Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 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.**

Irrtümer und technische Änderungen vorbehalten.
© 2009 Dell Inc. Alle Rechte vorbehalten.

Eine Vervielfältigung oder Wiedergabe dieser Materialien in jeglicher Weise ohne vorherige schriftliche Genehmigung von Dell Inc. ist strengstens untersagt.

In diesem Text verwendete Marken: *Dell*, das *DELL*-Logo, *Dell OpenManage* und *PowerEdge* sind Marken von Dell Inc.; *Microsoft*, *Windows*, *Windows Server*, Windows Vista und *Active Directory* sind entweder Marken oder eingetragene Marken von Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern; *Red Hat* und *Linux* sind eingetragene Marken von Red Hat, Inc. in den Vereinigten Staaten und anderen Ländern; *SUSE* ist eine eingetragene Marken von Novell Corporation. *Intel* und *Pentium* sind eingetragene Marken von Intel Corporation in den Vereinigten Staaten und anderen Ländern; *UNIX* ist eine eingetragene Marke von The Open Group in den Vereinigten Staaten und andern Ländern; VMware ist eine eingetragene Marke von VMware, Inc. in den Vereinigten Staaten und/oder anderen Gerichtsbarkeiten.

Copyright 1998-2006 The OpenLDAP Foundation. Alle Rechte vorbehalten. Der Weitervertrieb und die Nutzung in Quell- und Binärform ist mit oder ohne Änderungen gestattet, sofern durch die öffentliche Lizenz von OpenLDAP autorisiert. Eine Kopie dieser Lizenz ist in der Datei LICENSE im Verzeichnis der obersten Ebene der Verteilung erhältlich oder auch unter **www.OpenLDAP.org/license.html**. OpenLDAP ist eine eingetragene Marke der OpenLDAP Foundation. Individuelle Dateien und/oder beigetragene Pakete können durch andere Parteien urheberrechtlich geschützt sein und zusätzlichen Einschränkungen unterliegen. Diese Arbeit wird vom LDAP v3.3-Vertrieb der University of Michigan abgeleitet. Diese Arbeit enthält außerdem Materialien, die von öffentlichen Quellen stammen. Informationen zu OpenLDAP stehen unter **www.openldap.org/** zur Verfügung. Teil-Copyright 1998-2004 Kurt D. Zeilenga. Teil-Copyright 1998-2004 Net Boolean Incorporated. Teil-Copyright 2001-2004 IBM Corporation. Alle Rechte vorbehalten. Der Weitervertrieb und die Nutzung in Quell- und Binärform ist mit oder ohne Änderungen gestattet, sofern durch die öffentliche Lizenz von OpenLDAP autorisiert. Teil-Copyright 1999-2003 Howard Y.H. Chu. Teil-Copyright 1999-2003 Symas Corporation. Teil-Copyright 1998-2003 Hallvard B. Furuseth. Alle Rechte vorbehalten. Der Weitervertrieb und die Nutzung in Quell- und Binärform ist mit oder ohne Änderungen gestattet, sofern dieser Hinweis beibehalten wird. Die Namen der Inhaber des Urheberrechts dürfen nicht verwendet werden, um von dieser Software abgeleitete Produkte ohne vorherige schriftliche Genehmigung zu indossieren oder zu fördern. Diese Software wird ohne Mängelgewähr und ohne ausdrückliche oder stillschweigende Garantie zur Verfügung gestellt. Teil-Copyright (c) 1992-1996 Regents der University of Michigan. Alle Rechte vorbehalten. Der Weitervertrieb und die Nutzung in Quell- und Binärform ist gestattet, sofern dieser Hinweis beibehalten wird, und sofern anerkannt wird, dass die entsprechenden Materialien von der University of Michigan in Ann Arbor zur Verfügung gestellt wurden. Der Name der Universität darf ohne vorherige schriftliche Genehmigung nicht verwendet werden, um von dieser Software abgeleitete Produkte zu unterstützen oder zu fördern. Diese Software wird ohne Mängelgewähr und ohne ausdrückliche oder stillschweigende Garantie zur Verfügung gestellt. Alle anderen in dieser Dokumentation genannten Marken und Handelsbezeichnungen sind Eigentum der entsprechenden Hersteller und Firmen. Dell Inc. erhebt keinen Anspruch auf Markenzeichen und Handelsbezeichnungen mit Ausnahme der eigenen.

März 2009 Rev. A00

Zurück zum Inhaltsverzeichnis

Übersicht der RACADM-Unterbefehle

Integrated Dell™ Remote Access Controller Firmware Version 1.2-Benutzerhandbuch

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

---

help

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

Tabelle A-1. Befehl help

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

Zusammenfassung

```
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

---

config

Tabelle A-2 beschreibt die Unterbefehle **config** und **getconfig**.

Tabelle A-2. config/getconfig

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

Zusammenfassung

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

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

Unterstützte Schnittstellen

- Lokaler RACADM

Beschreibung

Mit dem Unterbefehl **config** können Sie die Konfigurationsparameter des iDRAC einzeln einstellen oder sie als Teil einer Konfigurationsdatei stapelverarbeiten. Wenn sich die Daten unterscheiden, wird das iDRAC-Objekt mit dem neuen Wert geschrieben.

Eingabe

Tabelle A-3 beschreibt die Optionen des Unterbefehls **config**.

Tabelle A-3. Optionen und Beschreibungen des Unterbefehls config

Option	Beschreibung
-f	Über die Option **-f** <*Dateiname*> kann **config** den Inhalt der durch <*Dateiname*> festgelegten Datei lesen und den iDRAC konfigurieren. Die Datei muss Daten enthalten, die dem unter Syntax der Konfigurationsdatei festgelegten Format entsprechen.
-p	Die Option **-p** bzw. die Kennwortoption weist **config** an, die Kennworteinträge in der config-Datei **-f** <*Dateiname*> zu löschen, nachdem 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. 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 an einen Index gekoppelte Gruppen gültig und kann zur Festlegung einer eindeutigen Gruppe verwendet werden. Der Index wird hier durch den Indexwert bestimmt und nicht durch einen "Benennungs"wert.
-c	Die Option **-c** bzw. die Überprüfungsoption wird zusammen mit dem Unterbefehl **config** verwendet und ermöglicht Ihnen, die **.cfg**-Datei zu parsen, um Syntaxfehler zu finden. Falls Fehler gefunden werden, wird die Zeilennummer zusammen mit einer kurzen Beschreibung des Fehlers angezeigt. Es kommen keine Schreibvorgänge zum iDRAC vor. Diese Option ist nur eine Kontrolle.

Ausgabe

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

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

Dieser Unterbefehl zeigt an, wie viele geschriebene Konfigurationsobjekte sich von wie vielen Objekten insgesamt in der **.cfg**-Datei befanden.

Beispiele

- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.110`

  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 den iDRAC oder konfiguriert ihn neu. Die Datei **myrac.cfg** kann mit dem Befehl **getconfig** erstellt werden. Die Datei **myrac.cfg** kann auch manuell bearbeitet werden, solange die Analyse-Richtlinien befolgt werden.

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

getconfig

Mit dem Unterbefehl **getconfig** können Sie iDRAC-Konfigurationsparameter einzeln abrufen oder alle iDRAC-Konfigurationsgruppen abrufen und in einer Datei speichern.

Eingabe

Tabelle A-4 beschreibt die Optionen des Unterbefehls **getconfig**.

ANMERKUNG: Die Option **-f** ohne Dateiangabe wird den Dateiinhalt an den Terminal-Bildschirm ausgeben.

Tabelle A-4. Optionen des Unterbefehls getconfig

Option	Beschreibung
-f	Die Option **-f** <*Dateiname*> weist **getconfig** an, die gesamte iDRAC-Konfiguration in eine Konfigurationsdatei zu schreiben. Diese Datei kann dann für Batch-Konfigurationsvorgänge verwendet werden, die den Unterbefehl **config** anwenden. **ANMERKUNG:** Die Option **-f** erstellt keine Einträge für die Gruppen **cfgIpmiPet** und **cfgIpmiPef**. Sie müssen mindestens ein Trap-Ziel einstellen, um die **cfgIpmiPet**-Gruppe zur 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, der 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 Hilfeoption zeigt eine Liste aller verfügbarer Konfigurationsgruppen an, die verwendet werden 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. Wenn die Option **-i** <*Index*> nicht festgelegt ist, 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 "Benennungs"wert.
-o	Die Option -o <*Objektname*> bzw. die Objektoption bestimmt den Objektnamen, der in der Abfrage verwendet wird. Diese Option kann mit der Option **-g** verwendet werden.
-u	Die Option **-u** <*Benutzername*> bzw. die Benutzernamensoption kann verwendet werden, um die Konfiguration für den festgelegten Benutzer anzuzeigen. Die Option <***Benutzername***> ist der Anmeldename des Benutzers.
-v	Die Option **-v** bzw. die ausführliche Option zeigt zusätzlich zu den Eigenschaften weitere Details an und wird mit der Option **-g** verwendet.

Ausgabe

Dieser Unterbefehl erzeugt eine Fehlerausgabe, wenn einer der folgenden Punkte 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 iDRAC zu **myrac.cfg**.

- `racadm getconfig -h`

  Zeigt eine Liste der verfügbaren Konfigurationsgruppen auf dem iDRAC 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 Benutzergruppeninstanz bei Index 2 mit ausführlichen Informationen zu den Eigenschaftswerten an.

Zusammenfassung

```
racadm getconfig -f <Dateiname>

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

racadm getconfig -u <Benutzername>

racadm getconfig -h
```

Unterstützte Schnittstellen

- Lokaler RACADM

---

getssninfo

Tabelle A-5 beschreibt den Unterbefehl **getssninfo**.

Tabelle A-5. Unterbefehl getssninfo

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

Zusammenfassung

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

Beschreibung

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

- Benutzername
- IP-Adresse (wenn anwendbar)
- Sitzungstyp (z. B. SSH oder Telnet)
- Konsolen in Gebrauch (Beispiel: Virtueller Datenträger oder Virtuelle KVM)

Unterstützte Schnittstellen

- Lokaler RACADM

Eingabe

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

Tabelle A-6. Optionen des Unterbefehls getssninfo

Option	Beschreibung
-A	Die Option **-A** eliminiert das Drucken von Datenkopfzeilen.
-u	Die Benutzernamenoption **-u** <*Benutzername*> begrenzt die ausgedruckte Ausgabe auf detaillierte Sitzungseinträge für den angegebenen Benutzernamen. Wird als Benutzername ein Sternchensymbol (*) angegeben, werden alle Benutzer aufgeführt. Es werden keine zusammenfassenden Informationen ausgedruckt, wenn diese Option angegeben wird.

Beispiele

- `racadm getssninfo`

Tabelle A-7 enthält ein Ausgabebeispiel des Befehls **racadm getssninfo**.

Tabelle A-7. Ausgabebeispiel des Unterbefehls getssninfo

Benutzer	IP-Adresse	Type	Konsolen
root	192.168.0.10	Telnet	Virtuelle KVM

- racadm getssninfo -A

  "root" 143.166.174.19 "Telnet" "KEINE"

- racadm getssninfo -A -u *

  "root" "143.166.174.19" "Telnet" "KEINE"

- "bob" "143.166.174.19" "GUI" "KEINE"

---

getsysinfo

Tabelle A-8 beschreibt den Unterbefehl **racadm getsysinfo**.

Tabelle A-8. getsysinfo

Befehl	Definition
getsysinfo	Zeigt Informationen zu iDRAC, System und Watchdog-Status an.

Zusammenfassung

```
racadm getsysinfo [-d] [-s] [-w] [-A]
```

Beschreibung

Mit dem Unterbefehl **getsysinfo** werden Informationen bezüglich iDRAC, verwaltetem Server und Watchdog-Konfiguration angezeigt.

Unterstützte Schnittstellen

- Lokaler RACADM

Eingabe

Tabelle A-9 beschreibt die Optionen des Unterbefehls **getsysinfo**.

Tabelle A-9. Optionen des Unterbefehls getsysinfo

Option	Beschreibung
-d	Zeigt iDRAC-Informationen an.
-s	Zeigt Systeminformationen an
-w	Zeigt Watchdog-Informationen an
-A	Unterdrückt das Drucken von Kopfzeilen und Beschriftungen.

Ausgabe

Mit dem Unterbefehl **getsysinfo** werden Informationen bezüglich iDRAC, verwaltetem Server und Watchdog-Konfiguration angezeigt.

Beispielausgabe

```
RAC Information:
RAC Date/Time           = Wed Aug 22 20:01:33 2007
Firmware Version        = 0.32
Firmware Build          = 13661
Last Firmware Update    = Mon Aug 20 08:09:36 2007

Hardware Version        = NA
Current IP Address      = 192.168.0.120
Current IP Gateway      = 192.168.0.1
Current IP Netmask      = 255.255.255.0
DHCP Enabled            = 1
MAC Address             = 00:14:22:18:cd:f9
Current DNS Server 1    = 10.32.60.4
Current DNS Server 2    = 10.32.60.5
DNS Servers from DHCP   = 1
Register DNS RAC Name   = 1
DNS RAC Name            = iDRAC-783932693338
Current DNS Domain      = us.dell.com

System Information:
System Model            = PowerEdge M600
System BIOS Version     = 0.2.1
BMC Firmware Version    = 0.32
Service Tag             = 48192
Host Name               = dell-x92i38xc2n
OS Name                 =
Power Status            = OFF

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

Beispiele

- `racadm getsysinfo -A -s`

  `"System Information:" "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "ON"`

- `racadm getsysinfo -w -s`

```
System Information:
System Model            = PowerEdge M600
System BIOS Version     = 0.2.1
BMC Firmware Version    = 0.32
Service Tag             = 48192
Host Name               = dell-x92i38xc2n
OS Name                 =
Power Status           = ON


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

Einschränkungen

Die Felder **Host-Name** und **BS-Name** in der **getsysinfo**-Ausgabeanzeige zeigen nur dann genaue Informationen an, wenn Dell OpenManage auf dem verwalteten Server installiert ist. Wenn OpenManage auf dem verwalteten Server nicht installiert ist, können diese Felder leer oder fehlerhaft sein.

---

getractime

Tabelle A-10 beschreibt den Unterbefehl **getractime**.

Tabelle A-10. getractime

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

Zusammenfassung

```
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

20071208201542.000000
```

Unterstützte Schnittstellen

- Lokaler RACADM

---

setniccfg

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

Tabelle A-11. setniccfg

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

Zusammenfassung

```
racadm setniccfg -d

racadm setniccfg -s [<IP-Adresse> <Netzmaske> <Gateway>]

racadm setniccfg -o [<IP-Adresse> <Netzmaske> <Gateway>]
```

Beschreibung

Der Unterbefehl **setniccfg** stellt die iDRAC-IP-Adresse ein.

- Die Option **-d** aktiviert DHCP für die NIC (Standardeinstellung: DHCP aktiviert).
- Die Option **-s** aktiviert statische IP-Einstellungen. IP-Adresse, Netzmaske und Gateway können angegeben werden. Ansonsten werden die vorhandenen statischen Einstellungen verwendet. <*IP-Adresse*>, <*Netzmaske*> und <*Gateway*> müssen als durch Punkte getrennte Zeichenketten eingegeben werden.

  ```
  racadm setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1
  ```

- Durch die Option **-o** wird die NIC vollständig deaktiviert. <*IP-Adresse*>, <*Netzmaske*> und <*Gateway*> müssen als durch Punkte getrennte Zeichenketten eingegeben werden.

  ```
  racadm setniccfg -o 192.168.0.120 255.255.255.0 192.168.0.1
  ```

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

---

getniccfg

Tabelle A-12 beschreibt den Unterbefehl **getniccfg**.

Tabelle A-12. getniccfg

Unterbefehl	Definition
getniccfg	Zeigt die aktuelle IP-Konfiguration für den iDRAC an.

Zusammenfassung

```
racadm getniccfg
```

Beschreibung

Der Unterbefehl **getniccfg** zeigt die aktuellen NIC-Einstellungen an.

Beispielausgabe

Mit dem Unterbefehl **getniccfg** wird eine entsprechende Fehlermeldung angezeigt, wenn der Vorgang nicht erfolgreich ist. Bei erfolgreicher Ausführung wird andernfalls 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

---

getsvctag

Tabelle A-13 beschreibt den Unterbefehl **getsvctag**.

Tabelle A-13. getsvctag

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

Zusammenfassung

```
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

---

racreset

Tabelle A-14 beschreibt den Unterbefehl **racreset**.

Tabelle A-14. racreset

Unterbefehl	Definition
racreset	Setzt den iDRAC zurück.

HINWEIS: Wenn Sie einen racreset-Unterbefehl ausgeben, kann der iDRAC bis zu eine Minute in Anspruch nehmen, um in einen einsatzfähigen Zustand zurückzukehren.

Zusammenfassung

```
racadm racreset
```

Beschreibung

Der Unterbefehl **racreset** gibt einen Reset an den iDRAC aus. Das Reset-Ereignis wird in das iDRAC-Protokoll eingetragen.

Beispiele

- `racadm racreset`

  Starten Sie die Soft-Reset-Sequenz für den iDRAC.

Unterstützte Schnittstellen

- Lokaler RACADM

---

racresetcfg

Tabelle A-15 beschreibt den Unterbefehl **racresetcfg**.

Tabelle A-15. racresetcfg

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

Zusammenfassung

```
racadm racresetcfg
```

Unterstützte Schnittstellen

- Lokaler RACADM

Beschreibung

Durch den Befehl **racresetcfg** werden alle vom Benutzer konfigurierten Einträge der Datenbankeigenschaften entfernt. Die Datenbank weist Standardeigenschaften für alle Einträge auf, die zur Wiederherstellung der ursprünglichen Standardeinstellungen des iDRAC verwendet werden.

HINWEIS: Mit diesem Befehl werden die aktuelle iDRAC-Konfiguration gelöscht und die iDRAC-Konfiguration auf die Standardeinstellungen zurückgesetzt. Nach dem Reset lauten der Standardname und das Standardkennwort **root** bzw. **calvin** und die IP-Adresse ist **192.168.0.120** plus die Nummer des Steckplatzes, den der Server im Gehäuse einnimmt.

---

serveraction

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

Tabelle A-16. serveraction

Unterbefehl	Definition
serveraction	Führt den Reset eines verwalteten Servers oder einen Einschalten/Ausschalten-Zyklus aus.

Zusammenfassung

```
racadm serveraction <Maßnahme>
```

Beschreibung

Der Unterbefehl **serveraction** ermöglicht Benutzern, Stromverwaltungsvorgänge auf dem Host-System auszuführen. Tabelle A-17 beschreibt die Stromregelungsoptionen zu **serveraction**.

Tabelle A-17. Optionen des Unterbefehls serveraction

Zeichenkette	Definition
<*Maßnahme*>	Bestimmt die Maßnahme. Die Optionen für die Zeichenkette <*Maßnahme*> sind: - **powerdown** - Fährt den verwalteten Server herunter. - **powerup** - Fährt den verwalteten Server hoch. - **powercycle** - Leitet einen Ein-/Ausschaltvorgang auf dem verwalteten Server ein. 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-Vorgang (Neustartvorgang) auf dem verwalteten Server aus.

Ausgabe

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

Unterstützte Schnittstellen

- Lokaler RACADM

---

getraclog

Tabelle A-18 beschreibt den Befehl **racadm getraclog**.

