✓	✓
Virtuelle Konsole	✗	✗	✓	✓
Gemeinsame Nutzung der virtuellen Konsole	✗	✗	✓	✓
Virtual Flash	✗	✗	✗	✓
Überwachung				
Sensorüberwachung und Warnmeldungen	✓ 1	✓	✓	✓
Echtzeit-Stromüberwachung	✗	✓	✓	✓
Echtzeit-Stromdiagramme	✗	✓	✓	✓
Historische Stromzähler	✗	✓	✓	✓
Protokollierung				
Systemereignisprotokoll (SEL)	✓	✓	✓	✓

RAC-Protokoll	✗	✓	✓	✓
Ablaufverfolgungsprotokoll	✗	✓	✓	✓
Remote-Syslog	✗	✓	✓	✓
[1] - Funktion ist nur über IPMI verfügbar, nicht über eine Web-GUI				
✓ = 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 einem Administrator 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 unterstützen (für Länder, in denen 128-Bit nicht zulässig ist), verwenden den SSL 3.0-Standard
- Konfiguration der Sitzungszeitüberschreitung (in Sekunden) über die Webschnittstelle oder SM-CLP
- Konfigurierbare IP-Anschlüsse (wo anwendbar)

  ANMERKUNG: Telnet unterstützt keine SSL-Verschlüsselung.

- Secure Shell (SSH), verwendet eine verschlüsselte Übertragungsschicht für höhere Sicherheit
- Beschränkung der Anmeldefehlschläge pro IP-Adresse, mit Anmeldeblockierung der IP-Adresse bei Überschreitung der Grenze
- Die 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 **support.dell.com / manuals**.

Unterstützte Betriebssysteme

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

Unterstützte Webbrowser

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

Unterstützte Remote-Zugriffsverbindungen

Tabelle 1-2 führt die Verbindungsfunktionen auf.

Tabelle 1-2. Unterstützte Remote-Zugriffsverbindungen

Verbindung	Funktionen
iDRAC6-NIC	- 10 MBit/s/100 MBit/s/Ethernet - DHCP-Unterstützung - SNMP-Traps und E-Mail-Ereignisbenachrichtigung - Unterstützung für SM-CLP-Befehls-Shell (Telnet, SSH und RACADM) und für Verfahren wie iDRAC6-Befehlre fü 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

Anschlussnummer	Funktion
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	Konsolenumleitung - Tastatur/Maus, virtueller Datenträgerdienst, virtueller Datenträger - sicherer Dienst, Konsolenumleitung - Video
* Konfigurierbarer Anschluss	

Tabelle 1-4. iDRAC6-Client-Anschlüsse

Anschlussnummer	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 Benutzerhandbuch enthalten die folgenden Dokumente weitere Informationen zum Setup und Betrieb des iDRAC6 auf dem System. Diese Dokumente sind auf der Dell Support-Website unter **support.dell.com/manuals** verfügbar.

- Die iDRAC6-Online-Hilfe enthält detaillierte Informationen zur Verwendung der webbasierten Schnittstelle.
- Das *Dell Lifecycle Controller-Benutzerhandbuch* enthält Informationen zum Unified Server Configurator (USC), dem Unified Server Configurator - Lifecycle Controller Enabled (USC - LCE) und Remote-Services.
- 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 IT Assistant-Benutzerhandbuch* enthält Informationen zur Verwendung des IT Assistant.
- Informationen zum Installieren eines iDRAC6 finden Sie im *Hardware-Benutzerhandbuch*.
- Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen über die Installation und Verwendung von Server Administrator.
- Das *Dell Update Packages-Benutzerhandbuch* enthält Informationen zum Abrufen und Verwenden von Dell Update Packages als Teil Ihrer Systemaktualisierungsstrategie.
- Informationen zur iDRAC6- und IPMI-Schnittstelle finden Sie im *Benutzerhandbuch für Dienstprogramme des Dell OpenManage Baseboard-Verwaltungs-Controllers*.

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

- In den mit dem System gelieferten Sicherheitshinweisen finden Sie wichtige Informationen zur Sicherheit und zu den Betriebsbestimmungen. Weitere Betriebsbestimmungen finden Sie auf der Website zur Einhaltung gesetzlicher Vorschriften unter **www.dell.com/regulatory_compliance.** Garantiebestimmungen können als separates Dokument beigelegt sein.
- In der zusammen mit der Rack-Lösung gelieferten *Rack-Installationsanleitung* ist 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, Anforderungen, Installation und der grundlegende Betrieb der Software beschrieben.
- In der Dokumentation zum Betriebssystem ist die Installation (sofern erforderlich), Konfiguration und Verwendung des Betriebssystems beschrieben.
- Die Dokumentation für alle separat erworbenen Komponenten enthält Informationen zur Konfiguration und 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.

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

Informationen zu den in diesem Dokument verwendeten Begriffen finden Sie im *Glossar*, das auf der Dell Support-Website unter **support.dell.com / manuals** zur Verfügung steht.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

WS-MAN-Schnittstelle verwenden

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Web Services for Management (WS-MAN) ist ein SOAP-basiertes Protokoll (Simple Object Access Protocol), das für die Systemverwaltung verwendet wird. WS-MAN bietet ein dialogfähiges Protokoll für Geräte, um Daten netzwerkübergreifend freizugeben und auszutauschen. iDRAC6 verwendet WS-MAN zur Übermittlung 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 bestimmten Schnittstellen für eine bestimmte Verwaltungsdomäne oder für einen bestimmten Funktionsbereich definiert. Des Weiteren 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 werden auf die folgenden DMTF-Profile und Dell-Erweiterungsprofile aufgeteilt:

Unterstützte CIM-Profile

Tabelle 11-1. Standard-DMTF

Standard-DMTF
1. Basisserver Definiert CIM-Klassen zur Darstellung des Host-Servers.
2. Serviceprozessor: Enthält die Definition von CIM-Klassen zur Darstellung des iDRAC6. **ANMERKUNG:** Das Profil des Basisservers (oben) und des Serviceprozessors sind in dem Sinne autonom, dass die Objekte, die sie beschreiben, alle anderen in den Komponentenprofilen definierten CIM-Objekte zusammenfassen.
3. Physische Anlagen: Definiert CIM-Klassen zur Darstellung der physischen Aspekte der verwalteten Elemente. iDRAC6 verwendet dieses Profil, um die FRU-Informationen des Hostservers und seiner Komponenten sowie die physische Topologie darzustellen.
4. SM-CLP-Administrator-Domäne Definiert CIM-Klassen zur Darstellung der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für die eigene CLP-Implementierung.
5. Stromzustandsverwaltung Definiert 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 Definiert CIM-Klassen zur Darstellung der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für die eigene CLP-Implementierung.
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 Definiert CIM-Klassen zur Darstellung 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 Definiert CIM-Klassen zur Darstellung von Rollen. iDRAC6 verwendet dieses Profil zum Konfigurieren von iDRAC6-Kontoberechtigungen.
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 Definiert CIM-Klassen zur Darstellung der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für die eigene CLP-Implementierung.
17. Profilregistrierung Definiert 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 Definiert CIM-Klassen zur Darstellung von 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.
Dell-Erweiterungen
1. Dell™ Active Directory-Client-Version 2.0.0 Definiert CIM- und Dell-Erweiterungsklassen zur Konfiguration des iDRAC6 Active Directory-Clients und der lokalen Berechtigungen für Active Directory-Gruppen.
2. Dells virtueller Datenträger Definiert CIM- und Dell-Erweiterungsklassen zur Konfiguration des virtuellen iDRAC6-Datenträgers. Erweitert das USB-Umleitungsprofil.
3. Dells 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 Definiert CIM- und Dell-Erweiterungsklassen zur Darstellung 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.

Die iDRAC6-WS-MAN-Implementierung verwendet SSL auf Anschluss 443 für Transportsicherheit und unterstützt die grundlegende und die Digest-Authentifizierung. Web Services-Schnittstellen können durch Einsatz von Client-Infrastrukturen wie Windows® WinRM und Powershell CLI, Open-Source-Dienstprogrammen wie WSMANCLI und Anwendungsprogrammierumgebungen wie Microsoft® .NET® genutzt werden.

Zusätzliche Implementierungsanleitungen, Informationsberichte, Profile und Codebeispiele stehen im Dell Enterprise Technology Center unter **www.delltechcenter.com** zur Verfügung. Weitere Informationen finden Sie auch an folgenden Stellen:

- DTMF-Website: **www.dmtf.org/standards/profiles/**
- WS-MAN, Anmerkungen zur Version, oder Infodatei.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6-SM-CLP-Befehlszeilenoberfläche verwenden

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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 zur 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 Profile, die unter Tabelle 11-1 "Unterstützte CIM-Profile" beschrieben sind.

Die folgenden Abschnitte bieten 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.

Es folgt ein Beispiel der SM-CLP-Befehlszeilensyntax.

```
<Verb> [<Optionen>] [<Ziel>] [<Eigenschaften>]
```

Während einer typischen SM-CLP-Sitzung können Sie Vorgänge mittels der in Tabelle 12-1 aufgeführten Verben ausführen.

Tabelle 12-1. Unterstützte CLI-Verben für System

Verb	Definition
cd	Navigiert durch den MAP mittels der Shell.
set	Stellt eine Eigenschaft auf einen bestimmten Wert ein.
help	Zeigt die Hilfe für ein bestimmtes Ziel an.
reset	Setzt das Ziel zurück.
show	Zeigt die Zieleigenschaften, Verben und Unterziele an.
start	Schaltet ein Ziel ein.
stop	Fährt ein Ziel herunter.
exit	Beendet die 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 12-2 enthält eine Liste von Zielen, die über das SM-CLP bereitgestellt werden, um die in Tabelle 12-1 beschriebenen Vorgänge zu unterstützen.

Tabelle 12-2. 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
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
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
admin1/system1/sp1/clpsvc1	CLP-Dienst-Protokolldienst
admin1/system1/sp1/clpsvc1/	CLP-Dienst-Protokollendpunkt

clpendpt*	
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
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
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
/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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Betriebssystem mittels VMCLI bereitstellen

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Das VMCLI-Dienstprogramm (Befehlszeilenoberfläche des virtuellen Datenträgers) ist eine Befehlszeilenoberfläche, welche die Funktionen des virtuellen Datenträgers von der 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
- Startimagedatei(en) des Betriebssystems

  Die Imagedatei muss das ISO-Image einer Betriebssystem-CD oder einer CD/DVD in 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>
```

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 Bereitstellungsimagedatei zur Bereitstellung des Betriebssystems an die Remote-Systeme verfügen, können Sie diesen Schritt überspringen.

   Wenn Sie über keine startfähige, vorkonfigurierte Bereitstellungsimagedatei 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:

   - Netzwerkbasierte Standardinstallationsverfahren befolgen.
   - Markieren Sie das Bereitstellungsimage als *schreibgeschützt*, um sicherzustellen, dass jedes Zielsystem dasselbe Bereitstellungsverfahren startet und ausführt.

4. Eines der folgenden Verfahren ausführen:

- 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 Übersicht auf hoher Ebene 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>* der iDRAC6-Benutzername, z. B. **root**, ist
- *<idrac-Benutzerkennwort>* ist das Kennwort für den iDRAC6-Benutzer, z. B. **calvin**
- *<iso9660-Image>* der Pfad zu einem ISO9660-Image der Betriebssystem-Installations-CD-ROM oder -DVD ist
- -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-Dienstprogramms verwenden

Das VMCLI-Dienstprogramm ist eine skriptfähige Befehlszeilenoberfläche, welche die Funktionen des virtuellen Datenträgers von der 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 Plug-ins des virtuellen Datenträgers übereinstimmen
- Automatische Terminierung, wenn die Option Einmal Starten 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.

VORSICHT: 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 enthält 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".

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 beliebigen 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®-Betriebssysteme)

`-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 Befehls-Shell-Funktionen des Betriebssystems, um das Dienstprogramm im Hintergrund auszuführen. 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.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Intelligent Platform Management Interface (IPMI) konfigurieren

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

---

IPMI konfigurieren

Dieser Abschnitt enthält Informationen zur Konfiguration und Verwendung 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".

IPMI mittels der webbasierten Schnittstelle konfigurieren

Weitere Informationen finden Sie unter "IPMI konfigurieren".

IPMI mittels RACADM-CLI konfigurieren

1. Melden Sie sich über eine der RACADM-Schnittstellen am Remote- System an. Siehe "RACADM im Remote-Zugriff verwenden".

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 <Ebene>
      ```

      wobei <*Ebene*> 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-Mindestberechtigungsebene bestimmt die Mindestberechtigung, die erforderlich ist, um IPMI SOL zu aktivieren. 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 *<Ebene>*

wobei <*Ebene*> 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.

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 die serielle IPMI-Verbindung.

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 Baudrate auf der seriellen IPMI 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.

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 <*Ebene*> 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 Roh-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".

Seriell-über-LAN mittels webbasierter Schnittstelle konfigurieren

Weitere Informationen finden Sie unter "IPMI konfigurieren".

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**.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Virtuellen Datenträger konfigurieren und verwenden

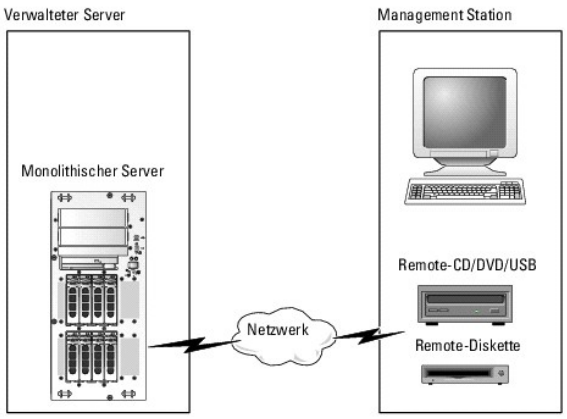
Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

---

Übersicht

Die Funktion **Virtueller Datenträger**, die über den Konsolenumleitungs-Viewer zugreifbar ist, gewährt dem verwalteten Server Zugriff auf Datenträger, die an ein Remote-System im Netzwerk verbunden sind. Abbildung 15-1 zeigt die gesamte Architektur des **virtuellen Datenträgers**.

Abbildung 15-1. 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 Abbilddatei 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 15-1 führt die unterstützten Laufwerkverbindungen für virtuelle Floppy-Laufwerke und virtuelle optische Laufwerke auf.

ANMERKUNG: Werden **virtuelle Datenträger** geändert, während sie verbunden sind, kann dies zum Anhalten der System-Startsequenz führen.

Tabelle 15-1. Unterstützte Laufwerkverbindungen

Unterstützte Verbindungen virtueller Floppy-Laufwerke	Unterstützte Verbindungen virtueller optischer Laufwerke
1,44 Zoll Legacy-Floppy-Laufwerk mit 1,44 Zoll-Diskette	CD-ROM, DVD, CDRW, Kombinationslaufwerk mit CD-ROM-Datenträger
USB-Floppy-Laufwerk mit 1,44 Zoll-Diskette	CD-ROM/DVD-Abbilddatei im Format ISO9660
1,44 Zoll-Disketten-Abbild	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 Runtime Environment (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 Konsolenumleitungs-Plugin ist eine 32-Bit-Java-Laufzeitumgebung (JRE) erforderlich. Sie können eine JRE von **java.sun.com** herunterladen.

△ **VORSICHT: Um den virtuellen Datenträger erfolgreich zu starten, stellen Sie bitte sicher, dass auf einem 64-Bit- oder 32-Bit-Betriebssystem eine 32-Bit-Version der JRE installiert ist. iDRAC6 unterstützt *weder* 64-Bit-Browser noch 64-Bit-JRE-Versionen. Es werden nur 32-Bit-Browser mit 32-Bit-Versionen der JRE unterstützt. 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 bei der iDRAC6-Webschnittstelle an.
2. Wählen Sie **System**→ Register **Konsole/Datenträger** → **Konfiguration**→ **Virtueller Datenträger** aus, um die Einstellungen des virtuellen Datenträgers zu konfigurieren.

   Tabelle 15-2 beschreibt die Konfigurationswerte des **virtuellen Datenträgers**.
3. Wenn Sie mit den Einstellungen fertig sind, klicken Sie auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 15-3.

Tabelle 15-2. 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** - Schließt den **virtuellen Datenträger** nur dann an den Server an, 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.
"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. Beim nächsten Start startet das System vom nächsten Gerät in der Startreihenfolge aus. Diese Option trennt die **virtuellen Datenträger**-Geräte automatisch, nachdem das System einmal gestartet wurde.

Tabelle 15-3. Schaltflächen der Konfigurationsseite

Schaltfläche	Beschreibung
Drucken	Druckt die Werte der **Konfiguration**, die auf dem Bildschirm erscheinen.
Aktualisieren	Lädt die Seite **Konfiguration** neu.
Anwenden	Speichert neue Einstellungen auf der Seite **Konfiguration**.

Virtuellen Datenträger ausführen

△ **VORSICHT: Geben Sie keinen racreset-Befehl aus, wenn eine Virtueller Datenträger-Sitzung ausgeführt wird. Andernfalls könnten unerwünschte Ergebnisse einschließlich Datenverlust auftreten.**

ANMERKUNG: Das Konsolen-Viewer-Fenster (Anwendung) 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 die virtuelle Floppy 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-Abbild oder ein verfügbares Floppy-Laufwerk. Unterstützte optische Laufwerke umfassen maximal ein verfügbares optisches Laufwerk oder eine einzige ISO-Abbilddatei.

Virtuellen Datenträger verbinden

Führen Sie die folgenden Schritte aus, um "Virtueller Datenträger" auszuführen:

1. Öffnen Sie einen unterstützten Webbrowser auf der Management Station.

2. Starten Sie die iDRAC6-Webschnittstelle. Weitere Informationen finden Sie unter "Zugriff auf die Webschnittstelle".

3. Wählen Sie **System**→ **Konsole/Datenträger**→ **Konsolenumleitung** und **Virtueller Datenträger** aus.

4. Die Seite **Konsolenumleitung** und **virtueller Datenträger** wird angezeigt. Informationen zum Ändern der Werte der angezeigten Attribute finden Sie unter "Virtuellen Datenträger konfigurieren".

   ANMERKUNG: Die **Floppy-Abbilddatei** unter **Floppy-Laufwerk** (falls zutreffend) wird u. U. angezeigt, da dieses Gerät als virtuelle Floppy 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 **Viewer 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 **iDRAC6 KVM** wird in einem separaten Fenster gestartet.

6. Klicken Sie auf **Virtueller Datenträger**→ **Starten Sie Virtueller Datenträger**.

   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. Wählen Sie das Kästchen links neben dem Datenträger ab, der abgetrennt werden soll.

8. Wählen Sie das Kästchen neben den Datenträgertypen aus, die Sie verbinden möchten.

   Wenn Sie eine Verbindung zu einem Diskettenabbild oder ISO-Abbild herstellen möchten, geben Sie (auf Ihrem lokalen Computer) den Pfad zum Abbild

ein oder klicken Sie auf die Schaltfläche **Abbild hinzufügen**, um zum Abbild zu navigieren**.**

Die Verbindung zum Datenträger wird hergestellt und das Fenster **Status** aktualisiert.

Verbindung des virtuellen Datenträgers abtrennen

1. Klicken Sie auf **Extras**→ **Virtuellen Datenträger starten**.
2. Wählen Sie das Kästchen neben dem Datenträger ab, den Sie abtrennen möchten.

   Die Verbindung zum Datenträger wird abgetrennt 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 wird oder ein VFlash angeschlossen wird, wird auf dem Host-Betriebssystem und dem BIOS ein zusätzliches Laufwerk mit der Bezeichnung "LCDRIVE" angezeigt. Das zusätzliche Laufwerk wird ausgeblendet, wenn der VFlash oder die Sitzung des virtuellen Datenträgers abgebrochen wird.

Starten vom virtuellen Datenträger

Das System-BIOS ermöglicht, von virtuellen optischen Laufwerken oder virtuellen Floppy-Laufwerken aus zu starten. Während des POST öffnen Sie 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 Floppy-Laufwerke 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 und ein startfähiger Datenträger vorhanden ist, startet das System vom 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".

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 vom virtuellen Datenträger, siehe Abschnitt "Starten vom virtuellen Datenträger", 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 virtueller Datenträger-Konsole auf.
2. Legen Sie die nächste CD/DVD in das optische Remote-Laufwerk ein.
3. Ordnen Sie diese CD/DVD von der virtueller Datenträger-Konsole zu (umleiten).

Das Einlegen einer neuen CD/DVD in das optische Remote-Laufwerk ohne erneutes Zuordnen funktioniert u. U. nicht.

Funktion Einmal starten

Mit der Funktion Einmal starten 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 Funktion Einmal starten:

1. Schalten Sie den Server ein und rufen Sie den BIOS Boot Manager auf.
2. Ändern Sie die Startreihenfolge zum Starten vom virtuellen Datenträgergerät.
3. Melden Sie sich über das Internet beim iDRAC6 an und klicken Sie auf **System**→ **Konsole/Datenträger**→ **Konfiguration**.
4. Wählen Sie die Option **Einmal starten aktivieren** unter Virtueller Datenträger.
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 physischer 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 Konfiguration der Software auf Ihrem System werden die virtuellen Datenträgerlaufwerke u. U. nicht automatisch geladen. Wenn Ihre Laufwerke nicht automatisch geladen werden, laden Sie sie unter Verwendung des Linux-Befehls **mount** manuell.

Häufig gestellte Fragen über virtuelle Datenträger

Tabelle 15-4 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 15-4. 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 Assistenten des virtuellen Datenträgers.
Welche Betriebssysteme unterstützen den iDRAC6?	Eine Liste unterstützter Betriebssysteme finden Sie unter "Unterstützte Betriebssysteme".
Welche Webbrowser unterstützen den iDRAC6?	Eine Liste unterstützter Webbrowser finden Sie unter "Unterstützte Webbrowser".
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.
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 Floppy oder den Virtual Flash ausfindig und ändern Sie die Gerätestartreihenfolge nach Bedarf. Machen Sie außerdem den virtuellen Datenträger startfähig, indem Sie im CMOS-Setup während der Startsequenz die Leertaste drücken. Um z. B. von einem CD-Laufwerk aus zu starten, konfigurieren Sie das CD-Laufwerk als erstes Laufwerk in der Startreihenfolge.
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 Diskettenimage • USB-Schlüssel, der vom Betriebssystem als Wechselplatte erkannt wird • Ein USB-Schlüsselimage
Wie kann ich meinen USB-Schlüssel startfähig machen?	Suchen Sie unter **support.dell.com** nach dem Startdienstprogramm von Dell, 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.
Ich kann meine virtuelle Diskette/CD auf einem System, welches das Red Hat Enterprise Linux- oder SUSE® Linux-Betriebssystem ausführt, 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 Floppy-Laufwerke 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* der in Schritt 4 gefundene Gerätename ist. /mnt/floppy ist der Bereitstellungspunkt.
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 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* der in Schritt 4 gefundene Gerätename ist. /mnt/floppy ist der Bereitstellungspunkt.
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 virtuelle Flash-Geräte werden als Verbund-USB-Gerät am Host-USB-BUS angeschlossen und sie verwenden einen gemeinsamen USB-Anschluss. Immer wenn ein virtuelles Datenträgergerät oder virtuelles Flash-USB-Gerät an den Host-USB-BUS angeschlossen oder davon abgetrennt wird, werden alle virtuellen Datenträger- und Flash-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 Flash-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.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6-Konfigurationsdienstprogramm verwenden

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

---

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:

- die 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
- die automatische Ermittlung aktivieren oder deaktivieren und den Bereitstellungsserver konfigurieren
- virtuelle Datenträger konfigurieren
- die Smart Card konfigurieren
- den administrativen Benutzernamen bzw. das administrative Kennwort ändern
- die iDRAC6-Konfiguration auf die Werkseinstellungen zurücksetzen
- SEL-Meldungen (Systemereignisprotokoll) anzeigen oder Meldungen aus dem Protokoll löschen
- LCD konfigurieren
- Systemdienste konfigurieren

Die Aufgaben, die Sie mit dem iDRAC6-Konfigurationsdienstprogramm ausführen können, können auch mit anderen Dienstprogrammen der iDRAC6- oder Dell™ OpenManage™-Software durchgeführt 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 <Strg><E> gedrückt haben, lassen Sie das System den Startvorgang beenden, starten Sie dann den Server neu 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 der iDRAC6-Einrichtungen, wie webbasierte Schnittstelle, Telnet/SSH, Konsolenumleitung und virtueller Datenträger zu ermöglichen.

Wenn Sie sich entscheiden, das LAN zu deaktivieren, wird die folgende Warnung angezeigt:

```
iDRAC6 Out-of-Band interface will be disabled if the LAN Channel is OFF.

Press any key to clear the message and continue.