Tabelle A-18. getraclog

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

Zusammenfassung

```
racadm getraclog -i

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

Beschreibung

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

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

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

Tabelle A-19. getraclog Unterbefehlsoptionen

Option	Beschreibung
-A	Zeigt die Ausgabe ohne Kopfzeilen oder Bezeichnungen an.
-c	Zeigt die maximale Anzahl zurückzugebender Einträge an.
-m	Zeigt jeweils einen Bildschirm mit Informationen an und fordert den Benutzer auf, fortzufahren (ähnlich dem UNIX-Befehl **more**).
-o	Zeigt die Ausgabe in einer einzelnen Zeile an.
-s	Gibt den für die Anzeige verwendeten Starteintrag an.

Ausgabe

Die Anzeige der Standardausgabe gibt Folgendes an: Datensatznummer, Zeitstempel, Quelle und Beschreibung. Der Zeitstempel beginnt um Mitternacht, dem 1. Januar und nimmt so lange zu, bis der verwaltete Server startet. Nach dem Start des verwalteten Servers wird die Systemzeit des verwalteten Servers für den Zeitstempel 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

---

clrraclog

Zusammenfassung

```
racadm clrraclog
```

Beschreibung

Mit dem Unterbefehl **clrraclog** werden alle vorhandenen Einträge aus dem iDRAC-Protokoll entfernt. Ein neuer Einzeldatensatz wird zur Aufzeichnung von Datum und Zeit des Löschens des Protokolls entfernt.

---

getsel

Tabelle A-20 beschreibt den Befehl **getsel**.

Tabelle A-20. getsel

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

Zusammenfassung

```
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 SEL an.

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

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

Tabelle A-21. getsel Unterbefehlsoptionen

Option	Beschreibung
-A	Gibt die Ausgabe ohne Anzeigekopfzeilen oder Bezeichnungen an.
-c	Zeigt die maximale Anzahl zurückzugebender Einträge an.
-o	Zeigt die Ausgabe in einer einzelnen Zeile an.
-s	Gibt den für die Anzeige verwendeten Starteintrag an.
-E	Platziert die 16 Byte Roh-SEL an das Ende jeder Ausgabezeile als Sequenz hexadezimaler Werte.
-R	Es werden nur die Rohdaten ausgedruckt.
-m	Zeigt jeweils einen Bildschirm mit Informationen an und fordert den Benutzer auf, fortzufahren (ähnlich dem UNIX-Befehl **more**).

Ausgabe

Die Anzeige der Standardausgabe gibt Folgendes an: Datensatznummer, Zeitstempel, Schweregrad und Beschreibung.

Zum Beispiel:

```
Record:         1
Date/Time:      16.11.05 22:40:43
Severity:       OK
Description:    Systemplatinen-SEL: Ereignisprotokollsensor für Systemplatine, gelöschtes Protokoll wurde bestätigt
```

Unterstützte Schnittstellen

- Lokaler RACADM

---

clrsel

Zusammenfassung

```
racadm clrsel
```

Beschreibung

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

Unterstützte Schnittstellen

- Lokaler RACADM

---

gettracelog

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

Tabelle A-22. gettracelog

Befehl	Definition
gettracelog -i	Zeigt die Anzahl der Einträge im **iDRAC-Ablaufverfolgungsprotokoll** an.
gettracelog	Zeigt das **Ablaufverfolgungsprotokoll** des iDRAC an.

Zusammenfassung

```
racadm gettracelog -i

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

Beschreibung

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

Tabelle A-23. gettracelog Unterbefehlsoptionen

Option	Beschreibung
-i	Zeigt die Anzahl der Einträge im **iDRAC-Ablaufverfolgungsprotokoll** an.
-m	Zeigt jeweils einen Bildschirm mit Informationen an und fordert den Benutzer auf, fortzufahren (ähnlich dem UNIX-Befehl **more**).
-o	Zeigt die Ausgabe in einer einzelnen Zeile an.
-c	gibt die Anzahl von Einträgen an, die angezeigt werden sollen.
-s	gibt den Starteintrag an, der angezeigt werden soll.
-A	Kopfzeilen oder Bezeichnungen nicht anzeigen.

Ausgabe

Die Anzeige der Standardausgabe gibt Folgendes an: Datensatznummer, Zeitstempel, Quelle und Beschreibung. Der Zeitstempel beginnt um Mitternacht, dem 1. Januar und nimmt so lange zu, bis der verwaltete Server startet. Nach dem Start des verwalteten Systems wird die Systemzeit des verwalteten Systems für den Zeitstempel verwendet.

Zum 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

---

sslcsrgen

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

Tabelle A-24. sslcsrgen

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

Zusammenfassung

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

racadm sslcsrgen -s
```

Beschreibung

Der Unterbefehl **sslcsrgen** kann verwendet werden, um eine CSR zu erstellen und die Datei zum lokalen 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

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

Tabelle A-25. 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*>), an den die CSR heruntergeladen wird.

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

Wenn keine Optionen angegeben werden, wird eine CSR erstellt und standardmäßig als **sslcsr** zum lokalen 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.

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

---

sslcertupload

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

Tabelle A-26. sslcertupload

Unterbefehl	Beschreibung
sslcertupload	Lädt ein benutzerdefiniertes SSL-Server- oder Zertifizierungsstellenzertifikat vom Client zum iDRAC hoch.

Zusammenfassung

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

Optionen

Tabelle A-27 beschreibt die Optionen des Unterbefehls **sslcertupload**.

Tabelle A-27. Optionen des Unterbefehls sslcertupload

Option	Beschreibung
-t	Gibt den hochzuladenden Zertifikatstyp an, entweder ein CA-Zertifikat oder ein Server-Zertifikat. 1 = Server-Zertifikat 2 = CA-Zertifikat
-f	Gibt den Dateinamen des hochzuladenden Zertifikats an. Wenn die Datei nicht festgelegt wird, wird die Datei **sslcert** im aktuellen Verzeichnis ausgewählt.

Der Befehl **sslcertupload** gibt bei Erfolg `0` und bei Nichterfolg einen anderen Wert als Null zurück.

Beispiel

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

Unterstützte Schnittstellen

- Lokaler RACADM

---

sslcertdownload

Tabelle A-28 beschreibt den Unterbefehl **sslcertdownload**.

Tabelle A-28. sslcertdownload

Unterbefehl	Beschreibung
sslcertdownload	Lädt ein SSL-Zertifikat vom RAC auf das Dateisystem des Clients herunter.

Zusammenfassung

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

Optionen

Tabelle A-29 beschreibt die Optionen des Unterbefehls **sslcertdownload**.

Tabelle A-29. Optionen des Unterbefehls sslcertdownload

Option	Beschreibung
-t	Gibt den Typ des herunterzuladenden Zertifikats an, entweder das Microsoft® Active Directory®-Zertifikat oder das Serverzertifikat. 1 = Server-Zertifikat 2 = Microsoft Active Directory-Zertifikat
-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 Nichterfolg einen anderen Wert als Null zurück.

Beispiel

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

Unterstützte Schnittstellen

- Lokaler RACADM

---

sslcertview

Tabelle A-30 beschreibt den Unterbefehl **sslcertview**.

Tabelle A-30. sslcertview

Unterbefehl	Beschreibung
sslcertview	Zeigt das SSL-Serverzertifikat oder das Zertifizierungsstellenzertifikat an, das auf dem iDRAC vorhanden ist.

Zusammenfassung

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

Optionen

Tabelle A-31 beschreibt die Optionen des Unterbefehls **sslcertview**.

Tabelle A-31. Optionen des Unterbefehls sslcertview

Option	Beschreibung
-t	Gibt den Typ des anzuzeigenden Zertifikats an, entweder das Microsoft Active Directory-Zertifikat oder das Serverzertifikat. 1 = Server-Zertifikat 2 = Microsoft Active Directory-Zertifikat
-A	Gibt keine Kopfzeilen/Bezeichnungen aus.

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

Unterstützte Schnittstellen

- Lokaler RACADM

---

testemail

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

Tabelle A-32. testemail-Konfiguration

Unterbefehl	Beschreibung
testemail	Testet die E-Mail-Warnungsfunktion für iDRAC

Zusammenfassung

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

Beschreibung

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

Stellen Sie vor dem Ausführen des Befehls testemail sicher, dass der festgelegte Index in der RACADM-**cfgEmailAlert**Gruppe aktiviert und korrekt konfiguriert ist. Tabelle A-33 führt Befehlsbeispiele für die Gruppe **cfgEmailAlert** auf.

Tabelle A-33. testemail-Konfiguration

Abhilfe	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 SNMP-IP-Adresse korrekt konfiguriert ist	racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr -i 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-34 beschreibt die Optionen des Unterbefehls **testemail**.

Tabelle A-34. testemail Unterbefehlsoption

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

Ausgabe

Keine

Unterstützte Schnittstellen

- Lokaler RACADM

---

testtrap

Tabelle A-35 beschreibt den Unterbefehl **testtrap**.

Tabelle A-35. testtrap

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

Zusammenfassung

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

Beschreibung

Mit dem Unterbefehl **testtrap** wird die SNMP-Trap-Warnmeldungsfunktion des iDRAC geprüft, indem ein Test-Trap vom iDRAC an einen festgelegten Ziel-Trap-Abhörer auf dem 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-36 enthält eine Liste und zugehörige Befehle für die Gruppe **cfgIpmiPet**.

Tabelle A-36. cfg E-Mail-Warnungs-Befehle

Abhilfe	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 zwischen 1 und 4 ist

Eingabe

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

Tabelle A-37. Optionen des Unterbefehls testtrap

Option	Beschreibung
-i	Gibt den Index der Trap-Konfiguration an, die für den Test verwendet werden soll. Gültige Werte sind zwischen 1 und 4.

Unterstützte Schnittstellen

- lokaler RACADM

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

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

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

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 iDRACs.

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

idRacProductInfo (Nur-Lese)

Zulässige Werte

Zeichenkette mit bis zu 63 ASCII-Zeichen.

Standardeinstellung

Integrierter Dell Remote Access Controller

Beschreibung

Eine Textzeichenkette, die das Produkt identifiziert.

idRacDescriptionInfo (Nur-Lese)

Zulässige Werte

Zeichenkette mit bis zu 255 ASCII-Zeichen

Standardeinstellung

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

Beschreibung

Eine Textbeschreibung des RAC-Typs.

idRacVersionInfo (Nur-Lese)

Zulässige Werte

Zeichenkette mit bis zu 63 ASCII-Zeichen.

Standardeinstellung

1.0

Beschreibung

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

idRacBuildInfo (schreibgeschützt)

Zulässige Werte

Zeichenkette mit bis zu 16 ASCII-Zeichen.

Standardeinstellung

Die aktuelle Build-Version der RAC Firmware. Zum Beispiel "05. 12. 06".

Beschreibung

Eine Zeichenkette mit der aktuellen Build-Version des Produkts.

idRacName (schreibgeschützt)

Zulässige Werte

Zeichenkette mit bis zu 15 ASCII-Zeichen

Standardeinstellung

iDRAC

Beschreibung

Ein vom Benutzer vergebener Name zur Identifizierung dieses Controllers.

idRacType (Nur-Lesen)

Standardeinstellung

8

Beschreibung

Identifiziert den Typ des Remote Access Controllers als iDRAC.

---

cfgLanNetworking

Diese Gruppe enthält Parameter zum Konfigurieren der iDRAC-NIC.

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

cfgDNSDomainNameFromDHCP (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

cfgDNSDomainName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette mit bis zu 250 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

""

Beschreibung

Der DNS-Domänenname. Dieser Parameter ist nur gültig, wenn **cfgDNSDomainNameFromDHCP** auf 0 (FALSE) eingestellt ist.

cfgDNSRacName (Lesen/Schreiben)

Zulässige Werte

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

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

Standardeinstellung

rac-*Service-Tag-Nummer*

Beschreibung

Zeigt den RAC-Namen an, der standardmäßig die RAC-*Service-Tag-Nummer* ist. 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 iDRAC-Namen auf dem DNS-Server.

cfgDNSServersFromDHCP (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

cfgDNSServer1 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die eine gültige IP-Adresse darstellt. Beispiel: 192.168.0.20.

Beschreibung

Gibt die IP-Adresse für den DNS-Server 1 an. Diese Eigenschaft ist nur gültig, wenn **cfgDNSServersFromDHCP** auf **0** (FALSE) eingestellt ist.

ANMERKUNG: **cfgDNSServer1** und **cfgDNSServer2** können auf identische Werte eingestellt werden, während sie Adressen austauschen.

cfgDNSServer2 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die eine gültige IP-Adresse darstellt. Beispiel: 192.168.0.20.

Standardeinstellung

0.0.0.0

Beschreibung

Ruft die für den DNS-Server 2 verwendete IP-Adresse ab. Dieser Parameter ist nur gültig, wenn **cfgDNSServersFromDHCP** auf 0 (FALSE) eingestellt ist.

ANMERKUNG: **cfgDNSServer1** und **cfgDNSServer2** können auf identische Werte eingestellt werden, während sie Adressen austauschen.

cfgNicEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert den iDRAC-Netzwerkschnittstellen-Controller. Wenn der NIC deaktiviert wird, ist der Zugriff auf die Remote-Netzwerkschnittstellen zum iDRAC nicht mehr möglich, und der iDRAC ist nur über die lokale RACADM-Schnittstelle verfügbar.

cfgNicIpAddress (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 IP-Adresse darstellt. Beispiel: 192.168.0.20.

Standardeinstellung

192.168.0.*n*

wobei *n* 120 plus die Steckplatznummer des Servers ist.

Beschreibung

Gibt die statische IP-Adresse an, die dem RAC zugewiesen werden soll. Diese Eigenschaft ist nur gültig, wenn **cfgNicUseDhcp** auf **0** (FALSE) eingestellt ist.

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 darstellt. Beispiel: 255.255.255.0.

Standardeinstellung

255.255.255.0

Beschreibung

Die für die statische Zuweisung der iDRAC-IP-Adresse verwendete Subnetzmaske. Diese Eigenschaft ist nur gültig, wenn **cfgNicUseDhcp** auf **0** (FALSE) eingestellt ist.

cfgNicGateway (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 Gateway-IP-Adresse darstellt. Beispiel: 192.168.0.1.

Standardeinstellung

192.168.0.1

Beschreibung

Die für die statische Zuweisung der RAC-IP-Adresse verwendete Gateway-IP-Adresse. Diese Eigenschaft ist nur gültig, wenn **cfgNicUseDhcp** auf **0** (FALSE) eingestellt ist.

cfgNicUseDhcp (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Gibt an, ob DHCP zum Zuweisen der iDRAC-IP-Adresse verwendet wird. Wenn diese Eigenschaft auf 1 (TRUE) eingestellt wird, werden die iDRAC-IP-Adresse, die Subnetzmaske sowie der Gateway vom DHCP-Server auf dem Netzwerk zugewiesen. Wenn diese Eigenschaft auf **0** (FALSE) eingestellt wird, werden die statische IP-Adresse, die Subnetzmaske und der Gateway über die Eigenschaften **cfgNicIpAddress**, **cfgNicNetmask** und **cfgNicGateway** zugewiesen.

cfgNicMacAddress (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette, die die RAC-NIC-MAC-Adresse darstellt.

Standardeinstellung

Die aktuelle MAC-Adresse der iDRAC-NIC. Beispiel: 00:12:67:52:51:A3.

Beschreibung

Die iDRAC-NIC-MAC-Adresse.

---

cfgUserAdmin

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

Es sind bis zu 16 Beispiele der Benutzergruppe gestattet. Jedes Beispiel vertritt die Konfiguration für einen einzelnen Benutzer.

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

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 werden. Tabelle B-1 beschreibt die Benutzerberechtigungs-Bitwerte, die zum Erstellen von Bitmasken kombiniert werden können.

Tabelle B-1. Bit-Masken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
Bei iDRAC anmelden	0x0000001
iDRAC konfigurieren	0x0000002
Benutzer konfigurieren	0x0000004
Protokolle löschen	0x0000008
Serversteuerungsbefehle ausführen	0x0000010
Auf die Konsolenumleitung zugreifen	0x0000020
Zugriff auf virtuelle Datenträger	0x0000040
Testwarnungen	0x0000080
Debug-Befehle ausführen	0x0000100

Beispiele

Tabelle B-2 enthält Beispiele von Berechtigungs-Bitmasken für Benutzer mit einer oder mehreren Berechtigungen.

Tabelle B-2. 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 Informationen zum iDRAC sowie zu den Serverkonfigurationen anzuzeigen.	0x00000001
Der Benutzer hat die Berechtigung, sich am iDRAC anzumelden und Konfigurationsänderungen vorzunehmen.	0x00000001 + 0x00000002 = 0x00000003
Der Benutzer kann sich am RAC anmelden und auf den virtuellen Datenträger sowie auf die Konsolenumleitung zugreifen.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 16.

Standardeinstellung

""

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 der Zeichenkette von doppelten Notierungen ("") löscht den Benutzer an diesem Index. Der Name kann nicht geändert werden. Sie müssen löschen und dann den Namen neu erstellen. 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 mit bis zu 20 ASCII-Zeichen

Standardeinstellung

""

Beschreibung

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

cfgUserAdminEnable

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert einen einzelnen Benutzer.

cfgUserAdminSolEnable

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

---

cfgEmailAlert

Diese Gruppe enthält Parameter zum Konfigurieren der RAC-E-Mail-Warnmeldungsfähigkeiten.

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

cfgEmailAlertIndex (schreibgeschützt)

Zulässige Werte

1 - 4

Standardeinstellung

Dieser Parameter wird beruhend auf den vorhandenen Instanzen bestückt.

Beschreibung

Der eindeutige Index einer Warnungsinstanz.

cfgEmailAlertEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Legt die Ziel-E-Mail-Adresse für E-Mail-Warnungen fest. Beispiel: Benutzer1@Firma.com.

cfgEmailAlertAddress

Zulässige Werte

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

Standardeinstellung

""

Beschreibung

Die E-Mail-Adresse der Warnungsquelle.

cfgEmailAlertCustomMsg

Zulässige Werte

Zeichenkette. Maximale Länge = 32.

Standardeinstellung

""

Beschreibung

Gibt eine benutzerdefinierte Meldung an, die mit der Warnung gesendet wird.

---

cfgSessionManagement

Diese Gruppe enthält Parameter zum Konfigurieren der Anzahl von Sitzungen, für die eine Verbindung zum iDRAC hergestellt werden kann.

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

cfgSsnMgtConsRedirMaxSessions (Lesen / Schreiben)

Zulässige Werte

1 - 2

Standardeinstellung

2

Beschreibung

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

cfgSsnMgtWebserverTimeout (Lesen / Schreiben)

Zulässige Werte

60 - 1920

Standardeinstellung

300

Beschreibung

Definiert die Zeitüberschreitung des Web Servers. Diese Eigenschaft legt die Zeitspanne in Sekunden fest, während der eine Verbindung im Leerlauf 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. Es ist erforderlich, dass Sie sich ab- und wieder anmelden, damit die neuen Einstellungen wirksam werden können.

Eine abgelaufene Web Server-Sitzung meldet die aktuelle Sitzung ab.

cfgSsnMgtSshIdleTimeout (Lesen / Schreiben)

Zulässige Werte

0 (Keine Zeitlimit)

60 - 1920

Standardeinstellung

300

Beschreibung

Definiert die Zeitüberschreitung für den Secure Shell-Leerlauf. Diese Eigenschaft legt die Zeitspanne in Sekunden fest, während der eine Verbindung im Leerlauf 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. Es ist erforderlich, dass Sie sich ab- und wieder anmelden, damit die neuen Einstellungen wirksam werden können.

Eine abgelaufene Secure Shell-Sitzung zeigt die folgende Fehlermeldung erst an, wenn <Eingabe> gedrückt wird:

```
Warnung: Sitzung nicht mehr gültig, mögliche Zeitüberschreitung
```

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

cfgSsnMgtTelnetIdleTimeout (Lesen / Schreiben)

Zulässige Werte

0 (Kein Zeitlimit)

60 - 1920

Standardeinstellung

300

Beschreibung

Definiert die Zeitüberschreitung des Telnet-Leerlaufs. Diese Eigenschaft legt die Zeitspanne in Sekunden fest, während der eine Verbindung im Leerlauf 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 wirksam werden können).

Eine abgelaufene Telnet-Sitzung zeigt die folgende Fehlermeldung erst an, wenn <Eingabe> gedrückt wird:

```
Warnung: Sitzung nicht mehr gültig, mögliche Zeitüberschreitung
```

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

---

cfgSerial

Diese Gruppe enthält Konfigurationsparameter für die iDRAC-Dienste.

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

cfgSerialSshEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

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

cfgSerialTelnetEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Telnet-Konsolenschnittstelle auf dem iDRAC.

---

cfgRacTuning

Diese Gruppe wird verwendet, um verschiedene iDRAC-Konfigurationseigenschaften, wie z. B. gültige Schnittstellen und Schnittstellensicherheits-Beschränkungen zu konfigurieren.

cfgRacTuneHttpPort (Lesen / Schreiben)

Zulässige Werte

10- 65535

Standardeinstellung

80

Beschreibung

Gibt die Anschlussnummer an, die für die HTTP-Netzwerkkommunikation mit dem RAC verwendet werden soll.

cfgRacTuneHttpsPort (Lesen / Schreiben)

Zulässige Werte

10- 65535

Standardeinstellung

443

Beschreibung

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

cfgRacTuneIpRangeEnable

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die IP-Adressenbereichs-Überprüfungsfunktion des iDRAC.

cfgRacTuneIpRangeAddr

Zulässige Werte

Zeichenkette, formatierte IP-Adresse. Beispiel: 192.168.0.44.

Standardeinstellung

192.168.1.1

Beschreibung

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

cfgRacTuneIpRangeMask

Zulässige Werte

Standard-IP-Maskenwerte mit linksbündigen Bits

Standardeinstellung

255.255.255.0

Beschreibung

Zeichenkette, formatierte IP-Adresse. Beispiel: 255.255.255.0.

cfgRacTuneIpBlkEnable

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die IP-Adressen-Blockierungsfunktion des RAC.

cfgRacTuneIpBlkFailCount

Zulässige Werte

2 - 16

Standardeinstellung

5

Beschreibung

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

cfgRacTuneIpBlkFailWindow

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 sie von der Zählung ausgeschlossen.

cfgRacTuneIpBlkPenaltyTime

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 iDRAC-SSH-Schnittstelle verwendete Anschlussnummer an.

cfgRacTuneTelnetPort (Lesen / Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

23

Beschreibung

Gibt die für dien iDRAC-Telnet-Schnittstelle verwendete Anschlussnummer an.

cfgRacTuneConRedirEncryptEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Verschlüsselt das Video in einer Konsolenumleitungssitzung.

cfgRacTuneConRedirPort(Lesen / Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

5900

Beschreibung

Gibt den Anschluss an, der für Tastatur- und Mausaktivitäten während der Konsolenumleitungstätigkeit mit dem iDRAC zu verwenden ist.

cfgRacTuneConRedirVideoPort (Lesen / Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

5901

Beschreibung

Gibt den Anschluss an, der für die Videoaktivitäten während der Konsolenumleitungstätigkeit mit dem iDRAC zu verwenden ist.

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

cfgRacTuneAsrEnable (Lesen / Schreiben)

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Erfassungsfunktion für den Bildschirm Letzter Absturz für iDRAC.

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

cfgRacTuneWebserverEnable (Lesen / Schreiben)

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

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

cfgRacTuneLocalServerVideo (Lesen / Schreiben)

Zulässige Werte

1 (aktiviert)

0 (deaktiviert)

Standardeinstellung

1

Beschreibung

Aktiviert das lokale Servervideo (schaltet es EIN) oder deaktiviert es (schaltet es AUS).

cfgRacTuneLocalConfigDisable (Lesen/Schreiben)

Zulässige Werte

0 (aktiviert)

1 (deaktiviert)

Standardeinstellung

0

Beschreibung

Deaktiviert Schreibzugriff auf die iDRAC-Konfigurationsdaten. Standardmäßig ist der Zugriff aktiviert.

ANMERKUNG: Der Zugriff kann mit dem lokalen RACADM oder der iDRAC-Webschnittstelle deaktiviert werden. Sobald er jedoch deaktiviert ist, kann der Zugriff nur über die iDRAC-Webschnittstelle erneut aktiviert werden.

---

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 (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

""

Beschreibung

Der Host-Name des verwalteten Servers.

ifcRacMnOsOsName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

""

Beschreibung

Der Betriebssystemname des verwalteten Servers.

---

cfgRacSecurity

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

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

cfgSecCsrCommonName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den allgemeinen Namen (CN) der CSR an.

cfgSecCsrOrganizationName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Organisationsnamen (O) an.

cfgSecCsrOrganizationUnit (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt die CSR-Organisationseinheit (OU) an.

cfgSecCsrLocalityName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Standort (L) an.

cfgSecCsrStateName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Zustandsnamen (S) an.

cfgSecCsrCountryCode (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 2.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Landescode (CC) an

cfgSecCsrEmailAddr (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Legt die CSR-E-Mail-Adresse fest.

cfgSecCsrKeySize (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 iDRAC-Datenträgers. Es ist eine Instanz der Gruppe zulässig. In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben.

cfgVirMediaAttached (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

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-/Disketten-Laufwerks am USB-Anschluss eines Systems. Wenn die Geräte angeschlossen sind, können Sie im Remote-Zugriff über die iDRAC-Webschnittstelle oder die CLI eine Verbindung zu den virtuellen Geräten herstellen. Durch die Einstellung dieses Objekts auf **0** werden die Komponenten veranlasst, die Verbindung zum USB-Bus abzutrennen.

ANMERKUNG: Das System muss neu gestartet werden, damit alle Änderungen aktiviert werden.

cfgVirAtapiSrvPort (Lesen / Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

3668

Beschreibung

Gibt die Schnittstellennummer an, die für verschlüsselte Verbindungen virtueller Datenträger zum iDRAC verwendet werden.

cfgVirAtapiSrvPortSsl (Lesen / Schreiben)

Zulässige Werte

Ein beliebiger unbenutzter Anschluss zwischen 0 und 65535 dezimal.

Standardeinstellung

3670

Beschreibung

Richtet die Schnittstelle ein, die für SSL-Verbindungen des virtuellen Datenträgers verwendet wird.

cfgVirMediaBootOnce (Lesen / Schreiben)

Zulässige Werte

1 (Aktiviert)

0 (Deaktiviert)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Einmal-Start-Funktion des virtuellen iDRAC-Datenträgers. Wenn diese Eigenschaft aktiviert ist, versucht diese Funktion beim Neustart des Host-Servers, über die virtuellen Datenträgerkomponenten zu starten - falls auf der Komponente der entsprechende Datenträger installiert ist.

cfgFloppyEmulation (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Wenn auf 0 eingestellt, 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 Floppy-Laufwerk von Windows-Betriebssystemen als Floppy-Laufwerk angesehen. Windows-Betriebssysteme weisen den Laufwerkbuchstaben A: oder B: zu.

---

cfgActiveDirectory

Diese Gruppe enthält Parameter, um die Funktion des iDRAC-Active Directory zu konfigurieren.

cfgADRacDomain (Lesen/Schreiben)

Zulässige Werte

Eine beliebige druckbare Textzeichenkette ohne Leerzeichen. Länge wird auf 254 Zeichen beschränkt.

Standardeinstellung

""

Beschreibung

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

cfgADRacName (Lesen/Schreiben)

Zulässige Werte

Eine beliebige druckbare Textzeichenkette ohne Leerzeichen. Länge wird auf 254 Zeichen beschränkt.

Standardeinstellung

""

Beschreibung

Name des iDRAC, 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 iDRAC. Ist diese Eigenschaft deaktiviert, wird stattdessen die Authentifizierung des lokalen iDRACs für Benutzeranmeldungen verwendet.

cfgADAuthTimeout (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

Zulässige Werte

15 - 300

Standardeinstellung

120

Beschreibung

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

cfgADRootDomain (Lesen / Schreiben)

Zulässige Werte

Eine beliebige druckbare Textzeichenkette ohne Leerraum. Länge wird auf 254 Zeichen beschränkt.

Standardeinstellung

""

Beschreibung

Root-Domäne der Domänengesamtstruktur.

cfgADSpecifyServerEnable (Lesen / Schreiben)

Zulässige Werte

1 oder 0 (True oder False)

Standardeinstellung

0

Beschreibung

1 (True) ermöglicht Ihnen, einen LDAP-Server anzugeben oder einen Server, der den globalen Katalog enthält. 0 (False) deaktiviert diese Option.

cfgADDomainController (Lesen / Schreiben)

Gültige IP-Adresse oder vollqualifizierter Domänenname (FQDN)

Standardeinstellung

Kein Standardwert

Beschreibung

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

cfgADGlobalCatalog (Lesen/Schreiben)

Zulässige Werte

Gültige IP-Adresse oder vollqualifizierter Domänenname (FQDN)

Standardeinstellung

Kein Standardwert

Beschreibung

iDRAC verwendet den von Ihnen festgelegten Wert, um auf dem Server des globalen Katalogs nach Benutzernamen zu suchen.

cfgADType (Lesen/Schreiben)

Zulässige Werte

1 = Aktiviert Active Directory mit dem erweiterten Schema.

2 = Aktiviert Active Directory mit dem Standardschema.

Standardeinstellung

1 = Erweitertes Schema

Beschreibung

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

---

cfgStandardSchema

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

cfgSSADRoleGroupIndex (schreibgeschützt)

Zulässige Werte

Ganzzahl von 1 bis 5.

Beschreibung

Index der Rollengruppe, wie im Active Directory verzeichnet.

cfgSSADRoleGroupName (Lesen/Schreiben)

Zulässige Werte

Eine beliebige druckbare Textzeichenkette ohne Leerraum. Länge wird auf 254 Zeichen beschränkt.

Standardeinstellung

(leer)

Beschreibung

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

cfgSSADRoleGroupDomain (Lesen/Schreiben)

Zulässige Werte

Eine beliebige druckbare Textzeichenkette ohne Leerraum. Länge wird auf 254 Zeichen beschränkt.

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-3 um rollenbasierte Autoritätsberechtigungen für eine Rollengruppe festzulegen.

Tabelle B-3. Bit-Masken für Berechtigungen der Rollengruppe

Rollengruppenberechtigung	Bit-Maske
Bei 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

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert SOL.

cfgIpmiSolBaudRate (Lesen/Schreiben)

Zulässige Werte

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, während der der iDRAC vor dem Übertragen eines teilweisen SOL-Zeichen-Datenpakets wartet. Dieser Wert besteht aus 1-basierten 5-ms-Stufen.

cfgIpmiSolSendThreshold (Read/Write)

Zulässige Werte

1 - 255

Standardeinstellung

255

Beschreibung

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

---

cfgIpmiLan

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

cfgIpmiLanEnable (Lesen/Schreiben)

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

0

Beschreibung

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

cfgIpmiLanPrivLimit (Lesen/Schreiben)

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

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

cfgIpmiLanAlertEnable (Lesen/Schreiben)

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert globale E-Mail-Warnmeldungen. Diese Eigenschaft überschreibt alle einzelnen E-Mail-Warnmeldungs-Eigenschaften des Typs aktivieren/deaktivieren.

cfgIpmiEncryptionKey (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von Hexadezimalziffern von 0 bis 20 Zeichen ohne Leerstellen.

Standardeinstellung

00000000000000000000

Beschreibung

IPMI-Verschlüsselungsschlüssel.

cfgIpmiPetCommunityName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette mit bis zu 18 Zeichen.

Standardeinstellung

public

Beschreibung

Der SNMP-Community-Name für Traps.

---

cfgIpmiPef

Diese Gruppe wird zum Konfigurieren 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.

cfgIpmiPefName (schreibgeschützt)

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

Der Name des Index-Filters.

Beschreibung

Gibt den Namen des Plattformereignisfilters an.

cfgIpmiPefIndex (schreibgeschützt)

Zulässige Werte

1 - 17

Standardeinstellung

Der Indexwert eines Plattformereignisfilter-Objekts.

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

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert einen spezifischen Plattformereignisfilter.

---

cfgIpmiPet

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

cfgIpmiPetIndex (Lesen/Schreiben)

Zulässige Werte

1 - 4

Standardeinstellung

Der entsprechende Indexwert.

Beschreibung

Eindeutiger Bezeichner für den Index, der dem Trap entspricht.

cfgIpmiPetAlertDestIpAddr (Lesen/Schreiben)

Zulässige Werte

Zeichenkette, die eine gültige IP-Adresse darstellt. Beispiel: `192.168.0.67`.

Standardeinstellung

0.0.0.0

Beschreibung

Gibt die Ziel-IP-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

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert einen spezifischen Trap.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC SMCLP-Eigenschaftendatenbank

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

/system1/sp1/account<1-16>

Dieses Ziel enthält Konfigurationsinformationen über die lokalen Benutzer, denen erlaubt wird, über verfügbare Remote-Schnittstellen auf den RAC zuzugreifen. Es sind bis zu 16 Beispiele der Benutzergruppe gestattet. Jede Instanz <1-16> repräsentiert die Konfiguration für einen individuellen lokalen Benutzer.

userid (schreibgeschützt)

Zulässige Werte

1-16

Standardeinstellung

Hängt von der Kontoinstanz ab, auf die zugegriffen wird.

Beschreibung

Legt die Instanz-ID oder die lokale Benutzer-ID fest.

username (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 16.

Standardeinstellung

""

Beschreibung

Eine Textzeichenkette, die den Namen des lokalen Benutzers für dieses Konto enthält. Die Zeichenkette darf weder Vorwärtsschrägstrich (/), noch Punkt (.), noch at-Symbol (@), noch Anführungszeichen (") enthalten. Durch Löschen des Kontos wird auch der Benutzer gelöscht. (Konto löschen<1-16>).

ANMERKUNG: Dieser Eigenschaftenwert muss auf einen eindeutigen Benutzernamen hinweisen.

oemdell_ipmilanprivileges (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.

password (Nur Schreiben)

Zulässige Werte

Eine Textzeichenkette mit einer Länge von 4 bis 20 Zeichen.

Standardeinstellung

""

Beschreibung

Enthält das Kennwort für den lokalen Benutzer. Benutzerkennwörter sind verschlüsselt und sind nicht sichtbar bzw. können nicht angezeigt werden, nachdem die Eigenschaft geschrieben wurde.

enabledstate (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

Hilft bei der Aktivierung oder Deaktivierung eines individuellen Benutzers.

solenabled (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

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

oemdell_extendedprivileges (Lesen/Schreiben)

Zulässige Werte

0x00000000 bis 0x000001ff

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 werden. Tabelle C-1 beschreibt die Benutzerberechtigungs-Bitwerte, die zum Erstellen von Bitmasken kombiniert werden können.

Tabelle C-1. Bit-Masken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
Bei iDRAC anmelden	0x0000001
iDRAC konfigurieren	0x0000002
Benutzer konfigurieren	0x0000004
Protokolle löschen	0x0000008
Serversteuerungsbefehle ausführen	0x0000010
Auf die Konsolenumleitung zugreifen	0x0000020
Zugriff auf virtuelle Datenträger	0x0000040
Testwarnungen	0x0000080
Debug-Befehle ausführen	0x0000100

Beispiele

Tabelle C-2 enthält Beispiele von Berechtigungs-Bitmasken für Benutzer mit einer oder mehreren Berechtigungen.

Tabelle C-2. 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 Serverkonfigurations-Informationen anzuzeigen.	0x00000001
Der Benutzer hat die Berechtigung, sich am iDRAC anzumelden und Konfigurationsänderungen vorzunehmen.	0x00000001 + 0x00000002 = 0x00000003
Der Benutzer kann sich am RAC anmelden und auf den virtuellen Datenträger sowie auf die Konsolenumleitung zugreifen.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

/system1/sp1/enetport1/*

Diese Gruppe enthält Parameter zum Konfigurieren der iDRAC-NIC. Es ist eine Instanz der Gruppe zulässig. Für alle Objekte in dieser Gruppe ist ein Reset des iDRAC-NIC erforderlich, wodurch ein kurzzeitiger Verlust der Konnektivität auftreten kann. Objekte, die die iDRAC-NIC-IP-Adresseneinstellungen ändern, schließen alle aktiven Benutzersitzungen und erfordern, dass Benutzer mit den aktualisierten IP-Adresseneinstellungen eine neue Verbindung herstellen.

macaddress (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette, die die RAC-NIC-MAC-Adresse darstellt.

Standardeinstellung

Die aktuelle MAC-Adresse der iDRAC-NIC. Beispiel: 00:12:67:52:51:A3.

Beschreibung

Enthält die iDRAC-NIC-MAC-Adresse.

/system1/sp1/enetport1/lanendpt1/ipendpt1

oemdell_nicenable (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert den iDRAC-Netzwerkschnittstellen-Controller. Wenn der NIC deaktiviert ist, werden die Remote-Netzwerkschnittstellen zum iDRAC unzugänglich und machen den iDRAC nur über die lokale RACADM-Schnittstelle verfügbar.

ipaddress (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die eine gültige IP-Adresse darstellt. Beispiel: 192.168.0.20.

Standardeinstellung

192.168.0.n (wobei n 120, zuzüglich der Steckplatznummer des Servers ist)

Beschreibung

Gibt die statische IP-Adresse an, die dem RAC zugewiesen werden soll. Diese Eigenschaft ist nur gültig, wenn oemdell_usedhcp auf 0 (deaktiviert) eingestellt ist.

subnetmask (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

255.255.255.0

Beschreibung

Die für die statische Zuweisung der iDRAC-IP-Adresse verwendete Subnetzmaske. Diese Eigenschaft ist nur gültig, wenn oemdell_usedhcp auf 0 (deaktiviert) eingestellt ist.

oemdell_usedhcp (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

Gibt an, ob DHCP zum Zuweisen der iDRAC-IP-Adresse verwendet wird. Wenn diese Eigenschaft auf 1 (aktiviert) eingestellt ist, werden die iDRAC-IP-Adresse, die Subnetzmaske sowie das Gateway vom DHCP-Server auf dem Netzwerk zugewiesen. Wenn diese Eigenschaft auf 0 (deaktiviert) eingestellt ist, erhalten die statische IP-Adresse, die Subnetzmaske und das Gateway Werte, die vom Benutzer manuell eingegeben wurden.

committed (Lesen/Schreiben)

Zulässige Werte

0 (Übernahme ausstehend)

1 (Übernommen)

Standardeinstellung

1

Beschreibung

Ermöglicht dem Benutzer, die IP-Adresse und/oder Subnetzmaske zu ändern, ohne die aktuelle Sitzung zu beenden. Wenn diese Eigenschaft auf 1 (übernommen) eingestellt ist, sind die IP-Adresse und die Subnetzmaske gültig. Durch eine Änderung entweder der IP-Adresse oder der Subnetzmaske wird diese Eigenschaft automatisch auf 0 gesetzt (Übernahme ausstehend). Damit die Netzwerkeinstellungen wirksam werden, muss die Eigenschaft auf 1 zurückgesetzt werden.

/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse ndpt1

oemdell_domainnamefromdhcp (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

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

oemdell_dnsdomainname (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette mit bis zu 254 ASCII-Zeichen Mindestens ein Zeichen muss ein alphabetisches Zeichen sein.

Standardeinstellung

""

Beschreibung

Enthält den DNS-Domänennamen. Diese Eigenschaft ist nur gültig, wenn oemdell_domainnamefromdhcp auf 0 (deaktiviert) eingestellt ist.

oemdell_dnsregisterrac (Lesen/Schreiben)

Zulässige Werte

0 (Unregistriert)

1 (Registriert)

Standardeinstellung

0

Beschreibung

Registriert den iDRAC-Namen auf dem DNS-Server.

oemdell_dnsracname (Lesen/Schreiben)

Zulässige Werte

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

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

Standardeinstellung

rac-Service-Tag-Nummer

Beschreibung

Zeigt den RAC-Namen an, der standardmäßig die RAC-Service-Tag-Nummer ist. Diese Eigenschaft ist nur gültig, wenn oemdell_dnsregisterrac auf 1 (deaktiviert) eingestellt ist.

oemdell_serversfromdhcp (Lesen / Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

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

/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse ndpt1/remotesap1

dnsserveraddress (Lesen / Schreiben)

Zulässige Werte

Eine Zeichenkette, die eine gültige IP-Adresse darstellt. Beispiel: 192.168.0.20.

Standardeinstellung

0.0.0.0

Beschreibung

Gibt die IP-Adresse für den DNS-Server 1 an. Diese Eigenschaft ist nur gültig, wenn oemdell_serversfromdhcp auf 0 (deaktiviert) eingestellt ist.