(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:

```
iDRAC6 Out-of-Band IPMI interface will be disabled if IPMI Over LAN is OFF.

(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" 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 18-1. 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-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.
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 für die IPv4-Verbindung.	
IPv4	Wählen Sie für IPv4-Protokollunterstützung **Aktiviert** oder **Deaktiviert.**
Verschlüsselungsschlüssel RMCP+	Drücken Sie die Eingabetaste, um den Wert zu bearbeiten, und <Esc>, wenn Sie den Vorgang abgeschlossen haben. Der Verschlüsselungsschlüssel RMCP+ ist eine aus 40 Zeichen bestehende hexadezimale Zeichenkette (Zeichen 0-9, a-f und A-F). RMCP+ ist eine IPMI-Erweiterung, die Authentifizierung und Verschlüsselung zur IPMI hinzufügt. Der Standardwert ist eine aus 40 Nullen bestehende Zeichenkette.
IP-Adressen-Quelle	Wählen Sie zwischen **DHCP** und **Statisch** aus. Wenn DHCP ausgewählt ist, werden die Felder **Ethernet-IP-Adresse**, **Subnetzmaske** und **Standard-Gateway** von einem DHCP-Server abgerufen. Wenn auf dem 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-Adressen-Quelle** 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-Adressen-Quelle** 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-Adressen-Quelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse des Standard-Gateways an. Wenn die **IP-Adressen-Quelle** 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 auf dem Netzwerk abzurufen. Wählen Sie **Aus**, um die unten stehenden DNS-Server-Adressen zu bestimmen.
DNS-Server 1	Wenn **DNS-Server von DHCP** auf **Aus** gesetzt ist, geben Sie die IP-Adresse des ersten DNS-Servers ein.
DNS-Server 2	Wenn **DNS-Server von DHCP** auf **Aus** gesetzt 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-Adressen-Quelle** 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-Adressen-Quelle** auf **AutoConfig** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse des Standard-Gateways an. Wenn die **IP-Adressen-Quelle** 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 auf dem Netzwerk abzurufen. Wählen Sie **Aus**, um die unten stehenden DNS-Server-Adressen zu bestimmen.
DNS-Server 1	Wenn **DNS-Server von DHCP** auf **Aus** gesetzt ist, geben Sie die IP-Adresse des ersten DNS-Servers ein.
DNS-Server 2	Wenn **DNS-Server von DHCP** 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**.

Virtuellen Datenträger konfigurieren

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 **Konsolenumleitungssitzungen** verfügbar gemacht.

Wenn Sie **Abgetrennt** auswählen, können Benutzer während **Konsolenumleitungssitzungen** 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 **Deaktiviert** oder **Aktiviert** auszuwählen.

Deaktivieren/Aktivieren führt zum **Abtrennen** und **Verbinden** aller virtuellen Datenträgergeräte vom USB-Bus.

Deaktivieren verursacht, dass der virtuelle Flash entfernt wird und nicht mehr verwendet werden kann.

ANMERKUNG: Dieses Feld ist schreibgeschützt, wenn keine SD-Karte mit mehr als 256 MB im iDRAC6-Express-Kartensteckplatz vorhanden ist.

VFlash formatieren

Wählen Sie diese Option zum Formatieren des VFlash aus. Beim Formatieren werden die auf der SD-Karte vorhandenen Daten gelöscht. Dieses Feld kann nur bearbeitet werden, wenn sich im Kartensteckplatz des iDRAC6 Enterprise eine SD-Karte befindet, die größer als 256 MB ist.

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

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 **support.dell.com/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.

Systemdienste abbrechen

Drücken Sie die Eingabetaste, 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.

Systembestandsaufnahme nach Neustart erfassen

Wählen Sie **Aktiviert** aus, um während des Startvorgangs die Erfassung von Bestandsaufnahmedaten zuzulassen. Weitere Informationen finden Sie im *Dell Lifecycle Controller-Benutzerhandbuch*, das auf der Dell Support-Website unter **support.dell.com/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.

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 18-2. LCD-Benutzerkonfiguration

LCD-Zeile 1	Drücken Sie <Pfeil nach recht>, <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	Wenn **LCD-Zeile 1** auf **Benutzerdefinierte Zeichenkette** eingestellt wird, zeigen Sie die Zeichenkette an, die auf dem LCD angezeigt werden soll, oder geben Sie sie ein. Die Zeichenkette kann maximal 62 Zeichen aufweisen.
LCD-Systemnetzteileinheiten	Wird **LCD-Zeile 1** auf **Systemstrom** eingestellt, wählen Sie **Watt** oder **BTU/h** aus, um die Einheit festzulegen, die auf dem LCD angezeigt werden soll.

LCD-Umgebungstemperatureinheiten	Wird **LCD-Zeile 1** auf **Umgebungstemp.** eingestellt, wählen Sie **Celsius** oder **Fahrenheit** aus, um die Einheit festzulegen, die auf dem LCD angezeigt werden soll.
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-KVM-Indikation	Wählen Sie **Aktiviert** aus, um die *Text-KVM* anzuzeigen, sobald eine virtuelle KVM auf der Einheit 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 wählen. Diese Einstellung definiert die Benutzerberechtigungsebene für die LCD.

LAN-Benutzerkonfiguration

Der LAN-Benutzer ist das iDRAC6-Administratorkonto, das standardmäßig **root** lautet. Drücken Sie die Eingabetaste, um das Untermenü der LAN-Benutzerkonfiguration anzuzeigen. Wenn Sie die Konfiguration des LAN-Benutzers abgeschlossen haben, drücken Sie <Esc>, um zum vorhergehenden Menü zurückzukehren.

Tabelle 18-3. LAN-Benutzerkonfiguration

Element	Beschreibung
Auto-Ermittlung	Die Funktion Auto-Ermittlung ermöglicht die automatische Ermittlung nicht bereitgestellter Systeme auf dem Netzwerk; sie richtet außerdem auf *sichere* Weise anfängliche Anmeldeinformationen ein, so dass 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, so dass 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 **support.dell.com / manuals** zur Verfügung steht. Führen Sie im Voraus die folgenden Maßnahmen in einer *gesonderten* Sitzung des **iDRAC6-Konfigurationshilfsprogramms** aus, *bevor Sie die Auto-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 die Auto-Ermittlungs-Funktion zu aktivieren. Standardmäßig ist diese Funktion **deaktiviert**. Wenn Sie ein Dell-System bestellt haben, auf dem die Auto-Ermittlungs-Funktion **aktiviert** ist, wird der iDRAC6 auf dem Dell-System mit aktiviertem DHCP und ohne standardmäßige Anmeldeinformationen für die Remote-Anmeldung versandt. Bevor Sie das Dell-System dem Netzwerk hinzufügen und die Auto-Ermittlungs-Funktion verwenden, ist Folgendes sicherzustellen: • DHCP-Server (Dynamisches Host-Konfigurationsprotokoll)/DNS (Domänennamensystem) sind konfiguriert. • Bereitstellungs-Webdienste sind installiert, konfiguriert und registriert.
Bereitstellungsserver	Dieses Feld wird verwendet, um den Bereitstellungsserver zu 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 Auto-Ermittlung aktiviert ist und nachdem die Auto-Ermittlung erfolgreich abgeschlossen wurde, werden die Benutzeranmeldeinformationen vom konfigurierten Bereitstellungsserver abgerufen, um zukünftige Remote-Bereitstellungen zu ermöglichen. Weitere Informationen finden Sie im *Dell Lifecycle Controller-Benutzerhandbuch*, das auf der Dell Support-Website unter **support.dell.com / 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 Auto-Ermittlung aktiviert ist.
Kontoberechtigung	Wählen Sie zwischen **Admin**, **Benutzer**, **Operator** und **Kein Zugriff** aus.
Kontobenutzername	Drücken Sie die Eingabetaste, um den Benutzernamen zu bearbeiten, und dann <Esc>, wenn Sie den Vorgang beendet haben. Der Standardbenutzername ist **root**.
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.

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 die Eingabetaste, um das Element auszuwählen. Die folgende Warnmeldung wird angezeigt:

```
Resetting to factory defaults will restore remote Non-Volatile user settings. Continue?

< NO (Cancel) >

< YES (Continue) >
```

```
(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 die Eingabetaste, um den iDRAC6 auf die Standardeinstellungen zurückzusetzen.

Menü des Systemereignisprotokolls

Das Menü **Systemereignisprotokoll** ermöglicht Ihnen, Meldungen des Systemereignisprotokolls (SEL) anzuzeigen und die Protokollmeldungen zu löschen. Drücken Sie die Eingabetaste, um das **Menü Systemereignisprotokoll** 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 die Eingabetaste. 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 die Eingabetaste.

Wenn Sie mit der Verwendung des SEL-Menüs fertig sind, drücken Sie <Esc>, um zum vorhergehenden Menü zurückzukehren.

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 auf die Eingabetaste, um Ihre Änderungen beizubehalten.

Wählen Sie **Änderungen verwerfen und beenden** aus und drücken Sie die Eingabetaste, um alle vorgenommenen Änderungen zu ignorieren.

Wählen Sie **Zum Setup zurückkehren** aus und drücken Sie auf die Eingabetaste, um zum iDRAC6-Konfigurationsdienstprogramm zurückzukehren.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Überwachungs- und Warnungsverwaltung

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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, wobei die Windows-Funktion "Automatisch Neustart durchführen" in den **Windows-Start und -Wiederherstellungs-Einstellungen** abgewählt 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 die **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 "Automatisch Neustart durchführen" deaktivieren

Um sicherzustellen, dass die Funktion "Bildschirm Letzter Absturz" der webbasierten iDRAC6-Schnittstelle richtig funktioniert, deaktivieren Sie die Option **Automatisch Neustart durchführen** 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 Symbol **System**.

2. Klicken Sie unter **Aufgaben** auf der linken Seite auf **Erweiterte Systemeinstellungen**.

3. Klicken Sie auf das Register **Erweitert**.

4. Klicken Sie unter **Starten und Wiederherstellen** 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 Symbol **System**.

2. Klicken Sie auf das Register **Erweitert**.
3. Klicken Sie unter **Autostarten und Wiederherstellen** auf **Einstellungen**.
4. Wählen Sie das Kontrollkästchen **Automatischer Neustart** ab.
5. Klicken Sie zweimal auf **OK**.

Plattformereignisse konfigurieren

Die Konfiguration von Plattformereignissen bietet einen 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:

- Assertionsfilter Lüfter kritisch
- Assertionsfilter Batteriewarnung
- Assertionsfilter Batterie kritisch
- Assertionsfilter diskrete Spannung kritisch
- Assertionsfilter Temperaturwarnung
- Assertionsfilter Temperatur kritisch
- Assertionsfilter Eingriff kritisch
- Filter Redundanz herabgesetzt
- Filter Redundanz verloren
- Assertionsfilter Prozessorwarnung
- Assertionsfilter Prozessor kritisch
- Filter Prozessor nicht vorhanden
- Assertionsfilter Netzteilwarnung
- Assertionsfilter Netzteil kritisch
- Filter Netzteil fehlt
- Assertionsfilter Ereignisprotokoll kritisch
- Assertionsfilter Watchdog kritisch
- Assertionsfilter Systemstromwarnung
- Assertionsfilter Systemstrom kritisch
- Assertionsfilter diskrete SD-Karte informativ
- Assertionsfilter diskrete SD-Karte kritisch
- Assertionsfilter diskrete SD-Karte 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 der webbasierten Schnittstelle entspricht und Sie diesen Filter auf die Erstellung 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

Weitere Informationen finden Sie unter "Plattformereignisfilter (PEF) konfigurieren".

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

Weitere Informationen finden Sie unter "Plattformereignis-Traps (PET) konfigurieren".

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 die Eingabetaste:

   ```
   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 Eingabeaufforderung ein:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <Name>
   ```

E-Mail-Warnungen konfigurieren

E-Mail-Warnungen mittels der Internet-Benutzeroberfläche konfigurieren

Weitere Informationen finden Sie unter "Konfiguration von E-Mail-Warnungen".

E-Mail-Warnungen 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 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 die Eingabetaste:

   ```
   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 die Eingabetaste:

   ```
   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-Warnung**s-Einstellungen konfiguriert sind, bevor die E-Mail-Warnungsfunktion getestet wird. Weitere Informationen finden Sie unter "E-Mail-Warnungen konfigurieren".

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. Anleitungen zum Konfigurieren dieser Einstellungen finden Sie in den Unterbefehlsbeschreibungen "**testtrap**" und "**testemail**".

Häufig gestellte Fragen zur SNMP- Authentifizierung

Warum wird die folgende Meldung angezeigt?

```
Remote Access: SNMP Authentication Failure (Remote-Zugriff: SNMP-Authentifizierungsfehler)
```

Als Teil der Ermittlung versucht IT Assistant, die Get- und Set-Community-Namen des Geräts zu überprüfen. Im 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: Das ist der für die Ermittlung verwendete 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 **Remote-Zugriff**→ **Netzwerk / Sicherheit**→ **Dienste** und klicken 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.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Wiederherstellung und Fehlerbehebung am verwalteten System

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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"
- "Stromverwaltung auf einem Remote-System"
- "POST-Startprotokolle verwenden"
- "Bildschirm des letzten Systemabsturzes anzeigen"

Erste Schritte, um Störungen an einem Remote- System zu beheben

Die folgenden Fragen werden im Allgemeinen für die Fehlerbehebung bei vorrangigen Problemen des verwalteten Systems 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"), und verwenden Sie die Konsolenumleitung und die Remote-Stromverwaltung (siehe "Stromverwaltung auf einem Remote-System"), 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

Um Stromverwaltungsmaßnahmen über die Webschnittstelle auszuführen, schlagen Sie unter "Durchführen von Stromsteuerungsmaßnahmen am Server" nach.

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.

Systeminformationen anzeigen

Die Seite **Systemzusammenfassung** ermöglicht Ihnen, auf einen Blick den Systemfunktionszustand sowie andere grundlegende iDRAC6-Informationen anzuzeigen und bietet Ihnen Verknüpfungen für den Zugriff auf die Systemfunktionszustands- und Informationsseiten. Sie können über diese Seite außerdem im Handumdrehen allgemeine Aufgaben starten und neue Ereignisse anzeigen, die im Systemereignisprotokoll (SEL) protokolliert wurden.

So greifen Sie auf die Seite **Systemzusammenfassung** zu: Erweitern Sie die **System**struktur und klicken Sie auf das Register **Eigenschaften**→ **Systemzusammenfassung**. Weitere Informationen finden Sie in der *iDRAC6-Online-Hilfe*.

Die Seite **Systemdetails** zeigt Informationen über die folgenden Systemkomponenten an:

- Hauptsystemgehäuse
- Remote-Access-Controller

Sie können auf die Seite **Systemdetails** zugreifen, indem Sie die **System**struktur 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 20-1. Systeminformationen

Feld	Beschreibung
Beschreibung	Systembeschreibung.
BIOS-Version	BIOS-Version des Systems.
Service-Tag-Nummer	Service-Tag-Nummer des Systems.
Host-Name	Name des Hostsystems.
Betriebssystemname	Betriebssystem, das auf dem System ausgeführt wird.

Tabelle 20-2. Automatische Wiederherstellung

Feld	Beschreibung
Wiederherstellungsmaßnahme	Wenn ein "hängendes System" 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 hängenden Systems, nach denen der iDRAC6 eine Wiederherstellungsmaßnahme ausführt.
Vorhandener Countdown	Der aktuelle Wert, in Sekunden, des Countdown-Zeitgebers.

Tabelle 20-3. Integrierte NIC-MAC-Adressen

Feld	Beschreibung
NIC 1	Zeigt die MAC-Adressen (Media Access Control) des integrierten NIC 1 (Network Interface Controller) an. MAC-Adressen identifizieren jeden Knoten in einem Netzwerk auf der Media Access Control-Ebene auf eindeutige Weise. iSCSI-NIC (Internet Small Computer System Interface) ist ein Netzwerkschnittstellen-Controller, bei dem der iSCSI-Stack auf dem Host-Computer ausgeführt wird. Ethernet-NICs unterstützen den drahtgebundenen Ethernetstandard und werden in den Systembus des Servers eingesteckt.
NIC 2	Zeigt die MAC-Adresse(n) des integrierten NIC 2 an, die diesen im Netzwerk eindeutig identifizieren.
NIC 3	Zeigt die MAC-Adresse(n) des integrierten NIC 3 an, die diesen im Netzwerk eindeutig identifizieren.
NIC 4	Zeigt die MAC-Adresse(n) des integrierten NIC 4 an, die diesen im Netzwerk eindeutig identifizieren.

Remote-Access-Controller

Tabelle 20-4. 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
Firmware-Version	iDRAC6-Firmware-Version

Aktualisierte Firmware	Datum, an dem die Firmware zuletzt aktualisiert wurde im Format: Tag Monat TT HH:MM:SS:JJJJ
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 20-5. 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 für den bevorzugten DNS-Server an.
Alternativer DNS-Server	Gibt die statische IPv4-Adresse für den alternativen DNS-Server an.

Tabelle 20-6. 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 iDRAC6-NIC-IPv6-Adresse an.
IP-Adresse 2...15	Gibt die zusätzlichen IPv6-Adressen für den iDRAC6-NIC an, falls verfügbar.
Autom. Konfiguration aktiviert	**Ja** oder **Nein**. AutoConfig gestattet dem Server Administrator die Abfrage der IPv6-Adresse für den iDRAC-NIC vom Server des dynamischen Host-Konfigurationsprotokolls (DHCPv6). Deaktiviert und löscht die Statische IP-Adresse, Präfixlänge und die Werte für das statische Gateway.
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 für den bevorzugten DNS-Server an.
Alternativer DNS-Server	Gibt die statische IPv6-Adresse für den alternativen DNS-Server an.

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 20-7.
3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Systemereignisprotokoll**, um fortzufahren (siehe Tabelle 20-7).

Tabelle 20-7. Statusanzeigesymbole

Symbol/Kategorie	Beschreibung
	Eine grüne Markierung zeigt eine fehlerfreie (normalen) 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 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 TT/MM/JJJJ hh:mm:ss, basierend auf dem 24-Stunden-Zeitsystem.
Beschreibung	Eine kurze Beschreibung des Ereignisses

Tabelle 20-8. Schaltflächen der SEL-Seite

Schaltfläche	Maßnahme
Drucken	Druckt das **SEL in der Sortierreihenfolge, in der es im Fenster erscheint.**
Aktualisieren	Lädt die Seite **SEL** hoch.
Protokoll löschen	Löscht das **SEL**. **ANMERKUNG:** Die Schaltfläche **Protokoll löschen** wird nur angezeigt, wenn Sie die Berechtigung **Protokolle löschen** besitzen.
Speichern unter	Öffnet ein Popup-Fenster, das es Ihnen ermöglicht, das **SEL** in einem Verzeichnis Ihrer Wahl zu speichern. **ANMERKUNG:** Wenn Sie Internet Explorer verwenden und beim Speichern auf ein Problem stoßen, laden Sie die kumulative Sicherheitsaktualisierung für Internet Explorer von der Support-Website von Microsoft unter support.microsoft.com herunter.

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 verwendbaren Optionen finden Sie unter "getsel".

Mit dem Befehl **clrsel** werden alle vorhandenen Aufzeichnungen aus dem SEL entfernt.

```
racadm clrsel
```

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: Start-Capture wird nur auf Java unterstützt und nicht auf Active-X.

So zeigen Sie die Start-Capture-Protokolle 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 offenes Start-Capture-Protokollvideo schließen, um ein anderes abspielen zu können. Sie können nicht zwei Protokolle gleichzeitig ansehen.
4. Klicken Sie auf **Wiedergabe→ Wiedergabe**, um das Start-Capture- Protokollvideo 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 das Register **Extras→ Internetoptionen→ Erweitert** auf und deaktivieren Sie die Option "*Verschlüsselte Seiten nicht auf der Festplatte speichern*".

Die iDRAC6 Express-Karte wird an den 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 Upgrade Successful` (`iDRAC6-Aktualisierung erfolgreich`). Schlägt die Bindung fehl, wird im SEL und LCD die folgende Meldung protokolliert: `iDRAC6 Upgrade Failed` (`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 is out-of-date. Please update to the latest firmware` (`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 Abschnitt **Remote-Zugriff**, Register **Netzwerk/Sicherheit**, um diese Funktion zu aktivieren.

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.

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** enthält die folgenden Schaltflächen (siehe Tabelle 20-9) oben rechts auf dem Bildschirm:

Tabelle 20-9. Schaltflächen der Seite "Bildschirm Letzter Absturz"

Schaltfläche	Maßnahme
Drucken	Druckt die Seite **Bildschirm Letzter Absturz**.
Aktualisieren	Lädt die Seite **Bildschirm Letzter Absturz** neu.

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 finden Sie unter "Das verwaltete System zur Erfassung des Bildschirms "Letzter Absturz" konfigurieren".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6 wiederherstellen und Fehler beheben

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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 **System**struktur auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Protokolle** und dann auf **iDRAC-Protokoll**.

Das **iDRAC-Protokoll** stellt die in Tabelle 21-1 aufgeführten Informationen zur Verfügung.

Tabelle 21-1. 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.

Schaltflächen auf der iDRAC-Anmeldeseite verwenden

Die Seite **iDRAC-Protokoll** enthält die unter Tabelle 21-2 aufgeführten Schaltflächen.

Tabelle 21-2. iDRAC-Protokoll-Schaltflächen

Schaltfläche	Maßnahme
Drucken	Druckt die Seite **iDRAC-Protokoll** aus.
Protokoll löschen	Löscht die Einträge des **iDRAC-Protokolls**. **ANMERKUNG:** Die Schaltfläche **Protokoll löschen** erscheint nur, wenn Sie die Berechtigung **Protokolle löschen** besitzen.
Speichern unter	Öffnet ein Popup-Fenster, das Ihnen ermöglicht, das **iDRAC-Protokoll** in einem Verzeichnis Ihrer Wahl zu speichern.

	ANMERKUNG: Wenn Sie Internet Explorer verwenden und beim Speichern auf ein Problem stoßen, laden Sie die kumulative Sicherheitsaktualisierung für Internet Explorer von der Support-Website von Microsoft unter **support.microsoft.com** herunter.
Aktualisieren	Lädt die Seite **iDRAC-Protokoll** neu.

Befehlszeile verwenden

Verwenden Sie den Befehl `getraclog`, um die iDRAC6-Protokolleinträge anzuzeigen.

```
racadm getraclog -i
```

Der Befehl **getraclog -i** zeigt die Anzahl der Einträge im iDRAC6-Protokoll an.

```
racadm getraclog [Optionen]
```

ANMERKUNG: Weitere Informationen finden Sie unter "getraclog".

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 21-3), 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.

So greifen Sie auf die Seite **Diagnosekonsole** zu: Klicken Sie in der **System**struktur auf **Remote-Zugriff**→ Register **Fehlerbehebung** → **Diagnosekonsole**.

Tabelle 21-3 beschreibt die Optionen, die auf der Seite **Diagnosekonsole** verfügbar sind. Geben Sie einen Befehl ein und klicken Sie auf **Senden**. Die Debug-Ergebnisse werden auf der Seite **Diagnosekonsole** angezeigt.

Zum Aktualisieren der Seite **Diagnosekonsole** klicken Sie auf **Aktualisieren**. Um einen anderen Befehl auszuführen, klicken Sie auf **Zurück zur Diagnoseseite**.

Tabelle 21-3. 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.
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 (Internet-Steuerungsmeldungsprotokoll) 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".

Server identifizieren verwenden

Die Seite **Identifizieren** ermöglicht Ihnen, die Systemidentifizierungsfunktion zu aktivieren.

Führen Sie zum Identifizieren des Servers Folgendes aus:

1. Klicken Sie auf **System→ Remote-Zugriff→ 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→ Remote-Zugriff→ Fehlerbehebung→ Identifizieren**.
2. Heben Sie auf dem Bildschirm **Identifizieren** die Auswahl der Option **Server identifizieren** auf.

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 **System**struktur auf **Remote-Zugriff**.
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".

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 steht nur auf Telnet- und SSH-Schnittstellen zur Verfügung. Weitere Informationen finden Sie unter dem Befehl "racdump".

---

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.

Weiter Informationen hierzu finden Sie bei den Unterbefehlen "coredump" und "coredumpdelete".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Sensoren

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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 das primäre Netzteil ausfällt.

ANMERKUNG: Wenn das System nur ein Netzteil aufweist, ist die Netzteilredundanz **deaktiviert**.

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
- System Board 0.9V PG
- System Board 1.5V ESB2 PG
- System Board 1.5V PG
- System Board 1.8V PG
- System Board 3.3V PG
- System Board 5V PG
- System Board Backplane PG
- System Board CPU VTT
- System Board Linear PG

Die Spannungssonden zeigen an, ob sich der Status der Sonden innerhalb des voreingestellten Bereichs für Warnungsschwellenwert und kritischen Schwellenwert befindet.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Zum Einstieg mit iDRAC6

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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 eine umfangreiche Auswahl an Funktionen, wie Konsolenumleitung, virtueller Datenträger, virtuelle KVM, Smart Card-Authentifizierung und einfache Anmeldung.

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 **support.dell.com / 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. Konfigurieren Sie bei der Verwendung eines Windows-Systems das Microsoft® Active Directory®, um auf den iDRAC6 zugreifen zu können, wodurch Ihnen ermöglicht wird, iDRAC6-Benutzerberechtigungen zu den vorhandenen Benutzern in der Active Directory-Software hinzuzufügen und zu steuern.
3. Konfigurieren Sie die Smart Card-Authentifizierung - Smart Card bietet eine zusätzliche Sicherheitsstufe für Ihr Unternehmen.
4. Konfigurieren Sie Remote-Zugriffspunkte wie Konsolenumleitung 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.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Kerberos-Authentifizierung aktivieren

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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 nun die Kerberos-basierte Active Directory®-Authentifizierung zur Unterstützung von Active Directory Smart Card-Anmeldungen und einfachen Anmeldungen.

Microsoft® Windows® 2000, Windows XP, Windows Server® 2003, Windows Vista® und Windows Server 2008 verwenden Kerberos als Standard-Authentifizierungsmethode.

Der iDRAC6 verwendet Kerberos, um zwei Typen von Authentifizierungsmechanismen zu unterstützen: einfache Anmeldung mit Active Directory und Active Directory Smart Card-Anmeldungen. Bei der einfachen Anmeldung verwendet der iDRAC6 die Anmeldeinformationen des Benutzers, die im Betriebssystem zwischengespeichert werden, nachdem sich der Benutzer mit einem gültigen Active Directory-Konto angemeldet hat.

Bei der Active Directory Smart Card-Anmeldung verwendet der iDRAC6 die 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**.

Sie können auch den folgenden RACADM-Zeitzonenabweichungsbefehl verwenden, um die Zeit zu synchronisieren:

```
racadm config -g cfgRacTuning -o

cfgRacTuneTimeZoneOffset <Abweichungswert>
```

Voraussetzungen für die einfache Anmeldung und die Active Directory-Authentifizierung unter Verwendung der Smart Card

- Konfigurieren Sie den iDRAC6 für die Active Directory-Anmeldung. Weitere Informationen finden Sie unter "Verwendung des Microsoft Active Directory zur Anmeldung beim iDRAC6".
- Registrieren Sie den iDRAC6 als Computer in der Active Directory-Root-Domäne.
  a. Klicken Sie auf **Remote-Zugriff**→ 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, welche 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 Authentifizierungsmechanismen 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 folgenden Kontoeigenschaften aktiviert haben:

- DES-Verschlüsselungstypen für dieses Konto verwenden
- Kerberos-Vorauthentifizierung nicht erforderlich

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.

---

iDRAC6 für die einfache Anmeldung und die Active Directory-Authentifizierung unter Verwendung der Smart Card konfigurieren

Das aus der Active Directory-Root-Domäne abgerufene Keytab auf den iDRAC6 hochladen:

1. Klicken Sie auf **Remote-Zugriff**→ Register **Netzwerk/Sicherheit** Unterregister→ **Verzeichnisdienst** → Klicken Sie auf **Microsoft Active Directory**.
2. Wählen Sie **Kerberos-Keytab hochladen** aus und klicken Sie auf **Weiter**.
3. Wählen Sie auf der Seite **Kerberos-Keytab hochladen** die hochzuladende Keytab-Datei aus und klicken Sie auf **Anwenden**.