/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse ndpt1/remotesap2

dnsserveraddress (Lesen / Schreiben)

Zulässige Werte

Eine Zeichenkette, die eine gültige IP-Adresse darstellt. Beispiel: 192.168.0.20.

Standardeinstellung

0.0.0.0

Beschreibung

Gibt die IP-Adresse für den DNS-Server 2 an. Diese Eigenschaft ist nur gültig, wenn oemdell_serversfromdhcp auf 0 (deaktiviert) eingestellt ist.

/system1/sp1/enetport1/lanendpt1/ipendpt1/remot esap1

defaultgatewayaddress (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die eine gültige Gateway-IP-Adresse darstellt. Beispiel: 192.168.0.1.

Standardeinstellung

192.168.0.1

Beschreibung

Die für die statische Zuweisung der RAC-IP-Adresse verwendete Gateway-IP-Adresse. Diese Eigenschaft ist nur gültig, wenn oemdell_usedhcp auf 0 (deaktiviert) eingestellt ist.

/system1/sp1/group<1-5>

Diese Gruppen enthalten Parameter zum Konfigurieren der Standardschemaeinstellungen für Active Directory.

oemdell_groupname (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette mit bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

""

Beschreibung

Enthält den Namen der Rollengruppe, wie in der Active Directory-Gesamtstruktur verzeichnet.

oemdell_groupdomain (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette mit bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

""

Beschreibung

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

oemdell_groupprivilege (Lesen/Schreiben)

Zulässige Werte

0x00000000 bis 0x000001ff

Standardeinstellung

""

Beschreibung

Verwenden Sie die Bitmaskennummern in der Tabelle B-3, um rollenbasierte Autoritätsberechtigungen für eine Rollengruppe einzustellen.

Tabelle C-3. Bit-Masken für Berechtigungen der Rollengruppe

Rollengruppe	Berechtigungs-Bitmaske
Anmeldung bei iDRAC	0x00000001
iDRAC konfigurieren	0x00000002
Benutzer konfigurieren	0x00000004
Protokolle löschen	0x00000008
Serversteuerungsbefehle ausführen	0x00000010
Zugriff auf die Konsolenumleitung	0x00000020
Zugriff auf virtuelle Datenträger	0x00000040
Testwarnungen	0x00000080
Debug-Befehle ausführen	0x00000100

/system1/sp1/oemdell_adservice1

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

enabledstate (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Active Directory-Benutzerauthentifizierung auf dem iDRAC. Ist diese Eigenschaft deaktiviert, wird stattdessen die Authentifizierung des lokalen iDRACs für Benutzeranmeldungen verwendet.

oemdell_adracname (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette mit bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

"

Beschreibung

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

oemdell_adracdomain (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette mit bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

"

Beschreibung

Die Active Directory-Domäne, in der sich der iDRAC befindet.

oemdell_adrootdomain (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette mit bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

"

Beschreibung

Root-Domäne der Domänenstruktur.

oemdell_timeout (Lesen/Schreiben)

Zulässige Werte

15 - 300

Standardeinstellung

120

Beschreibung

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

oemdell_schematype (Lesen/Schreiben)

Zulässige Werte

1 (Erweitertes Schema)

2 (Standardschema)

Standardeinstellung

1

Beschreibung

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

oemdell_adspecifyserverenable (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

Ermöglicht dem Benutzer, einen LDAP- oder einen globalen Katalogserver festzulegen.

oemdell_addomaincontroller (Lesen/Schreiben)

Zulässige Werte

Eine gültige IP-Adresse oder ein vollqualifizierter Domänenname (FQDN)

Standardeinstellung

""

Beschreibung

Vom Benutzer festgelegter Wert, der den iDRAC zum Durchsuchen des LDAP-Servers nach Benutzernamen verwendet.

oemdell_adglobalcatalog (Lesen/Schreiben)

Zulässige Werte

Eine gültige IP-Adresse oder ein FQDN.

Standardeinstellung

Kein Standardwert

Beschreibung

Vom Benutzer festgelegter Wert, der den iDRAC zum Durchsuchen des Servers des globalen Katalogs nach Benutzernamen verwendet.

/system1/sp1/oemdell_racsecurity1

Diese Gruppe wird für die Konfiguration von Einstellungen verwendet, die mit der iDRAC-SSL-CSR-Funktion (Zertifikatsignierungsanforderung) in Beziehung stehen. Alle Eigenschaften in dieser Gruppe müssen konfiguriert werden, bevor vom iDRAC aus eine CSR erstellt wird.

commonname (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

""

Beschreibung

Gibt den allgemeinen Namen der CSR an.

organizationname (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

""

Beschreibung

Gibt den Namen der CSR-Organisation an.

oemdell_organizationunit (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

""

Beschreibung

Gibt den Namen der CSR-Organisationseinheit an.

oemdell_localityname (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Standort an.

oemdell_statename (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

""

Beschreibung

Gibt den Namen des CSR-Staates n an.

oemdell_countrycode (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 2 Zeichen.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Ländercode an.

oemdell_emailaddress (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von bis zu 254 Zeichen.

Standardeinstellung

""

Beschreibung

Legt die CSR-E-Mail-Adresse fest.

oemdell_keysize (Lesen/Schreiben)

Zulässige Werte

1024

2048

4096

Standardeinstellung

1024

Beschreibung

Gibt die asymmetrische SSL-Schlüsselgröße für die CSR an.

/system1/sp1/oemdell_ssl1

Enthält Parameter, die notwendig zur Erstellung von Zertifikatsregistrierungsanforderungen (CSRs) und zur Ansicht von Zertifikaten sind.

generate (Lesen/Schreiben)

Zulässige Werte

0 (Nicht erstellen)

1 (Erstellen)

Standardeinstellung

0

Beschreibung

Erstellt eine CSR, wenn auf 1 eingestellt. Stellen Sie die Eigenschaften im oemdell_racsecurity1-Ziel ein, bevor die CSR erstellt wird.

oemdell_status (schreibgeschützt)

Zulässige Werte

CSR nicht gefunden

CSR erstellt

Standardeinstellung

CSR nicht gefunden

Beschreibung

Zeigt den Status des vorherigen Erstellen-Befehls, wenn vorhanden, der während der aktuellen Sitzung ausgegeben wurde.

oemdell_certtype (Lesen/Schreiben)

Zulässige Werte

SSL

AD

CSR

Standardeinstellung

SSL

Beschreibung

Bestimmt den anzuzeigenden Zertifikatstyp (AD oder SSL) und hilft bei der Erstellung einer CSR mithilfe der Eigenschaft **Erstellen**.

/system1/sp1/oemdell_vmservice1

Diese Gruppe enthält Parameter zum Konfigurieren der Funktion des virtuellen iDRAC-Datenträgers.

enabledstate (Lesen/Schreiben)

Zulässige Werte

VMEDIA_DETACH

VMEDIA_ATTACH

VMEDIA_AUTO_ATTACH

Standardeinstellung

VMEDIA_ATTACH

Beschreibung

Wird verwendet, um virtuelle Geräte an das System per USB-Bus anzuschließen, was dem Server ermöglicht, gültige, mit dem System verbundene USB-Massenspeichergeräte zu erkennen. Dies entspricht dem Anschließen eines lokalen USB-CDROM-/Disketten-Laufwerks am USB-Anschluss eines Systems. Wenn die Geräte angeschlossen sind, können Sie im Remote-Zugriff über die iDRAC-Webschnittstelle oder die CLI eine Verbindung zu den virtuellen Geräten herstellen. Durch die Einstellung dieser Eigenschaft auf 0 werden die Komponenten veranlasst, die Verbindung zum USB-Bus zu trennen.

oemdell_singleboot (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Einmal-Start-Funktion des virtuellen iDRAC-Datenträgers. Wenn diese Eigenschaft beim Neustart des Hostservers aktiviert wirdt, wird der Server versuchen, von den virtuellen Datenträgergeräten zu starten.

oemdell_floppyemulation (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

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 Floppy-Laufwerk von Windows-Betriebssystemen als Floppy-Laufwerk angesehen. Windows-Betriebssysteme weisen den Laufwerksbuchstaben A: oder B: zu.

/system1/sp1/oemdell_vmservice1/tcpendpt1

portnumber (Lesen/Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

3668

Beschreibung

Gibt die Anschlussnummer an, die für verschlüsselte Verbindungen virtueller Datenträger zum iDRAC verwendet werden.

oemdell_sslenabled (schreibgeschützt)

Zulässiger Wert

FALSE

Standardeinstellung

FALSE

Beschreibung

Zeigt an, dass SSL auf dem Anschluss deaktiviert ist.

portnumber (Lesen / Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

3670

Beschreibung

Gibt dieAnschlussnummer an, die für verschlüsselte Verbindungen virtueller Datenträger zum iDRAC verwendet werden.

oemdell_sslenabled (schreibgeschützt)

Zulässiger Wert

TRUE

Standardeinstellung

TRUE

Beschreibung

Zeigt an, dass SSL auf dem Anschluss deaktiviert ist.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

RACADM- und SM-CLP-Äquivalenzen

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

Tabelle D-1 führt die RACADM-Gruppen und -Objekte auf und ggf. SM-SLP-äquivalente Speicherorte im SM-CLP-MAP.

Tabelle D-1. RACADM-Gruppen/-Objekte und SM-CLP-Äquivalenzen

RACADM-Gruppen/-Objekte	SM-CLP	Beschreibung
idRacInfo		
idRacName		Zeichenkette mit bis zu 15 ASCII-Zeichen Standardeinstellung: **iDRAC**.
idRacProductInfo		Zeichenkette mit bis zu 63 ASCII-Zeichen. Standard: **Integrated Dell Remote Access Controller**.
idRacDescriptionInfo		Zeichenkette mit bis zu 255 ASCII-Zeichen Standard: **Diese Systemkomponente enthält einen vollständigen Satz von Remote-Verwaltungsfunktionen für Dell PowerEdge-Server**.
idRacVersionInfo		Zeichenkette mit bis zu 63 ASCII-Zeichen. Standardeinstellung: **1**
idRacBuildInfo		Zeichenkette mit bis zu 16 ASCII-Zeichen.
idRacType		Standardeinstellung: **8**
cfgActiveDirectory	**/system1/sp1/oemdell_adservice1**	
cfgADEnable	enablestate	0 zum Deaktivieren, 1 zum Aktivieren. Standardeinstellung: **0**
cfgADRacName	oemdell_adracname	Zeichenkette von bis zu 254 Zeichen.
cfgADRacDomain	oemdell_adracdomain	Zeichenkette von bis zu 254 Zeichen.
cfgADRootDomain	oemdell_adrootdomain	Zeichenkette von bis zu 254 Zeichen.
cfgADAuthTimeout	oemdell_timeout	15 bis 300 Sekunden. Standardeinstellung: **120**
cfgADType	oemdell_schematype	1 für Standardschema, 2 für erweitertes Schema. Standardeinstellung: **1**
cfgADSpecifyServerEnable	oemdell_adspecifyserverenable	Legt, wenn aktiviert, einen LDAP-Server oder einen Server des globalen Katalogs fest. 0 zum Deaktivieren, 1 zum Aktivieren. Standardeinstellung: **0**
cfgADDomainController	oemdell_addomaincontroller	DNS-Name oder IP-Adresse des in der LDAP-Suche verwendeten Domänen-Controllers.
cfgADGlobalCatalog	oemdell_adglobalcatalog	DNS-Name oder IP-Adresse des in der LDAP-Suche verwendeten Servers des globalen Katalogs.
cfgStandardSchema		
cfgSSADRoleGroupIndex	**/system1/sp1/group1** *bis* **/system1/sp1/group5**	RACADM - Gruppenindex-ID (1-5). SM-CLP - ausgewählt mit Adressenpfad.
cfgSSADRoleGroupName	oemdell_groupname	Zeichenkette von bis zu 254 Zeichen.
cfgSSADRoleGroupDomain	oemdell_groupdomain	Zeichenkette von bis zu 254 Zeichen.
cfgSSADRoleGroupPrivilege	oemdell_grouppprivilege	Bitmaske mit Werten zwischen 0x00000000 und 0x000001ff.
cfgLanNetworking	**/system1/sp1/enetport1**	
cfgNicMacAddress	macaddress	Die MAC-Adresse der Schnittstelle. Kann nicht bearbeitet werden.
	/system1/sp1/enetport1/lanendpt1/ipendpt1	
cfgNicEnable	oemdell_nicenable	0 zum Deaktivieren der NIC, 1 zum Aktivieren der NIC. Standardeinstellung: **0**
cfgNicUseDHCP	oemdell_usedhcp	0 zur Konfiguration statischer Netzwerkadressen, 1 zur Verwendung von DHCP. Standardeinstellung: **0**
cfgNicIpAddress	ipaddress	Die iDRAC-IP-Adresse. Standard: **192.168.0.120** plus die Serversteckplatznummer.
cfgNicNetmask	subnetmask	Subnetzmaske für das iDRAC-Netzwerk. Standardeinstellung: **255.255.255.0**
	committed	Wenn sich Gruppenwerte ändern, wird **committed** auf 0 eingestellt, um darauf hinzuweisen, dass die neuen Werte nicht gespeichert wurden. Stellen Sie den Wert auf 1 ein, um die neue Konfiguration zu speichern. Standardeinstellung: **1**

	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1	
cfgDNSDomainName	oemdell_dnsdomainname	Zeichenkette von bis zu 250 ASCII-Zeichen. Mindestens ein Zeichen muss alphabetisch sein.
cfgDNSDomainNameFromDHCP	oemdell_domainnamefromdhcp	Auf 1 einstellen, um den Domänennamen von DHCP abzurufen. Standardeinstellung: **0**
cfgDNSRacName	oemdell_dnsracname	Zeichenkette mit bis zu 63 ASCII-Zeichen. Mindestens ein Zeichen muss alphabetisch sein. Standard: **iDRAC** *plus die Dell Service-Tag-Nummer*.
cfgDNSRegisterRac	oemdell_dnsregisterrac	Auf 1 einstellen, um den iDRAC-Namen in DNS zu registrieren. Standardeinstellung: **0**
cfgDNSServersFromDHCP	oemdell_dnsserversfromdhcp	Auf 1 einstellen, um DNS-Server-Adressen von DHCP abzurufen. Standardeinstellung: **0**
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer1	dnsserveraddresses1	Eine Zeichenkette, die die IP-Adresse eines DNS-Servers repräsentiert.
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap2	
cfgDNSServer2	dnsserveraddresses2	Eine Zeichenkette, die die IP-Adresse eines DNS-Servers repräsentiert.
	/system1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1	
cfgNicGateway	defaultgatewayaddress	Eine Zeichenkette, die die IP-Adresse des Standard-Gateways repräsentiert. Standardeinstellung: **192.168.0.1**
cfgRacVirtual	**/system1/sp1/oemdell_vmservice1**	
cfgFloppyEmulation	oemdell_floppyemulation	Auf 1 einstellen, um Diskettenemulation zu aktivieren. Standardeinstellung: **0**
cfgVirMediaAttached	enabledstate	Auf 1 (RACADM)/ VMEDIA_ATTACH (SM-CLP) einstellen, um mit Datenträger zu verbinden. Standardeinstellung: 1 (RACADM)/ VMEDIA_ATTACH (SM-CLP)
cfgVirMediaBootOnce	oemdell_singleboot	Auf 1 einstellen, um nächsten Start vom ausgewählten Datenträger aus durchzuführen. Standardeinstellung **0**.
	/system1/sp1/oemdell_vmservice1/tcpendpt1	
	oemdell_sslenabled	Auf 1 einstellen, wenn SSL für das erste virtuelle Datenträgergerät aktiviert ist, auf 0 einstellen, wenn nicht. Kann nicht bearbeitet werden.
cfgVirAtapiSvrPort	portnumber	Für das erste virtuelle Datenträgergerät zu verwendender Anschluss. Standardeinstellung: **3668**
	/system1/sp1/oemdell_vmservice1/tcpendpt2	
	oemdell_sslenabled	Auf 1 einstellen, wenn SSL für das zweite virtuelle Datenträgergerät aktiviert ist, auf 0 einstellen, wenn nicht. Kann nicht bearbeitet werden.
cfgVirAtapiSvrPortSsl	portnumber	Für das zweite virtuelle Datenträgergerät zu verwendender Anschluss. Standardeinstellung: **3670**
cfgUserAdmin	**/system1/sp1/account1** *bis* **/system1/sp1/account16**	
cfgUserAdminEnable	enabledstate	Auf 1 einstellen, um Benutzer zu aktivieren. Standardeinstellung: **0**
cfgUserAdminIndex	userid	Benutzerindex, von 1 bis 16.
cfgUserAdminIpmiLanPrivilege	oemdell_ipmilanprivileges	2 (Benutzer), 3 (Operator), 4 (Administrator) oder 15 (Kein Zugriff). Standardeinstellung: **4**
cfgUserAdminPassword	Kennwort	Eine Zeichenkette mit bis zu 20 ASCII-Zeichen
cfgUserAdminPrivilege	oemdell_extendedprivileges	Bitmaskenwert zwischen 0x00000000 und 0x000001ff. Standardeinstellung: **0x00000000**
cfgUserAdminSolEnable	solenabled	Auf 1 einstellen, um Benutzer die Verwendung von Seriell über LAN zu gestatten. Standardeinstellung: **0**
cfgUserAdminUserName	username	Zeichenkette von bis zu 16 Zeichen.
cfgEmailAlert		

cfgEmailAlertAddress		E-Mail-Zieladresse, bis zu 64 Zeichen.
cfgEmailAlertCustomMsg		In E-Mail zu sendende Nachricht, bis zu 32 Zeichen.
cfgEmailAlertEnable		Auf 1 einstellen, um die E-Mail-Warnung zu aktivieren. Standardeinstellung: **0**
cfgEmailAlertIndex		Index der E-Mail-Warnungsinstanz. Zahl von 1 bis 4.
cfgSessionManagement		
cfgSsnMgtConsRedirMaxSessions		Anzahl gleichzeitig zugelassener Konsolenumleitungssitzungen (1 oder 2). Standardeinstellung: **2**
cfgSsnMgtSshIdleTimeout		Anzahl der Sekunden im Leerlauf, bevor für die SSH-Sitzung eine Zeitüberschreitung eintritt. 0 zum Deaktivieren der Zeitüberschreitung oder 60-1920 Sekunden. Standardeinstellung: **300**
cfgSsnMgtTelnetIdleTimeout		Anzahl der Sekunden im Leerlauf, bevor für eine Telnet-Sitzung eine Zeitüberschreitung eintritt. 0 zum Deaktivieren der Zeitüberschreitung oder 60-1920 Sekunden. Standardeinstellung: **300**
cfgSsnMgtWebserverTimeout		Anzahl der Sekunden im Leerlauf, bevor für die Webschnittstellensitzung eine Zeitüberschreitung eintritt. 60-1920 Sekunden. Standardeinstellung: **300**
cfgRacTuning		
cfgRacTuneConRedirEnable		Auf 1 einstellen, um Konsolenumleitung zu aktivieren, auf 0 einstellen, um sie zu deaktivieren. Standardeinstellung:**1**
cfgRacTuneConRedirEncrypt Aktivieren		Auf 1 einstellen, um Verschlüsselung des Konsolenumleitungs-Netzwerkdatenverkehrs zu aktivieren; auf 0 einstellen, um sie zu deaktivieren. Standardeinstellung: **1**
cfgRacTuneConRedirPort		Für die Konsolenumleitung zu verwendender Anschluss. Standardeinstellung: **5900**
cfgRacTuneConRedirVideoPort		Für die Konsolenvideoumleitung zu verwendender Anschluss. Standardeinstellung: **5901**
cfgRacTuneHttpPort		Die für Webschnittstellen-HTTP zu verwendender Anschluss. Standardeinstellung: **80**
cfgRacTuneHttpsPort		Die für sicheres Webschnittstellen-HTTPS zu verwendender Anschluss. Standardeinstellung: **443**
cfgRacTuneIpBlkEnable		Auf 1 einstellen, um IP-Blockierung zu aktivieren. Standardeinstellung: **0**
cfgRacTuneIPBlkFailCount		Anzahl der fehlgeschlagenen, zu zählenden Anmeldeversuche, bevor IP blockiert wird (2 bis 16). Standardeinstellung: **5**
cfgRacTuneIpBlkFailWindow		Zeitspanne in Sekunden, während der die fehlgeschlagenen Anmeldeversuche gezählt werden (10 bis 65535). Standardeinstellung: **60**
cfgRacTuneIpBlkPenaltyTime		Zeitspanne in Sekunden, während der eine blockierte IP blockiert bleibt (10 bis 65535). Standardeinstellung: **300**
cfgRacTuneIpRangeAddr		Basis-IP-Adresse für IP-Bereichsfilter. Standardeinstellung: **192.168.0.1**
cfgRacTuneIpRangeEnable		Auf 1 einstellen, um IP-Bereichsfilterung zuzulassen. Standardeinstellung: 0
cfgRacTuneIpRangeMask		Bitmaske zur Auswahl gültiger IP-Adressen auf Basisadresse angewendet. Standardeinstellung: **255.255.255.0**
cfgRacTuneLocalServerVideo		Auf 1 einstellen, um lokale iKVM-Konsole zu aktivieren. Standardeinstellung: **1**
cfgRacTuneSshPort		Für den SSH-Dienst zu verwendender Anschluss. Standardeinstellung: **22**
cfgRacTuneTelnetPort		Für den SSH-Dienst zu verwendender Anschluss. Standardeinstellung: **23**
cfgRacTuneWebserverEnable		Auf 1 einstellen, um die iDRAC-Webschnittstelle zu aktivieren. Standardeinstellung: **1**
ifcRacManagedNodeOS		
ifcRacMnOsHostname		Host-Name des verwalteten Servers. Zeichenkette von bis zu 255 Zeichen.
ifcRacMnOsOsName		Name des Betriebssystems des verwalteten Servers. Eine Zeichenkette von bis zu 255 Zeichen.
cfgRacSecurity	**/system1/sp1/oemdell_racsecurity1**	
cfgRacSecCsrCommonName	commonname	Allgemeiner Name des Active Directory. Zeichenkette von bis zu 254 Zeichen.
cfgRacSecCsrCountryCode	oemdell_countrycode	Active Directory, Landesvorwahl. 2 Zeichen.
cfgRacSecCsrEmailAddr	oemdell_emailaddress	Die für die Zertifikatsignierungsanforderung zu verwendende E-Mail-Adresse. Zeichenkette von bis zu 254 Zeichen.
cfgRacSecCsrKeySize	oemdell_keysize	Länge des Verschlüsselungsschlüssels (512, 1024 oder 2048). Standardeinstellung: **1024**.
cfgRacSecCsrLocalityName	oemdell_localityname	Name des Active Directory-Speicherorts. Zeichenkette von bis zu 254 Zeichen.
cfgRacSecCsrOrganizationName	organizationname	Name der Active Directory-Organisation. Zeichenkette von bis zu 254 Zeichen.
cfgRacSecCsrOrganizationUnit	oemdell_organizationunit	Name der Active Directory-Organisationseinheit. Zeichenkette von bis zu 254 Zeichen.
cfgRacSecCsrStateName	oemdell_statename	Active Directory, Name des Staats. Zeichenkette von bis zu 254 Zeichen.

cfgIpmiSol		
cfgIpmiSolAccumulateInterval		Höchstanzahl der abzuwartenden Millisekunden, bevor ein teilweises Seriell über LAN-Paket gesendet wird (1 bis 255). Standardeinstellung: **10**
cfgIpmiSolBaudRate		Die für Seriell über LAN zu verwendende Baudrate (19200, 57600, 115200). Standardeinstellung: **115200**
cfgIpmiSolEnable		Auf 1 einstellen, um die Seriell über LAN-Funktion zu aktivieren. Standardeinstellung: **0**
cfgIpmiSolSendThreshold		Maximale Anzahl der zu erfassenden Zeichen, bevor SOL-Daten gesendet werden (1 bis 255). Standardeinstellung: **255**
cfgIpmiSolMinPrivilege		Erforderliche Mindestberechtigung für die Verwendung von SOL. 2 (Benutzer), 3 (Operator) oder 4 (Administrator). Standardeinstellung: **4**
cfgIpmiLan		
cfgIpmiEncryptionKey		Eine aus 0 bis 40 Hexadezimalzahlen bestehende Zeichenkette. Standardeinstellung: **0000000000000000000000000000000000000000**
cfgIpmiLanAlertEnable		Auf 1 einstellen, um IPMI LAN-Warnungen zu aktivieren. Standardeinstellung: **0**
cfgIpmiLanEnable		Auf 1 einstellen, um die IPMI über LAN-Schnittstelle zu aktivieren. Standardeinstellung: **0**
cfgIpmiPetCommunityName		Eine Zeichenkette von bis zu 18 Zeichen. Standardeinstellung: **öffentlich**
cfgIpmiPef		
cfgIpmiPefAction		Die zu treffende Maßnahme bei Feststellung eines Ereignisses. 0 (keine), 1 (Herunterfahren), 2 (Reset), 3 (Aus- und einschalten). Standardeinstellung: **0**
cfgIpmiPefEnable		Auf 1 einstellen, um Plattformereignisfilterung zu aktivieren. Standardeinstellung: **0**
cfgIpmiPefIndex		Die Indexnummer des Plattformereignisfilters. (1 - 17)
cfgIpmiPefName		Der Name des Plattformereignisses, eine aus bis zu 254 Zeichen bestehende Zeichenkette. Kann nicht bearbeitet werden.
cfgIpmiPet		
cfgIpmiPetAlertDestIpAddr		IP-Adresse des Plattformereignis-Trap-Empfängers. Standardeinstellung: **0.0.0.0**
cfgIpmiPetAlertEnable		Auf 1 einstellen, um den Plattformereignis-Trap zu aktivieren. Standardeinstellung: **1**
cfgIpmiPetIndex		Indexnummer (1-4) des Plattformereignis-Traps.

Tabelle D-2. RACADM-Unterbefehle und SM-CLP-Äquivalenzen

RACADM-Unterbefehl	SM-CLP	Beschreibung
sslcsrgen -g	set /system1/sp1/oemdell_ssl1 oemdell_certtype=CSR set /system1/sp1/oemdell_ssl1 generate=1 dump -destination <iDRAC-Zertifikatsignierungsanforderung-TFTP-URI> /system1/sp1/oemdell_ssl1	Erstellt eine SSL-Zertifikatsignierungsanforderung (CSR) und lädt sie herunter.
sslcsrgen -s	show /system1/sp1/oemdell_ssl1 oemdell_status	Gibt Auskunft über den Status eines CSR-Erstellungsverfahrens.
sslcertupload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <iDRAC-Serverzertifikat-TFTP-URI> /system1/sp1/oemdell_ssl1	Lädt das iDRAC-Serverzertifikat zum iDRAC hoch.
sslcertupload -t 2	set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD load -source <ActiveDirectory-Zertifikat-TFTP-URI> /system1/sp1/oemdell_ssl1	Lädt das Active Directory-Zertifikat zum iDRAC hoch.
sslcertdownload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <iDRAC-Serverzertifikat-TFTP-URI> /system1/sp1/oemdell_ssl1	Lädt das iDRAC-Serverzertifikat vom iDRAC herunter.
sslcertdownload -t 2	set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD load -source <ActiveDirectory-Zertifikat-TFTP-URI> /system1/sp1/oemdell_ssl1	Lädt das Active Directory-Zertifikat vom iDRAC herunter.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC-Übersicht

Integrated Dell™ Remote Access Controller Firmware Version 1.2-Benutzerhandbuch

Der Integrated Dell™ Remote Access Controller (iDRAC) ist eine Systemverwaltungs-Hardware- und Software-Lösung, die Remote-Verwaltungsfähigkeiten, Wiederherstellung für abgestürzte Systeme sowie Stromsteuerungsfunktionen für Dell PowerEdge™-Systeme bietet.

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

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

Verwaltete Server werden in einem Dell M1000e-Systemgehäuse mit modularen Netzteilen, Kühlungslüftern und einem Gehäuseverwaltungscontroller (CMC) installiert. Der CMC überwacht und verwaltet alle im Gehäuse installierten Komponenten. Ein redundanter CMC kann für den Fall eines Ausfalls des primären CMCs als Hot-Failover hinzugefügt werden. Das Gehäuse bietet über seine LCD-Anzeige, Verbindungen der lokalen Konsole sowie seine Webschnittstelle Zugriff auf die iDRACs.

Alle Netzwerkverbindungen zum iDRAC finden über die CMC-Netzwerkschnittstelle statt (CMC-RJ45-Anschluss bezeichnet als "GB1"). Der CMC leitet den Datenverkehr zu den iDRACs auf seinen Servern über ein privates, internes Netzwerk. Dieses private Verwaltungsnetzwerk befindet sich außerhalb des Serverdatenpfads und untersteht nicht der Steuerung des Betriebssystems, d. h. es ist *bandextern*. Die *bandinternen* Netzwerkschnittstellen des verwalteten Servers sind über im Gehäuse installierte E/A-Module (IOMs) zugänglich.

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

---

iDRAC-Verwaltungsfunktionen

Der iDRAC enthält die folgenden Verwaltungsfunktionen:

- Registrierung des dynamischen Domänennamensystems (DDNS)
- Remote-Systemverwaltung und -überwachung über eine Webschnittstelle, die lokale RACADM-Befehlszeilenoberfläche über die Konsolenumleitung sowie die SM-CLP-Befehlszeile über eine Telnet/SSH-Verbindung
- Unterstützung für Microsoft Active Directory®-Authentifizierung - Fasst iDRAC-Benutzer-IDs und -kennwörter unter Verwendung des Standardschemas oder eines erweiterten Schemas in Active Directory zusammen
- Konsolenumleitung - Bietet Tastatur-, Video- und Mausfunktionen für Remote-Systeme
- Virtueller Datenträger - Ermöglicht einem verwalteten Server, auf das lokale Datenträgerlaufwerk der Verwaltungsstation oder auf ISO CD/DVD-Images einer Netzwerkfreigabe zuzugreifen
- Überwachung - Zugriff auf Systeminformationen und Komponentenstatus
- Zugriff auf Systemprotokolle - Zugriff auf das Systemereignisprotokoll, das iDRAC-Protokoll und den Bildschirm des letzten Absturzes des abgestürzten oder nicht reagierenden Systems, unabhängig vom Zustand des Betriebssystems
- Dell OpenManage™-Softwareintegration - Ermöglicht den Start der iDRAC-Webschnittstelle von Dell OpenManage Server Administrator oder von IT Assistent
- iDRAC-Warnung - Weist Sie über eine E-Mail-Nachricht oder einen SNMP-Trap auf potenzielle Probleme des verwalteten Knotens hin
- Remote-Stromverwaltung - Remote-Stromverwaltungsfunktionen wie Herunterfahren und Reset von einer Verwaltungskonsole aus
- Unterstützung für die intelligente Plattform-Verwaltungsschnittstelle (IPMI)
- SSL-Verschlüsselung - Bietet sichere Remote-Systemverwaltung über die Webschnittstelle
- Sicherheitsverwaltung auf Kennwortebene - Verhindert den unbefugten Zugriff auf ein Remote-System
- Rollenbasierte Autorität - Zuweisbare Berechtigungen für verschiedene Systemverwaltungs-Tasks

---

iDRAC-Sicherheitsfunktionen

Der iDRAC enthält die folgenden Sicherheitsfunktionen:

- Benutzerauthentifizierung durch Microsoft Active Directory (optional) oder durch hardwaregespeicherte Benutzer-IDs und Kennwörter

- Rollenbasierte Berechtigung, die einem Adminstrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren
- Benutzer-ID- und Kennwort-Konfiguration über die Webschnittstelle oder SM-CLP
- SM-CLP- and Webschnittstellen, die 128-Bit- und 40-Bit-Verschlüsselung unterstützen (für Länder, in denen 128-Bit nicht zulässig sind), verwenden den SSL 3.0-Standard
- Konfiguration der Sitzungszeitüberschreitung (in Sekunden) über die Webschnittstelle oder SM-CLP
- Konfigurierbare IP-Schnittstellen (wo anwendbar)

  ANMERKUNG: Telnet unterstützt SSL-Verschlüsselung nicht.

- Secure Shell (SSH), die eine verschlüsselte Übertragungsschicht zum Zweck höherer 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 iDRAC herstellen

---

Unterstützte Plattformen

Der iDRAC unterstützt die folgenden PowerEdge-Systeme im Dell PowerEdge M1000e-Systemgehäuse:

- PowerEdge M600
- PowerEdge M605
- PowerEdge M805
- PowerEdge M905

Informationen zu den neuesten unterstützten Plattformen finden Sie in der Infodatei zu iDRAC und dem *Dell PowerEdge-Kompatibilitätshandbuch*, das sich auf Dells Support-Website unter **support.dell.com** befindet.

Unterstützte Betriebssysteme

Tabelle 1-1 führt die Betriebssysteme auf, die den iDRAC unterstützen.

Neueste Informationen befinden sich im *Kompatibilitätshandbuch zu Dell OpenManage Server Administrator* auf Dells Support-Website unter **support.dell.com**.

Tabelle 1-1. Unterstützte Betriebssysteme

Betriebssystem-Familie	Betriebssystem
Microsoft Windows	Microsoft® Windows Server® 2003 R2 Standard und Enterprise (32-Bit x86) Editions mit SP2 Microsoft Windows Server 2003 Web, Standard und Enterprise (32-Bit x86) Editions mit SP2 Microsoft Windows Server 2003 Standard und Enterprise (x64) Editions mit SP2 Microsoft Windows Storage Server 2003 R2 Express-, Workgroup-, Standard- und Enterprise x64-Editionen mit SP2 Microsoft Windows Server 2008 Web, Standard und Enterprise (32-Bit x 86) Editions Microsoft Windows Server 2008 Web, Standard, Enterprise und Datacenter (x64) Editions **ANMERKUNG:** Achten Sie beim Installieren des Windows Server 2003 mit Service Pack 1 auf Änderungen an den DCOM-Sicherheitseinstellungen. Weitere Informationen finden Sie in Artikel 903220 auf der Support-Website von Microsoft unter **support.microsoft.com/kb/903220**.
Red Hat® Linux®	Enterprise Linux WS, ES und AS (Version 4) (x86 und x86_64) Enterprise Linux 5 (x86 und x86-64)
SUSE® Linux	Enterprise Server 9 mit Aktualisierung 2 und Aktualisierung 3 (x86_64) Enterprise Server 10 (Gold) (x86_64)

Unterstützte Webbrowser

Tabelle 1-2 führt die als iDRAC-Clients unterstützten Webbrowser auf.

Neueste Informationen befinden sich in der iDRAC-Infodatei und dem *Kompatibilitätshandbuch zu Dell OpenManage Server Administrator* auf Dells Support-Website unter **support.dell.com**.

ANMERKUNG: Aufgrund von ernsthaften Sicherheitslücken wird SSL 2.0 nicht mehr unterstützt. Ihr Browser muss so konfiguriert sein, dass SSL 3.0 für eine einwandfreie Arbeitsweise aktiviert werden kann.

Tabelle 1-2. Unterstützte Web-Browser

Betriebssystem	Unterstützter Internet-Browser
Windows	Internet Explorer 6.0 mit Service Pack 2 (SP2), nur für Windows XP und Windows 2003 R2 SP2 Internet Explorer 7.0, nur für Windows Vista, Windows XP, Windows 2003 R2 SP2 und Windows Server 2008 Mozilla Firefox 2.0, für Windows (nur Java vKVM/vMedia-Konsole)
Linux	Mozilla Firefox 1.5, nur auf SUSE Linux (Version 10) Mozilla Firefox 2.0, auf Red Hat Enterprise Linux 4 und 5 (32-Bit oder 64-Bit) und Suse Linux Enterprise Server 10 (32-Bit oder 64-Bit)

Unterstützte Remote-Zugriffs-Verbindungen

Tabelle 1-3 führt die Verbindungsfunktionen auf.

Tabelle 1-3. Unterstützte Remote-Zugriffs-Verbindungen

Verbindung	Funktionen
iDRAC-NIC	• 10Mbps/100Mbs/1Gbps Ethernet über CMC Gb Ethernet-Schnittstelle • DHCP-Unterstützung • SNMP-Traps und E-Mail-Ereignis-Benachrichtigung • Unterstützung für SM-CLP-Befehlsshell (Telnet oder SSH), für Verfahren wie iDRAC-Konfigurations-, Systemstart-, Reset-, Einschalt- und Herunterfahren-Befehle • Unterstützung für IPMI-Dienstprogramme, wie z. B. ipmitool und ipmishell

iDRAC-Schnittstellen

Tabelle 1-4 führt die Anschlüsse auf, die iDRAC auf Verbindungen abhört. Tabelle 1-5 kennzeichnet die Anschlüsse, die der iDRAC als Client verwendet. Diese Informationen sind erforderlich, wenn Firewalls für den Remote-Zugriff auf einen iDRAC geöffnet werden.

Tabelle 1-4. Abhöranschlüsse des iDRAC-Servers

Anschlussnummer	Funktion
22*	Secure Shell (SSH)
23*	Telnet
80*	http
443*	HTTPS
623	RMCP/RMCP+
3668*, 3669*	Virtueller Datenträger-Dienst
3770*, 3771*	Virtueller Datenträger - Sicherer Dienst
5900*	Konsolenumleitung: Tastatur/Maus
5901*	Konsolenumleitung: Video
* Konfigurierbarer Anschluss	

Tabelle 1-5. iDRAC-Client-Schnittstellen

Anschlussnummer	Funktion
25	SMTP
53	DNS
68	DHCP-zugewiesene IP-Adresse
69	TFTP
162	SNMP-Trap
636	LDAPS

Weitere nützliche Dokumente

Zusätzlich zu diesem *Benutzerhandbuch* enthalten die folgenden Dokumente weitere Informationen zum Setup und Betrieb des iDRAC auf dem System:

- Die iDRAC-Online-Hilfe enthält Informationen über die Verwendung der Webschnittstelle.
- Das *Dell Chassis Management Controller-Benutzerhandbuch* enthält Informationen zur Verwendung des Controllers, der alle Module im Gehäuse verwaltet, das den PowerEdge-Server enthält.
- Das *Dell OpenManage IT Assistant-Benutzerhandbuch* enthält Informationen über die Anwendung des IT Assistant.
- Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen über die Installation und Verwendung von Server Administrator.
- Das *Benutzerhandbuch zu Dell Update Packages* enthält Informationen zum Abrufen und Verwenden von Dell Update Packages als Teil Ihrer Systemaktualisierungsstrategie.

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

- Das *Produktinformationshandbuch* enthält wichtige Informationen zu Sicherheits- und Betriebsbestimmungen. Garantiebestimmungen können als separates Dokument beigelegt sein.
- Im zusammen mit der Rack-Lösung gelieferten *Rack-Installationshandbuch* bzw. in der *Rack-Installationsanleitung* wird beschrieben, wie das System in einem Rack installiert wird.
- Das *Handbuch zum Einstieg* enthält eine Übersicht über die Systemfunktionen, Einrichtung des Systems und technische Daten.
- Im *Hardware-Benutzerhandbuch* erhalten Sie Informationen über Systemfunktionen, zur Fehlerbehebung am System und zum Installieren oder Austauschen von Systemkomponenten.
- In der Dokumentation zur Systemverwaltungssoftware sind die Merkmale, die Anforderungen, die Installation und der grundlegende Einsatz der Software beschrieben.
- In der Dokumentation zum Betriebssystem wird beschrieben, wie das Betriebssystem installiert (sofern erforderlich), konfiguriert und verwendet wird.
- Dokumentationen für alle separat erworbenen Komponenten enthalten Informationen zur Konfiguration und zur Installation dieser Zusatzgeräte.
- Möglicherweise sind auch aktualisierte Dokumente beigelegt, in denen Änderungen am System, an der Software oder an der Dokumentation beschrieben sind.