Sie können die Datei auch mithilfe von CLI-racadm-Befehlen auf den iDRAC6 hochladen. Der folgende Befehl dient zum Hochladen der Keytab-Datei auf den iDRAC6:

```
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.

Active Directory-Benutzer für die einfache Anmeldung konfigurieren

Bevor Sie die einfache Anmeldung mit Active Directory verwenden, stellen Sie sicher, dass der iDRAC6 bereits für die Active Directory-Anmeldung konfiguriert ist und das Domänenbenutzerkonto, das Sie zur Anmeldung am System verwenden werden, für die Anmeldung des iDRAC6 mit Active Directory aktiviert wurde.

Vergewissern Sie sich außerdem, 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". 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.

Informationen zum Aktivieren der einfachen Anmeldung über die GUI und die CLI finden Sie unter "iDRAC6 zur Verwendung der einfachen Anmeldung konfigurieren".

Unter Verwendung der einfachen Anmeldung für Active Directory-Benutzer am iDRAC6 anmelden

ANMERKUNG: Stellen Sie bei der Anmeldung am iDRAC6 sicher, dass Sie über die neuesten Laufzeitkomponenten der Microsoft Visual C++ 2005-Bibliotheken verfügen. Weitere Informationen finden Sie auf der Microsoft-Website.

1. Melden Sie sich unter Verwendung eines gültigen Active Directory-Kontos am System an.
2. Geben Sie die Internetadresse des iDRAC6 in die Adresszeile Ihres Browsers ein.

   ANMERKUNG: Je nach Browser-Einstellungen werden Sie eventuell aufgefordert, das ActiveX-Plug-in für einfache Anmeldung herunterzuladen und zu installieren, falls Sie diese Funktion zum ersten Mal verwenden.

   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.

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.

Vergewissern Sie sich außerdem, 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". 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.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

VFlash-Medienkarte zur Verwendung mit iDRAC6 konfigurieren

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Die VFlash-Medienkarte 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 gewöhnliches USB Flash Key-Gerät. Informationen zum Installieren und Entfernen der VFlash-Medienkarte auf dem System finden Sie im *Hardware-Benutzerhandbuch* unter **support.dell.com / manuals**.

VFlash-Medienkarte über die iDRAC6- Webschnittstelle konfigurieren

Eigenschaften der SD-Karte

ANMERKUNG: Dieser Abschnitt wird nur angezeigt, wenn eine SD-Karte mit Lese-/Schreib-Fähigkeit in den SD-Kartensteckplatz des Servers eingesteckt wurde. Andernfalls wird die folgende Meldung angezeigt:

```
SD card not detected. Please insert an SD card of size 256MB or greater.

(SD-Karte konnte nicht ermittelt werden. Setzen Sie bitte eine SD-Karte mit mindestens 256 MB Speicherplatz ein.)
```

1. Kontrollieren Sie, ob die VFlash-Medienkarte installiert wurde.
2. Öffnen Sie einen unterstützten Webbrowser und melden Sie sich an der iDRAC6-Webschnittstelle an.
3. Klicken Sie in der Systemstruktur auf **System**.
4. Wählen Sie das Register **VFlash**.

Daraufhin wird das Fenster **VFlash** angezeigt.

Tabelle 16-1 führt die Optionen von **Eigenschaften der SD-Karte** auf.

Tabelle 16-1. Eigenschaften der SD-Karte

Attribut	Beschreibung
Größe des virtuellen Schlüssels	Dieses Feld ermöglicht Ihnen, die Größe zu bestimmen, die auf der SD-Karte vom VFlash-Schlüssel in Anspruch genommen werden soll. Wählen Sie eine Größe für den virtuellen Schlüssel aus und klicken Sie auf **Anwenden**. Der virtuelle Schlüssel wird gemäß der angegebenen Größe neu initialisiert, löscht alle vorhandenen Daten und formatiert einen Abschnitt der SD-Karte. **ANMERKUNG:** Wenn Sie eine lizenzierte 1-GB-SD-Karte eingesetzt haben, können Sie entweder 256 MB oder 512 MB als Partitionsgröße auswählen. Wenn Sie eine nicht lizenzierte SD-Karte einer beliebigen Größe eingesetzt haben, können Sie nur 256 MB als Partitionsgröße auswählen. Wenn Sie unter Verwendung von WS-MAN ein Image hochgeladen haben, hängt die maximale entstehende Partitionsgröße von der Größe des Image ab. Beispiel: Wenn Sie ein 500-MB-Abbild hochgeladen haben, kann eine 1-GB-Größe des virtuellen Schlüssels nicht mit einer lizenzierten 1-GB-Karte erstellt werden, da 500 MB bereits vom Image in Anspruch genommen werden. Klicken Sie in diesem Falle auf die Schaltfläche **Initialisieren**, um die Karte neu zu initialisieren, und wählen Sie dann 1 GB als Größe des virtuellen Schlüssels aus.
Datenträgertyp	Zeigt an, ob eine SD-Karte der Marke Dell oder der Marke eines anderen Unternehmens in den Steckplatz der SD-Karte eingesetzt wurde. Wenn die SD-Karte lizenziert ist, wird Dell VFlash gefolgt von der Größe der SD-Karte angezeigt. Wenn die Karte nicht lizenziert ist, wird Non-Dell SD Card (Nicht-Dell-SD-Karte) angezeigt.
Image	Zeigt den Namen der auf der SD-Karte erstellten Imagedatei an. Es wird als VFlash verwendet.
ID-Datei	Zeigt den Namen der auf der SD-Karte erstellten Textdatei an. Es bietet Informationen über das VFlash-Image.
VFlash verbinden	Markieren Sie diese Option zum Verbinden des VFlash. Hierdurch wird die auf der SD-Karte erstellte Imagedatei **ManagedStore.IMG** als USB-Schlüssel der ausgewählten Größe gezeigt. **ANMERKUNG:** Der VFlash kann nur verbunden werden, wenn sich ein gültiges **ManagedStore.IMG**-Image auf der SD-Karte befindet.
Initialisieren	Klicken Sie auf **Initialisieren**, um das VFlash-Image **ManagedStore.IMG** auf der SD-Karte zu erstellen. **ANMERKUNG:** Die Option **Initialisieren** wird nur aktiviert, wenn eine VFlash-Medienkarte vorhanden ist. Außerdem kann die SD-Karte nur formatiert werden, wenn die Option **VFlash verbinden** nicht markiert ist.

	ANMERKUNG: Die Dateien **ManagedStore.IMG** und **ManagedStore.ID**, die auf der GUI-Seite von VFlash angezeigt werden, sind auf dem Betriebssystem des Host-Servers nicht sichtbar. Auf der SD-Karte sind sie hingegen sichtbar. **VORSICHT: Wenn Sie während des Hochladens einer großen Imagedatei an beliebiger Stelle klicken, die Seite aktualisieren oder zur Seite VFlash zurückkehren, wird möglicherweise die Meldung** `"SD card unavailable, used by another application" (SD-Karte nicht verfügbar; wird von anderer Anwendung verwendet)` **angezeigt. Abhängig von der Partition oder der ausgewählten Größe der Imagedatei kann diese Meldung bis zu zwei Stunden lang angezeigt werden.**
Anwenden	Speichert die aktuelle Konfiguration. Wenn Sie die Größe des virtuellen Schlüssels unter Verwendung des Dropdown-Menüs ändern, klicken Sie auf **Anwenden**, um einen neuen virtuellen Schlüssel mit der festgelegten Größe zu erstellen. Alle vorhandenen Daten werden gelöscht. Dieser Vorgang kann je nach Größe des ausgewählten virtuellen Schlüssels mehrere Minuten in Anspruch nehmen.

VFlash-Laufwerk

ANMERKUNG: Die Funktion zum Hochladen der Imagedatei steht nur zur Verfügung, wenn sich auf der SD-Karte ein gültiges **ManagedStore.IMG**-Image befindet und die Option **VFlash verbinden** nicht markiert ist.

Tabelle 16-2 führt die Einstellungen des **VFlash-Laufwerks** auf.

Tabelle 16-2. VFlash-Laufwerk

Attribut	Beschreibung
Imagedatei	Wählen Sie auf dem Client-Computer eine lokale Datei aus, die auf dem Remote-Server als VFlash-USB-Schlüssel gezeigt werden soll. Sie können Notfall-Startimagedateien und Diagnosehilfsprogramme direkt auf dem VFlash-Datenträger speichern. Bei der Imagedatei kann es sich um ein DOS-startfähiges Diskettenimage handeln, z. B. eine ***.img**-Datei für Windows® oder eine **diskboot.img**-Datei des Red Hat® Enterprise Linux®-Datenträgers für Linux. Sie können **diskboot.img** zum Erstellen einer Rettungsdisk verwenden oder eine Festplatte zum Ausführen von Netzwerkinstallationen erstellen. Mit VFlash können Sie ein beständiges Image für künftige allgemeine Zwecke oder Notfälle speichern.
Hochladen	Klicken Sie auf diese Option, um die ausgewählte Imagedatei auf die SD-Karte hochzuladen. Nachdem die Imagedatei vollständig hochgeladen wurde, wird sie auf der SD-Karte als **ManagedStore.IMG** gespeichert. **ANMERKUNG:** Das Hochladen von ISO-Imagedatei wird in dieser Version nicht unterstützt und kann während des Hochladens zu Fehlern führen.

VORSICHT: Sie werden nicht in der Lage sein, das Virtual Flash-Laufwerk durch Rechtsklicken auf das Laufwerk und Auswählen der Option "Eject" ("Auswerfen") aus dem Windows-Betriebssystem des verwalteten Servers auszuwerfen. Verwenden Sie zum sicheren Entfernen des Laufwerks die Option, die im Systembereich in der unteren rechten Ecke des Systems verfügbar ist.

Wenn Sie auf der Seite VFlash auf eine Schaltfläche klicken, während eine Anwendung wie WSMAN Provider, das iDRAC6-Konfigurationshilfsprogramm oder RACADM VFlash verwendet, oder wenn Sie zu einer anderen GUI-Seite navigieren, zeigt iDRAC6 möglicherweise eine leere Seite mit der Meldung `"VFlash is currently in use by another process. Try again after some time." ("VFlash wird momentan von einem anderen Ablauf in Anspruch genommen. Versuchen Sie es nach einer Weile erneut.")` an.

Größe des virtuellen Flash-Schlüssels anzeigen

Das Dropdown-Menü **Größe des virtuellen Schlüssels** zeigt die aktuelle Größeneinstellung an.

VFlash-Medienkarte mit RACADM konfigurieren

VFlash-Medienkarte aktivieren oder deaktivieren

Öffnen Sie eine lokale Konsole auf dem Server, melden Sie sich an und geben Sie Folgendes ein:

```
racadm cfgRacVirtual cfgVirMediaKeyEnable [ 1 oder 0 ]
```

`1` = aktiviert, `0` = deaktiviert.

ANMERKUNG: Weitere Informationen über cfgRacVirtual, einschließlich Ausgabedetails, finden Sie unter cfgRacVirtual.

ANMERKUNG: Der RACADM-Befehl funktioniert nur, wenn eine VFlash-Medienkarte vorhanden ist. Wenn keine Karte vorhanden ist, wird die folgende Meldung angezeigt: *FEHLER: Der gewünschte Vorgang kann nicht ausgeführt werden. Stellen Sie sicher, dass eine nicht schreibgeschützte SD-Karte eingesetzt ist.*

VFlash-Medienkarte zurücksetzen

Öffnen Sie eine Telnet/SSH-Textkonsole für den Server, melden Sie sich an und geben Sie Folgendes ein:

```
racadm vmkey reset
```

VORSICHT: Beim Zurücksetzen der VFlash-Medienkarte mit dem RACADM-Befehl wird die Größe des Schlüssels auf 256 MB zurückgesetzt und alle vorhandenen Daten werden gelöscht.

ANMERKUNG: Weitere Informationen zu vmkey finden Sie unter "vmkey". Der RACADM-Befehl funktioniert nur, wenn eine VFlash-Medienkarte vorhanden ist. Wenn keine Karte vorhanden ist, wird die folgende Meldung angezeigt: *ERROR: Unable to perform the requested operation. Make sure that a SD Card is inserted. (FEHLER: Der gewünschte Vorgang kann nicht ausgeführt werden. Stellen Sie sicher, dass eine SD-Karte eingesetzt ist.)*

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Stromüberwachung und -verwaltung

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Dell™ PowerEdge™-Systeme enthalten viele neue und erweiterte Stromverwaltungsfunktionen. Die gesamte Plattform, von der Hardware zur Firmware bis hin zur Systems Management-Software, wurde mit einem Schwerpunkt auf Energieeffizienz, Stromüberwachung und Stromverwaltung 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 Chassis-Design 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 Rackebene 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:

- Den 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
- Den Schwellenwert für das Strombudget des Servers anzeigen

Den 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** erscheint und liefert die folgenden Informationen:
   - **Redundanzstatus der Netzteile**: Mögliche Werte sind:
   - **Voll**: Die Netzteile PS1 und PS2 sind vom gleichen Typ und funktionieren richtig.
   - **Ausgefallen**: Die Netzteile PS1 und PS2 sind nicht vom gleichem Typ oder ein Netzteil ist defekt. Keine Redundanz.
   - **Deaktiviert**: Nur eines der beiden Netzteile steht zur Verfügung. Keine Redundanz.
   - **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.
   - **Maximale Leistung in Watt** zeigt die maximale Leistung des Netzteils in Watt an, d. h. die dem System zur Verfügung stehende Gleichstromspannung. 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 Höchstleistung in Watt nicht unbedingt der Eingangsleistung. Beispiel: Wenn die Effizienz des Netzteils 89 % beträgt und die Höchstleistung 717 W beträgt, liegt die Eingangsleistung 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 Stromverwaltungsmaßnahmen auszuführen, benötigen Sie **Administrator**rechte.

1. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
2. Klicken Sie auf das Register **Stromverwaltung**.
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.

Minimum des potenziellen Stromverbrauchs - Zeigt den niedrigsten Schwellenwert für das Strombudget an, den Sie angeben können.

Maximum des potenziellen Stromverbrauchs - Zeigt den höchsten Schwellenwert für das Strombudget an, den Sie angeben können. 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 über cfgServerPower, einschließlich Ausgabedetails, finden Sie unter cfgServerPower.

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 spezifizieren 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 das Register **Stromverwaltung**.
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 **Strombudgetschwellenwerte** 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 ein maximaler potenzieller 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. Markieren Sie **Aktiviert**, um den Schwellenwert zu aktivieren, oder lassen Sie die Funktion unmarkiert. Wenn Sie **Aktiviert** angeben, erzwingt das System den benutzerspezifischen Schwellenwert. Bei **unmarkierter** Funktion, begrenzt das System die Leistung nicht.
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 %>
```

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

Um die Stromüberwachungsdaten anzuzeigen:

1. Melden Sie sich an der iDRAC6-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Stromüberwachung** aus. Die Seite **Stromüberwachung** wird angezeigt.

Die Informationen auf der Seite **Stromüberwachung** wird nachstehend 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.

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 die Spitzenstromstärke innerhalb des Intervalls zwischen Startzeit und Spitzenzeiten 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 eine 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.

Stromverbrauch

- 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: Zeit des maximalen und minimalen Stromverbrauchs.

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

Durch Klicken auf diese Schaltfläche werden Diagramme aufgerufen, welche den iDRAC6-Stromverbrauch und den aktuellen Stromverbrauch während der letzten Stunde in Watt und Ampere anzeigen. 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 im Diagramm gezeichneten Datenpunkte zeigen jeweils Durchschnittsmesswerte über einen Zeitraum von 5 Minuten an. Aus diesem Grund widerspiegeln die Diagramme kurze Abweichungen oder den aktuellen Verbrauch eventuell nicht.

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 das Register **Stromverwaltung**. 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.
   - **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.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Sicherheitsfunktionen konfigurieren

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Der iDRAC6 enthält die folgenden Sicherheitsfunktionen:

- Erweiterte Sicherheitsoptionen für den iDRAC6-Aministrator:
  - Mit der Option Konsolenumleitung deaktivieren können Benutzer des *lokalen* Systems die Konsolenumleitung anhand der iDRAC6-Konsolenumleitungsfunktion deaktivieren.
  - Die Deaktivierungsfunktion für die lokale Konfiguration ermöglicht dem *Remote*-iDRAC6-Administrator, die Fähigkeit zur Konfiguration des iDRAC6 selektiv zu deaktivieren von:
  - BIOS-POST, Options-ROM
  - dem Betriebssystem aus 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 der Grenze
- 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 (graphische Benutzeroberfläche) deaktivieren, indem sie **Remote-Zugriff**→ **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 eine oder beide dieser Optionen gleichzeitig aktivieren. Zusätzlich zur Aktivierung über die webbasierte Schnittstelle können Administratoren diese Optionen auch unter Verwendung lokaler RACADM-Befehle 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 eine Aktualisierung auf diese Version vorzunehmen, erweitern Sie das BIOS unter Verwendung des BIOS-Aktualisierungspakets, das auf der Dell Support-Website unter **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
```

VORSICHT: 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 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 die Microsoft Windows®-Vorinstallationsumgebung 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-Zugriffs-Geräte benötigen diejenigen, die für die Wartung von Server-Software-Stacks zuständig sind, eventuell keine Administratorrechte für den Zugriff auf Remote-Zugriffs-Geräte. 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-Zugriffs-Geräte konfigurieren. Administratoren von Remote-Zugriffs-Geräten 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 Kommunikation des DRAC deaktiviert werden, woraufhin Administratoren die Firmware über eine serielle Verbindung auf ihre standardmäßigen Einstellungen zurücksetzen müssen.

Virtuelle iDRAC6-Remote-KVM deaktivieren

Administratoren können die iDRAC6-Remote-KVM 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 Konsolenumleitung 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 Remote-vKVM unter Verwendung des folgenden Befehls deaktivieren:

```
racadm LocalConRedirDisable 1
```

Der Befehl LocalConRedirDisable deaktiviert die vorhandenen Fenster der Remote-vKVM-Sitzung, wenn er mit 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 eigens wieder aufheben, um die Remote-vKVM erneut zu aktivieren. Die Aufhebung kann durch die Verwendung des Arguments 0 vorgenommen werden:

```
racadm LocalConRedirDisable 0
```

In verschiedenen Situationen ist die Deaktivierung von iDRAC6-Remote-vKVM 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 Falle können sie die Remote-vKVM während des System-POST deaktivieren, indem Sie den Befehl `LocalConRedirDisable` anwenden. Es empfiehlt sich u. U., die Sicherheit zu erhöhen, indem die Remote-vKVM 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)"
- "Zertifikatsignierungsanforderung (CSR)"
- "Zugriff auf das SSL-Hauptmenü"
- "Zertifikatsignierungsanforderung erstellen"

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 an einem SSL-aktivierten Client selbst

- Ermöglicht dem Client, sich am Server selbst zu authentifizieren
- Ermöglicht beiden Systemen, eine verschlüsselte Verbindung herzustellen

Dieses Verschlüsselungsverfahren gewährt einen optimalen 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). Um hohe Sicherheit über das Internet zu gewährleisten, ersetzen Sie das Web Server SSL-Zertifikat, indem Sie eine Anforderung an den iDRAC6 senden, eine neue Zertifikatsignierungsanforderung (CSR) zu erstellen.

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-Industrie auf Grund seiner hohen Standards bezüglich der zuverlässigen Sicherheitsüberprüfung, Identifizierung und weiterer wichtiger Sicherheitskriterien anerkannt ist. Beispiele für CAs sind 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 **System**struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **SSL**.

Verwenden Sie das **SSL-Hauptmenü** (siehe Tabelle 23-1), um eine CSR zu erstellen, ein bestehendes Serverzertifikat hochzuladen oder ein bestehendes Serverzertifikat anzuzeigen. Die CSR-Informationen werden in der iDRAC6-Firmware gespeichert. Tabelle 23-2 beschreibt die auf der **SSL-Seite** verfügbaren Schaltflächen.

Tabelle 23-1. 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.
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-codierte 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.

Tabelle 23-2. Schaltflächen im SSL-Hauptmenü

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **SSL-Hauptmenü**.
Aktualisieren	Lädt die Seite **SSL-Hauptmenü** erneut.
Weiter	Wechselt zur nächsten Seite.

Zertifikatsignierungsanforderung erstellen

ANMERKUNG: Jede CSR überschreibt die vorherige CSR der Firmware. Damit der iDRAC Ihre signierte CSR 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 23-3 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. Tabelle 23-4 beschreibt die auf der Seite **Zertifikatsignierungsanforderung (CSR) erstellen** verfügbaren Schaltflächen.

Tabelle 23-3. Optionen der Seite "Zertifikatsignierungsanforderung (CSR) erstellen"

Feld	Beschreibung
Allgemeiner Name	Der genaue Name, der zertifiziert werden soll (normalerweise der Web Server-Domänenname, z. B. **www.xyzcompany.com**). Nur alphanumerische Zeichen, Bindestriche, Unterstriche, Leerzeichen und Punkte sind gültig.
Name der Organisation	Der mit dieser Organisation assoziierte Name (zum Beispiel, XYZ GmbH). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Organisationseinheit	Der mit einer organisatorischen Einheit assoziierte Name, z. B. eine Abteilung (zum Beispiel IT). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Ort	Die Stadt oder ein anderer Standort des Unternehmens, das zertifiziert wird (z. B. München). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie keine Unterstreichungszeichen oder andere Zeichen, um Wörter zu trennen.
Name des Bundeslands oder Kantons	Das Bundesland oder der Kanton, in dem sich das Unternehmen, das sich für eine Zertifizierung bewirbt, befindet (z. B. Bayern). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie keine Abkürzungen.
Landescode	Der Name des Landes, in dem sich das Unternehmen, das sich um Zertifikat bewirbt, befindet. Verwenden Sie das Dropdown-Menü, um das Land auszuwählen.
E-Mail	Die mit der CSR verknüpfte 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.

Tabelle 23-4. Schaltflächen der Seite Zertifikatsignierungsanforderung (CSR) erstellen

Schaltfläche	Beschreibung
Drucken	Die Seite **Zertifikatsignierungsanforderung (CSR) erstellen** drucken.
Aktualisieren	Die Seite **Zertifikatsignierungsanforderung (CSR) erstellen** neu laden.
Zurück zum SSL-Hauptmenü	Zurück zur Seite **SSL-Hauptmenü**.
Erstellen	Eine CSR erstellen

Serverzertifikat anzeigen

1. Auf der Seite **SSL-Hauptmenü** wählen Sie **Serverzertifikat anzeigen** aus und klicken auf **Weiter.**

   Tabelle 23-5 erläutert die Felder und zugehörigen Beschreibungen, die im **Zertifikat**-Fenster aufgeführt werden.

2. Klicken Sie auf der Seite **Serverzertifikat anzeigen** auf die entsprechende Schaltfläche, um fortzufahren.

Tabelle 23-5. 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".

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 **System**struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Dienste**.
3. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Lokale Konfiguration (Tabelle 23-6)
   - Web Server (Tabelle 23-7)
   - SSH (Tabelle 23-8)
   - Telnet (Tabelle 23-9)
   - Remote-RACADM (Tabelle 23-10)
   - SNMP-Agent (Tabelle 23-11)
   - Automatisierter Systemwiederherstellungs-Agent (Tabelle 23-12)

   Verwenden Sie den **Automatisierten Systemwiederherstellungs-Agent**, 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 übernehmen**.
5. Klicken Sie auf der Seite **Dienste** auf die entsprechende Schaltfläche, um fortzufahren. Siehe Tabelle 23-13.

Tabelle 23-6. 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 23-7. Web Server-Einstellungen

Einstellung	Beschreibung
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**.
Zeitüberschreitung	Die Zeit in Sekunden, für die eine Verbindung inaktiv 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 auch 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-Anschlussnummer	Der vom iDRAC verwendete Anschluss, der auf eine Serververbindung abhört. Die Standardeinstellung ist **80**.
HTTPS-Anschlussnummer	Der vom iDRAC verwendete Anschluss, der auf eine Serververbindung abhört. Die Standardeinstellung ist **443**.

Tabelle 23-8. SSH-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert SSH. Wenn markiert, weist das Kontrollkästchen darauf hin, dass SSH aktiviert ist.
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.**
Anschlussnummer	Der Anschluss, den der iDRAC6 auf eine Browser-Verbindung abhört. Die Standardeinstellung ist **22.**

Tabelle 23-9. Telnet-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert Telnet. Wenn markiert, ist Telnet aktiviert.
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.**
Anschlussnummer	Der Anschluss, den der iDRAC6 auf eine Telnet-Verbindung abhört. Die Standardeinstellung ist **23.**

Tabelle 23-10. Remote-RACADM- Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert/deaktiviert Remote-RACADM. Wenn markiert, ist Remote-RACADM aktiviert.
Aktive Sitzungen	Die Anzahl der aktuellen Sitzungen auf dem System.
Aktive Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich **Max. Sitzungen**.

Tabelle 23-11. Einstellungen des SNMP-Agenten

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert den SNMP-Agenten. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Community-Name	Der Name der Community, welche die IP-Adresse für das SNMP-Warnungsziel enthält. Der Community-Name kann bis zu 31 Zeichen (keine Leerzeichen) lang sein. Die Standardeinstellung ist **public**.

Tabelle 23-12. Einstellung des automatisierten Systemwiederherstellungs-Agenten

Einstellung	Beschreibung
Aktiviert	Aktiviert den automatisierten Systemwiederherstellungs-Agenten.

Tabelle 23-13. Schaltflächen der Seite "Dienste"

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Dienste**.
Aktualisieren	Aktualisiert die Seite **Dienste**.
Änderungen übernehmen	Wendet die Einstellungen für die Seite **Dienste** an.

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.

Eine vollständige Liste von **cfgRacTune**-Eigenschaften finden Sie unter "Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank".

Tabelle 23-14. 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 signifikanten 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

Es folgt ein Beispielbefehl für den IP-Filter-Setup.

"RACADM im Remote-Zugriff verwenden" enthält weitere Informationen über RACADM und RACADM-Befehle.

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 unten gezeigt.

```
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, wie unten gezeigt:

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

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:

- Die Anzahl von zulässigen Anmeldefehlversuchen
- Der Zeitrahmen in Sekunden, während dem die Fehlversuche auftreten müssen
- Die Zeitspanne in Sekunden, während der die "schuldige" IP-Adresse gehindert wird, eine Sitzung zu beginnen, nachdem die zulässige Anzahl von Fehlversuchen überschritten wurde

Die Anmeldefehlversuche von einer spezifischen 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: Connection closed by remote host (ssh exchange identification: Verbindung vom Remote-Host geschlossen).

Eine vollständige Liste von **cfgRacTune**-Eigenschaften finden Sie unter "Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank".

Tabelle 23-15 führt die vom Benutzer definierten Parameter auf.

Tabelle 23-15. 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 Anmeldefehlversuchen einer IP-Adresse fest, bevor die Anmeldeversuche 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 Anmeldeversuche.

```
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 **System**struktur auf **Remote-Zugriff**.
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 23-16 beschreibt die Einstellungen der Seite **Netzwerksicherheit**.
5. Klicken Sie auf der Seite **Netzwerksicherheit** auf die entsprechende Schaltfläche, um fortzufahren. Unter Tabelle 23-17 finden Sie eine Beschreibung der Schaltflächen der Seite **Netzwerksicherheit**.

Tabelle 23-16. 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.
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 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.
IP-Bereichs-Subnetzmaske	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Subnetzmaske muss in Form einer Netzmaske sein, wobei die signifikanteren 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 die IP-Adressen-Blockierungsfunktion, mit der während einer festgelegten Zeitspanne die Anzahl von Anmeldefehlversuchen

aktiviert	einer spezifischen IP-Adresse eingeschränkt wird.
IP-Blockierung, Zählung von Fehlversuchen	Legt die Anzahl von Anmeldefehlversuchen einer IP-Adresse fest, bevor die Anmeldeversuche 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 Strafzeit für die IP-Blockierung auszulösen.
Strafzeit für IP-Blockierung	Die Zeitspanne in Sekunden, während der Anmeldeversuche von einer IP-Adresse aufgrund übermäßiger Fehlversuche zurückgewiesen werden.

Tabelle 23-17. Schaltflächen der Seite "Netzwerksicherheit"

Schaltfläche	**Beschreibung**
Drucken	Druckt die Seite **Netzwerksicherheit**
Aktualisieren	Lädt die Seite **Netzwerksicherheit** neu
Änderungen übernehmen	Speichert die Änderungen, die auf der Seite **Netzwerksicherheit** vorgenommen wurden.
Zurück zur Seite Netzwerkkonfiguration	Wechselt zur Seite **Netzwerk** zurück.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Grundlegende Installation des iDRAC6

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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

Bevor Sie beginnen

Stellen Sie die folgenden Artikel aus dem Lieferumfang des Systems bereit, 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. Für erste Schritte mit dem auf dem System installierten iDRAC6 schlagen Sie unter "Übersicht zu Softwareinstallation und -konfiguration" nach.

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 die Eingabetaste. 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 Remote-Zugriffs-Gerätenetzwerkschnittstelle 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 Remote-Zugriffs-Gerätenetzwerkschnittstelle 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 Remote-Zugriffs-Gerätenetzwerkschnittstelle 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 alle Datenübertragungen auf NIC 1 zurück, jedoch nur, nachdem der ursprüngliche NIC 1-Fehler korrigiert wurde. Diese Option steht auf iDRAC6 Enterprise möglicherweise nicht zur Verfügung.

4. Konfigurieren Sie die LAN-Parameter des Netzwerk-Controllers zur Verwendung von DHCP oder einer statischen IP-Adressen-Quelle.
   a. Wählen Sie mit der Nach-unten-Pfeiltaste **LAN-Parameter** aus, und drücken Sie die Eingabetaste.
   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 **Ethernet- IP-Adresse**, **Subnetzmaske** und **Standard-Gateway**-Einstellungen.
   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".

iDRAC6-Software installieren

So installieren Sie die iDRAC6-Software:

1. Installieren Sie die Software auf dem verwalteten System. Siehe "Software auf dem verwalteten System installieren".
2. Installieren Sie die Software auf der Management Station. Siehe "Software auf der Management Station installieren".

Konfiguration des iDRAC6

So konfigurieren Sie den iDRAC6:

1. Wählen Sie eines der folgenden Konfigurationshilfsprogramme aus:
   - Webbasierte Oberfläche - siehe "iDRAC6 mittels der Webschnittstelle konfigurieren".
   - RACADM-CLI - siehe "iDRAC6-SM-CLP-Befehlszeilenoberfläche verwenden".
   - Telnet-Konsole - siehe "Telnet-Konsole verwenden".

   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".
3. iDRAC6-Benutzer hinzufügen und konfigurieren Siehe "iDRAC6- Benutzer hinzufügen und konfigurieren".
4. Konfigurieren Sie den Webbrowser, um auf die webbasierte Schnittstelle zuzugreifen. Siehe "Konfiguration eines unterstützten Webbrowsers".
5. Deaktivieren Sie die Microsoft® Windows®-Option "Automatischer Neustart". Siehe "Die Windows-Option "Automatisch Neustart durchführen" deaktivieren".
6. Aktualisieren Sie die iDRAC6-Firmware. Siehe "iDRAC6-Firmware aktualisieren".

Software auf dem verwalteten System installieren

Die Installation von Software auf dem verwalteten System ist optional. Ohne diese 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".

Software auf der Management Station installieren

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

- DVD root - Enthält das Dell Systems Build und Update-Dienstprogramm, das Informationen zur Server-Einrichtung und Systeminstallation bereitstellt
- SYSMGMT - Enthält die Systems Management Software-Produkte 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 **support.dell.com/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".
- RACADM-CLI - siehe "iDRAC6-Firmware über RACADM aktualisieren".
- Dell-Aktualisierungspakete - siehe "iDRAC6-Firmware mittels Dell Update Packages für unterstützte Windows- und Linux-Betriebssysteme aktualisieren".

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 Sie 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

Weitere Informationen finden Sie unter "iDRAC6 Firmware/Systemdienste-Wiederherstellungsimage aktualisieren".

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.

   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.

   Beispiel:

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

   wobei *Pfad* der Speicherort auf dem TFTP-Server ist, in dem **firmimg.d6** gespeichert ist.

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: device descriptor not accepting address 2, error -71
```

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

Browser-Cache löschen

Nach der Firmware-Aktualisierung löschen Sie den Cache des Webbrowsers.

Weitere Informationen finden Sie unter "Löschen Sie den Cache des Browsers".

Konfiguration 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 den Internet Explorer-Webbrowser, 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.

32-Bit- und 64-Bit-Webbrowser

Die webbasierte iDRAC6-Schnittstelle wird auf 64-Bit-Webbrowsern nicht unterstützt. Wenn Sie einen 64-Bit-Browser öffnen, auf die Konsolenumleitungsseite zugreifen und versuchen, das Plug-in zu installieren, schlägt das Installationsverfahren fehl. Wenn dieser Fehler nicht bestätigt wurde und Sie dieses Verfahren wiederholen, wird die Konsolenumleitungsseite geladen, obwohl die Plug-in-Installation während des ersten Versuchs fehlgeschlagen ist. Dieses Problem tritt auf, weil der Webbrowser die Plug-in-Informationen im Profilverzeichnis speichert, obwohl das Plug-in-Installationsverfahren fehlgeschlagen ist. Um dieses Problem zu lösen, installieren Sie einen unterstützten 32-Bit-Webbrowser, führen ihn aus und melden Sie sich am iDRAC6 an.

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 Konsolenumleitung auf einem Red Hat® Enterprise Linux®-Client (Version 4) mit einer GUI für vereinfachtes Chinesisch ausführen, erscheinen das Anzeigemenü 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 einen Befehlterminal.
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 am 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".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6 mittels der Webschnittstelle konfigurieren

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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 über SM-CLP finden Sie unter "iDRAC6-SM-CLP-Befehlszeilenoberfläche verwenden" und über RACADM-Befehle unter "Übersicht der RACADM-Unterbefehle" und "Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank".

VORSICHT: Wenn Sie den Browser durch Klicken auf "Aktualisierung" oder durch Drücken von F5 aktualisieren, werden Sie möglicherweise von der Web-GUI-Sitzung 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.

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

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

   wobei *iDRAC-IP-Adressé* 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 eine der folgenden Eingaben 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*>. Hier wird 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 Drop-Down-Menü *Dieser iDRAC* aus, wenn Sie den Domänennamen als Teil des Benutzernamens angegeben haben.
4. Klicken Sie auf **OK** oder drücken Sie die Eingabetaste.

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 ordnungsgemäß 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.

VORSICHT: 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-Register und -Fenster verwenden

Beim Öffnen neuer Register und Fenster weisen unterschiedliche Versionen von Webbrowsern unterschiedliche Verhalten auf. Microsoft Internet Explorer 6 unterstützt keine Register. Deshalb wird jedes geöffnete Browserfenster zu einer neuen iDRAC6-Webschnittstellen-Sitzung. Internet Explorer (IE) Version 7 und IE 8 bieten die Option, sowohl Register als auch Fenster zu öffnen. Jedes Register übernimmt die Merkmale des zuletzt geöffneten Registers. Drücken Sie <`Strg`–`T`>, um ein neues Register zu öffnen, und <`Strg`–`N`>, um ein neues Browserfenster in der aktiven Sitzung zu öffnen. Sie werden mit den bereits authentifizierten Anmeldeinformationen angemeldet. Durch das Schließen eines beliebigen Registers laufen alle Register der iDRAC6-Webschnittstelle ab. Wenn sich außerdem ein Benutzer in einem Register mit Hauptbenutzerberechtigungen anmeldet und dann in einem anderen Register als Administrator, erhalten beide geöffneten Register Administratorrechte.

Das Verhalten der Register in Mozilla Firefox 2 und Firefox 3 ist identisch mit dem Registerverhalten in IE 7 and IE 8; neue Register leiten neue Sitzungen ein. Bildschirme, die mit einem Firefox-Browser gestartet werden, werden mit denselben Berechtigungen betrieben wie das zuletzt geöffnete Fenster. Wenn z. B. ein Firefox-Fenster mit einem angemeldeten Hauptbenutzer und ein anderes Fenster mit Administratorrechten geöffnet wird, haben **beide** Benutzer Administratorrechte.

Tabelle 4-1. Benutzerrechte-Verhalten in unterstützten Browsern

Browser	Registerverhalten	Fensterverhalten
Microsoft Internet Explorer 6	-	Neue Sitzung
Microsoft IE7 und IE8	Von letzter geöffneter Sitzung	Neue Sitzung
Firefox 2 und Firefox 3	Von letzter geöffneter Sitzung	Von letzter geöffneter Sitzung

iDRAC6-NIC konfigurieren

Für diesen Abschnitt wird angenommen, dass der iDRAC6 bereits konfiguriert wurde und über das Netzwerk auf ihn zugegriffen werden kann. Hilfe bei der ersten iDRAC6-Netzwerkkonfiguration finden Sie unter "Konfiguration des iDRAC6".

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 iDRAC6-KVM-Sitzung ausgeführt wird.

ANMERKUNG: Eventuell wird die folgende Meldung eingeblendet, wenn das System während des POST anhält: Strike the F1 key to continue, F2 to run the system setup program (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 **Remote-Zugriff**→ **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. Wenn Sie die erforderlichen Einstellungen eingegeben haben, klicken Sie auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-8.

Tabelle 4-2. Netzwerkeinstellungen

Einstellung	Beschreibung
NIC-Auswahl	Konfiguriert den aktuellen Modus aus den vier möglichen Modi: · Dediziert **ANMERKUNG:** Diese Option steht nur auf iDRAC 6 Enterprise-Karten zur Verfügung. · Freigegeben (LOM1) · Freigegeben für Failover: LOM2 · Freigegeben für Failover: Alle LOMs **ANMERKUNG:** Diese Option steht auf iDRAC6 Enterprise möglicherweise nicht zur Verfügung. **ANMERKUNG:** iDRAC6 kommuniziert nicht lokal über denselben physischen Anschluss, wenn **NIC-Auswahl** auf den Modus **Freigegeben** oder **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.
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 der 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 Hub 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)**.
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.
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 das 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.

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.
Präfixlänge	Konfiguriert die Präfixlänge der IPv6-Adresse. Diese 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 iDRAC6-NIC-IPv6-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 das 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** eingegeben werden.
Bevorzugter DNS-Server	Konfiguriert die statische IPv6-Adresse für den bevorzugten DNS-Server. Zum Ändern dieser Einstellung müssen Sie erst

	DHCP zum Abrufen von DNS-Serveradressen verwenden abwählen.
Alternativer DNS-Server	Konfiguriert die statische IPv6-Adresse für den alternativen DNS-Server. Zum Ändern dieser Einstellung müssen Sie erst **DHCP zum Abrufen von DNS-Serveradressen verwenden** abwählen.

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**.
Verschlüsselungsschlüssel	Konfiguriert den Verschlüsselungsschlüssel: 0 bis 20 Hexadezimalzeichen (keine Leerstellen erlaubt). Die Standardeinstellung ist leer.

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.

Tabelle 4-8. Schaltflächen der Seite "Netzwerkkonfiguration"

Schaltfläche	Beschreibung
Drucken	Druckt die **Netzwerk**-Werte aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Netzwerk** erneut.
Erweiterte Einstellungen	Öffnet die Seite **Netzwerksicherheit**, auf der Benutzer den IP-Bereich sowie IP-Blockierungsattribute eingeben können.
Anwenden	Speichert alle neuen Einstellungen, die auf der Seite **Netzwerk** vorgenommen wurden. **ANMERKUNG:** Wenn Sie Änderungen an den Einstellungen der NIC-IP-Adresse vornehmen, werden alle Benutzersitzungen geschlossen und Benutzer müssen unter Verwendung der aktualisierten IP-Adresseneinstellungen eine neue Verbindung zur iDRAC6-Webschnittstelle herstellen. Alle anderen Änderungen erfordern, dass der NIC zurückgesetzt wird, was einen kurzzeitigen Verlust der Verbindungen verursachen kann.

IP-Filterung und IP-Blockierung konfigurieren

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

1. Klicken Sie auf **Remote-Zugriff**→ **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 4-9 beschreibt die Einstellungen der **Seite Netzwerksicherheit**. Wenn Sie mit den Einstellungen fertig sind, klicken Sie auf **Anwenden**.
3. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-10.

Tabelle 4-9. 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 signifikanten Bitstellen in der IP-Adresse. Die Subnetzmaske muss in Form einer Netzmaske sein, wobei die signifikanteren Bits alles Einsen (1) sind mit einem einzigen 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 Anmeldefehlversuchen einer IP-Adresse fest, bevor die Anmeldeversuche 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 Strafzeit für die IP-Blockierung auszulösen. Die Standardeinstellung ist **3600.**
Strafzeit für IP-Blockierung	Der Zeitraum in Sekunden, während dem Anmeldeversuche von einer IP-Adresse auf Grund übermäßiger Fehler zurückgewiesen werden. Die Standardeinstellung ist **3600.**

Tabelle 4-10. Schaltflächen der Seite "Netzwerksicherheit"

Schaltfläche	Beschreibung
Drucken	Druckt die Werte der **Netzwerksicherheit** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Netzwerksicherheit** erneut.
Anwenden	Speichert alle neuen Einstellungen, die Sie auf der Seite **Netzwerksicherheit** vorgenommen haben.
Zur Seite "Netzwerkkonfiguration" zurückkehren.	Wechselt zur **Netzwerk**seite zurück.

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 4-11 aufgeführt.

Tabelle 4-11. Plattformereignisfilter

Index	Plattformereignis
1	Assertion Lüfter kritisch
2	Assertion Batteriewarnung
3	Assertion Batterie kritisch
4	Assertion diskrete 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	Prozessor nicht vorhanden
13	Assertion Netzteilwarnung
14	Assertion Netzteil kritisch
15	Netzteil nicht vorhanden
16	Assertion Ereignisprotokoll kritisch
17	Assertion Watchdog kritisch
18	Assertion Systemstromwarnung
19	Assertion Systemstrom kritisch
20	Assertion diskrete SD-Karte informativ
21	Assertion diskrete SD-Karte kritisch
22	Assertion diskrete SD-Karte 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 Einstellungen für Plattformereignis-Traps oder E-Mail-Warnungen konfigurieren.

1. Melden Sie sich über einen unterstützten Webbrowser am Remote- System an. Siehe "Zugriff auf die Webschnittstelle".
2. Klicken Sie auf **System**→ **Warnungsverwaltung**→ **Plattformereignisse**.
3. Wählen Sie in der ersten Tabelle das Kontrollkästchen **Plattformereignisfilter-Warnungen aktivieren** aus und klicken Sie dann auf **Anwenden**.

   ANMERKUNG: Plattformereignisfilter-Warnungen aktivieren muss aktiviert sein, damit eine Warnung an ein gültiges, konfiguriertes Ziel gesendet werden kann (PET oder E-Mail).

4. Klicken Sie in der nächsten Tabelle, **Liste der Plattformereignisfilter**, auf den Filter, den Sie konfigurieren möchten.
5. Wählen Sie auf der Seite **Plattformereignisse einstellen** die entsprechende **Maßnahme zum Herunterfahren** aus oder wählen Sie **Keine** aus.
6. Wählen Sie **Warnung erstellen** aus oder ab, um diese Maßnahme zu aktivieren bzw. zu deaktivieren.

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

7. Klicken Sie auf **Anwenden**.

   Sie werden zur Seite **Plattformereignisse** zurückgeführt, auf der die von Ihnen übernommenen Änderungen in der **Liste der Plattformereignisfilter** angezeigt werden**.**

8. Wiederholen Sie die Schritte 4 bis 7, um zusätzliche Plattformereignisfilter zu konfigurieren.

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" beschriebenen Verfahren befolgt haben.
3. Klicken Sie auf **System**→ **Warnungsverwaltung**→ **Trap-Einstellungen**.
4. Klicken Sie entweder in der **IPv4-Ziel-Liste** oder in der **IPv6-Ziel-Liste** auf eine Zielnummer, um IPv4- oder IPv6-SNMP-Warnungsziele zu konfigurieren.
5. Wählen Sie auf der Seite **Plattformereigniswarnungsziel einstellen** entweder **Ziel aktivieren** aus oder ab. Ein markiertes Kontrollkästchen weist darauf hin, dass die IP-Adresse zum Empfangen von Warnungen aktiviert ist. Ein abgewähltes Kontrollkästchen bedeutet, dass die IP- Adresse zum Empfangen von Warnungen deaktiviert ist.
6. Geben Sie eine gültige IP-Adresse eines Plattformereignis-Trap-Ziels ein und klicken Sie dann auf **Anwenden**.
7. Klicken Sie zum Testen der konfigurierten Warnung auf **Test-Trap senden**, um die konfigurierte Warnung zu testen, oder klicken Sie auf **Zurück zur Seite Plattformwarnungsziel**.

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

   Auf der Seite **Plattformereigniswarnungsziele** werden die von Ihnen vorgenommenen Änderungen entweder in der IPv4- oder IPv6-**Ziel-Liste** angezeigt**.**

8. Geben Sie im Feld **Community-Zeichenkette** den entsprechenden iDRAC-SNMP-Community-Namen ein. Klicken Sie auf **Anwenden**.

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

9. Wiederholen Sie die Schritte 4 bis 7, um zusätzliche IPv4- oder IPv6- Zielnummern zu konfigurieren.

ANMERKUNG: Wenn Sie einen Plattformereignisfilter deaktivieren, wird auch der Trap deaktiviert, der diesem "fehlerhaft" werdenden Sensor zugeordnet ist. Traps, die mit Übergängen der Art "fehlerhaft zu funktionstüchtig" assoziiert werden, werden stets erstellt, wenn die Option **Plattformereignisfilter-Warnungen aktivieren** markiert oder aktiviert ist. Beispiel: Wenn Sie die Option **Warnung erstellen** für den **Assertionsfilter diskrete SD-Karte informativ** deaktivieren und die SD-Karte entfernen, wird der zugeordnete Trap nicht angezeigt. Der Trap wird erstellt, wenn Sie die SD-Karte erneut einsetzen. Wenn Sie jedoch den Plattformereignisfilter aktivieren, wird sowohl beim Entfernen als auch beim Einsetzen ein Trap erstellt.

Konfiguration von E-Mail-Warnungen

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" beschriebenen Verfahren befolgt haben.
3. Klicken Sie auf **System**→ **Warnungsverwaltung**→ **E-Mail- Warnungseinstellungen**.
4. Klicken Sie in der Tabelle unter **Ziel-E-Mail-Adressen** auf die **E-Mail- Warnungsnummer**, für die Sie eine Zieladresse konfigurieren möchten.
5. Wählen Sie auf der Seite **E-Mail-Warnung einstellen** die Option **E-Mail- Warnung aktivieren** aus oder ab. Ein markiertes Kontrollkästchen weist darauf hin, dass die E-Mail-Adresse zum Empfangen der Warnungen aktiviert ist. Ein abgewähltes Kontrollkästchen bedeutet, dass die E-Mail- Adresse zum Empfangen von Warnungen deaktiviert ist.
6. Geben Sie in das Feld **Ziel-E-Mail-Adresse** eine gültige E-Mail-Adresse ein.
7. Geben Sie im Feld **E-Mail-Beschreibung** eine kurze Beschreibung ein, die in der E-Mail angezeigt werden soll.
8. Klicken Sie auf **Anwenden**.
9. Klicken Sie zum Testen der konfigurierten E-Mail-Warnung auf **Test-E- Mail senden**. Falls nicht, klicken Sie auf **Zurück zur Seite E-Mail- Warnungsziel**.
10. Klicken Sie auf **Zurück zur Seite E-Mail-Warnungsziel** und geben Sie eine gültige SMTP-IP-Adresse in das Feld **SMTP- [E-Mail-] Server-IP-Adresse** 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.

11. Klicken Sie auf **Anwenden**.
12. Wiederholen Sie die Schritte 4 bis 9, um zusätzliche E-Mail- Warnungsziele zu konfigurieren.

IPMI konfigurieren

1. Melden Sie sich über einen unterstützten Webbrowser am Remote- System an.
2. Konfigurieren Sie IPMI-über-LAN.
   a. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.
   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 **System**struktur auf **Remote-Zugriff**.
   b. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Seriell-über-LAN**.
   c. Auf der Seite **Seriell-über-LAN** wählen Sie **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. Im Menü **Seriell** ändern Sie den seriellen IPMI-Verbindungsmodus auf die entsprechende Einstellung.

Unter **IPMI-Seriell** klicken Sie auf das Dropdown-Menü **Verbindungsmoduseinstellung** und wählen 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 **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.

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 **support.dell.com / manuals**.

---

iDRAC6-Benutzer konfigurieren

Genauere Informationen finden Sie unter "iDRAC6-Benutzer hinzufügen und konfigurieren".

---

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 einen optimalen 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 Web Server-SSL-Zertifikat 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-Industrie dafür anerkannt ist, hohe Standards 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 **Remote-Zugriff→ 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 4-12 beschreibt die o. g. Optionen auf der Seite **SSL**.

Tabelle 4-12. 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. Damit eine Zertifizierungsstelle Ihre CSR annimmt, muss die CSR in der Firmware mit dem von der Zertifizierungsstelle zurückgesendeten 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

ANMERKUNG: Jede neue Zertifikatsignierungsanforderung (CSR) überschreibt alle vorangegangenen in der Firmware gespeicherten CSR-Daten. Damit der iDRAC Ihre CSR akzeptiert, muss die signierte CSR in der Firmware mit dem von der Zertifizierungsstelle zurückgesendeten Zertifikat übereinstimmen.

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 4-13 beschreibt die CSR-Attribute.

3. Klicken Sie zum Erstellen der CSR auf **Erstellen** und laden Sie sie auf Ihren lokalen Computer herunter.

4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-14.

Tabelle 4-13. Attribute für die Zertifikatsignierungsanforderung erstellen

Feld	Beschreibung
Allgemeiner Name	Der genaue Name, der zertifiziert werden soll (normalerweise der Domänenname des iDRAC, z. B. **www.xyzcompany.com**). Gültig sind alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Leerstellen und Punkte.
Name der Organisation	Der mit dieser Organisation assoziierte Name (zum Beispiel, XYZ Gesellschaft). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Organisationseinheit	Der einer Organisationseinheit, z. B. eine IT-Abteilung, zugeordnete Name. Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Ort	Die Stadt oder ein anderer Standort des Unternehmens, das zertifiziert wird (z. B. München). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie kein Unterstreichungszeichen oder andere Zeichen, um Wörter zu trennen.
Name des Bundeslands oder Kantons	Das Bundesland oder der Kanton, in dem sich das Unternehmen, das sich für eine Zertifizierung bewirbt, befindet (z. B. Bayern). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie keine Abkürzungen.
Landescode	Der Name des Landes, in dem sich das Unternehmen, das sich für eine Zertifizierung bewirbt, befindet.
E-Mail	Die mit der CSR verknüpfte 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.

Tabelle 4-14. Schaltflächen der Seite "Zertifikatsignierungsanforderung (CSR) erstellen"

Schaltfläche	Beschreibung
Drucken	Druckt die auf dem Bildschirm **Zertifikatsignierungsanforderung erstellen** angezeigten Werte aus.
Aktualisieren	Lädt die Seite **Zertifikatsignierungsanforderung erstellen** neu.
Erstellen	Erstellt eine CSR und fordert den Benutzer dann auf, sie in einem bestimmten Verzeichnis zu speichern.
Zurück zum SSL-Hauptmenü	Bringt den Benutzer zur Seite **SSL** zurück.

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 die entsprechende Seitenschaltfläche, um fortzufahren. Siehe Tabelle 4-15.

Tabelle 4-15. Schaltflächen der Seite "Zertifikat hochladen"

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Zertifikat hochladen**.
Zurück zum SSL-Hauptmenü	Zurück zur Seite **SSL-Hauptmenü**
Anwenden	Wendet das Zertifikat auf die iDRAC6-Firmware an.

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 4-16 erläutert die Felder und zugehörigen Beschreibungen, die in der Tabelle **Zertifikat** aufgeführt sind.

2. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-17.

Tabelle 4-16. 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

Tabelle 4-17. Schaltflächen der Seite "Serverzertifikat anzeigen"

Schaltfläche	Beschreibung
Drucken	Druckt die Werte für **Serverzertifikat anzeigen** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Serverzertifikat anzeigen** erneut.
Zurück zum SSL-Hauptmenü	Kehrt zur Seite **SSL** zurück.

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: Weitere Informationen zur Active Directory-Konfiguration und zur Konfiguration von Active Directory mit erweitertem Schema oder Standardschema finden Sie unter "iDRAC6-Verzeichnisdienst verwenden".

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

1. Klicken Sie auf **Remote-Zugriff→ Netzwerk/Sicherheit**.

2. Klicken Sie auf **Active Directory**, um die Seite **Active Directory- Konfiguration und Verwaltung** zu öffnen.

   Tabelle 4-18 führt die Optionen der Seite **Active Directory-Konfiguration und Verwaltung** auf.

3. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-19.

Tabelle 4-18. 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. Werte sind **Ja** und **Nein**.
Schemaauswahl	Gibt an, ob derzeit das Standardschema oder das erweiterte Schema mit Active Directory verwendet wird. **ANMERKUNG:** In dieser Version werden die Smart Card-basierte Zweifaktor-Authentifizierung (TFA) und die einfache Anmeldung (SSO) nicht unterstützt, wenn Active Directory für das erweiterte Schema konfiguriert ist.
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.
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.
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.
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.

Tabelle 4-19. Schaltflächen der Seite "Active Directory-Konfiguration und Verwaltung"

Schaltfläche	Definition
Drucken	Druckt die Werte aus, die auf der Seite "Active Directory-Konfiguration und Verwaltung" angezeigt werden.
Aktualisieren	Lädt die Seite Active Directory-Konfiguration und Verwaltung neu.
Active Directory konfigurieren	Ermöglicht es Ihnen, Active Directory zu konfigurieren. Genauere Informationen zur Konfiguration finden Sie unter "iDRAC6-Verzeichnisdienst verwenden".
Einstellungen testen	Ermöglicht es Ihnen, die Konfiguration von Active Directory mithilfe der von Ihnen festgelegten Einstellungen zu testen. Einzelheiten zur Verwendung der Option **Einstellungen testen** finden Sie unter "iDRAC6-Verzeichnisdienst verwenden".