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

- Anmerkungen zur Version oder Infodateien sind eventuell eingeschlossen, um Aktualisierungen am System oder der Dokumentation in letzter Minute zu bieten, oder fortgeschrittenes technisches Referenzmaterial, das für erfahrene Benutzer oder Techniker beabsichtigt ist.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC konfigurieren

Integrated Dell™ Remote Access Controller Firmware Version 1.2-Benutzerhandbuch

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

Bevor Sie beginnen

Legen Sie vor der Konfiguration des iDRAC folgende Artikel zurecht:

- *Benutzerhandbuch zur Dell Chassis Management Controller-Firmware*
- CD *Dell PowerEdge Installation and Server Management*
- CD *Dell Systems Management Consoles*
- CD *Dell PowerEdge Service and Diagnostic Utilities*
- CD *Dell PowerEdge Documentation*

Schnittstellen zur Konfiguration des iDRAC

Sie können den iDRAC mithilfe des iDRAC-Konfigurationsdienstprogramms, der iDRAC-Webschnittstelle, der lokalen RACADM-CLI oder der SM-CLP-CLI konfigurieren. Die lokale RACADM-CLI steht nach der Installation des Betriebssystems und der Dell PowerEdge-Server Management-Software auf dem verwalteten Server zur Verfügung. Tabelle 2-1 beschreibt diese Schnittstellen.

Für höhere Sicherheit kann der Zugang zu der iDRAC-Konfiguration über das iDRAC-Konfigurationsdienstprogramm oder die lokale RACADM-CLI durch einen RADADM-Befehl (siehe Übersicht der RACADM-Unterbefehle) oder von der GUI (siehe Lokalen Konfigurationszugriff aktivieren oder deaktivieren) deaktiviert werden.

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

Tabelle 2-1. Konfigurationsschnittstellen

Schnittstelle	Beschreibung
iDRAC-Konfiguration Dienstprogramm	Wird zum Zeitpunkt des Starts auf das iDRAC-Konfigurationshilfsprogramm zugegriffen, ist dieses beim Installieren eines neuen PowerEdge-Servers nützlich. Verwenden Sie es zum Einrichten des Netzwerks und grundlegender Sicherheitsfunktionen sowie zum Aktivieren anderer Funktionen.
iDRAC-Webschnittstelle	Die iDRAC-Webschnittstelle ist eine browserbasierte Verwaltungsanwendung, die Sie zur interaktiven Verwaltung des iDRAC und zur Überwachung des verwalteten Servers verwenden können. Sie stellt die primäre Schnittstelle für alltägliche Aufgaben wie die Überwachung des Systemzustands, die Anzeige des Systemereignisprotokolls, die Verwaltung lokaler iDRAC-Benutzer und das Starten der CMC-Webschnittstelle und der Konsolenumleitungssitzungen dar.
CMC-Webschnittstelle	Zusätzlich zum Überwachen und Verwalten des Gehäuses kann die CMC-Webschnittstelle auch dazu verwendet werden, den Status des verwalteten Servers anzuzeigen, iDRAC-Netzwerkeinstellungen zu konfigurieren, sowie den verwalteten Server zu starten, anzuhalten oder zurückzusetzen.
Gehäuse-LCD-Bedienfeld	Das LCD-Bedienfeld des Gehäuses, das den iDRAC enthält, kann zur Anzeige des High-Level-Status der Server im Gehäuse verwendet werden. Während der ursprünglichen Konfiguration des CMC erlaubt Ihnen der Konfigurationsassistent, die DHCP-Konfiguration des iDRAC-Netzwerkbetriebs zu aktivieren.
Lokaler RACADM	Die Befehlszeilenoberfläche des lokalen RACADM wird auf dem lokalen Server ausgeführt. Es kann entweder von der iKVM oder von einer Konsolenumleitungssitzung, die von der iDRAC-Webschnittstelle aus eingeleitet wurde, auf sie zugegriffen werden. RACADM wird auf dem verwalteten Server installiert, wenn Sie den Dell OpenManage Server Administrator installieren. RACADM-Befehle bieten Zugriff auf fast alle Funktionen des iDRAC. Sie können Sensordaten, Protokolleinträge bei Systemereignissen sowie die im iDRAC geführten aktuellen Status- und Konfigurationswerte kontrollieren. Sie können iDRAC-Konfigurationswerte verändern, lokale Benutzer verwalten, Funktionen aktivieren und deaktivieren sowie Stromfunktionen wie das Herunterfahren oder Neustarten des verwalteten Servers ausführen.
iVM-CLI	Die iDRAC-Befehlszeilenoberfläche des virtuellen Datenträgers (iVM-CLI) bietet dem verwalteten Server Zugriff auf Datenträger auf der Verwaltungsstation. Sie ist hilfreich beim Entwickeln von Skripts zum Installieren von Betriebssystemen auf mehreren verwalteten Servern.
SM-CLP	SM-CLP ist die Implementierung des im DRAC umgesetzten Serververwaltungs-/Workgroup-Serververwaltungs-Befehlszeilenprotokolls. Auf die SM-CLP-Befehlszeile kann durch die Anmeldung bei iDRAC über Telnet oder SSH zugegriffen werden. SM-CLP-Befehle setzen einen nützlichen Teilsatz der Befehle des lokalen RACADM um. Die Befehle sind hilfreich beim Scripting, da sie von der Befehlszeile einer Management Station aus ausgeführt werden können. Die Befehlsausgabe kann in eindeutigen Formaten,

	einschließlich XML, abgerufen werden, wodurch das Scripting und die Integration mit vorhandenen Berichterstattungs- und Verwaltungshilfsprogrammen erleichtert wird. Ein Vergleich der RACADM- und SM-CLP-Befehle ist unter RACADM- und SM-CLP-Äquivalenzen aufgeführt.
IPMI	IPMI definiert einen Standard für integrierte Verwaltungssubsysteme wie den iDRAC zur Kommunikation mit anderen integrierten Systemen und Verwaltungsanwendungen. Sie können die iDRAC-Webschnittstellen-, SM-CLP- oder RACADM-Befehle zur Konfiguration von IPMI-Plattformereignisfiltern (PEFs) und Plattformereignis-Traps (PETs) verwenden. PEFs bewirken, dass der iDRAC auswählbare Maßnahmen ausführt (z. B. den Neustart des verwalteten Servers), wenn er einen entsprechenden Zustand feststellt. PETs weisen den iDRAC an, E-Mail- oder IPMI-Warnungen zu senden, wenn er bestimmte Ereignisse oder Zustände feststellt. Sie können auch standardmäßige IPMI-Hilfsprogramme wie **ipmitool** und **ipmishell** bei iDRAC verwenden, wenn Sie IPMI-über-LAN aktivieren.

Konfigurations-Tasks

Dieser Abschnitt stellt eine Übersicht der Konfigurations-Tasks für die Verwaltungsstation, den iDRAC und den verwalteten Server dar. Die auszuführenden Tasks schließen die Konfiguration des iDRAC ein, damit er im Remote-Zugriff eingesetzt werden kann, die Konfiguration der iDRAC-Funktionen, die Sie verwenden möchten, die Installation des Betriebssystems auf dem verwalteten Server und die Installation der Verwaltungssoftware auf der Verwaltungsstation und dem verwalteten Server.

Die zum Ausführen der einzelnen Tasks verwendbaren Konfigurations-Tasks sind unterhalb des Tasks aufgeführt.

ANMERKUNG: Bevor die in diesem Handbuch besprochenen Konfigurationsverfahren ausgeführt werden können, müssen die CMC- und E/A-Module im Gehäuse installiert und konfiguriert werden und der PowerEdge-Server muss physisch im Gehäuse installiert sein.

Verwaltungsstation konfigurieren

Richten Sie eine Verwaltungsstation ein, indem Sie die Dell OpenManage-Software, einen Webbrowser sowie andere Softwaredienstprogramme installieren.

- Siehe Konfiguration der Verwaltungsstation

iDRAC-Netzwerkbetrieb konfigurieren

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

ANMERKUNG: Greifen Sie auf die iDRAC-Konfiguration über das iDRAC-Konfigurationsdienstprogramm zu oder die lokale RACADM-CLI kann durch einen RADADM-Befehl (siehe Übersicht der RACADM-Unterbefehle) oder von der GUI (siehe Lokalen Konfigurationszugriff aktivieren oder deaktivieren) deaktiviert werden.

ANMERKUNG: Eine Änderung der iDRAC-Netzwerkeinstellungen unterbricht alle aktuellen Netzwerkverbindungen zum iDRAC.

ANMERKUNG: Die Option zum Konfigurieren des Servers über das LCD-Bedienfeld ist *nur* während der ersten CMC-Konfiguration verfügbar. Sobald das Gehäuse bereitgestellt ist, kann der iDRAC nicht mehr über das LCD-Bedienfeld neu konfiguriert werden.

ANMERKUNG: Das LCD-Bedienfeld kann zum Aktivieren des DHCP zur Konfiguration des iDRAC-Netzwerks verwendet werden. Wenn Sie statische Adressen zuweisen möchten, ist es erforderlich, dass Sie das iDRAC-Konfigurationshilfsprogramm oder die CMC-Webschnittstelle verwenden.

- LCD-Bedienfeld des Gehäuses - siehe *Benutzerhandbuch zur Dell Chassis Management Controller-Firmware*.
- iDRAC-Konfigurationsdienstprogramm - siehe LAN
- CMC-Webschnittstelle - siehe Netzwerkbetrieb mittels der CMC-Webschnittstelle konfigurieren
- RACADM - siehe cfgLanNetworking

iDRAC-Benutzer konfigurieren

Benutzer und Berechtigungen für den lokalen iDRAC einrichten. Der iDRAC führt eine Tabelle mit sechzehn lokalen Benutzern der Firmware. Sie können für diese Benutzer Benutzernamen, Kennwörter und Rollen einrichten.

- iDRAC-Konfigurationsdienstprogramm (konfiguriert nur den Benutzer auf Administratorebene) - siehe LAN-Benutzerkonfiguration
- iDRAC-Webschnittstelle - siehe iDRAC-Benutzer hinzufügen und konfigurieren
- RACADM - siehe iDRAC-Benutzer hinzufügen

Active Directory konfigurieren

Zusätzlich zu den lokalen Benutzern des iDRAC können Sie Microsoft® Active Directory® zum Authentifizieren von iDRAC-Benutzeranmeldungen verwenden.

- Siehe iDRAC mit Microsoft Active Directory verwenden

IP-Filterung und IP-Blockierung konfigurieren

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

- iDRAC-Webschnittstelle - siehe IP-Filterung und IP-Blockierung konfigurieren
- RACADM - siehe IP-Filterung konfigurieren (IpBereich), IP-Blockierung konfigurieren

Plattformereignisse konfigurieren

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

Konfigurieren Sie Plattformereignisfilter (PEFs) zum Auswählen der Ereignisse, die Sie feststellen möchten, wie z. B. das Neustarten eines verwalteten Servers beim Feststellen eines Ereignisses.

- iDRAC-Webschnittstelle - siehe Plattformereignisfilter (PEF) konfigurieren
- RACADM - siehe PEF konfigurieren

Konfigurieren Sie Plattformereignis-Traps (PETs) zum Senden von Warnungsbenachrichtigungen an eine IP-Adresse, wie z. B. eine Verwaltungsstation mit IPMI-Software, oder zum Senden einer E-Mail an eine festgelegte E-Mail-Adresse.

- iDRAC-Webschnittstelle - siehe Plattformereignis-Traps (PET) konfigurieren
- RACADM - PET konfigurieren

Lokalen Konfigurationszugriff aktivieren oder deaktivieren

Zugriff auf kritische Konfigurationsparameter, wie z. B. Netzwerkkonfiguration und Benutzerberechtigungen, kann deaktiviert werden. Sobald er deaktiviert ist, bleibt die Einstellung beim Neustart beständig. Konfigurationsschreibzugriff wird sowohl für das lokale RACADM-Programm als auch für das iDRAC-Konfigurationsdienstprogramm (beim Start) blockiert. Internetzugriff auf Konfigurationsparameter wird nicht behindert und Konfigurationsdaten stehen immer zur Ansicht zur Verfügung. Informationen über die iDRAC-Webschnittstelle finden Sie unter Lokalen Konfigurationszugriff aktivieren oder deaktivieren. cfgRac-Tuning-Befehle siehe cfgRacTuning.

Seriell über LAN konfigurieren

Seriell über LAN (SOL) ist eine IPMI-Funktion, die Ihnen ermöglicht, den E/A des seriellen Anschlusses des verwalteten Servers über das Netzwerk umzuleiten. SOL aktiviert die Konsolenumleitungsfunktion für iDRAC.

- iDRAC-Webschnittstelle - siehe Lokalen Konfigurationszugriff aktivieren oder deaktivieren
- Siehe auch GUI-Konsolenumleitung verwenden

iDRAC-Dienste konfigurieren

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

- iDRAC-Webschnittstelle - siehe iDRAC-Dienste konfigurieren
- RACADM - siehe iDRAC-Telnet- und SSH-Dienste mittels lokalem RACADM konfigurieren

SSL konfigurieren

SSL für den iDRAC-Web Server konfigurieren.

- iDRAC-Webschnittstelle - siehe Secure Sockets Layer (SSL)
- RACADM - siehe cfgRacSecurity, sslcsrgen, sslcertupload, sslcertdownload, sslcertview

Virtuellen Datenträger konfigurieren

Konfigurieren Sie die Funktion des virtuellen Datenträgers, so dass Sie das Betriebssystem auf dem PowerEdge-Server installieren können. Der virtuelle Datenträger ermöglicht dem verwalteten Server, auf Datenträgergeräte der Verwaltungsstation oder auf ISO-CD/DVD-Images einer Netzwerkfreigabe zuzugreifen, als wären sie Geräte auf dem verwalteten Server.

- iDRAC-Webschnittstelle - siehe Virtuellen Datenträger konfigurieren und verwenden

- iDRAC-Konfigurationsdienstprogramm - siehe Virtueller Datenträger

Managed Server-Software installieren

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

- Konsolenumleitung - siehe Softwareinstallation auf dem verwalteten Server
- iVM-CLI - siehe Befehlszeilenoberflächen-Dienstprogramm des virtuellen Datenträgers verwenden

Verwalteten Server für die Funktion Bildschirm Letzter Absturz konfigurieren

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

- Verwalteter Server - siehe Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz, Die Windows-Option Automatischer Neustart deaktivieren

---

Netzwerkbetrieb mittels der CMC- Webschnittstelle konfigurieren

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

ANMERKUNG: Der Standardbenutzername für das CMC-Modul ist **root**, und das Standardkennwort ist **calvin**.

ANMERKUNG: Die CMC-IP-Adresse steht auf der iDRAC-Webschnittstelle zur Verfügung, wenn Sie auf **System**→ **Remote-Zugriff**→ **CMC** klicken. Es ist auch möglich, die CMC-Webschnittstelle von dieser Seite aus zu starten.

1. Melden Sie sich über den Webbrowser bei der CMC- Webbenutzeroberfläche an, indem Sie eine Internetadresse im Format https://<*CMC-IP-Adresse*> oder https://<*CMC-DNS-Name*> eingeben.
2. Geben Sie den Benutzernamen und das Kennwort für den CMC ein, und klicken Sie auf **OK**.
3. Klicken Sie auf das Plus-Symbol (+) neben **Chassis** (Gehäuse) in der linken Spalte und anschließend auf **Server**.
4. Klicken Sie auf **Setup**→ **Netzwerk bereitstellen.**
5. Aktivieren Sie das LAN für den Server durch Markieren des Kontrollkästchens neben dem Server unterhalb der Überschrift **LAN aktivieren**.
6. Aktivieren oder deaktivieren Sie IPMI über LAN, indem Sie das Kontrollkästchen neben dem Server unter der Überschrift **Enable IPMI over LAN** (IPMI-Über-LAN aktivieren) markieren bzw. die Markierung entfernen.
7. Aktivieren oder deaktivieren Sie DHCP für den Server, indem Sie das Kontrollkästchen neben dem Server unterhalb der Überschrift **DHCP aktiviert** markieren oder seine Markierung aufheben.
8. Ist DHCP deaktiviert, geben Sie die statische IP-Adresse, die Netzmaske und das Standard-Gateway für den Server ein.
9. Klicken Sie auf **Änderungen anwenden** am unteren Seitenrand.

Verbindungen der FlexAddress-Mezzanine- Kartenarchitektur anzeigen

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

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

Die Konfiguration der Funktion FlexAddress wird mithilfe der CMC-Webschnittstelle ausgeführt. Weitere Informationen zur Funktion FlexAddress und deren Konfiguration finden Sie im *Benutzerhandbuch zur Dell Chassis Management Controller-Firmware Version 1.20*.

Sobald die Funktion FlexAddress aktiviert und für das Gehäuse konfiguriert wurde, klicken Sie auf **System**→ **Eigenschaften**→ **WWN/MAC**, damit eine Liste der installierten Mezzanine-Karten, der Architekturen und Anschlüsse, mit denen sie verbunden sind, des Architekturanschluss-Standorts, des Architekturtyps und der Server-konfigurierten oder Gehäuse-zugewiesenen MAC-Adressen für jedes installierte und eingebettete Ethernet und den optionalen Mezzanine-Kartenanschluss angezeigt wird.

Klicken Sie auf **System**→ **Eigenschaften**→ **Zusammenfassung**, um eine Liste der installierten Mezzanine-Karten, des installierten Mezzanine-Kartentyps und der FlexAddress, falls konfiguriert, anzuzeigen.

---

iDRAC-Firmware aktualisieren

Durch das Aktualisieren der iDRAC-Firmware wird ein neues Firmware-Image im Flash-Speicher des iDRAC installiert. Die Firmware kann anhand einer der folgenden Methoden aktualisiert werden:

- SM-CLP-Befehl **load**
- iDRAC-Webschnittstelle
- Dell Update Package (für Linux oder Microsoft Windows)
- DOS-iDRAC-Firmware-Aktualisierungsdienstprogramm
- CMC-Webschnittstelle (nur wenn iDRAC-Firmware beschädigt ist)

Firmware-Paket oder Update Package herunterladen

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

Laden Sie zum Aktualisieren der iDRAC-Firmware über die iDRAC-Webschnittstelle oder SM-CLP oder zum Wiederherstellen des iDRAC mittels der CMC-Webschnittstelle das als selbstextrahierendes Archiv verpackte Binärbild herunter.

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

Laden Sie zum Aktualisieren der iDRAC-Firmware anhand des DOS-iDRAC-Firmware-Aktualisierungsdienstprogramms sowohl das Aktualisierungsdienstprogramm als auch das Binärbild herunter, die in selbstextrahierenden Archivdateien verpackt sind.

Firmware-Aktualisierung ausführen

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

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

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

Legen Sie beim Verwenden des SM-CLP-Befehls **load** das Firmware-Binärbild in einem Verzeichnis ab, wo ein TFTP-Server (Einfaches Dateiübertragungsprotokoll) es an den iDRAC weiterleiten kann. Siehe iDRAC-Firmware mittels SM-CLP aktualisieren.

Legen Sie das Firmware-Binärbild bei Verwendung der iDRAC-Webschnittstelle oder der CMC-Webschnittstelle auf einer Festplatte ab, auf die die Verwaltungsstation zugreifen kann, von der aus Sie die Webschnittstelle ausführen. Siehe iDRAC-Firmware aktualisieren.

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

Die CMC-Webschnittstelle kann *nur* dann zum Aktualisieren der Firmware verwendet werden, wenn der CMC feststellt, dass die iDRAC-Firmware beschädigt ist, was eintreten könnte, wenn der Aktualisierungsvorgang der iDRAC-Firmware vor dessen Abschluss unterbrochen wird. Siehe iDRAC-Firmware mittels CMC wiederherstellen.

ANMERKUNG: Nachdem der CMC die iDRAC-Firmware aktualisiert hat, erstellt der iDRAC neue SHA1- und MD5-Schlüssel für das SSL-Zertifikat. Da die Schlüssel von denen im offenen Webbrowser abweichen, müssen alle mit dem iDRAC verbundenen Browserfenster nach der Firmwareaktualisierung geschlossen werden. Wenn die Browserfenster nicht geschlossen sind, wird die Fehlermeldung **Ungültiges Zertifikat** eingeblendet.