Konfiguration und Verwaltung von allgemeinem LDAP

iDRAC6 bietet eine allgemeine Lösung zur Unterstützung der LDAP-basierten Authentifizierung (Lightweight Directory Access Protocol). Für diese Funktion ist auf den Verzeichnisdiensten keine Schemaerweiterung erforderlich. Informationen zur Konfiguration des allgemeinen LDAP-Verzeichnisdiensts finden Sie unter "Allgemeiner LDAP-Verzeichnisdienst".

iDRAC6-Dienste konfigurieren

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

1. Klicken Sie auf **Remote-Zugriff→ Netzwerk/Sicherheit**. Klicken Sie auf das Register **Dienste**, um die Konfigurationsseite **Dienste** anzuzeigen.
2. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Informationen zur lokalen Konfiguration - siehe Tabelle 4-20

- Web Server - siehe Tabelle 4-21 für Informationen zu Web Server-Einstellungen
- SSH - siehe Tabelle 4-22 für Informationen zu SSH-Einstellungen
- Telnet - siehe Tabelle 4-23 für Informationen zu Telnet-Einstellungen
- Remote-RACADM - siehe Tabelle 4-24 für Informationen zu Remote-RACADM-Einstellungen
- SNMP-Agent - siehe Tabelle 4-25 für Informationen zu SNMP-Einstellungen
- Automatisierter Systemwiederherstellungs-Agent (ASR-Agent) - siehe Tabelle 4-26 für Informationen zu ASR-Agent-Einstellungen

3. Klicken Sie auf **Anwenden**.

4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-27.

Tabelle 4-20. 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 4-21. Web Server-Einstellungen

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

Tabelle 4-22. SSH-Einstellungen

Einstellung	Beschreibung
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.**
Anschlussnummer	Der Anschluss, den der iDRAC6 auf eine SSH-Verbindung abhört. Die Standardeinstellung ist **22.**

Tabelle 4-23. Telnet-Einstellungen

Einstellung	Beschreibung
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.**
Anschlussnummer	Der Anschluss, den der iDRAC6 auf eine Telnet-Verbindung abhört. Die Standardeinstellung ist **23.**

Tabelle 4-24. Remote-RACADM- Einstellungen

Einstellung	Beschreibung
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 4-25. SNMP-Einstellungen

Einstellung	Beschreibung
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. Der Name der Community, welche die IP-Adresse für das SNMP-Warnungsziel enthält. Der Community-Name kann aus bis zu 31 nicht leeren Zeichen bestehen. Die Standardeinstellung ist **öffentlich**.

Tabelle 4-26. Einstellung des automatisierten Systemwiederherstellungs-Agenten

Einstellung	Beschreibung
Aktiviert	Aktiviert/deaktiviert den automatisierten Systemwiederherstellungs-Agenten. Wenn markiert, ist der automatisierte Systemwiederherstellungs-Agent aktiviert.

Tabelle 4-27. Schaltflächen der Seite "Dienste"

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Dienste**.
Aktualisieren	Aktualisiert die Seite **Dienste**.
Anwenden	Wendet die Einstellungen für die Seite **Dienste** an.

---

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 **Remote-Zugriff** und dann auf das Register **Aktualisierung.**
3. Klicken Sie auf der Seite **Hochladen/Zurücksetzen [Schritt 1 von 3])** auf **Durchsuchen** oder geben Sie den Pfad zum Firmware-Image an, das Sie unter **support.dell.com** heruntergeladen haben, oder zum Systemdienste- Wiederherstellungsimage.

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

   Beispiel:

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

   ODER

   `\\192.168.1.10\Aktualisierungen\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:

```
File upload in progress... (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 Imagedatei erfolgreich hochgeladen wurde und alle Überprüfungsvorgänge durchlaufen sind, wird der Name der Imagedatei eingeblendet. 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 im Kontrollkästchen **Konfiguration beibehalten** entfernen, 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 mithilfe des iDRAC6-Konfiguratonsdienstprogramms während des BIOS-POST 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 Systemdienste-Wiederherstellungs-Aktualisierung erfolgreich abgeschlossen ist/fehlschlägt, wird eine entsprechende Fehlermeldung angezeigt.

Zurücksetzen der iDRAC6-Firmware

iDRAC6 verfügt über die Möglichkeit, zwei Firmware-Image gleichzeitig beizubehalten. Sie haben die Möglichkeit, vom Firmware-Image Ihrer Wahl aus zu starten (oder auf diese zurückzusetzen).

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

   Klicken Sie auf **System→ Remote-Zugriff** und dann auf das Register **Aktualisieren**.

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 im Kontrollkästchen **Konfiguration beibehalten** entfernen, 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 mithilfe des iDRAC6-Konfigurationsdienstprogramms während des BIOS-POST oder mit dem racadm-Befehl (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. Wenn ein Fehler auftritt, wird eine entsprechende Fehlermeldung eingeblendet.

Remote-Syslog

Mit der iDRAC6-Funktion Remote-Syslog können Sie das RAC-Protokoll und das Systemereignisprotokoll (SEL) im Remote-Zugriff auf einen externen Syslog-

Server schreiben. Sie können sämtliche Protokolle der gesamten Serverfarm von einem zentralen Protokoll aus lesen.

Für das Remote-Syslog-Protokoll ist keine Benutzerauthentifizierung erforderlich. Damit die Protokolle im Remote-Syslog-Server eingegeben werden können, ist sicherzustellen, dass zwischen dem iDRAC6 und dem Remote-Syslog-Server eine ordnungsgemäße Netzwerkkonnektivität besteht, und dass der Remote-Syslog-Server auf demselben Netzwerk ausgeführt wird wie der 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 4-28 führt die Remote-Syslog-Einstellungen auf.

Tabelle 4-28. 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.
Anschlussnummer	Geben Sie die Anschlussnummer des Remote-Syslog-Servers ein. Die Anschlussnummer 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 von 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 <Anschlussnummer>; 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→** Register **Setup → Erstes Startlaufwerk** aus. Der Bildschirm **Erstes Startlaufwerk** wird angezeigt.

Tabelle 4-29 führt die Einstellungen für **Erstes Startlaufwerk** auf.

Tabelle 4-29. 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.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Erweiterte iDRAC6-Konfiguration

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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".

---

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

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

Konfigurieren Sie zuerst das BIOS, um die serielle Konsolenumleitung 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....On with serial redirection via com2
   ```

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

   ANMERKUNG: Sie können die serielle Kommunikation auf **On with serial redirection via com1 (Eingeschaltet mit serieller Umleitung über COM1)** einstellen, solange das Adressfeld des seriellen Anschlusses, serielles Gerät2, auch auf COM1 eingestellt ist.

   ```
   serial port address....Serial device1 = com1, serial device2 = com2
   ```

   ```
   external serial connector....Serial device 1
   ```

   ```
   failsafe baud rate....115200
   ```

   ```
   remote terminal type....vt100/vt220
   ```

   ```
   redirection after boot....Enabled
   ```

   ```
   (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 auch RACADM-Befehle im Remote-Zugriff ausführen. Siehe "RACADM im Remote-Zugriff verwenden".

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 **System**struktur und klicken Sie auf **Remote-Zugriff**.
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 zur Konfiguration von Linux für die Konsolenumleitung während des Startvorgangs finden Sie unter "Linux während des Starts für die Umleitung der seriellen Konsole konfigurieren".

Telnet-Konsole verwenden

Telnet mittels 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 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 den 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 Telnet-Konsolenumleitung aktivieren

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

Terminaltyp → **ANSI** aus.

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

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:

   ```
   Backspace will be sent as delete. (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 an der Windows-Eingabeaufforderung ergibt nicht die volle Funktionalität (einige Tasten reagieren nicht und es werden keine Grafiken angezeigt).

Es werden nur vier SSH-Sitzungen gleichzeitig unterstützt. Die Sitzungszeitüberschreitung wird durch die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert, wie unter "Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank" beschrieben.

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 <Anschlussnummer>
```

Weitere Informationen zu den Eigenschaften `cfgSerialSshEnable` und `cfgRacTuneSshPort` finden Sie unter "Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank".

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 Umleitung der seriellen 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 Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine ordnungsgemäße Textanzeige sicherzustellen, Andernfalls werden einige Textanzeigen möglicherweise nicht richtig dargestellt werden.

Die Datei **/etc/grub.conf** muss wie folgt bearbeitet werden:

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 generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# NOTICE:  You do not have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /, e.g.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=/dev/sdal
#          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 RAC-Konsolenumleitung angezeigt. Zum Deaktivieren der grafischen Schnittstelle kommentieren Sie die Zeile aus, die mit splashimage beginnt.

2. Um GRUB-Optionen das Starten mehrerer Konsolensitzungen über die serielle RAC-Verbindung zu ermöglichen, fügen Sie die folgende Zeile zu allen Optionen hinzu:

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

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

Anmeldung zur Konsole nach dem Start aktivieren

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

Fügen Sie eine neue Zeile hinzu, um agetty auf dem seriellen COM2-Anschluss 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  This file describes how the INIT process should set up
#          the system in a certain run-level.
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have
#       networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
```

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

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

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

```
# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

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
```

---

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:

Konfigurieren Sie das **BIOS**, um die serielle Verbindung 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 den Bildschirm **Serial Communication** folgendermaßen ein:

   Externer serieller Anschluss... Remote-Zugriffsgerät

   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.

Als nächstes stellen Sie eine Verbindung mit dem DB-9- oder Nullmodemkabel von der Management Station zum Server des verwalteten Knotens her. Siehe "DB-9- oder Nullmodemkabel für die serielle Konsole anschließen".

Vergewissern Sie sich dann, dass die Terminalemulationssoftware der Management Station für serielle Verbindung konfiguriert ist. Siehe "Terminalemulationssoftware der Management Station konfigurieren".

Konfigurieren Sie schließlich die iDRAC6-Einstellungen zum Aktivieren der seriellen Verbindung. Sie können die Konfiguration über RACADM oder 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 **System**struktur und klicken Sie auf **Remote-Zugriff**.
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 **System**struktur und klicken Sie auf **Remote-Zugriff**.
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 Dropdown-Menü **Einstellungen des Datenübertragungsmodus** in **Direktverbindung - grundlegender Modus**.

   Für Direktverbindung mit Terminalmodus:

   Ändern Sie im Abschnitt **Serielle IPMI** das Dropdown-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".

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 Terminalemulationssoftware 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 Konsolenumleitung umschalten

Der iDRAC6 unterstützt Escape-Tastenfolgen, die eine Umschaltung zwischen serieller RAC-Schnittstellenkommunikation und serieller Konsolenumleitung 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 **serial communication** auf **On with serial redirection via com1 (Eingeschaltet mit serieller Umleitung über COM1)** einstellen, solange das **serial port address (Adressfeld des seriellen Anschlusses)**, **serial device2 (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 Terminalemulationsprogramm (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 von serieller Konsolenumleitung auf 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 von der seriellen RAC-Schnittstellenkommunikation auf die serielle Konsolenumleitung umzuschalten, verwenden Sie die folgende Tastenfolge:

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

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 BIOS-Textkonsolenumleitung 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 Minicom-Versionen können geringfügig abweichen, erfordern jedoch dieselben grundlegenden Einstellungen. Verwenden Sie die Informationen in "Erforderliche Minicom-Einstellungen für die Emulation der seriellen Konsole" 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 an 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 Eingabetaste.
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 Eingabetaste.
10. Wählen Sie **Modem und Wählen** aus, und drücken Sie die Eingabetaste.

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 Eingabetaste, um das Menü **Modem-Wählen und Parameter-Setup** zu beenden.

14. Wählen Sie **Setup als config_name speichern** aus und drücken Sie die Eingabetaste.

15. Wählen Sie **Minicom beenden** aus und drücken Sie die Eingabetaste.

16. Geben Sie an 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 Textkonsolenumleitung 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 zum Konfigurieren einer beliebigen Minicom-Version Tabelle 5-6.

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 Konsolenumleitung konfigurieren

HyperTerminal ist das Zugriffsdienstprogramm des seriellen Anschluss von Microsoft Windows. Um die Größe Ihres Konsolenbildschirms angemessen einzustellen, verwenden Sie Hilgraeve HyperTerminal Private Edition, Version 6.3.

VORSICHT: Alle Versionen der Microsoft Windows-Betriebssysteme enthalten die Terminalemulationssoftware Hilgraeve HyperTerminal. Die integrierte Version enthält jedoch nicht alle Funktionen, die zur Konsolenumleitung erforderlich sind. Sie können statt dessen eine beliebige Terminalemulationssoftware verwenden, die die Emulationsmodi VT100/VT220 oder ANSI unterstützt. Ein vollständiger VT100/VT220- oder ANSI-Terminalemulator, der Konsolenumleitung auf Ihrem System unterstützt, ist beispielsweise Hilgraeve HyperTerminal Private Edition 6.3. Außerdem kann die Verwendung des Befehlszeilenfensters zum Ausführen einer Umleitung der seriellen Telnet-Konsole dazu führen, dass fehlerhafte Zeichen angezeigt werden.

So konfigurieren Sie HyperTerminal für die serielle Konsolenumleitung:

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	Keine
Stoppbits	1
Datenflusssteuerung	Hardware

Seriellen Modus und Terminalmodus konfigurieren

IPMI und seriellen iDRAC6 konfigurieren

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.

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

3. Konfigurieren Sie die seriellen IPMI-Einstellungen.

   Beschreibung der seriellen IPMI-Einstellungen 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 übernehmen**.

6. Klicken Sie auf der Seite **Seriell** auf die entsprechende Schaltfläche, um fortzufahren. Eine Beschreibung der Einstellungen für die Seite der seriellen Konfiguration ist unter Tabelle 5-10 verfügbar.

Tabelle 5-8. Serielle IPMI-Einstellungen

Einstellung	Beschreibung
Verbindungsmoduseinstellungen	• 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.
Datenflusssteuerung	• Keine - Hardware-Datenflusssteuerung Aus • RTS/CTS - Hardware-Datenflusssteuerung Ein
Beschränkung der Kanalberechtigungsebene	• Administrator • Operator • Benutzer

Tabelle 5-9. Serielle iDRAC6-Einstellungen

Einstellung	Beschreibung
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.
Umleitung aktiviert	Aktiviert oder deaktiviert die Konsolenumleitung. 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 Konsole geschriebenen Zeichen enthält. Maximum und Standard = 8192 Zeichen.
Anmeldungsbefehl	Die bei gültiger Anmeldung auszuführende iDRAC6-Befehlszeile.

Tabelle 5-10. Einstellungen der Seite "Seriell"

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Seriell** aus.
Aktualisieren	Aktualisiert die Seite **Seriell**.
Änderungen übernehmen	Übernimmt die IPMI- und seriellen iDRAC6-Änderungen.
Terminalmodus-Einstellungen	Öffnet die Seite **Terminalmodus-Einstellungen**.

Terminalmodus konfigurieren

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
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 5-11.
5. Klicken Sie auf **Änderungen übernehmen**.
6. Klicken Sie auf der Seite **Terminalmodus-Einstellungen** auf die entsprechende Schaltfläche, um fortzufahren. Eine Beschreibung der Schaltflächen der Seite "Terminalmodus-Einstellungen" finden Sie unter Tabelle 5-12.

Tabelle 5-11. 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.

Tabelle 5-12. Schaltflächen der Seite "Terminalmodus-Einstellungen"

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Terminalmodus-Einstellungen** aus.
Aktualisieren	Aktualisiert die Seite **Terminalmodus-Einstellungen**.
Zur Konfiguration des seriellen Anschlusses zurückkehren	Kehrt zur Seite **Konfiguration des seriellen Anschlusses** zurück.
Änderungen übernehmen	Übernimmt die Änderungen der Terminalmodus-Einstellungen.

---

iDRAC6-Netzwerkeinstellungen konfigurieren

△ **VORSICHT: 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"
- RACADM-CLI - siehe "cfgLanNetworking"
- iDRAC6-Konfigurationsdienstprogramm - siehe "System zur Verwendung eines iDRAC6 konfigurieren"

ANMERKUNG: Wird der iDRAC6 in einer Linux-Umgebung bereitgestellt, finden Sie entsprechende Informationen unter "RACADM installieren".

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 5-13 beschreibt alle iDRAC6-Schnittstellen.

Tabelle 5-13. 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 hierzu finden Sie unter "RACADM im Remote-Zugriff verwenden". **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`
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 ein ungesichertes Protokoll, das alle Daten, einschließlich Kennwörtern, als unformatierten Text 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 relevanter Dokumente finden Sie unter "Grundlegende Installation des iDRAC6".

RACADM bietet eine Remote-Fähigkeits-Option (-**r**), mit der eine Verbindung zum verwalteten System hergestellt werden kann und RACADM-Unterbefehle von einer Remote-Konsole oder einer Management Station aus 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 Standardzertifikatspeicher 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".

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors.

(Sicherheitswarnung: Zertifikat ist ungültig - Name auf Zertifikat ist ungültig oder stimmt nicht mit Standortnamen überein

Ausführung wird fortgesetzt. Verwenden Sie die Option -S, 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:

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Racadm not continuing execution of the command.

(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.

RACADM Übersicht

```
racadm -r <iDRAC6-IP-Adresse> -u <Benutzername> -p <Kennwort> <Unterbefehl> <Optionen des Unterbefehls>

racadm -i -r <iDRAC6-IP-Adresse> <Unterbefehl> <Optionen des Unterbefehls>
```

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> <Optionen des Unterbefehls>

racadm -i -r <iDRAC6-IP-Adresse>:<Anschluss> <Unterbefehl> <Optionen des Unterbefehls>
```

RACADM-Optionen

Tabelle 5-14 führt die Optionen für den RACADM-Befehl auf.

Tabelle 5-14. 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 5-15 enthält eine Beschreibung der einzelnen RACADM-Unterbefehle, die Sie in RACADM ausführen können. Eine ausführliche Auflistung aller RACADM-Unterbefehle einschließlich der Syntax und gültiger Einträge finden Sie unter "Übersicht der RACADM-Unterbefehle".

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

```
racadm help
```

Tabelle 5-15. RACADM-Unterbefehle

Befehl	Beschreibung
help	Führt iDRAC6-Unterbefehle auf.
help *<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.
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 unterschiedlichen 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 Service-Tag-Nummern 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 Stromverwaltungsvorgänge 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.
vmkey	Setzt die virtuelle Flash-Größe auf die Standardgröße (256 MB) zurück.

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:

ERROR: Unable to connect to RAC at specified IP address

(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.

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 **racadm.cfg**-Konfigurationsdatei aus den abgerufenen Informationen. 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 an der Eingabeaufforderung Folgendes ein:

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

4. Setzen Sie den konfigurierten Ziel-iDRAC6 zurück.

   Geben Sie an 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 an der Eingabeaufforderung Folgendes ein:

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

VORSICHT: 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:

- Erstellt werden
- 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 unter "getconfig".

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, ist der Wert des verankerten Objekts für die Unterscheidung der einzelnen Indizes ausschlaggebend.

  Der Parser liest in allen Indizes von dem iDRAC6 für diese Gruppe. Alle Objekte innerhalb dieser Gruppe sind einfache Modifizierungen, wenn der iDRAC6 konfiguriert wird. Wenn ein modifiziertes Objekt einen neuen Index darstellt, wird der Index während der Konfiguration auf dem iDRAC6 erstellt.

- In einer **.cfg**-Datei können Sie keinen Index Ihrer Wahl angeben.

  Indizes können erstellt und gelöscht werden, so dass die Gruppe im Laufe der Zeit über Fragmente verwendeter und nicht verwendeter Indizes verfügen kann. Wenn ein Index vorhanden ist, wird er modifiziert. Wenn kein Index vorhanden ist, wird der erste verfügbare Index verwendet. Diese Methode sorgt für Flexibilität, wenn indizierte Einträge hinzugefügt werden, wobei Sie keine genauen Index-Übereinstimmungen zwischen allen verwalteten RACs erzielen müssen. Neue Benutzer werden dem ersten verfügbaren Index hinzugefügt. Dadurch kann eine **.cfg**-Datei, die auf einem iDRAC6 korrekt geparst und ausgeführt wird, auf einem anderen möglicherweise nicht richtig ausgeführt werden, falls alle Indizes belegt sind und ein neuer Benutzer hinzugefügt werden muss.

- Verwenden Sie den Unterbefehl **racresetcfg**, um mehrere iDRAC6 mit identischen Eigenschaften zu konfigurieren.

  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.

VORSICHT: 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 werden in Gruppen organisiert, wie unter "Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank" definiert.

  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.

  Leerstellen nach dem Wert werden ignoriert. Eine Leerstelle 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 **.cfg**-Parser ignoriert einen Index-Objekt-Eintrag.

  Benutzer können *nicht* angeben, welcher Index verwendet werden soll. Wenn der Index bereits vorhanden ist, wird dieser entweder verwendet oder ein neuer Eintrag wird im ersten verfügbaren Index für diese Gruppe erstellt.

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

ANMERKUNG: Sie können eine indizierte Gruppe manuell mit folgendem Befehl erstellen:
`racadm config-g <Gruppenname>-o <verankertes Objekt>-i <Index 1-16> <eindeutiger Ankername>`

- Die Zeile für eine indizierte Gruppe kann *nicht* aus einer **.cfg**-Datei gelöscht werden.

  Benutzer müssen ein indiziertes Objekt manuell mit folgendem Befehl entfernen:

  ```
  racadm config -g <Gruppenname> -o <Objektname> -i <Index 1-16> ""
  ```

ANMERKUNG: Eine Nullzeichenkette (durch die beiden Zeichen "" gekennzeichnet) weist den iDRAC6 an, den Index für die angegebene Gruppe zu löschen.

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]

  cfgUserAdminUserName=<BENUTZERNAME>
  ```

  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.

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 mithilfe des folgenden Befehls das Objekt **cfgNicUseDhcp** geschrieben und diese Funktion aktiviert 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 zur Konfiguration von Netzwerkeigenschaften mit dem iDRAC6-Konfigurationsdienstprogramm finden Sie unter "System zur Verwendung eines iDRAC6 konfigurieren".

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 5-16 bietet eine Beschreibung der einzelnen Modi.

Tabelle 5-16. 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 Namenszertifikats 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 **System**struktur auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Netzwerk**.
3. In der Tabelle **Allgemeine Einstellungen**:
   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 Zertifikatsignierungsanforderungen (CSRs) und zur Ausgabe von Zertifikaten finden Sie unter "iDRAC6-Datenübertragung mit SSL und digitalen Zertifikaten sichern".

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 aangibt, 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 zur Ausgabe von Zertifikaten finden Sie unter "iDRAC6-Datenübertragung mit SSL und digitalen Zertifikaten sichern".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6-Benutzer hinzufügen und konfigurieren

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

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 eintritt.

---

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 **Remote-Zugriff**→ **Netzwerk/Sicherheit**→ **Benutzer**.

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

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

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

   Auf der Seite **Benutzer-Hauptmenü** (siehe Tabelle 6-2 und Tabelle 6-8) 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 zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 6-7.

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.
Zustand	Zeigt den Anmeldezustand des Benutzers an: aktiviert oder deaktiviert. (Die Standardeinstellung ist deaktiviert). **ANMERKUNG:** Benutzer 2 ist standardmäßig aktiviert.
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:** Benutzernamen auf dem iDRAC6 dürfen keine nicht unterstützten Zeichen wie "**/**" (Schrägstrich),

	"****" (umgekehrter Schrägstrich), "**.**" (Punkt) und **@** enthalten. Ein Leerzeichen in Kombination mit anderen Zeichen ist zulässig, aber ein Leerraum ist nicht zulässig. **ANMERKUNG:** Wenn der Benutzername geändert wird, erscheint der neue Name erst bei der nächsten Benutzeranmeldung in der Benutzeroberfläche.
RAC-Berechtigung	Zeigt die Gruppe (Berechtigungsebene) an, welcher der Benutzer zugewiesen ist (Administrator, Operator, schreibgeschützt oder keine).
LAN-Benutzerberechtigung	Zeigt die IPMI-LAN-Berechtigungsebene an, welcher der Benutzer zugewiesen ist (Administrator, Operator, schreibgeschützt oder keine).
Benutzerberechtigung serielle Schnittstelle	Zeigt die Berechtigungsebene der seriellen IPMI-Schnittstelle an, welcher der Benutzer zugewiesen ist (Administrator, Operator, schreibgeschützt oder keine).
Seriell-über-LAN-Berechtigung	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 Zertifizierungsstelle hochladen	Ermöglicht Ihnen, das Zertifikat der vertrauenswürdigen Zertifizierungsstelle auf den iDRAC hochzuladen und in das Benutzerprofil zu importieren.
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.
Kennwort ändern	Aktiviert die Felder **Neues Kennwort** und **Neues Kennwort bestätigen**. Wenn diese Option nicht markiert ist, kann das **Kennwort** des Benutzers nicht geändert werden.
Neues Kennwort	Geben Sie ein **Kennwort** mit bis zu 20 Zeichen ein. Die Zeichen werden nicht angezeigt.
Neues Kennwort bestätigen	Geben Sie das Kennwort des iDRAC-Benutzers erneut ein, um es zu bestätigen.

Tabelle 6-3. 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.
Protokolle löschen	Ermöglicht dem Benutzer, die iDRAC-Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer, Serversteuerungsbefehle auszuführen.

Auf die Konsolenumleitung zugreifen	Ermöglicht dem Benutzer, die Konsolenumleitung auszuführen.
Zugriff auf virtuellen 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

Benutzergruppe	**Gewährte Berechtigungen**
Administrator	**Am iDRAC anmelden**, **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf virtuellen Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Operator	Auswahl einer beliebigen Kombination der folgenden Berechtigungen: **Am iDRAC anmelden**, **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Server-Maßnahmenbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf virtuellen Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Schreibgeschützt.	**Am iDRAC anmelden**
Keine	Keine zugewiesenen Berechtigungen

Tabelle 6-7. Schaltflächen der Seite "Benutzerkonfiguration"

Schaltfläche	**Maßnahme**
Drucken	Druckt die Werte der **Benutzerkonfiguration** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Benutzerkonfiguration** erneut.
Zurück zur Benutzerseite	Wechselt zur **Benutzerseite** zurück.
Änderungen übernehmen	Speichert alle neuen Einstellungen, die an der Benutzerkonfiguration vorgenommen wurden.

Authentifizierung mit öffentlichem Schlüssel über SSH

iDRAC6 unterstützt Authentifizierung mit öffentlichem Schlüssel (PKA) über SSH. Diese Authentifizierungsmethode verbessert die automatisierte SSH-Skripterstellung durch Beseitigung des Bedarfs, ein(e) Benutzer-ID/Kennwort einzubetten bzw. deren/dessen Eingabe anzufordern.

Bevor Sie beginnen

Sie können bis zu 4 öffentliche Schlüssel *pro Benutzer* konfigurieren, die über eine SSH-Schnittstelle verwendet werden können. Stellen Sie vor dem Hinzufügen oder Löschen öffentlicher Schlüssel sicher, dass Sie den Anzeigebefehl verwenden, um zu prüfen, 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 die Einrichtung automatisierter 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 vorhandene Schlüssel nicht bereits den Index belegen, dem der neue Schlüssel hinzugefügt werden soll. Der iDRAC6 führt keine Prüfungen durch, um sicherzustellen, dass vorherige Schlüssel gelöscht werden, bevor ein neuer hinzugefügt wird. Sobald ein neuer Schlüssel hinzugefügt wurde, tritt er automatisch in Kraft, solange die SSH-Schnittstelle aktiviert ist.

Erstellen 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 Möglichkeiten, das öffentliche/private Schlüsselpaar zu erstellen: mit der Anwendung *PuTTY Key Generator* für Clients unter Windows bzw. mit *ssh-keygen*-CLI für Clients unter Linux. Das CLI-Dienstprogramm *ssh-keygen* wird standardmäßig auf allen Standardinstallationen geliefert.

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

So verwenden Sie den *PuTTY Key Generator* 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 erstellenden Schlüssels aus. (SSH-1 wird nicht unterstützt).
2. Die unterstützten Schlüsselerstellungsalgorithmen sind nur RSA und DSA. Geben Sie die Anzahl der 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 **Erstellen** und bewegen Sie die Maus im Fenster gemäß Anleitung. Nachdem der Schlüssel erstellt wurde, können Sie das Schlüsselanmerkungsfeld ändern. Sie können auch einen Kennsatz eingeben, um den Schüssel sicher zu machen. Speichern Sie den privaten Schüssel auf jeden Fall.

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 das Format RFC 4716 aufweisen. Wenn sie dieses Format nicht aufweisen, muss eine Konvertierung in dieses Format vorgenommen werden.

Erstellen öffentlicher Schlüssel für Linux

Die Anwendung *ssh-keygen* für Linux-Clients ist ein Befehlszeilen-Hilfsprogramm ohne graphische Benutzeroberfläche.

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

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

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

Hierbei

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

gibt die Option **-b** 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. Nachdem der Befehl ausgeführt wurde, laden Sie die Datei mit dem öffentlichen Schlüssel hoch.

VORSICHT: 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 die ssh-agent-Weiterleitung von Schlüsseln nicht.

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.

Beispiel:

Anmeldung:

```
ssh Benutzername@<Domäne>
```

oder

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

wobei IP-Adresse die IP-Adresse des iDRAC6 ist.

Senden von racadm-Befehlen:

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

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

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

1. Klicken Sie auf **Remote-Zugriff**→ **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.

Tabelle 6-8. SSH-Schlüsselkonfigurationen

Option	Beschreibung
SSH-Schlüssel hochladen	Ermöglicht dem lokalen Benutzer, eine öffentliche SSH-Schlüsseldatei (Sichere Shell) hochzuladen. Wird ein Schlüssel hochgeladen, wird der Inhalt der Schlüsseldatei in einem nicht-editierbaren Textfeld auf der Seite **Benutzerkonfiguration** angezeigt.
SSH-Schlüssel anzeigen/entfernen	Ermöglicht dem lokalen Benutzer, einen bestimmten 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 6-9. SSH-Schlüssel hochladen

Option	Beschreibung
Datei/Text	Wählen Sie die Option **Datei** aus und geben Sie den Pfad zu dem Speicherort ein, an dem sich der Schlüssel befindet. Sie können auch die Option **Text** auswählen und den Inhalt der Schlüsseldatei in das Feld einfügen. Sie können neue Schlüssel hochladen oder vorhandene Schlüssel überschreiben. Klicken Sie zum Hochladen einer Schlüsseldatei auf **Durchsuchen**, wählen Sie die Datei aus und klicken Sie dann auf die Schaltfläche **Anwenden**.
Durchsuchen	Klicken Sie auf diese Schaltfläche, um den vollständigen Pfad und den Dateinamen des Schlüssels zu ermitteln.

Die Seite **SSH-Schlüssel anzeigen/entfernen** ermöglicht Ihnen, die öffentlichen SSH-Schlüssel des Benutzers anzuzeigen oder zu entfernen.

Tabelle 6-10. SSH-Schlüssel anzeigen/entfernen

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

SSH-Schlüssel unter Verwendung des RACADM hochladen, anzeigen und löschen

Hochladen

Der Hochlademodus ermöglicht Ihnen, eine Schlüsseldatei hochzuladen oder den Schlüsseltext auf der Befehlszeile zu kopieren. Sie können nicht gleichzeitig einen Schlüssel hochladen und kopieren.

Lokales RACADM und Remote-RACADM:

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

telnet/ssh/seriell-RACADM:

```
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
```

PK-SSH-Authentifizierungsschlüsseldatei erfolgreich zum RAC hochgeladen.

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

Ansicht

Der Ansichtsmodus ermöglicht dem Benutzer, einen vom Benutzer festgelegten Schlüssel oder alle Schlüssel anzuzeigen.

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

racadm sshpkauth -i <2 bis 16> -v -k alle
```

Löschen

Der Modus "Löschen" ermöglicht dem Benutzer, einen vom Benutzer festgelegten 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 alle
```

Unter "sshpkauth" finden Sie Informationen zu den Unterbefehlsoptionen.

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, wie unter "Übersicht der RACADM-Unterbefehle" beschrieben, und führen Sie unter Verwendung derselben Konfigurationsdatei den Unterbefehl **racadm config** auf den einzelnen 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.

VORSICHT: 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** anzeigen oder bearbeiten, die alle iDRAC6-Konfigurationsparameter enthält.

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:
   - RAC-Berechtigung
   - LAN-Benutzerberechtigung
   - Benutzerberechtigung serielle Schnittstelle
   - Seriell-über-LAN-Berechtigung
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 bestimmten administrativen Berechtigungen (rollenbasierte Autorität) zu aktivieren, müssen Sie zuerst einen verfügbaren Benutzerindex suchen, indem Sie die unter "Bevor Sie beginnen" beschriebenen Schritte ausführen. Geben Sie im Anschluss daran die folgenden Befehlszeilen mit dem neuen Benutzernamen und Kennwort ein.

ANMERKUNG: Unter Tabelle B-2 ist eine Liste gültiger Bitmaskenwerte für bestimmte Benutzerberechtigungen verfügbar. Der Standardberechtigungswert ist 0, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt.

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6-Verzeichnisdienst verwenden

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Ein Verzeichnisdienst führt eine zentrale 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 von Active Directory zum Erkennen von iDRAC6-Benutzern wird auf den Betriebssystemen Microsoft Windows® 2000, Windows Server® 2003 und Windows Server 2008 unterstützt.

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
Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern den Zugriff auf das System zu genehmigen
Protokolle löschen	Ermöglicht dem Benutzer, die iDRAC6-Protokolle zu löschen
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer, RACADM-Befehle auszuführen
Auf die Konsolenumleitung zugreifen	Ermöglicht dem Benutzer, die Konsolenumleitung 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

---

Voraussetzungen zur Aktivierung der Active Directory-Authentifizierung für den 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 schon 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".

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 des *Standardschemas* 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 des erweiterten Schemas oder des Standardschemas 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 Lösung des Standardschemas ist, dass keine Erweiterung des Schemas notwendig ist, da alle erforderlichen Objektklassen in der Microsoft-Standardkonfiguration des Active Directory-Schemas enthalten sind.

Übersicht des Active Directory mit erweitertem Schema

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

Active Directory-Schema erweitern

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 mit 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 Active Directory-Benutzer- und Computer-MMC-Snap-In-Erweiterung sind auf der DVD *Dell Systems Management Tools and Documentation* verfügbar. Nähere Informationen finden Sie unter "Erweiterung des Active Directory-Schemas" und "Installation der Dell-Erweiterungen auf dem Active Directory-Benutzer- und -Computer-Snap-In". Einzelheiten zur Erweiterung des Schemas für den iDRAC6 und zur Installation des Active Directory-Benutzer- und -Computer-MMC-Snap-In finden Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch* unter **support.dell.com / manuals**.

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

Active Directory-Schemaerweiterungen

Bei den Active Directory-Daten handelt es sich um eine dezentrale 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 enthalten sind. 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 eindeutigen Attribute und Klassen hinzufügen, um umgebungsspezifische Bedürfnisse zu erfüllen. Dell hat das Schema um die erforderlichen Änderungen zur Unterstützung der Remote-Verwaltungsauthentifizierung 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 (Objektbezeichner) und eindeutig verknüpfte Attribut-IDs für die Attribute und Klassen erhalten, die dem Verzeichnisdienst hinzugefügt werden.

Die Dell-Dateierweiterung lautet: dell

Die Dell Basis-OID lautet: 1.2.840.113556.1.8000.1280

Der RAC-LinkID-Bereich ist: 12070 bis 12079

Übersicht über die 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

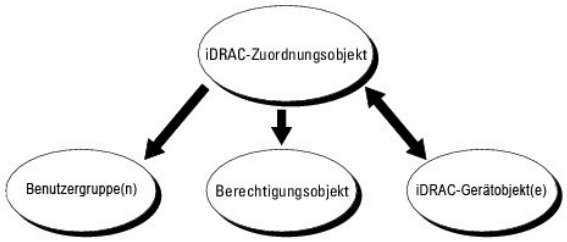
Für jeden physischen iDRAC auf dem Netzwerk, den Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein iDRAC-Geräteobjekt erstellen. Sie können mehrere Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt nach Bedarf 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 Sie müssen ein iDRAC-Geräteobjekt für jeden iDRAC auf dem Netzwerk besitzen, das zum Zweck der Authentifizierung und Autorisierung mit dem iDRAC mit dem Active Directory integriert werden soll.

Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer bzw. Gruppen und auch iDRAC-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die *Benutzer*, die *Berechtigungen* auf 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 Product-Member des Verbindungsobjektes hinzugefügt werden.

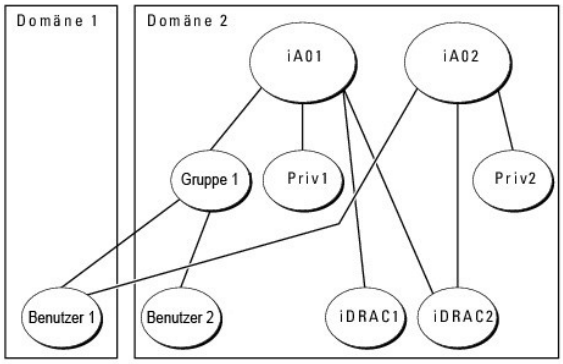
Benutzer, Benutzergruppen oder verschachtelte Benutzergruppen jeglicher Domäne können dem Verbindungsobjekt hinzugefügt werden. Lösungen mit erweitertem Schema unterstützen jede Art von Benutzergruppe sowie jede Benutzergruppe, die über mehrere Domänen verschachtelt und von Microsoft Active Directory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

Berechtigungen unter Verwendung des erweiterten Schemas ansammeln

Der Mechanismus zur Authentifizierung des erweiterten Schemas unterstützt das Ansammeln von Berechtigungen von unterschiedlichen Berechtigungsobjekten, die mit demselben Benutzer über verschiedene Zuordnungsobjekte verknüpft sind. Mit anderen Worten sammelt die Authentifizierung des erweiterten Schemas Berechtigungen an, um dem Benutzer den Supersatz aller zugewiesenen 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. Berechtigungen für einen Benutzer ansammeln



Die Abbildung zeigt zwei Zuordnungsobjekte - iA01 und iA02. Benutzer1 ist über beide Verbindungsobjekte mit dem iDRAC2 verbunden. Benutzer1 verfügt daher über die angesammelten Berechtigungen, die sich aus der Kombination der Berechtigungen für die Objekte Priv1 und Priv2 auf dem iDRAC2 ergeben.

Angenommen, Priv1 hat folgende Berechtigungen: Anmeldung, virtuelle Datenträger, Protokolle löschen; und Priv2 hat folgende Berechtigungen: am iDRAC anmelden, 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.

Schemaerweiterung des Active Directory zum Zugriff auf den iDRAC 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 in der vorgegebenen Reihenfolge ausführen:

1. Erweitern Sie das Active Directory-Schema (s. "Active Directory- Schema erweitern").

2. Erweitern Sie das Active Directory-Benutzer- und -Computer-Snap-In (s. "Installation der Dell-Erweiterung zum Microsoft Active Directory- Benutzer- und

Computer-Snap-In").

3. Fügen Sie iDRAC6-Benutzer und deren Berechtigungen zum Active Directory hinzu (s. "iDRAC-Benutzer und -Berechtigungen zum Microsoft Active Directory hinzufügen").

4. Aktivieren Sie SSL auf allen Domänen-Controllern (siehe "SSL auf einem Domänen-Controller aktivieren").

5. Konfigurieren Sie die iDRAC6 Active Directory-Eigenschaften entweder über die iDRAC6-Webschnittstelle oder das RACADM-Hilfsprogramm (siehe "Konfiguration des Microsoft Active Directory mit erweitertem Schema unter Verwendung der webbasierten iDRAC6-Schnittstelle" oder "Konfiguration des Microsoft Active Directory mit erweitertem Schema unter Verwendung von RACADM").

Mit der Erweiterung des Active Directory-Schemas werden dem Active Directory-Schema eine Dell-Organisationseinheit, Schemaklassen und -attribute sowie Beispielberechtigungen und Zuordnungsobjekte 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** ist zur Erweiterung des Schemas auf älteren Remote-Zugriff-Produkten wie DRAC 4 und DRAC 5, und der Ordner **Remote_Management_Advanced** ist zur Erweiterung des Schemas auf iDRAC6.

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Files**. Informationen zur Verwendung des Dell Schema Extender zum Erweitern des Active Directory-Schemas befinden sich unter "Dell Schema Extender verwenden".

Sie können den 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 **Willkommen**-Bildschirm 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- Administratorrechte ein.

4. Klicken Sie auf **Weiter**, um den Dell Schema Extender auszuführen.

5. Klicken Sie auf **Fertig stellen**.

   Das Schema wird erweitert. Um die Schemaerweiterung 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 Snap-in für das Active Directory-Schema finden Sie in der Microsoft-Dokumentation.

Tabelle 7-2. Klassendefinitionen für zum Active Directory-Schema hinzugefügte Klassen

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	Keine
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	Einzelbewertung
dellPrivilegeMember Die Liste von dellPrivilege-Objekten, die zu diesem Attribut gehören.	1.2.840.113556.1.8000.1280.1.1.2.1 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Liste der dellRacDevice- und DelliDRACDevice-Objekte, die dieser Rolle angehören. Dieses Attribut ist die Vorwärtsverknüpfung zur dellAssociationMembers-Rückwärtsverbindung. Link-ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE, wenn der Benutzer Anmeldungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.3 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.4 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.5 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE, wenn der Benutzer Protokolllöschungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.7 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE, wenn der Benutzer Konsolenumleitungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.8 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE, wenn der Benutzer Rechte für den virtuellen Datenträger auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE, wenn der Benutzer Testwarnungsbenutzerrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.10 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE, wenn der Benutzer Debug-Befehl-Admin-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion Die aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren.	1.2.840.113556.1.8000.1280.1.1.2.12 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Dieses Attribut ist der aktuelle RAC-Typ für das dellRacDevice-Objekt und die Rückwärtsverknüpfung zur dellAssociationObjectMembers-Vorwärtsverknüpfung.	1.2.840.113556.1.8000.1280.1.1.2.13 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Liste der dellAssociationObjectMembers, die diesem Produkt angehören. Dieses Attribut ist die Rückwärtsverknüpfung zum verknüpften dellProductMembers-Attribut. Link-ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Installation der Dell-Erweiterung zum Microsoft Active Directory-Benutzer- und Computer-Snap-In

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 das 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.

Unter "Öffnen des Microsoft Active Directory-Benutzer- und Computer-Snap-In" finden Sie weitere Informationen.

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 **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 **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
- Ein Berechtigungsobjekt erstellen
- Ein Zuordnungsobjekt erstellen
- Konfigurieren eines Zuordnungsobjekts

iDRAC-Geräteobjekt erstellen

1. Klicken Sie im Fenster **Konsolenstamm** (MCC) mit der rechten Maustaste auf einen Container.

2. Wählen Sie **Neu→ Dell Remote Management Object Advanced**.

   Das Fenster **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" eingeben werden.

4. Wählen Sie **iDRAC-Geräteobjekt**.

5. Klicken Sie auf **OK**.

Berechtigungsobjekte erstellen

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

1. Klicken Sie im Fenster **Konsolenstamm** (MMC) mit der rechten Maustaste auf einen Container.

2. Wählen Sie **Neu→ Dell Remote Management Object Advanced**.

   Das Fenster **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.

Zuordnungsobjekte erstellen

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

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

   Hierdurch wird das Fenster **Neues Objekt** geöffnet.
3. Geben Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Zuordnungsobjekt**.
5. Wählen Sie den Wirkungsbereich für das **Zuordnungsobjekt**.
6. Klicken Sie auf **OK**.

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**.
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, dass 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. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
4. Klicken Sie auf das Register **Netzwerk/Sicherheit** → Register **Verzeichnisdienst** → **Microsoft Active Directory**.
5. 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 **Schritt 1 von 4 Active Directory-Konfiguration und Verwaltung** wird angezeigt.
6. Markieren Sie unter **Zertifikat-Einstellungen** die Option **Überprüfung des Zertifikats aktivieren**, falls Sie das SSL-Zertifikat der Active Directory-Server überprüfen möchten, andernfalls gehen Sie zu Schritt 9.
7. Geben Sie unter **Active Directory-CA-Zertifikat hochladen** 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.
8. Klicken Sie auf **Hochladen.**

   Die Zertifikatsinformationen für das Active Directory-CA-Zertifikat, das Sie hochgeladen haben, wird angezeigt.
9. Geben Sie unter **Kerberos-Keytab hochladen** den Pfad der Keytab-Datei ein, oder suchen Sie die Datei mit der Suchfunktion. Klicken Sie auf **Hochladen**. Das Kerberos-Keytab wird in den iDRAC6 hochgeladen.
10. Klicken Sie auf **Weiter**, um zur Seite **Schritt 2 von 4 Active Directory- Konfiguration und Verwaltung)** zu wechseln.
11. Klicken Sie auf **Active Directory aktivieren.**

VORSICHT: In dieser Version werden die Smart Card-basierte Zweifaktor-Authentifizierung (TFA) und die einfache Anmeldung (SSO) nicht unterstützt, wenn Active Directory für das erweiterte Schema konfiguriert ist.

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**. 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.
14. Geben Sie die **Zeitüberschreitung** in Sekunden ein, um festzulegen, wie lange der iDRAC6 auf Antworten des Active Directory wartet. Der Standardwert beträgt 120 Sekunden.
15. Wählen Sie die Option **Lookup von Domänen-Controllern mit DNS** aus, um die Active Directory-Domänen-Controller mittels einer DNS-Anfrage abzurufen. Die Domänen-Controller-Serveradressen 1-3 werden ignoriert. Wählen Sie **Benutzerdomäne über Anmeldung** aus, um die DNS-Anfrage mit dem Domänennamen des anmeldenden Benutzers auszuführen. 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 **Erweitertes Schema** ausgewählt wird, befinden sich die Domänen-Controller, wo sich das iDRAC6-Geräteobjekt und die Zuordnungsobjekte befinden.
16. 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. Es wird keine DNS-Anfrage ausgeführt. Geben Sie die IP-Adresse oder den vollständigen qualifizierten Domänennamen (FQDN) des Domänen-Controllers an. Wenn die Option **Domänen-Controller-Adressen angeben** ausgewählt wird, muss mindestens eine der drei Adresse konfiguriert werden. iDRAC6 versucht so lange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte. Wenn **Erweitertes Schema** ausgewählt ist, sind dies die Adressen der Domänen-Controller, wo 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.
17. Klicken Sie auf **Weiter**, um zur Seite **Schritt 3 von 4 Active Directory- Konfiguration und Verwaltung** zu wechseln.
18. Wählen Sie unter **Schemaauswahl** die Option **Erweitertes Schema** aus.

19. Klicken Sie auf **Weiter**, um zur Seite **Schritt 4 von 4 Active Directory- Konfiguration und Verwaltung** zu wechseln.

20. 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.

21. Klicken Sie auf **Fertig stellen**, um die Einstellungen des Active Directory mit erweitertem Schema **z**u speichern.

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

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

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

    Die Testergebnisse und das Testprotokoll werden angezeigt. Weitere Informationen finden Sie unter "Einstellungen testen".

    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 **Remote-Zugriff**→ **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 cfgDomainController1 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController2 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController3 <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 des erweiterten Schemas 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.

VORSICHT: In dieser Version werden Smart Card-basierte Zweifaktor-Authentifizierung (TFA) und einfache Anmeldung (SSO) nicht unterstützt, wenn Active Directory für das erweiterte Schema konfiguriert ist.

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 hochzuladen.

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 finden Sie unter "SSL-Zertifikat der iDRAC6-Firmware importieren".

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

2. 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
   ```

3. 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>
   ```

4. 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.

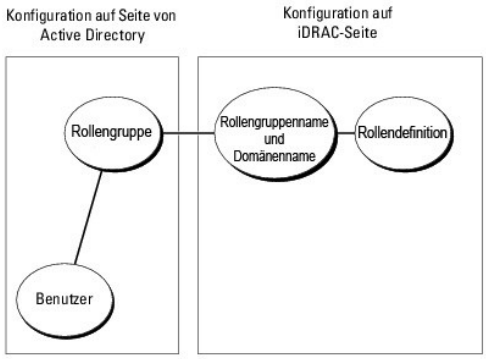
   Weitere Informationen über Benutzerdomänen finden Sie unter "Verwendung des Microsoft Active Directory zur Anmeldung beim iDRAC6".

5. Drücken Sie die **Eingabetaste**, um die Konfiguration des Active Directory mit erweitertem Schema abzuschließen.

Übersicht des Active Directory mit Standardschema

Wie in Abbildung 7-3 dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration sowohl im Active Directory als auch im 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.

Tabelle 7-9. Standardberechtigungen der Rollengruppe

Rollengruppen	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
Rollengruppe 1	Administrator	**Anmeldung am iDRAC**, **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **Auf die Konsolenumleitung zugreifen**, **Zugriff auf virtuellen Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**	0x000001ff
Rollengruppe 2	Operator	**Anmelden am iDRAC**, **iDRAC konfigurieren, Serversteuerungsbefehle ausführen**, **Auf Konsolenumleitung zugreifen**, **Zugriff auf virtuellen Datenträger**, **Testwarnungen, Diagnosebefehle ausführen**	0x000000f9
Rollengruppe 3	Schreibgeschützt.	Am iDRAC anmelden	0x00000001
Rollengruppe 4	Keine	Keine zugewiesenen Berechtigungen	0x00000000
Rollengruppe 5	Keine	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bitmasken-Werte werden nur verwendet, wenn das Standardschema mit dem RACADM eingerichtet wird.

Szenarien mit einer Domänen und mehreren Domänen

Wenn sich alle anmeldenden Benutzer und Rollengruppen sowie die verschachtelten Benutzergruppen in derselben Domäne befinden, müssen lediglich die Adressen der Domänen-Controller auf dem iDRAC6 konfiguriert werden. In diesem Szenario einer einfachen Domäne wird jede Art von Gruppe unterstützt.

Wenn die anmeldenden Benutzer und Rollengruppen oder eine verschachtelte Benutzergruppe mehreren Domänen angehören, müssen Global Catalog Server-Adressen auf dem iDRAC6 konfiguriert werden. In diesem Szenario mit mehreren Domänen müssen alle Rollengruppen und, wenn vorhanden, alle verschachtelten Benutzergruppen einer universellen Gruppe 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. Der Gruppenname muss entweder über die Webschnittstelle oder mit RACADM auf dem iDRAC6 eingerichtet werden (siehe"Konfiguration des Microsoft Active Directory mit Standardschema unter Verwendung der webbasierten iDRAC6-Schnittstelle" oder "Konfiguration des Microsoft Active Directory mit Standardschema unter Verwendung von RACADM").
3. Fügen Sie den Active Directory-Benutzer als ein Mitglied der Active Directory-Gruppe hinzu, um auf den iDRAC6 zuzugreifen.

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. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
4. Klicken Sie auf das Register **Netzwerk/Sicherheit** → Register **Verzeichnisdienst** → **Microsoft Active Directory**.
5. 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 **Schritt 1 von 4 Active Directory-Konfiguration und Verwaltung** wird angezeigt.
6. Markieren Sie unter **Zertifikat-Einstellungen** die Option **Überprüfung des Zertifikats aktivieren**, falls Sie das SSL-Zertifikat der Active Directory-Server überprüfen möchten; andernfalls gehen Sie zu Schritt 9**.**
7. 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.
8. Klicken Sie auf **Hochladen.**

   Die Zertifikatsinformationen für das gültige Active Directory-CA-Zertifikat werden angezeigt.
9. Geben Sie unter **Kerberos-Keytab hochladen** den Pfad der Keytab-Datei ein, oder suchen Sie die Datei mit der Suchfunktion. Klicken Sie auf **Hochladen**. Das Kerberos-Keytab wird in den iDRAC6 hochgeladen.
10. Klicken Sie auf **Weiter**, um zur Seite **Schritt 2 von 4 Active Directory- Konfiguration und Verwaltung)** zu wechseln.
11. Wählen Sie **Active Directory aktivieren**.
12. Wählen Sie **Einfache Anmeldung aktivieren**, wenn Sie sich bei iDRAC6 anmelden möchten, ohne Ihre Benutzeranmeldeinformationen für die Domäne, z. B. Benutzername und Kennwort, einzugeben.
13. Klicken Sie auf **Hinzufügen**, um den Benutzer-Domänennamen einzugeben.
14. Geben Sie den Namen der Benutzerdomäne in die Eingabeaufforderung ein und klicken Sie **OK**.
15. Geben Sie die **Zeitüberschreitung** in Sekunden ein, um anzugeben, wie lange der iDRAC6 auf Antworten des Active Directory wartet. Der Standardwert beträgt 120 Sekunden.

16. Wählen Sie die Option **Lookup von Domänen-Controllern mit DNS** aus, um die Active Directory-Domänen-Controller mittels einer DNS-Anfrage abzurufen. Die Domänen-Controller-Serveradressen 1-3 werden ignoriert. Wählen Sie **Benutzerdomäne über Anmeldung** aus, um die DNS-Anfrage mit dem Domänennamen des anmeldenden Benutzers auszuführen. 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 **Standardschema** ausgewählt ist, befinden sich die Domänen-Controller, wo sich die Benutzerkonten und Rollengruppen befinden.

17. 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. Es wird keine DNS-Anfrage ausgeführt. Geben Sie die IP-Adresse oder den vollständigen qualifizierten Domänennamen (FQDN) des Domänen-Controllers an. Wenn die Option **Domänen-Controller-Adressen angeben** ausgewählt wird, muss mindestens eine der drei Adresse konfiguriert werden. iDRAC6 versucht so lange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte. Wenn **Standardschema** ausgewählt ist, sind dies die Adressen der Domänen-Controller, wo sich die Benutzerkonten und 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.

18. Klicken Sie auf **Weiter**, um zur Seite **Schritt 3 von 4 Active Directory- Konfiguration und Verwaltung** zu wechseln.