ANMERKUNG: Wenn Sie die iDRAC-Firmware von Version 1.20 auf eine frühere Version zurückdatieren, muss das vorhandene Internet Explorer ActiveX Browser-Plugin auf jeder Windows-basierten Management Station gelöscht werden, damit die Firmware eine kompatible Version des ActiveX-Plugins installieren kann. Um das ActiveX-Plugin zu löschen, wechseln Sie zu **c:\WINNT\Downloaded Program Files** und löschen Sie die Datei **DELL IMC-KVM-Viewer**.

DOS-Aktualisierungsdienstprogramm verwenden

Starten Sie zum Aktualisieren der iDRAC-Firmware unter Verwendung des DOS-Aktualisierungsdienstprogramms den verwalteten Server zu DOS, und führen Sie den Befehl **idrac16d** aus. Die Syntax für den Befehl lautet:

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

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

Die Optionen sind wie folgt:

`-f` - erzwingt die Aktualisierung. Die Option `-f` kann dazu verwendet werden, die Firmware auf ein früheres Image *zurückzustufen*.

`-i=<Dateiname>` - bestimmt das Dateinamen-Image, das das Firmware-Image enthält. Diese Option ist erforderlich, wenn der Firmware-Dateiname geändert wurde und jetzt vom Standardnamen **firmimg.imc** abweicht.

`-l=<Protokolldatei>` - protokolliert die Ausgabe der Aktualisierungsaktivität. Diese Option wird für das Debuggen verwendet.

HINWEIS: Wenn Sie zum Befehl **idrac16d** falsche Argumente eingeben oder die Option -h angeben, tritt in der Gebrauchsausgabe eventuell eine zusätzliche Option, -nopresconfig, auf. Diese Option wird zum Aktualisieren der Firmware ohne Bewahren von Konfigurationsinformationen verwendet. Diese Option sollte **nicht** verwendet werden, da durch sie alle vorhandenen iDRAC-Konfigurationsinformationen wie IP-Adressen, Benutzer und Kennwörter *gelöscht* werden.

Überprüfen der Digitalsignatur

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

Fall der Gnu Privacy Guard (GPG) noch nicht auf dem System installiert ist, installieren Sie ihn jetzt, damit Digitalsignaturen verifiziert werden können. Zur Verwendung des Standardüberprüfungsverfahrens führen Sie folgende Schritte durch:

1. Laden Sie den öffentlichen Dell Linux-GnuPG-Schlüssel herunter, falls er nicht bereits vorhanden ist, indem Sie zu **lists.us.dell.com** wechseln und auf den Link **Öffentlicher Dell-GPG-Schlüssel** klicken. Speichern Sie die Datei auf Ihr lokales System. Der Standardname lautet **linux-security- publickey.txt**.

2. Importieren Sie den öffentlichen Schlüssel zur vertrauenswürdigen gpg- Datenbank durch Ausführen des folgenden Befehls:

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

ANMERKUNG: Zum Abschließen des Verfahrens müssen Sie einen eigenen privaten Schlüssel besitzen.

3. Um eine Warnung bzgl. eines nicht vertrauenswürdigen Schlüssels zu vermeiden, ändern Sie die Vertrauensstufe für den öffentlichen Dell-GPG-Schlüssel.

   e. Geben Sie den folgenden Befehl ein:

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

   f. Geben Sie im GPG-Schlüsseleditor fpr ein. Die folgende Meldung wird eingeblendet:

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

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

   g. Geben Sie, während Sie sich im GPG- Schlüsselbearbeitungsprogramm befinden, trust ein. Das folgende Menü wird eingeblendet:

   ```
   Please decide how far you trust this user to correctly verify other users' keys (by looking at passports, checking fingerprints from
   different sources, etc.)


     1 = I don't know or won't say
     2 = I do NOT trust
     3 = I trust marginally
     4 = I trust fully
     5 = I trust ultimately
     m = back to the main menu

   Your decision?
   ```

   h. Geben Sie 5 <Eingabe> ein. Die folgende Eingabeaufforderung wird eingeblendet:

   ```
   Do you really want to set this key to ultimate trust? (y/N)
   ```

   i. Geben Sie y <Eingabe> ein, um Ihre Auswahl zu bestätigen.

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

   Der öffentliche Schlüssel muss nur einmal importiert und bestätigt werden.

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

   ANMERKUNG: Jedes Linux-Aktualisierungspaket enthält eine separate Signaturdatei, die auf derselben Webseite wie das Aktualisierungspaket angezeigt wird. Sie benötigen sowohl das Aktualisierungspaket als auch die zugehörige Signaturdatei zur Verifizierung. Standardmäßig erhält die Signaturdatei denselben Namen wie der DUP-Dateiname, mit der Erweiterung **.sign**. Wenn zum Beispiel ein Linux-DUP **PEM600_BIOS_LX_2.1.2.BIN** bezeichnet wird, dann ist sein Signaturdateiname **PEM600_BIOS_LX_2.1.2.BIN.sign**. Das iDRAC-Firmware-Image hat auch eine zugeordnete **.sign**-Datei, die im selbstextrahierenden Archiv mit dem Firmware-Image enthalten ist. Klicken Sie zum Herunterladen der Dateien mit der rechten Maustaste auf den Download-Link, und verwenden Sie die Dateioption **Ziel speichern unter...**.

5. Überprüfen Sie das Aktualisierungspaket:

   ```
   gpg --verify <Linux-Update Package Signaturdateiname> <Linux-Update Package Dateiname>
   ```

Im folgenden Beispiel werden die Schritte zum Überprüfen eines PowerEdge M600-BIOS-Aktualisierungspakets dargestellt:

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

   - PEM600_BIOS_LX_2.1.2.BIN.sign

- PEM600_BIOS_LX_2.1.2.BIN

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

   ```
   gpg --import <linux-security-publickey.txt>
   ```

   Die folgende Ausgabemeldung wird eingeblendet:

   ```
   gpg: key 23B66A9D: "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>" not changed
   gpg: Total number processed: 1
   gpg: unveräunchanged: 1
   ```

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

   a. Geben Sie folgenden Befehl ein:

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

   b. Geben Sie in der Befehlsaufforderung die folgenden Befehle ein:

      ```
      fpr
      trust
      ```

   c. Geben Sie 5 <Eingabe> ein, um Ich habe absolutes Vertrauen aus dem Menü auszuwählen.

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

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

   Damit ist die Validierung des öffentlichen Schlüssels von Dell abgeschlossen.

4. Überprüfen Sie die Digitalsignatur des PEM600-BIOS-Pakets durch Ausführen des folgenden Befehls:

   ```
   gpg --verify PEM600_BIOS_LX_2.1.2.BIN.sign PEM600_BIOS_LX_2.1.2.BIN
   ```

   Die folgende Ausgabemeldung wird eingeblendet:

   ```
   gpg: Signature made Fri Jul 11 15:03:47 2008 CDT using DSA key ID 23B66A9D
   gpg: Good signature from"Dell, Inc. (Product Group) <linux-security@dell.com>"
   ```

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

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

Löschen Sie den Cache Ihres Browsers

Damit die Funktionen im neuesten iDRAC verwendet werden können, muss der Browser-Cache zur Entfernung/Löschung aller *alter* Webseiten, die eventuell im System gespeichert sind, gelöscht werden.

Internet Explorer

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf **Extras** und dann auf **Internetoptionen**.

   Das Fenster **Internetoptionen** wird angezeigt.

3. Klicken Sie auf die Registerkarte **Allgemein**.
4. Klicken Sie unter **Temporäre Internetdateien** auf **Dateien löschen**.

   Das Fenster **Dateien löschen** wird angezeigt.

5. Setzen Sie ein Häkchen bei **Alle Offlineinhalte löschen** und klicken Sie dann auf **OK**.
6. Klicken Sie auf OK, um das Fenster **Internetoptionen** zu schließen.

Firefox

1. Starten Sie Firefox.
2. Klicken Sie auf **Bearbeiten**→ **Einstellungen**.
3. Klicken Sie auf die Registerkarte **Datenschutz**.
4. Klicken Sie auf **Cache jetzt löschen**.
5. Klicken Sie auf **Close** (Schließen).

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfiguration der Verwaltungsstation

Integrated Dell™ Remote Access Controller Firmware Version 1.2-Benutzerhandbuch

Eine Verwaltungsstation ist ein Computer zum Überwachen und Verwalten der PowerEdge-Server und anderer Module im Gehäuse. In diesem Abschnitt werden Softwareinstallations- und konfigurations-Tasks beschrieben, über die eine Verwaltungsstation zum Arbeiten mit dem iDRAC eingerichtet wird. Befolgen Sie vor dem Konfigurieren des iDRAC die in diesem Abschnitt beschriebenen Verfahren, um sicherzustellen, dass Sie die Hilfsprogramme installiert und konfiguriert haben, die Sie benötigen.

Schritte zum Einrichten der Verwaltungsstation

Führen Sie zum Einrichten der Verwaltungsstation folgende Schritte aus:

1. Netzwerk für Verwaltungsstation einrichten.
2. Installieren und konfigurieren Sie einen unterstützten Internet-Browser.
3. Installieren Sie eine Java-Laufzeitumgebung (JRE) (optional für Windows).
4. Installieren Sie Telnet- oder SSH-Clients, falls erforderlich.
5. Installieren Sie einen TFTP-Server, falls erforderlich.
6. Installieren Sie Dell OpenManage IT Assistant (optional).

Netzwerkvoraussetzungen für die Verwaltungsstation

Damit die Verwaltungsstation auf den iDRAC zugreifen kann, muss sie sich auf demselben Netzwerk wie die mit "GB1" bezeichnete CMC RJ45-Anschlussschnittstelle befinden. Es ist möglich, das CMC-Netzwerk von dem Netzwerk zu isolieren, auf dem sich der verwaltete Server befindet, sodass die Verwaltungsstation, nicht jedoch der verwaltete Server, LAN-Zugriff auf den iDRAC hat.

Durch die Verwendung der iDRAC-Konsolenumleitungsfunktion (siehe GUI-Konsolenumleitung verwenden) können Sie selbst dann auf die Konsole des verwalteten Servers zugreifen, wenn Sie keinen Netzwerkzugriff auf die Serverschnittstellen haben. Sie können auf dem verwalteten Server auch verschiedene Verwaltungsfunktionen ausführen, wie z. B. den Neustart des Computers unter Verwendung von iDRAC-Einrichtungen. Um auf Netzwerk- und Anwendungsdienste zuzugreifen, die auf dem verwalteten Server gehostet werden, benötigen Sie jedoch eventuell eine zusätzliche NIC im Verwaltungscomputer.

Einen unterstützten Web-Browser konfigurieren

Die folgenden Abschnitte enthalten Anleitungen zum Konfigurieren der unterstützten Webbrowser zur Verwendung mit der iDRAC-Webschnittstelle. Eine Liste unterstützter Webbrowser wird unter Unterstützte Webbrowser angeboten.

Webbrowser öffnen

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

ANMERKUNG: In einigen Situationen, meistens während der ersten Sitzung nach einer Firmwareaktualisierung, wird Benutzern von Internet Explorer 6 eventuell die Meldung **mit Fehlern abgeschlossen** eingeblendet, die in der Statusleiste des Browsers zusammen mit einer teilweise erstellten Seite im Hauptfenster des Browsers angezeigt wird. Dieser Fehler kann auch bei Konnektivitätsproblemen auftreten. Es handelt sich dabei um ein bekanntes Problem bei Internet Explorer 6. Schließen Sie den Browser und starten Sie ihn erneut.

Webbrowser zur Verbindung mit der Webschnittstelle konfigurieren

Wenn Sie von einer Verwaltungsstation aus eine Verbindung zur iDRAC-Webschnittstelle herstellen, die über einen Proxyserver mit dem Internet verbunden

ist, muss der Webbrowser so konfiguriert werden, dass er von diesem Server aus auf das Internet zugreifen kann.

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

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

   Das Fenster **Internetoptionen** wird angezeigt.

   ANMERKUNG: Unterschiedliche Versionen von Internet Explorer besitzen standardmäßig unterschiedliche Sicherheitsebenen. Um sicherzustellen, dass Ihr System einwandfrei funktioniert, klicken Sie auf die Registerkarte **Erweitert** und prüfen Sie, ob bei **Installation auf Nachfrage aktivieren (anderes)**, **Drittbrowsererweiterungen aktivieren**, **Sun Java aktiviert** und **SSL 3.0 verwenden** Häkchen gesetzt sind (Namen können abhängig von Ihrer Version variieren). Wenn Sie an diesen Einstellungen Veränderungen vornehmen, starten Sie den Internet Explorer neu.
3. Klicken Sie auf die Registerkarte **Verbindungen**.
4. Klicken Sie unter **LAN-Einstellungen (Lokales Netzwerk)** auf **LAN- Einstellungen**.
5. Wenn das Kästchen **Proxyserver verwenden** markiert ist, wählen Sie das Kästchen **Proxyserver für lokale Adressen deaktivieren** aus.
6. Klicken Sie zweimal auf **OK**.

iDRAC zur Liste vertrauenswürdiger Domänen hinzufügen

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

Lokalisierte Versionen der Webschnittstelle anzeigen

Die iDRAC-Webschnittstelle wird in den folgenden Betriebssystemsprachen unterstützt:

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

Die ISO-Sprachcodes, die in den runden Klammern stehen, kennzeichnen die spezifischen Sprachvarianten, die unterstützt werden. Die Verwendung der Schnittstelle mit anderen Dialekten oder Sprachen wird nicht unterstützt und funktioniert eventuell nicht wie vorgesehen. Bei einigen unterstützten Sprachen ist es eventuell erforderlich, das Browserfenster auf 1024 Pixel anzupassen, um alle Funktionen zu sehen.

Die iDRAC-Webschnittstelle wurde für den Einsatz mit lokalisierten Tastaturen für die oben aufgeführten spezischen Sprachvarianten entwickelt. Einige Funktionen der iDRAC-Webschnittstelle, wie z. B. Konsolenumleitung, können zusätzliche Schritte für den Zugriff auf bestimmte Funktionen/Buchstaben erfordern. Weitere Einzelheiten, wie lokalisierte Tastaturen in diesen Situationen verwendet werden, finden Sie unter Video Viewer verwenden. Die Verwendung anderer Tastaturen wird nicht unterstützt und könnte unerwartete Probleme verursachen.

Internet Explorer 6.0 (Windows)

Um eine lokalisierte Version der iDRAC-Webschnittstelle in Internet Explorer anzuzeigen, führen Sie folgende Schritte aus:

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 auf <Strg>.
5. Wählen Sie Ihre bevorzugte Sprache aus, und klicken Sie auf **Nach oben**, um die Sprache an die Spitze der Liste zu bewegen.
6. Klicken Sie im Fenster **Spracheinstellung** auf **OK**.

7. Klicken Sie auf **OK**.

Firefox 1.5 (Linux)

Um eine lokalisierte Version der iDRAC-Webschnittstelle in Firefox 1.5 anzuzeigen, führen Sie folgende Schritte aus:

1. Klicken Sie auf **Bearbeiten**→ **Einstellungen** und dann auf die Registerkarte **Erweitert**.
2. Klicken Sie im Abschnitt **Sprache** auf **Auswählen**.
3. Klicken Sie auf **Sprache zum Hinzufügen auswählen...**.
4. Wählen Sie eine unterstützte Sprache aus, und klicken Sie auf **Hinzufügen**.
5. Wählen Sie Ihre bevorzugte Sprache aus, und klicken Sie auf **Nach oben**, um sie an die Spitze der Liste zu bewegen.
6. Klicken Sie im Menü Sprachen auf **OK**.
7. Klicken Sie auf **OK**.

Firefox 2.0 (Linux oder Windows)

Um eine lokalisierte Version der iDRAC-Webschnittstelle in Internet Explorer anzuzeigen, führen Sie folgende Schritte aus:

1. Klicken Sie auf **Extras**→ **Einstellungen** und dann auf die Registerkarte **Erweitert**.
2. Klicken Sie unter **Sprache** auf **Auswählen**.

   Das Fenster **Sprachen** wird eingeblendet.
3. Klicken Sie dann im Drop-Down-Menü **Sprache zum Hinzufügen auswählen...** auf eine unterstützte Sprache, um diese auszuwählen, und klicken Sie dann auf **Hinzufügen**.
4. Klicken Sie auf die gew+nschte Sprache und dann auf **Nach oben**, bis die Sprache an oberster Stelle in der Liste steht.
5. Klicken Sie auf **OK**, um das Fenster **Sprachen** zu schließen.
6. Klicken Sie auf **OK**, um das Fenster **Optionen** zu schließen.

Gebietsschema in Linux einstellen

Für die korrekte Anzeige des Konsolenumleitungs-Viewers ist ein UTF-8-Zeichensatz erforderlich. Ist Ihre Anzeige entstellt, überprüfen Sie das Gebietsschema, und setzen Sie ggf. den Zeichensatz zurück.

In den folgenden Schritten wird gezeigt, wie der Zeichensatz auf einem Red Hat® Enterprise Linux®-Client mit einer GUI in vereinfachtem Chinesisch eingerichtet wird:

1. Öffnen Sie einen Befehls-Terminal.
2. Geben Sie locale ein, und drücken Sie auf <Eingabe>. Eine der folgenden Ausgabe ähnliche Ausgabe wird eingeblendet:

```
LANG=zh_CN.UTF-8
LC_CTYEP="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 nicht zh_CN.UTF-8" einschließen, fahren Sie mit Schritt 4 fort.

4. Bearbeiten Sie die Datei **/etc/sysconfig/i18n** mit einem Textverarbeitungsprogramm.

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:

   ```
   LANF="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.

Wenn Sie von einer anderen Sprache umschalten, ist sicherzustellen, dass diese Korrektur noch gültig ist. Ist dies nicht der Fall, wiederholen Sie das Verfahren.

Whitelist-Funktion in Firefox deaktivieren

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

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

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

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

3. In der Spalte **Einstellungsname** machen Sie **xpinstall.whitelist.required** ausfindig, und doppelklicken Sie darauf.

   Die Werte für **Einstellungsname**, **Status**, **Typ** und **Wert** ändern sich zu fett gedrucktem Text. Der Wert **Status** ändert sich zu **Vom Benutzer eingestellt**, und der Wert **Wert** ändert sich zu **Falsch**.

4. Machen Sie in der Spalte **Einstellungsname xpinstall.enabled** ausfindig.

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

Java-Laufzeitumgebung (JRE) installieren

ANMERKUNG: 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 Internet Explorer verwenden, wenn Sie eine JRE installieren und den Konsolen-Viewer in der iDRAC-Webschnittstelle konfigurieren, bevor Sie den Viewer starten. Weitere Informationen finden Sie unter Konfiguration der Konsolenumleitung auf der iDRAC-Webschnittstelle.

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

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

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

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

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

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

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

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

Telnet- oder SSH-Clients installieren

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

ANMERKUNG: Es kann jeweils nur eine aktive Telnet- oder SSH-Verbindung zum iDRAC existieren. Wenn eine aktive Verbindung besteht, werden andere Verbindungsversuche abgelehnt.

Telnet mit iDRAC

Telnet ist bei Microsoft® Windows®- und Linux-Betriebssystemen eingeschlossen und kann von einer Befehlsshell aus ausgeführt werden. Sie können auch einen kommerziellen oder frei erhältlichen Telnet-Client installieren, der mehr Bedienungsfunktionen als die mit Ihrem Betriebssystem eingeschlossene Standardversion enthält.

Wenn Ihre Verwaltungsstation Windows XP oder Windows 2003 ausführt, kann ein Problem mit den Zeichen in einer iDRAC-Telnet-Sitzung auftreten. Dieses Problem kann sich als eingefrorene Anmeldung äußern, bei der die Eingabetaste nicht reagiert und keine Kennwort-Eingabeaufforderung eingeblendet wird.