19. Wählen Sie unter **Schemaauswahl** die Option **Standardschema** aus.

20. Klicken Sie auf **Weiter,** um zur **Seite Schritt 4a von 4 Active Directory- Konfiguration und Verwaltung** zu gehen.

21. 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 Global Catalog-Server des Active Directory verwendet werden soll. Global Catalog-Serveradressen 1-3 werden ignoriert. 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. Ein Global Catalog-Server ist nur für das Standardschema erforderlich, für den Fall, dass sich die Benutzerkonten und Rollengruppen auf verschiedenen Domänen befinden.

22. Wählen Sie die Option **Global Catalog-Serveradressen angeben** aus und geben Sie die IP-Adresse oder den vollständigen qualifizierten Domänennamen (FQDN) des Global Catalog-Servers ein. Es wird keine DNS-Anfrage ausgeführt. Es muss mindestens eine der drei Adressen konfiguriert werden. iDRAC6 versucht so lange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte. Ein Global Catalog-Server ist nur für das Standardschema erforderlich, für den Fall, dass 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 Global Catalog-Server 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 universelle Gruppe verwendet werden.

23. Klicken Sie unter **Rollengruppen** auf eine **Rollengruppe**.

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

24. Geben Sie den **Gruppennamen** der Rolle an.

    Der **Gruppenname** der Rolle identifiziert die Rollengruppe im Active Directory, die dem iDRAC zugeordnet ist.

25. Geben Sie die **Gruppendomäne** der Rolle an, d. h. die Domäne der Rollengruppe.

26. Geben Sie die **Rollengruppenberechtigungen** an, indem Sie die **Rollengruppenberechtigungsebene** auswählen. Wenn Sie zum Beispiel **Administrator** auswählen, werden alle Berechtigungen für diese Berechtigungsebene ausgewählt.

27. 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.**

28. Konfigurieren Sie, falls erforderlich, weitere Rollengruppen.

29. Klicken Sie auf **Fertig stellen**, um zur **Seite Active Directory- Konfiguration und Verwaltung** zurückzukehren.

30. Klicken Sie auf **Einstellungen überprüfen**, um die Einstellungen des Active Directory-Standardschemas zu prüfen.

31. Geben Sie Ihren iDRAC6-Benutzernamen und das Kennwort ein.

    Die Testergebnisse und das Testprotokoll werden angezeigt. Weitere Informationen finden Sie unter "Einstellungen testen".

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 **Remote-Zugriff**→ **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 <Bitmaskenwert für
   spezifische Benutzerberechtigungen>
   ```

   ANMERKUNG: Siehe Tabelle B-2 für Bitmasken-Zahlenwerte.

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController1 <Vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController2 <Vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController3 <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 "Aternativer Servername" des Zertifikats Ihres Domänen-Controllers übereinstimmen, wenn Sie die Überprüfung des Zertifikats aktiviert haben.

   ANMERKUNG: Geben Sie unbedingt den FQDN des Domänen-Controllers ein, *nicht* nur den FQDN der Domäne selbst. Geben Sie z. B. `servername.dell.com` ein und nicht `dell.com`.

   ANMERKUNG: Mindestens eine der 3 Adressen muss konfiguriert werden. iDRAC6 versucht so lange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte. Im Standardschema sind dies die Adressen der Domänen-Controller, auf denen sich die Benutzerkonten und die Rollengruppen befinden.

   ```
   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <Vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ```
   rracadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <Vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <Vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ANMERKUNG: Der Global Catalog-Server 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 universelle Gruppe 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 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 hochzuladen.

   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 finden Sie unter "SSL-Zertifikat der iDRAC6-Firmware importieren".

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

2. 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
   ```

3. 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>
```

4. 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 über Benutzerdomänen finden Sie unter "Verwendung des Microsoft Active Directory zur Anmeldung beim iDRAC6".

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 den Namen (z. B. benutzername@domäne.com) und das Kennwort eines Textbenutzers eingeben, um die Überprüfung durchzuführen. Je nach 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 möglichen Lösungen im Testprotokoll. Informationen zu den häufigsten Fehlermeldungen finden Sie unter "Häufig gestellte Fragen zu Active Directory".

Wenn Sie Ihre Einstellungen ändern müssen, wählen Sie das Register **Active Directory** und ändern Sie die Konfiguration Schritt für Schritt.

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.

1. Aktivieren Sie SSL auf jedem einzelnen Domänen-Controller, indem Sie das SSL-Zertifikat für jeden Controller installieren.
   a. Klicken Sie auf **Start**→ **Verwaltungstools**→ **Sicherheitsrichtlinie für Domänen**.
   b. Erweitern Sie den Ordner **Richtlinien öffentlicher Schlüssel,** klicken Sie mit der rechten Maustaste auf **Einstellungen der automatischen Zertifikatanforderung** und klicken Sie auf **Automatische Zertifikatanforderung**.
   c. Klicken Sie im **Assistenten für automatische Zertifikatanforderung** auf **Weiter** und wählen Sie **Domänen-Controller** aus.
   d. 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, können die folgenden Schritte abweichen.

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

1. Suchen Sie den Domänen-Controller, der den Microsoft Enterprise-CA- Dienst ausführt.
2. Wählen Sie **Start**→ **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** auf Windows 2000-Systemen**)** und wählen Sie **Snap-In hinzufügen/entfernen**.
5. Klicken Sie im Fenster **Snap-In hinzufügen/entfernen** auf **Hinzufügen**.
6. Wählen Sie im Fenster **Eigenständiges Snap-In** die Option **Zertifikate** aus und klicken Sie auf **Hinzufügen**.
7. Wählen Sie **Computer-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 Stamm-CA-Zertifikat, klicken Sie mit der rechten Maustaste darauf, wählen Sie **Alle Aufgaben** aus, und klicken Sie auf **Exportieren...**.

12. Klicken Sie im **Zertifikatexport-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" oder "Konfiguration des Microsoft Active Directory mit Standardschema unter Verwendung von RACADM".

    Um das Zertifikat über die Webschnittstelle hochzuladen, siehe "Konfiguration des Microsoft Active Directory mit erweitertem Schema unter Verwendung der webbasierten iDRAC6-Schnittstelle" oder "Konfiguration des Microsoft Active Directory mit Standardschema unter Verwendung der webbasierten iDRAC6-Schnittstelle".

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 versandt.

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 in der Liste aufgeführt ist, müssen Sie sie auf allen Ihren Domänen-Controllern installieren.

5. Klicken Sie auf **Weiter** und wählen Sie aus, ob Windows den Zertifikatspeicher automatisch aufgrund des Zertifikattyps auswählen oder nach einem Zertifikatspeicher Ihrer Wahl suchen soll.

6. Klicken Sie auf **Fertig stellen** und dann auf **OK**.

Verwendung des Microsoft Active Directory zur Anmeldung beim iDRAC6

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 Webschnittstelle einloggen und die Benutzerdomänen bereits konfiguriert sind, können Sie in einem Pulldown-Menü unter sämtlichen Benutzerdomänen wählen. Wenn Sie eine Benutzerdomäne aus dem Pulldown-Menü wählen, sollten Sie nur den Benutzernamen eingeben. Wenn Sie **Diesen iDRAC** wählen, können Sie sich nach wie vor als Active Directory-Benutzer anmelden, wenn Sie die zuvor beschriebene Anmeldesyntax "Verwendung des Microsoft Active Directory zur Anmeldung beim iDRAC6" verwenden.

Sie können sich auch unter Verwendung der Smart Card am iDRAC6 anmelden. Weitere Informationen finden Sie unter "Anmeldung am iDRAC6 über die Smart Card".

ANMERKUNG: Der Windows 2008 Active Directory-Server unterstützt nur die Zeichenkette <benutzername>@<domänenname> mit einer maximalen Länge von 256 Zeichen.

Verwendung des Microsoft Active Directory für die einfache Anmeldung

Sie können iDRAC6 aktivieren, um mithilfe von Kerberos, einem Netzwerk-Authentifizierungsprotokoll, die einfache Anmeldung zu ermöglichen. Weitere Informationen zur Einrichtung des iDRAC6 zur Verwendung der einfachen Anmeldung über Active Directory finden Sie unter "Kerberos-Authentifizierung aktivieren".

iDRAC6 zur Verwendung der einfachen Anmeldung konfigurieren

1. Klicken Sie auf **Remote-Zugriff**→ Register **Netzwerk/Sicherheit** → Register **Verzeichnisdienst** → **Microsoft Active Directory**→ und wählen Sie **Active Directory konfigurieren** aus.

2. Wählen Sie auf der Seite **Schritt 2 von 4 Active Directory-Konfiguration und Verwaltung** die Option **Einfache Anmeldung aktivieren**. Die Option **Einfache Anmeldung aktivieren** wird nur aktiviert, wenn Sie die Option **Active Directory aktivieren** ausgewählt haben.

   Mit der Option **Einfache Anmeldung aktivieren** können Sie sich direkt nach der Anmeldung bei der Workstation beim iDRAC6 anmelden, ohne die Benutzeranmeldeinformationen 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 bereits konfiguriert haben, mit dem Sie sich unter Verwendung der Active Directory-Anmeldeinformationen beim iDRAC6 anmelden möchten. Der iDRAC6 verwendet die zwischengespeicherten Active Directory-Anmeldeinformationen, um Sie anzumelden.

   Zum Aktivieren der einfachen Anmeldung über die CLI führen Sie den RACADM-Befehl aus:

   ```
   racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
   ```

Anmelden beim iDRAC6 unter Verwendung der einfachen Anmeldung

1. Melden Sie sich mit Ihrem Netzwerkkonto bei der Workstation an.

2. Geben Sie Folgendes ein, um die iDRAC6-Webseite abzurufen:

   `https://<IP-Adresse>`

   Wenn die Standard-HTTPS-Anschlussnummer (Anschluss 443) geändert wurde, 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-Seite zur einfachen Anmeldung wird angezeigt.

3. Klicken Sie auf **Anmelden**.

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.

Allgemeiner LDAP-Verzeichnisdienst

iDRAC6 bietet eine allgemeine Lösung zur Unterstützung der LDAP-basierten Authentifizierung (Lightweight Directory Access Protocol). Für diese Funktion ist keine Schemaerweiterung in Ihren Verzeichnisdiensten 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 für den Verzeichnisdienst spezifische Maßnahme ist das Schema. Sie können beispielsweise unterschiedliche Attributnamen für die Gruppe, den Benutzer und die Verknüpfung zwischen dem Benutzer und der Gruppe haben.

Diese Maßnahmen können in iDRAC6 konfiguriert werden.

Anmeldesyntax (Verzeichnisbenutzer gegenüber lokalem Benutzer)

Anders als beim Active Directory werden Sonderzeichen ("@", "\" und "/") nicht verwendet, um einen LDAP-Benutzer von einem lokalen Benutzer zu unterscheiden. Der anmeldende Benutzer gibt nur den Benutzernamen ein und lässt den Domänennamen aus. iDRAC6 nimmt den Benutzernamen an, wie er erscheint, und unterteilt ihn nicht in Benutzername und Benutzerdomäne. Wenn das allgemeine LDAP aktiviert ist, versucht iDRAC6 zuerst, den Benutzer als Verzeichnisbenutzer anzumelden. Schlägt dieser Vorgang fehl, wird die Anfrage lokaler Benutzer aktiviert.

ANMERKUNG: Die Active Directory-Anmeldungssyntax weist keine Verhaltensänderung 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-Verzeichnisdiensts unter Verwendung der webbasierten iDRAC6-Schnittstelle

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
3. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
4. Klicken Sie auf die Register **Netzwerk/Sicherheit** → Register **Verzeichnisdienst** → **Allgemeiner LDAP-Verzeichnisdienst**.
5. Die Seite **Allgemeines LDAP - Konfiguration und Verwaltung** zeigt die aktuellen allgemeinen iDRAC6-LDAP-Einstellungen an. Verwenden Sie den Bildlauf, um an den unteren Rand der Seite **Allgemeines LDAP - Konfiguration und Verwaltung** zu gelangen und klicken Sie auf **Allgemeines LDAP konfigurieren**.

   ANMERKUNG: In dieser Version wird nur das Active Directory mit Standardschema (SSAD) ohne Erweiterungen unterstützt.

   Die Seite **Schritt 1 von 3 Allgemeines LDAP - Konfiguration und Verwaltung** wird angezeigt. Verwenden Sie diese Seite, um das digitale Zertifikat zu konfigurieren, das beim Kommunizieren mit einem allgemeinen LDAP-Server während der Initiierung von SSL-Verbindungen verwendet wird. Für diese Kommunikationen wird LDAP-über-SSL (LDAPS) verwendet. Wenn Sie die Zertifikatsüberprüfung aktivieren, laden Sie das Zertifikat der Zertifizierungsstelle hoch, die das Zertifikat ausgegeben hat, das vom LDAP-Server während der Initiierung von SSL-Verbindungen verwendet wird. Das Zertifizierungsstellenzertifikat wird verwendet, um die Authentizität des Zertifikats zu überprüfen, das während der SSL-Initiierung vom LDAP-Server bereitgestellt wird.

   ANMERKUNG: In dieser Version wird ein nicht auf einem SSL-Anschluss basierendes LDAP-Bind nicht unterstützt. Es wird nur LDAP-über-SSL unterstützt.

6. Markieren Sie unter **Zertifikatseinstellungen** die Option **Zertifikatsüberprüfung** aktivieren, um die Zertifikatsüberprüfung zu aktivieren. Wenn aktiviert, verwendet iDRAC6 das Zertifizierungsstellenzertifikat zum Überprüfen des LDAP- Serverzertifikats während des SSL-Handshake (Secure Socket Layer); wenn deaktiviert, überspringt iDRAC6 den Schritt der Zertifikatsüberprüfung beim SSL-Handshake. Sie können die Zertifikatsüberprüfung während des Testens deaktivieren, oder wenn Ihr Systemadministrator den Domänen-Controllern im Sicherheitsbereich ohne Überprüfen ihrer SSL-Zertifikate vertraut.

VORSICHT: Stellen Sie sicher, dass während der Zertifikatserstellung im Subjektfeld des LDAP-Serverzertifikats CN = open LDAP FQDN eingestellt ist (Beispiel: CN= openldap.lab). Das LDAP-Serveradressfeld in iDRAC6 muss so eingestellt werden, dass es mit der FQDN-Adresse übereinstimmt, damit die Zertifikatsüberprüfung funktionieren kann.

7. Geben Sie unter **CA-Zertifikat für den Verzeichnisdienst hochladen** 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.

8. Klicken Sie auf **Hochladen.**

   Das Zertifikat der Stamm-Zertifizierungsstelle, die alle SSL-Serverzertifikate (Security Socket Layer) des Domänen-Controllers unterzeichnet, wird hochgeladen.

9. Klicken Sie auf **Weiter**, um zur Seite **Schritt 2 von 3 Allgemeines LDAP - Konfiguration und Verwaltung** zu wechseln. Verwenden Sie diese Seite, um Standortinformationen zu allgemeinen LDAP-Servern und Benutzerkonten zu konfigurieren.

   ANMERKUNG: In dieser Version werden Smart Card-basierte Zweifaktor-Authentifizierung (TFA) und einfache Anmeldung (SSO) nicht für den allgemeinen LDAP-Verzeichnisdienst unterstützt.

10. Wählen Sie **Allgemeines LDAP aktivieren** aus.

    ANMERKUNG: In dieser Version werden verschachtelte Gruppen nicht unterstützt. Die Firmware sucht nach dem direkten Mitglied der Gruppe, um den Benutzer-DN abzugleichen. Es werden außerdem nur einfache Domänen unterstützt. Cross Domains werden nicht unterstützt.

11. Markieren Sie die Option **Abgegrenzten Namen zum Suchen nach Gruppenmitgliedschaft verwenden**, um den abgegrenzten Namen (DN) als Gruppenmitglieder zu verwenden. iDRAC6 vergleicht den aus dem Verzeichnis abgerufenen Benutzer-DN mit den Mitgliedern der Gruppe. Wenn nicht markiert, wird der vom anmeldenden Benutzer angegebene Benutzername für den Vergleich mit den Mitgliedern der Gruppe verwendet.

12. Geben Sie in das Feld **LDAP-Serveradresse** den vollständigen qualifizierten Domänennamen (FQDN) oder die IP-Adresse des LDAP- Servers ein. Sie können mehrere redundante LDAP-Server festlegen, die derselben Domäne dienen, indem Sie eine Liste bereitstellen, in der alle Server durch Kommas getrennt aufgeführt sind. iDRAC6 versucht so lange, nacheinander mit jedem Server eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte.

13. Geben Sie den für LDAP-über-SSL verwendeten Anschluss im Feld **LDAP- Serveranschluss** ein. Die Standardeinstellung lautet 636.

14. Geben Sie in das Feld **Bind-DN** den DN eines Benutzers ein, der zum Binden an den Server verwendet wird, wenn nach dem DN des anmeldenden Benutzers gesucht wird. Wenn nicht angegeben, wird ein anonymes Bind verwendet.

15. Geben Sie das **Bind-Kennwort** ein, das in Verbindung mit dem **Bind-DN** verwendet werden soll. Dies ist erforderlich, wenn kein anonymes Bind zulässig ist.

16. Geben Sie in das Feld **Gesuchter Base-DN** den DN der Teilstruktur des Verzeichnisses ein, von dem sämtliche Suchen ausgehen sollten.

17. Geben Sie in das Feld **Benutzeranmeldungsattribut** das Benutzerattribut ein, das gesucht werden soll. Die Standardeinstellung lautet UID. Es wird empfohlen, dass dies innerhalb der ausgewählten Base-DN eindeutig ist, da ansonsten ein Suchfilter konfiguriert werden muss, um die Eindeutigkeit des anmeldenden Benutzers zu gewährleisten. Wenn der Benutzer-DN nicht eindeutig durch die Suchkombination von Attribut und Suchfilter identifiziert werden kann, schlägt die Anmeldung fehl.

18. Geben Sie im Feld **Attribut der Gruppenmitgliedschaft** an, welches LDAP-Attribut zum Überprüfen auf Gruppenmitgliedschaft verwendet werden soll. Hierbei sollte es sich um ein Attribut der Gruppenklasse handeln. Wenn nicht angegeben, verwendet iDRAC6 die Attribute *Mitglied* und *Eindeutiges Mitglied*.

19. Geben Sie in das Feld **Suchfilter** einen gültigen LDAP-Suchfilter ein. Verwenden Sie den Filter, wenn das Benutzerattribut den anmeldenden Benutzer innerhalb des ausgewählten Base-DN nicht eindeutig identifizieren kann. Wenn nicht angegeben, wird der Wert automatisch auf *objectClass=** eingestellt, was bewirkt, dass nach allen Objekten in der Struktur gesucht wird. Dieser zusätzliche, vom Benutzer konfigurierte Suchfilter gilt nur für die Benutzer-DN-Suche und nicht für die Gruppenmitgliedschaftssuche.

20. Klicken Sie auf **Weiter**, um zur Seite **Schritt 3a von 3 Allgemeines LDAP - Konfiguration und Verwaltung** zu wechseln. Verwenden Sie diese Seite, um die Berechtigungsgruppen zu konfigurieren, die für die Genehmigung von Benutzern verwendet werden. Wenn das allgemeine LDAP aktiviert ist, werden Rollengruppen verwendet, um die Genehmigungsregel 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.

21. Klicken Sie unter **Rollengruppen** auf eine **Rollengruppe**.

    Die **Seite Schritt 3b von 3 Allgemeines LDAP - Konfiguration und Verwaltung** wird angezeigt. Verwenden Sie diese Seite zur Konfiguration der einzelnen Rollengruppen, die zur Steuerung der Genehmigungsregel für Benutzer verwendet werden.

22. Geben Sie den **Abgegrenzten Gruppennamen [DN]** ein, der die Rollengruppe im allgemeinen LDAP-Verzeichnisdienst identifiziert, der mit dem iDRAC6 in Verbindung steht.

23. Geben Sie im Abschnitt **Rollengruppenberechtigungen** die mit der Gruppe verknüpften Berechtigungen 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 führt Sie automatisch zur Seite **Schritt 3a von 3 Allgemeines LDAP - Konfiguration und Verwaltung zurück, wo Ihre Rollengruppeneinstellungen angezeigt werden.**

25. Konfigurieren Sie zusätzliche Rollengruppen je nach Bedarf.

26. Klicken Sie auf **Finish**, um zur Zusammenfassungs**seite Allgemeines LDAP - Konfiguration und Verwaltung** zurückzuwechseln.

27. Klicken Sie auf **Testeinstellungen**, um die allgemeinen LDAP-Einstellungen zu überprüfen.

28. Geben Sie den Benutzernamen und das Kennwort eines Verzeichnisbenutzers ein, der dazu ausgewählt wurde, die LDAP- Einstellungen zu testen. Das Format hängt davon ab, welches *Benutzeranmeldungsattribut* verwendet wird, und der eingegebene Benutzername muss mit dem Wert des ausgewählten Attributs übereinstimmen.

    Die Testergebnisse und das Testprotokoll werden angezeigt. Sie haben die Konfiguration des allgemeinen LDAP-Verzeichnisdiensts abgeschlossen.

Konfiguration des allgemeinen LDAP-Verzeichnisdiensts unter Verwendung von RACADM

```
racadm config -g cfgldap -o cfgLdapEnable 1
```

```
racadm config -g cfgldap -o cfgLdapServer <FQDN oder IP-Adresse>

racadm config -g cfgldap -o cfgLdapPort <Anschlussnummer>

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 nachstehenden 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

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.

SSO arbeitet jetzt mit iDRAC6.

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 **Remote-Zugriff**→ 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 der iDRAC6 bei bestehender SSL-Verbindung mit dem Server das hochgeladene CA-Zertifikat zur Überprüfung des Active Directory Server-Zertifikats. Die häufigsten Gründe für das Scheitern der Zertifikatvalidierung 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 Host-Namen (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 Global Catalog-Adressen konfigurieren?

Wenn Sie ein erweitertes Schema verwenden, wird die Global Catalog-Adresse nicht verwendet.

Wenn Sie das Standardschema verwenden und Benutzer und Rollengruppen verschiedenen Domänen angehören, sind Global Catalog-Adressen erforderlich. In diesem Fall kann nur die universelle Gruppe verwendet werden.

Wenn Sie das Standardschema verwenden und alle Benutzer und alle Rollengruppen derselben Domäne angehören, sind keine Global Catalog-Adressen 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 Global Controller-Adresse(n) konfiguriert sind, fragt iDRAC6 weiterhin den Global Catalog ab. Wenn zusätzliche Berechtigungen vom Global Catalog 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 erzwingt eine hohe Sicherheit, um die Identität des Domänen-Controllers, mit dem iDRAC6 eine Verbindung herstellt, zu gewährleisten. 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".

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 Gültigkeit des iDRAC6-Zertifikats mit dem 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 erweiterten Schema arbeiten, prüfen Sie, ob der **Gruppenname** und **Gruppendomänenname** mit der Konfiguration in Ihrem Active Directory übereinstimmen.

3. Überprüfen Sie die SSL-Zertifikate des Domain-Controllers, um sicherzustellen, dass die iDRAC6-Zeit innerhalb der Gültigkeitsdauer des Zertifikats liegt.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Smart Card-Authentifizierung konfigurieren

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Der iDRAC6 unterstützt Zweifaktor-Authentifizierung (TFA), wenn die **Smart Card-Anmeldung** aktiviert ist.

Für herkömmliche Authentifizierungsschemata werden der Benutzername und das Kennwort zur Authentifizierung 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.

Smart Card-Anmeldung am iDRAC6 konfigurieren

Wechseln Sie zum Aktivieren der iDRAC6-Funktion Smart Card-Anmeldung über die webbasierte Schnittstelle zu **Remote-Zugriff**→ **Netzwerk/Sicherheit**→ **Smart Card und wählen Sie Aktivieren** aus.

Wenn Sie:

- **Aktivieren** oder **Mit Remote-Racadm aktivieren** auswählen, werden Sie bei allen nachfolgenden Anmeldeversuchen über die webbasierte Schnittstelle zu einer Smart Card-Anmeldung aufgefordert.

  Wenn Sie **Aktivieren** auswählen, werden alle bandexternen CLI-Schnittstellen (Befehlszeilenoberfläche), z. B. Telnet, SSH, serieller, Remote-RACADM und IPMI-über-LAN deaktiviert, weil diese Dienste nur Einzelfaktor-Authentifizierung unterstützen.

  Wenn Sie **Mit Remote-Racadm aktivieren** auswählen, werden alle bandexternen CLI-Schnittstellen außer Remote-RACADM deaktiviert.

  ANMERKUNG: Dell empfiehlt iDRAC6-Administratoren, die Einstellung **Mit Remote-Racadm aktivieren** nur zu verwenden, 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.

- Smart Card-Konfiguration **deaktivieren** (Standardeinstellung). Diese Auswahloption deaktiviert die TFA-Smart Card-Anmeldefunktion. Sie werden bei der nächsten Anmeldung an der iDRAC6-GUI aufgefordert, einen Microsoft® Active Directory®- oder lokalen Anmelde-Benutzernamen und ein Kennwort einzugeben. Die Webschnittstelle verwendet diese Standard-Anmeldeaufforderung.
- **CRL-Prüfung für Smart Card-Anmeldung aktivieren**, das iDRAC-Zertifikat des Benutzers, das vom CRL-Verteilungsserver (Certificate Revocation List, Zertifikatsperrliste) heruntergeladen wird, wird in der CRL auf Widerrufung überprüft.

  ANMERKUNG: Die CRL-Verteilungsserver werden in den Smart Card-Zertifikaten der Benutzer aufgeführt.

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 **Remote-Zugriff**→ **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.

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 das CA-Zertifikat ebenfalls in eine Datei mit 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

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".

ANMERKUNG: Wenn der Smart Card-Benutzer im Active Directory vorhanden ist, werden sowohl ein Active Directory-Kennwort als auch eine Smart Card-PIN benötigt.

Sie können das Active Directory über **Remote-Zugriff→ Netzwerk/Sicherheit→ Verzeichnisdienst→Microsoft Active Directory** konfigurieren.

Smart Card konfigurieren

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

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf **Smart Card**.
3. Konfigurieren Sie die Einstellungen für die Smart Card-Anmeldung.

   Tabelle 8-1 enthält Informationen über die Einstellungen der Seite **Smart Card**.
4. 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 sind auf ihre Standardeinstellungen gesetzt. ▪ **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. ▪ **Mit Remote-Racadm aktiviert** - Aktiviert die Smart Card-Anmeldung zusammen mit Remote-RACADM. Alle anderen bandexternen CLI-Schnittstellen werden deaktiviert. **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.
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. 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 **Remote-Zugriff→ 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-Plug-in 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>`

   Wenn die Standard-HTTPS-Anschlussnummer (Anschluss 443) geändert wurde, 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>`

   Wenn die Standard-HTTPS-Anschlussnummer (Anschluss 443) geändert wurde, 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 ein und klicken Sie auf **Anmeldung**.

   Das PIN-Popup-Dialogfeld wird angezeigt.

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

4. Geben Sie zur Authentifizierung des Benutzers das Active Directory- Benutzerkennwort ein und klicken Sie auf **OK**.

   Sie werden über Ihre in Active Directory festgelegten Anmeldeinformationen beim iDRAC6 angemeldet.

ANMERKUNG: Wenn der Smart Card-Benutzer in Active Directory vorhanden ist, werden sowohl ein Active Directory-Kennwort als auch eine Smart Card-PIN benötigt. In zukünftigen Versionen wird das Active Directory-Kennwort u. U. nicht mehr erforderlich sein.

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 Plug-in kann das Smart Card-Laufwerk nicht erkennen.

Stellen Sie sicher, dass die Smart Card auf dem Microsoft Windows®-Betriebssystem unterstützt wird. Windows unterstützt nur eine beschränkte Anzahl von Smart Card-Krytographiedienstanbieter.

Tipp: Sie können generell überprüfen, ob die Smart Card-Krytographiedienstanbieter auf einem bestimmten Client vorhanden sind, indem Sie die Smart Card bei der Windows-Anmeldung (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 erhalten.

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 cfgActiveDirectory -o cfgADSmartCardLogonEnable 0`
- 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 vKVM-Sitzung 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. Details finden Sie in 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 von einander abweichen. Sie können die **RAC-Zeit** auf der Seite **System→ Remote-Zugriff→ Eigenschaften→ iDRAC-Informationen** und die Domänen-Controller-Zeit nachprüfen, indem Sie mit der rechten Maustaste in die rechte untere Ecke des Bildschirms klicken. Der Zeitzonenoffset wird in der Popup-Anzeige dargestellt. Für US Central Standard Time (CST) ist dies -6. Verwenden Sie den folgenden Befehl für den RACADM-Zeitzonenoffset, um die iDRAC6-Zeit zu synchronisieren (durch Remote- oder Telnet/SSH-RACADM): `racadm config -g cfgRacTuning –o cfgRacTuneTimeZoneOffset <Offset-Wert in Minuten>`. Wenn die Systemzeit z. B. GMT -6 (US CST) ist und die Uhrzeit 14:00 Uhr, stellen Sie die iDRAC6-Zeit auf die GMT-Zeit von 18:00 Uhr, wozu Sie "360" in den oben aufgeführten Befehl für den Offset eingeben müssen. Sie können auch *cfgRacTuneDaylightoffset* verwenden, um die Sommerzeitdifferenz zu berücksichtigen. Hierdurch können Sie vermeiden, jedes Jahr zu diesen beiden Anlässen die Zeit umzustellen, wenn die Zeitumstellung vorgenommen wird, oder berücksichtigen Sie sie im Offset des oben aufgeführten Beispiels einfach, indem Sie "300" wählen.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

GUI-Konsolenumleitung verwenden

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.3-Benutzerhandbuch

Dieser Abschnitt enthält Informationen über die Verwendung der iDRAC6-Konsolenumleitungsfunktion.

Übersicht

Mit der iDRAC6-Konsolenumleitungsfunktion können Sie im Remote-Zugriff im grafischen Modus oder Textmodus auf die lokale Konsole zugreifen. Mittels der Konsolenumleitung können Sie ein oder mehrere iDRAC6-aktivierte Systeme von einem 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 mit anderen teilen, im Remote-Zugriff und sofort.

Konsolenumleitung verwenden

ANMERKUNG: Wenn Sie eine Konsolenumleitungssitzung öffnen, zeigt der verwaltete Server nicht an, dass die Konsole umgeleitet wurde.

ANMERKUNG: Wenn bereits eine Konsolenumleitungssitzung von der Management Station zum iDRAC6 offen ist, führt ein Versuch, eine neue Sitzung von derselben Management Station zum selben iDRAC6 zu öffnen, dazu, dass die bestehende Sitzung aktiviert wird. Es wird keine neue Sitzung hergestellt.

ANMERKUNG: Von einer Management Station können mehrere Konsolenumleitungen zu mehreren iDRAC6-Controllern gleichzeitig geöffnet werden.

Die Seite **Konsolenumleitung** ermöglicht Ihnen, das Remote-System zu verwalten, indem Sie Tastatur, Video und Maus auf Ihrer lokalen Management Station verwenden, um die entsprechenden Geräte auf dem 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 eine Konsolenumleitungssitzung:

- Es können maximal vier gleichzeitige Konsolenumleitungssitzungen unterstützt werden. Alle Sitzungen zeigen dieselbe verwaltete Serverkonsole gleichzeitig an.
- Zwei Sitzungen können von derselben Client-Konsole (Management Station) aus für einen Remote-Server geöffnet werden (eine pro Plugin-Typ). Es sind mehrere Sitzungen zu mehreren Remote-Servern von demselben Client aus möglich.
- Eine Konsolenumleitungssitzung darf nicht über einen Webbrowser auf dem verwalteten System gestartet werden.
- Die erforderliche verfügbare Netzwerk-Mindestbandbreite beträgt 1 MB/s.

Die erste Konsolenumleitungssitzung zum iDRAC6 ist eine Sitzung mit vollem Zugriff. Wenn ein zweiter Benutzer eine Konsolenumleitungssitzung anfordert, wird der erste Benutzer entsprechend benachrichtigt und erhält die Option, eine Freigabe-Anforderung an den zweiten Benutzer zu senden. Der zweite Benutzer wird benachrichtigt, dass ein anderer Benutzer die Steuerung hat.

Management Station konfigurieren

Zur Verwendung der Konsolenumleitung auf der Management Station führen Sie die folgenden Maßnahmen durch:

1. Installieren und konfigurieren Sie einen unterstützten Webbrowser. Weitere Informationen finden Sie in den folgenden Abschnitten:
   - "Unterstützte Webbrowser"
   - "Konfiguration eines unterstützten Webbrowsers"
2. Wenn Sie Firefox verwenden oder den Java® Viewer mit Internet Explorer verwenden möchten, müssen Sie eine Java-Laufzeitumgebung (JRE) installieren. Wenn Sie den Internet Explorer-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:

     Do not save encrypted pages to disk (Speichern Sie keine verschlüsselten Seiten auf das Laufwerk.)

4. Wenn Sie IE zum Starten einer vKVM-Sitzung 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.

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 iDRAC6-KVM <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 vKVM 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.

So löschen Sie ältere Versionen von Active-X-Viewer für IE6:

1. Öffnen Sie die Eingabeaufforderung und ändern Sie das Verzeichnis zu WINDOWS\Downloaded Program Files (Heruntergeladene Programmdateien).

2. Führen Sie **regsvr32 /u VideoViewer.ocx** aus.

3. Löschen Sie die folgenden Dateien: AvctKeyboard.dll, AvctVirtualMediaDE.dll, AvctVirtualMediaES.dll, AvctVirtualMediaFR.dll, AvctVirtualMediaJA.dll, AvctVirtualMediaZH.dll, VideoViewerDE.dll, VideoViewerES.dll, VideoViewerFR.dll, VideoViewerJA.dll, VideoViewerZH.dll und VirtualMediaDLL.dll.

4. Löschen Sie die Add-ons für *Session Viewer* und/oder *Video Viewer*, die von Internet Explorer verwendet wurden.

So löschen Sie ältere Versionen von Active-X-Viewer für IE7:

1. Schließen Sie den Video Viewer und den Internet Explorer-Browser.

2. Öffnen Sie den Internet Explorer-Browser wieder, wechseln Sie zu **Internet Explorer→ Extras→ Add-ons verwalten** und klicken Sie auf **Add-ons aktivieren oder 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 *Video Viewer*-Add-on.

So löschen Sie ältere Versionen von Active-X-Viewer für IE8:

1. Schließen Sie den Video Viewer und den Internet Explorer-Browser.

2. Öffnen Sie den Internet Explorer-Browser wieder, wechseln Sie zu **Internet Explorer→ Extras→ Add-Ons verwalten** und klicken Sie auf **Add-ons aktivieren oder 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 *Video Viewer*-Add-on aus und klicken Sie auf die Verknüpfung **Details**.

5. Wählen Sie aus dem Fenster **Details** die Option **Entfernen** aus.

6. Schließen Sie die Fenster **Details** und **Add-ons verwalten**.

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

1. Führen Sie bei Eingabeaufforderung `javaws-viewer` oder `javaws- uninstall` aus

2. Der **Java Cache-Viewer** wird angezeigt.

3. Löschen Sie die Elemente mit der Bezeichnung *iDRAC6 Console Redirection Client (iDRAC6-Konsolenumleitungs-Client)*.

Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

Tabelle 10-1 listet die unterstützten Bildschirmauflösungen und entsprechenden Bildwiederholfrequenzen für eine Konsolenumleitungssitzung auf, die auf dem verwalteten Server ausgeführt wird.

Tabelle 10-1. Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

Bildschirmauflösung	Bildwiederholfrequenz (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60

Konsolenumleitung auf der iDRAC6-Webschnittstelle konfigurieren

Um auf der iDRAC6-Webschnittstelle eine Konsolenumleitung zu konfigurieren, führen Sie folgende Schritte aus:

1. Klicken Sie auf **System**→ **Konsole/Datenträger**→ **Konfiguration**, um die iDRAC-Konsolenumleitungseinstellungen zu konfigurieren.
2. Konfigurieren Sie die Konsolenumleitungseigenschaften. Tabelle 10-2 beschreibt die Einstellungen für die Konsolenumleitung.
3. Wenn Sie fertig sind, klicken Sie auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 10-3.

Tabelle 10-2. Eigenschaften der Konsolenumleitungskonfiguration

Eigenschaft	Beschreibung
Aktiviert	Klicken Sie, um die Konsolenumleitung zu aktivieren oder zu deaktivieren. Wenn diese Option markiert ist, zeigt dies an, dass die Konsolenumleitung aktiviert ist. Die Standardoption ist **Aktiviert**. **ANMERKUNG:** Das Aktivieren oder Löschen der Option **Aktiviert** nach dem Start der virtuellen KVM-Sitzung kann zur Unterbrechung aller vorhandenen virtuellen KVM-Sitzungen führen.
Max. Sitzungen	Zeigt die Anzahl der maximal möglichen Konsolenumleitungssitzungen an: 1 bis 4. Verwenden Sie das Dropdown-Menü, um die maximal zulässigen Konsolenumleitungssitzungen zu ändern. Die Standardeinstellung ist **2.**
Aktive Sitzungen	Zeigt die Anzahl der Sitzungen aktiver Konsolen an. Dieses Feld ist schreibgeschützt.
Remote-Präsenz-Anschluss	Die Netzwerkanschlussnummer, die zur Verbindung mit der Tastatur/Maus-Option der Konsolenumleitung 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 KVM-Sitzung kann zur Unterbrechung aller vorhandenen virtuellen KVM-Sitzungen 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 KVM-Sitzung kann zur Unterbrechung aller vorhandenen virtuellen KVM-Sitzungen führen.
Lokales Servervideo aktiviert	Die Markierung weist darauf hin, dass die Ausgabe an den iDRAC6-KVM-Monitor während der Konsolenumleitung deaktiviert wird. Hierdurch wird sichergestellt, dass die unter Verwendung der **Konsolenumleitung** ausgeführten Aufgaben auf dem lokalen Monitor des verwalteten Servers nicht sichtbar sind.
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: Für Informationen zur Verwendung des virtuellen Datenträgers mit Konsolenumleitung, siehe Virtuellen Datenträger konfigurieren und verwenden.

Die Schaltflächen in Tabelle 10-3 sind auf der Seite **Konfiguration** verfügbar.

Tabelle 10-3. Schaltflächen der Konfigurationsseite

Schaltfläche	Definition
Drucken	Druckt die Seite aus
Aktualisieren	Lädt die Seite **Konfiguration** neu
Anwenden	Speichert neue oder geänderte Einstellungen

Konsolenumleitungssitzung öffnen

Wenn Sie eine Konsolenumleitungssitzung öffnen, startet die Dell™ Virtual KVM Viewer-Anwendung, und der Desktop des Remote-Systems wird im Viewer eingeblendet. Über die Virtual KVM Viewer-Anwendung können die Maus- und Tastaturfunktionen des Remote-Systems von der lokalen Management Station aus gesteuert werden.

ANMERKUNG: Der vKVM-Start von einer Windows Vista®-Management Station kann Neustartmeldungen des vKVM hervorrufen. Sie können dies vermeiden, indem Sie die entsprechenden Zeitüberschreitungswerte an den folgenden Stellen einstellen: **Systemsteuerung→Energieoptionen→Energiesparmodus→Erweiterte Einstellungen→ Festplatte→ Festplatte ausschalten nach <Zeitüberschreitung>** und unter **Systemsteuerung→ Energieoptionen→ Hochleistung→ Erweiterte Einstellungen→ Festplatte→ Festplatte ausschalten nach <Zeitüberschreitung>**.

Führen Sie folgende Schritte aus, um auf der Webschnittstelle eine Konsolenumleitungssitzung zu öffnen:

1. Klicken Sie auf **System→ Konsole/Datenträger→ Konsolenumleitung und virtueller Datenträger**.
2. Verwenden Sie die Information in Tabelle 10-4, um sicherzustellen, dass eine Konsolenumleitungssitzung verfügbar ist.

   Falls Sie einige der angezeigten Eigenschaftswerte neu konfigurieren möchten, finden Sie entsprechende Informationen unter Konsolenumleitung auf der iDRAC6-Webschnittstelle konfigurieren.

Tabelle 10-4. Konsolenumleitung

Eigenschaft	Beschreibung
Konsolenumleitung aktiviert	Ja/Nein (markiert\unmarkiert)
Videoverschlüsselung aktiviert	Ja/Nein (markiert\unmarkiert)
Max. Sitzungen	Zeigt die maximale Anzahl unterstützter Konsolenumleitungssitzungen an.
Aktive Sitzungen	Zeigt die aktuelle Anzahl aktiver Konsolenumleitungssitzungen an
Lokales Servervideo aktiviert	Ja = Aktiviert; Nein = Deaktiviert.
Remote-Präsenz-Anschluss	Die Netzwerkanschlussnummer, die zur Verbindung mit der Tastatur/Maus-Option der Konsolenumleitung 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:** Bei 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 korrekten Installieren und Ausführen des Active-X-Plugin die 32-Bit-Version des "Microsoft Visual C++ 2005 SP1 Redistributable Package (x86)" bereit. Dieses Paket ist zum Starten der vKVM-Sitzung auf auf einem Internet Explorer-Browser erforderlich.

ANMERKUNG: Für Informationen zur Verwendung des virtuellen Datenträgers mit Konsolenumleitung, siehe Virtuellen Datenträger konfigurieren und verwenden.

Die Schaltflächen in Tabelle 10-5 sind auf der Seite **Konsolenumleitung und Virtuelle Medien** verfügbar.

Tabelle 10-5. Schaltflächen der Seite "Konsolenumleitung und virtueller Datenträger"

Schaltfläche	Definition
Aktualisieren	Lädt die Seite **Konsolenumleitung und virtueller Datenträger** neu.
Viewer starten	Öffnet eine Konsolenumleitungssitzung auf dem Remote-Zielsystem.
Drucken	Druckt die Seite **Konsolenumleitung und virtueller Datenträger** aus.

3. Wenn eine Konsolenumleitungssitzung verfügbar ist, klicken Sie auf **Viewer starten**.

   ANMERKUNG: Es ist möglich, dass nach dem Starten der Anwendung mehrere Dialogfelder eingeblendet werden. 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 mit **Sicherheitswarnung**en 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 iDRAC6-KVM-Viewer-Anwendung angezeigt.

4. Zwei Mauszeiger erscheinen im Viewer-Fenster: einer für das Remote- System und einer für das lokale System. Sie können durch Auswahl der Option **Einzel-Cursor** unter **Extras** im iDRAC6-KVM-Menü auf einen Einzel-Cursor umschalten.

---

iDRAC6-KVM (Video Viewer) verwenden

Der iDRAC6-KVM (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 der iDRAC6-KVM in einem separaten Fenster gestartet.

ANMERKUNG: Wird der Remote-Server ausgeschaltet, wird die Meldung **Kein Signal** angezeigt.

Der iDRAC6-KVM 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 Konsolenumleitung und virtueller Datenträger** auf **Hilfe**.

Wenn Sie eine Konsolenumleitungssitzung starten und der iDRAC6-KVM angezeigt wird, ist es eventuell notwendig, die Mauszeiger zu synchronisieren.

Tabelle 10-6 beschreibt die Menüoptionen, die im Viewer zur Verfügung stehen.

Tabelle 10-6. Auswahlmöglichkeiten auf der Viewer-Menüleiste

Menüelement	Element	Beschreibung
"Reißzwecken"-Symbol	-	Klicken Sie auf das "Reißzwecken"-Symbol, um die iDRAC6-KVM-Menüleiste zu sperren. Hierdurch wird verhindert, dass 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 Gerät virtualisieren, indem Sie die Option in der Spalte **Zugeordnet** markieren. Das Gerät wird jetzt dem Server zugeo rückgängig gemacht werden, indem Sie die Markierung des Kontrollkästchens aufheben. Die Schaltfläche **Details** zeigt ein Feld an, das die virtuellen Geräte aufführt und auch die Lese-/Schreibaktivität für die
Extras	Sitzungsoptionen	Das Fenster "Sitzungsoptionen" bietet zusätzliche Steuerungseinstellungen für den Session Viewer. Dieses Fenster er **Maus**. Sie können den **Modus Tastaturdurchgang** über das Register Allgemein steuern. Wählen Sie **Alle Tastenanschläge ar** Tastenanschläge der Management Station an das Remote-System durchzureichen. Das Maus-Register enthält zwei Abschnitte: **Einzel-Cursor** und **Mausbeschleunigung**. Die Funktion **Einzel-Cursor** wird Mausausrichtungsprobleme auf einigen Remote-Betriebssystemen auszugleichen. Sobald der Viewer in den Modus **Ein** Mauszeiger im Viewer-Fenster blockiert. Drücken Sie die Terminierungstaste, um diesen Modus zu beenden. Wählen S 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 S Client-Cursor ist ebenso im Viewer-Frame blockiert. Der Benutzer wird nicht in der Lage sein, den Cursor außerhalb de bis er die **Terminierungstaste** drückt, wie im Register **Sitzungsoptionen** - **Maus** angegeben.
	Statistik	Diese Menüoption startet einen Dialog, der Leistungsstatistiken für den Viewer anzeigt. Die angezeigten Werte sind: - Frame-Rate - Bandbreite - Komprimierung - Paketrate
Datei	In Datei erfassen	Erfasst den aktuellen Remote-Systembildschirm in einer **.bmp**-Datei auf Windows oder in einer **.png**-Datei auf Linux. Ei dem Sie die Datei an einem angegebenen Standort speichern können. **ANMERKUNG:** Das **.bmp**-Dateiformat auf Windows oder das **.png**-Dateiformat auf Linux gelten nur für das systemeige unterstützt nur die Dateiformate **.jpg** und **.jpeg**.
	Beenden	Wenn Sie die Konsole nicht mehr verwenden und sich abgemeldet haben (hierzu den Abmeldevorgang des Remote-Sy Menü **Datei** die Option **Beenden** aus, um das Fenster **iDRAC6-KVM** zu schließen.
	Makros	Wenn Sie ein Makro auswählen oder den für das Makro angegebenen Hotkey eingeben, wird die Maßnahme auf dem I iDRAC6-KVM bietet die folgenden Makros: - Alt+Strg+Entf - Alt+Tab - Alt+Esc - Strg+Esc - Alt+Leertaste - Alt+Eingabe - Alt+Bindestrich - Alt+F4

		ı Druck ı Alt+Druck ı F1 ı Pause ı Tabulatortaste ı Strg+Eingabe ı SysRq ı Alt+LUmsch+RUmsch+Esc ı Strg+Alt+Rücktaste ı Alt+F? (Wobei F? für die Tasten F1-F12 steht) ı Strg+Alt+F? (Wobei F? für die Tasten F1-F12 steht)
Strom	System EINschalten	Schaltet das System ein.
	System AUSschalten	Schaltet das System aus.
	Ordentliches Herunterfahren	Fährt das System herunter.
	Softwareneustart	Startet das System neu, ohne es auszuschalten.
	Hardwareneustart	Schaltet das System aus und startet es dann erneut.
Hilfe	Inhalt und Index	Bietet Anleitungen dazu, wie die Onlinehilfe anzuwenden ist.
	Info zu iDRAC6-KVM	Zeigt die **iDRAC6 KVM**-Version an.

Lokales Server-Video deaktivieren oder aktivieren

Sie können den iDRAC6 so konfigurieren, dass iDRAC6-KVM-Verbindungen 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 Konsolenumleitung auf** 1 konfigurieren.

ANMERKUNG: Beim Deaktivieren (Ausschalten) des lokalen Videos auf dem Server sind der Monitor, die Tastatur und die Maus, die an die iDRAC6-KVM 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), wählen Sie das Kontrollkästchen **Lokales Servervideo aktiviert** auf der Seite **Konfiguration** ab, 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**.

---

vKVM und virtuellen Datenträger im Remote- Zugriff starten

Sie können vKVM/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 vKVM/Viewer für den virtuellen Datenträger geleitet.

ANMERKUNG: Internet Explorer unterstützt Anmeldungen des Typs Lokal, Active Directory (AD), Smart Card (SC) und Einfache Anmeldung (SSO). Firefox unterstützt nur lokale und AD-Anmeldungen.

URL-Format

Wenn Sie `link<IP>/console` im Browser eingeben, müssen Sie je nach Anmeldekonfiguration eventuell das normale manuelle Anmeldeverfahren befolgen. Wenn SSO nicht aktiviert ist und die lokale, AD- oder SC-Anmeldung aktiviert ist, wird die jeweilige Anmeldeseite angezeigt. Wenn die Anmeldung erfolgreich verläuft, wird die vKVM/vMedia-Anzeige nicht gestartet. Sie werden stattdessen auf die iDRAC6-GUI-Startseite umgeleitet.

Allgemeine Fehlerszenarien

Tabelle 10-7 führt allgemeine Fehlerszenarien auf, sowie die Gründe für diese Fehler und das iDRAC6-Verhalten.

Tabelle 10-7. Fehlerszenarien

Fehlerszenarien	Grund	Verhalten

Anmeldung fehlgeschlagen	Sie haben entweder einen ungültigen 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 KVM/virtueller Datenträger ist nicht verfügbar.	Der iDRAC6-KVM-Viewer wurde nicht gestartet. Leitet zur iDRAC6-GUI-Startseite um.
Nicht ausreichende Berechtigungen	Sie verfügen nicht über die Berechtigungen für die Konsolenumleitung und den virtuellen Datenträger.	Der iDRAC6-KVM-Viewer wurde nicht gestartet und Sie werden zur GUI-Seite der Konsolen-/Datenträgerkonfiguration umgeleitet.
Konsolenumleitung deaktiviert	Konsolenumleitung ist auf dem System deaktiviert.	Der iDRAC6-KVM-Viewer wurde nicht gestartet und Sie werden zur GUI-Seite der Konsolen-/Datenträgerkonfiguration umgeleitet.
Unbekannte URL-Parameter ermittelt	Die eingegebene URL enthält undefinierte Parameter.	Die Meldung Seite nicht gefunden (404) wird angezeigt.

Häufig gestellte Fragen zur Konsolenumleitung

Tabelle 10-8 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 10-8. Konsolenumleitung verwenden: Häufig gestellte Fragen

Frage	Antwort
vKVM meldet sich nicht ab, wenn die bandexterne Web-GUI abgemeldet ist.	Die vKVM- und vMedia-Sitzungen bleiben auch dann aktiv, wenn die Websitzung abgemeldet ist. Schließen Sie die vMedia- und vKVM-Viewer-Anwendungen, um sich von der entsprechenden Sitzung abzumelden.
Kann eine neue Remote-Konsolenvideositzung gestartet werden, wenn das lokale Video auf dem Server ausgeschaltet ist?	Ja.
Warum dauert es 15 Sekunden, um das lokale Video auf dem Server auszuschalten, nachdem eine Anforderung 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 **Konsolenumleitungskonfiguration** der iDRAC6-Webschnittstelle angezeigt. Der RACADM-CLI-Befehl **racadm getconfig -g cfgRacTuning** zeigt den Status im Objekt **cfgRacTuneLocalServerVideo** an.
Ich kann vom Fenster Konsolenumleitung den unteren Teil des Systembildschirms nicht sehen.	Stellen Sie sicher, dass die Bildschirmauflösung der Management Station auf 1280 x 1024 eingestellt ist. Versuchen Sie, auch die Bildlaufleisten beim iDRAC6-KVM-Client zu verwenden.
Das Konsolenfenster ist entstellt.	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 KVM 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 Konsolenumleitungssitzung die richtige Maus für das Betriebssystem ausgewählt ist. Stellen Sie sicher, dass die Option **Einzel-Cursor** unter **Extras** im iDRAC6-KVM-Menü auf dem iDRAC6-KVM-Client ausgewählt ist. Der Standard ist der Doppel-Cursor-Modus.
Warum kann ich keine Tastatur oder Maus verwenden, während ich ein Microsoft-Betriebssystem mithilfe einer iDRAC6-Konsolenumleitung im Remote-Zugriff installiere?	Wenn Sie im Remote-Zugriff ein unterstütztes Microsoft-Betriebssystem auf einem System, auf dem die Konsolenumleitung im BIOS aktiviert ist, installieren, 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 Konsolenumleitung im BIOS ausschalten. Diese Nachricht wird durch Microsoft erstellt, um den Benutzer darauf hinzuweisen, dass die Konsolenumleitung aktiviert ist. Um sicherzustellen, dass diese Meldung nicht eingeblendet wird, schalten Sie die Konsolenumleitung 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 Konsolenumleitungssitzung aufbaue?	Eine Konsolenumleitungssitzung wird vom lokalen System aus konfiguriert. Dies wird nicht unterstützt.

Erhalte ich eine Warnungsmeldung, wenn ich eine Konsolenumleitungssitzung 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.
Welche Bandbreite benötige ich, um eine Konsolenumleitungssitzung auszuführen?	Zum Erzielen einer guten Leistung wird eine Verbindungsgeschwindigkeit von 5 MB/s empfohlen. Eine 1 MB/s-Verbindung ist zum Erzielen der Mindestleistung vorgeschrieben.
Was sind die Mindestsystemanforderungen für meine Management Station zum Ausführen der Konsolenumleitung?	Die Management Station erfordert einen Intel® Pentium® III 500-MHz-Prozessor mit mindestens 256 MB RAM.
Warum wird die Meldung **Kein Signal** im iDRAC6-KVM-Video Viewer angezeigt?	Sie sehen diese Meldung möglicherweise, da das iDRAC Virtual KVM-Plugin nicht das Desktop-Video des Remote-Servers 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 iDRAC-KVM-Video Viewer 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.

Zurück zum Inhaltsverzeichnis