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

Die Rücktaste für die Telnet-Sitzung konfigurieren

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

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

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

   ```
   telnet
   ```

   Wenn Sie eine Telnet-Sitzung ausführen, drücken Sie auf die Taste <Strg><]>.
3. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   set bsasdel
   ```

   Die folgende Meldung wird eingeblendet:

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

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

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

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

   ```
   telnet
   ```

SSH mit iDRAC

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

Sie können auf einer Verwaltungsstation PuTTY (Windows) oder `OpenSSH` (Linux) verwenden, um eine Verbindung zum iDRAC eines verwalteten Servers herzustellen. Wenn während des Anmeldeverfahrens ein Fehler auftritt, gibt der **ssh**-Client eine Fehlermeldung aus. Der Meldungstext hängt vom Client ab und wird nicht vom iDRAC gesteuert.

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

Es wird immer jeweils nur eine Telnet- oder SSH-Sitzung unterstützt. Die Sitzungs-Zeitüberschreitung wird durch die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert, wie unter Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank beschrieben.

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

ANMERKUNG: SSHv1 wird nicht unterstützt.

Tabelle 3-1. Verschlüsselungs-Schemata

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

TFTP-Server installieren

ANMERKUNG: Wenn Sie die iDRAC-Webschnittstelle lediglich zur Übertragung von SSL-Zertifikaten und zum Hochladen neuer iDRAC-Firmware verwenden, ist kein TFTP-Server erforderlich.

Das einfache Dateiübertragungsprotokoll (TFTP) ist eine vereinfachte Form des Dateiübertragungsprotokolls (FTP). Es wird mit den SM-CLP- und RACADM-Befehlszeilenoberflächen zum Übertragen von Dateien an den und vom iDRAC verwendet.

Es ist nur dann notwendig, Dateien an den oder vom iDRAC zu kopieren, wenn Sie die iDRAC-Firmware aktualisieren oder Zertifikate auf dem iDRAC installieren. Wenn Sie beim Ausführen dieser Tasks SM-CLP oder RACADM auswählen, muss ein TFTP-Server auf einem Computer ausgeführt werden, auf den der iDRAC über eine IP-Nummer oder einen DNS-Namen zugreifen kann.

Sie können den Befehl **netstat -a** auf einem Windows- oder Linux-Betriebssystem verwenden, um festzustellen, ob bereits ein Abhören durch einen TFTP-Server stattfindet. Schnittstelle 69 ist die Standard-TFTP-Schnittstelle. Wenn kein Server ausgeführt wird, haben Sie die folgenden Möglichkeiten:

- Finden Sie einen anderen Computer auf dem Netzwerk, auf dem ein TFTP-Dienst ausgeführt wird
- Wenn Sie Linux verwenden, installieren Sie einen TFTP-Server von Ihrer Verteilung aus
- Wenn Sie Windows verwenden, installieren Sie einen kommerziellen oder kostenlosen TFTP-Server

---

Dell OpenManage IT Assistant installieren

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

- CD *Dell Systems Management Consoles* - Enthält die neuesten Systemverwaltungs-Konsolenprodukte von Dell, einschließlich Dell OpenManage IT Assistant.
- CD *Dell PowerEdge Service and Diagnostic Utilities* - Bietet die zur Konfiguration des Systems erforderlichen Hilfsprogramme und stellt Firmware, Diagnoseprogramme sowie Dell-optimierte Treiber für das System zur Verfügung.
- CD *Dell PowerEdge Documentation* - Hilft Ihnen, mit Dokumentationen für Systeme, Systems Management Software-Produkten, Peripheriegeräten und RAID-Controllern auf dem neuesten Stand zu bleiben.
- Support-Website und Infodateien von Dell - Suchen Sie in den Infodateien und auf Dells Support-Website unter **support.dell.com** nach aktuellen Informationen zu Ihren Dell-Produkten.

Verwenden Sie die CD *Dell System Management Consoles* zur Installation der Verwaltungskonsolensoftware einschließlich Dell OpenManage IT Assistant auf der Verwaltungsstation. Anleitungen zum Installieren dieser Software sind im *Schnellinstallationshandbuch* enthalten.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Verwalteten Server konfigurieren

Integrated Dell™ Remote Access Controller Firmware Version 1.2-Benutzerhandbuch

In diesem Abschnitt werden die Tasks zum Einrichten des verwalteten Servers zur Erweiterung der Remote-Verwaltungsfähigkeiten beschrieben. Diese Tasks schließen die Installation der Dell Open Manage Server Administrator-Software und die Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz ein.

Softwareinstallation auf dem verwalteten Server

Die Verwaltungssoftware von Dell schließt die folgenden Funktionen ein:

- Lokale RACADM-CLI - ermöglicht, den iDRAC vom verwalteten System aus zu konfigurieren und verwalten. Sie stellt ein leistungsfähiges Tool für Scripting-Konfiguration und Verwaltungs-Tasks dar.
- Der Server Administrator muss die iDRAC-Bildschirmfunktion "Letzter Absturz" verwenden.
- Server Administrator - eine Webschnittstelle, die die Verwaltung des Remote-Systems von einem Remote-Host auf dem Netzwerk ermöglicht.
- Server Administrator Instrumentation Service - bietet Zugriff auf detaillierte Fehler- und Leistungsinformationen, die von industriestandardgemäßen Systemverwaltungsagenten gesammelt werden, und ermöglicht die Remote-Verwaltung überwachter Systeme, einschließlich Herunterfahren, Start und Sicherheit.
- Server Administration Storage Management Service - enthält Speicherverwaltungsinformationen in einer integrierten graphischen Ansicht.
- Server Administrator-Protokolle - zeigt Befehlsprotokolle an, die vom oder an das System ausgegeben wurden, sowie überwachte Hardwareereignisse, POST-Ereignisse und Systemwarnungen. Sie können die Protokolle auf der Homepage anzeigen, drucken oder als Berichte speichern und sie als E-Mail an einen festgelegten Service-Kontakt senden.

Verwenden Sie die CD *Dell PowerEdge Installation and Server Management* zum Installieren von Server Administrator. Anleitungen zum Installieren dieser Software sind im *Schnellinstallationshandbuch* enthalten.

Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz

Der iDRAC kann den Bildschirm Letzter Absturz erfassen, damit Sie ihn in der Webschnittstelle anzeigen und die Ursache des Absturzes des verwalteten Systems feststellen und beheben können. Führen Sie folgende Schritte aus, um die Funktion Bildschirm Letzter Absturz zu aktivieren.

1. Installieren Sie die Software des verwalteten Servers. Weitere Informationen zum Installieren der Managed Server-Software finden Sie im *Server Administrator-Benutzerhandbuch*.

2. Wenn Sie ein Microsoft® Windows®-Betriebssystem ausführen, ist sicherzustellen, dass die Funktion des automatischen Neustarts in den **Windows-Start- und Wiederherstellungs-Einstellungen** abgewählt ist. Siehe Die Windows-Option Automatischer Neustart deaktivieren.

3. Aktivieren Sie den Bildschirm Letzter Absturz (standardmäßig deaktiviert) in der iDRAC-Webschnittstelle.

   Klicken Sie zum Aktivieren des Bildschirms Letzter Absturz in der iDRAC-Webschnittstelle auf **System**→ **Remote-Zugriff**→ **iDRAC**→ **Netzwerk/Sicherheit**→ **Dienste** und markieren Sie das Kontrollkästchen **Aktivieren** unter der Überschrift "Einstellungen des Agenten zur automatischen Systemwiederherstellung".

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

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

4. Aktivieren Sie in der Server Administrator-webbasierten Schnittstelle den Zeitgeber für **Autom. Wiederherstellung** und stellen Sie die Maßnahme **Autom. Wiederherstellung** auf **Reset**, **Ausschalten** oder **Aus- und einschalten** ein.

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

   Der Bildschirm Letzter Absturz ist nicht verfügbar, wenn die Maßnahme **Automatische Wiederherstellung** auf **Herunterfahren** oder **Aus- und einschalten** eingestellt ist, falls der verwaltete Server ausgeschaltet wird.

Die Windows-Option Automatischer Neustart deaktivieren

Um sicherzustellen, dass der iDRAC in der Lage ist, den Bildschirm Letzter Absturz zu erfassen, deaktivieren Sie die Option **Automatischer Neustart** auf

verwalteten Servern, auf denen Microsoft Windows Server® oder Windows Vista® ausgeführt wird.

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC mittels der Webschnittstelle konfigurieren

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

Der iDRAC enthält eine Webschnittstelle, anhand derer Sie die iDRAC-Eigenschaften und -Benutzer konfigurieren, Remote-Verwaltungs-Tasks ausführen sowie Fehlerbehebungsmaßnahmen auf ein (verwaltetes) Remote-System anwenden können. Verwenden Sie die iDRAC-Webschnittstelle für die tägliche Systemverwaltung. Dieses Kapitel gibt darüber Auskunft, wie allgemeine Systemverwaltungs-Tasks über die iDRAC-Webschnittstelle ausgeführt werden und enthält Links zu dazugehörigen Informationen.

Die meisten Webschnittstellen-Konfigurationsaufgaben können auch über Befehle des lokalen RACADM oder über SM-CLP-Befehle ausgeführt werden.

Befehle des lokalen RACADM werden vom verwalteten Server aus ausgeführt. Weitere Informationen zum lokalen RACADM finden Sie unter Befehlszeilenoberfläche des lokalen RACADM verwenden.

SM-CLP-Befehle werden in einer Shell ausgeführt, auf die über eine Telnet- oder SSH-Verbindung im Remote-Verfahren zugegriffen werden kann. Weitere Informationen zu SM-CLP finden Sie unter iDRAC-SM-CLP-Befehlszeilenoberfläche verwenden.

Zugriff auf die Webschnittstelle

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

1. Öffnen Sie ein unterstütztes Web-Browser-Fenster.

   Weitere Informationen finden Sie unter Unterstützte Webbrowser.

2. Geben Sie in das Feld **Adresse** `https://<iDRAC-IP-address>` ein und drücken Sie auf <Eingabe>.

   Wenn die Standard-HTTPS-Portnummer (Port 443) geändert wurde, geben Sie folgendes ein:

   `https://<iDRAC-IP-address>:<port-number>`

   wobei *iDRAC-IP address* die IP-Adresse des iDRAC und *port-number* die HTTPS-Anschlussnummer ist.

   Das iDRAC-**Anmelde**-Fenster wird eingeblendet.

Anmeldung

Sie können sich als iDRAC-Benutzer oder als Microsoft® Active Directory®-Benutzer anmelden. Der Standardbenutzername und das Standardkennwort lauten **root** bzw. **calvin**.

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

Um sich anzumelden, führen Sie die folgenden Schritte aus.

1. Geben Sie eine der folgenden Eingaben in das Feld **Benutzername** ein:

   - Ihren iDRAC-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: <*Domäne*>\<*Benutzername*>, <*Domäne*>/<*Benutzername*> oder <*Benutzer*>@<*Domäne*>. Es wird bei ihnen 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 iDRAC-Benutzerkennwort oder Ihr Active Directory-Benutzerkennwort ein. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

3. Klicken Sie auf **OK**, oder drücken Sie auf 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 erreicht wurde.

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

Mehrere Browser-Register und -Fenster verwenden

Beim Öffnen neuer Register und Fenster weisen unterschiedliche Versionen von Webbrowsern unterschiedliche Verhalten auf. Jedes Fenster öffnet in einer neuen Sitzung, jedoch nicht jedes neue Register. Microsoft Internet Explorer 6 unterstützt keine Register. Deshalb wird jedes geöffnete Browserfenster zu einer neuen iDRAC-Webschnittstellen-Sitzung. Bei Internet Explorer 7 können sowohl Register als auch Fenster geöffnet werden. Jedes Register übernimmt die Merkmale des zuletzt geöffneten Registers. Wenn sich zum Beispiel ein Benutzer mit Hauptbenutzerberechtigungen in einem Register und dann in einem anderen Register als Administrator anmeldet, dann erhalten beide geöffneten Register Administratorrechte. Durch das Schließen eines beliebigen Registers laufen alle Register der iDRAC-Webschnittstelle ab.

Das Register- und Fensterverhalten in Firefox ist genauso wie in Internet Explorer 7.

---

iDRAC-NIC konfigurieren

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

Netzwerk und IPMI-LAN-Einstellungen konfigurieren

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

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

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC**.
2. Klicken Sie auf das Register **Netzwerk/Sicherheit**, um die Seite **Netzwerkkonfiguration** zu öffnen.

   Tabelle 5-1 und Tabelle 5-2 beschreiben die **Netzwerkeinstellungen** und **IPMI-LAN-Einstellungen** auf der Seite **Netzwerk**.
3. Wenn Sie die erforderlichen Einstellungen eingegeben haben, klicken Sie auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-3.

Tabelle 5-1. Netzwerkeinstellungen

Stellung	Beschreibung
NIC aktivieren	Wenn markiert, weist dies darauf hin, dass die NIC aktiviert ist und die verbleibenden Steuerungen dieser Gruppe aktiviert werden. Wenn eine NIC deaktiviert ist, wird die Datenübertragung zum und vom iDRAC über das Netzwerk blockiert. Die Standardeinstellung ist **aus**.
MAC-Adresse (Media Access Control)	Zeigt die Medienzugriffssteuerungs-Adresse (MAC) an, die die einzelnen Knoten in einem Netzwerk eindeutig identifiziert. Die MAC-Adresse kann nicht geändert werden.
Verwenden Sie DHCP (für die NIC-IP-Adresse)	Fordert den iDRAC auf, eine IP-Adresse für die NIC vom Server für das dynamische Host-Konfigurationsprotokoll (DHCP) abzurufen. Deaktiviert auch die Steuerungen **für Statische IP-Adresse**, **Statische Subnetzmaske** und **Statisches Gateway**. Die Standardeinstellung ist **aus**.
Statische IP-Adresse	Ermöglicht Ihnen, eine statische IP-Adresse für die iDRAC-NIC einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, wählen Sie das Kontrollkästchen **DHCP verwenden (für NIC-IP-Adresse)** ab.

Statische Subnetzmaske	Ermöglicht Ihnen, eine Subnetzmaske für die iDRAC-NIC einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, wählen Sie zuerst das Kontrollkästchen **DHCP verwenden (für NIC-IP-Adresse)** ab.
Statischer Gateway	Ermöglicht Ihnen, einen statischen Gateway für die iDRAC-NIC einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, wählen Sie zuerst das Kontrollkästchen **DHCP verwenden (für NIC-IP-Adresse)** ab.
DHCP zum Abrufen von DNS-Serveradressen verwenden	Aktivieren Sie DHCP zum Abrufen von DNS-Server-Adressen, indem Sie das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** auswählen. Wenn Sie DHCP nicht zum Abrufen der DNS-Server-Adressen verwenden, geben Sie die IP-Adressen in die Felder **Statischer bevorzugter DNS-Server** und **Statischer 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 **Statischer bevorzugter DNS-Server** und **Statischer alternativer DNS-Server** eingetragen werden.
Statischer bevorzugter DNS-Server	Ermöglicht dem Benutzer, eine statische IP-Adresse für den bevorzugten DNS-Server einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, muss zuerst das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** abgewählt werden.
Statischer bevorzugter DNS-Server	Verwendet die sekundäre DNS-Server-IP-Adresse nur, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden nicht ausgewählt** ist. Geben Sie eine IP-Adresse mit 0.0.0.0 ein, wenn kein alternativer DNS-Server vorhanden ist.
iDRAC auf DNS registrieren	Registriert den iDRAC-Namen auf dem DNS-Server. Die Standardeinstellung ist **Deaktiviert**.
DNS iDRAC-Name	Zeigt den iDRAC-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 darstellt. Beispiel: idrac-00002.
DHCP für den DNS-Domänennamen verwenden	Verwendet den Standard-DNS-Domänennamen. Wenn das Kästchen 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**. **ANMERKUNG:** Wenn das Kontrollkästchen **DHCP für den DNS-Domänennamen verwenden** ausgewählt werden soll, müssen Sie auch das Kontrollkästchen **DHCP verwenden (für NIC-IP-Adresse)** auswählen.
DNS-Domänenname	Der Standard-**DNS-Domänenname** ist leer. Wenn das Kontrollkästchen **DHCP für den DNS-Domänennamen verwenden** ausgewählt ist, ist diese Option grau unterlegt und das Feld kann nicht geändert werden.
Community-Zeichenkette	Enthält die Community-Zeichenkette, die für die vom iDRAC gesendeten Warnungs-Traps des **einfachen Netzwerkverwaltungsprotokolls (SNMP)** verwendet werden soll. SNMP-Warnungs-Traps werden vom iDRAC übertragen, wenn ein Plattformereignis auftritt. Die Standardeinstellung ist **öffentlich**.
SMTP-Serveradresse	Die IP-Adresse des Servers des **einfachen Mail-Übertragungsprotokolls (SMTP**), mit dem der iDRAC kommuniziert, um im Falle eines Plattformereignisses E-Mail-Warnungen auszusenden. Die Standardeinstellung ist **127.0.0.1.**

Tabelle 5-2. IPMI LAN-Einstellungen

Stellung	Beschreibung
IPMI-Über-LAN aktivieren	Wenn markiert, weist dies darauf hin, dass der IPMI LAN-Kanal aktiviert ist. Die Standardeinstellung ist **aus**.
Beschränkung der Channel-Berechtigungsebene	Konfiguriert die höchste Berechtigungsebene für den Benutzer, die auf dem LAN-Kanal akzeptiert werden kann. Wählen Sie eine der folgenden Optionen aus: **Administrator**, **Operator** oder **Benutzer**. Die Standardeinstellung ist **Administrator**.
Verschlüsselungsschlüssel	Konfiguriert den Verschlüsselungsschlüssel: 0 bis 20 Hexadezimalzeichen (keine Leerstellen erlaubt). Die Standardeinstellung ist leer.

Tabelle 5-3. Schaltflächen der Seite Netzwerkkonfiguration

Schaltfläche	Beschreibung
Erweiterte Einstellungen	Öffnet die Seite **Netzwerksicherheit**, auf der Benutzer den IP-Bereich sowie IP-Blockierungsattribute eingeben können.
Drucken	Druckt die Werte der **Netzwerkkonfiguration** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Netzwerkkonfiguration** erneut.
Anwenden	Speichert alle neuen Einstellungen, die Sie auf der Seite Netzwerkkonfiguration vorgenommen haben. **ANMERKUNG:** Wenn Sie Änderungen an den Einstellungen der NIC-IP-Adresse vornehmen, werden alle Benutzersitzungen geschlossen und Benutzer müssen unter Verwendung der aktualisierten IP-Adresseneinstellungen eine neue Verbindung zur iDRAC-Webschnittstelle herstellen. Alle anderen Änderungen erfordern, dass die NIC zurückgesetzt wird, was einen kurzzeitigen Verlust der Konnektivität 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 **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Netzwerk/Sicherheit**, um die Seite **Netzwerkkonfiguration** zu öffnen.
2. Klicken Sie auf **Erweiterte Einstellungen**, um die Netzwerksicherheitseinstellungen zu konfigurieren.

   Tabelle 5-4 beschreibt die Einstellungen der Seite **Netzwerksicherheit**.
3. Wenn Sie mit den Einstellungen fertig sind, klicken Sie auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-5.

Tabelle 5-4. Einstellungen der Seite Netzwerksicherheit

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

Tabelle 5-5. 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.
Zurück zur Netzwerkseite	Wechselt zur **Netzwerk**seite zurück.

Plattformereignisse konfigurieren

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

Die filterbaren Plattformereignisse sind unter Tabelle 5-6 aufgeführt.

Tabelle 5-6. Filterbaren Plattformereignisse

Index	Plattformereignis
1	Assertion Batteriewarnung
2	Assertion Batterie kritisch
3	Diskrete Spannung, Assertion Kritisch
4	Assertion Temperaturwarnung
5	Assertion Temperatur kritisch
6	Redundanz herabgesetzt
7	Redundanz verloren
8	Assertion Prozessorwarnung
9	Assertion Prozessor kritisch
10	Assertion Prozessor nicht vorhanden
11	Assertion Ereignisprotokoll kritisch
12	Assertion Watchdog kritisch

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 (wie eines Systemneustarts) konfiguriert ist, wird die Maßnahme ausgeführt.

Plattformereignisfilter (PEF) konfigurieren

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

1. Melden Sie sich bei der iDRAC-Webschnittstelle an. Siehe Zugriff auf die Webschnittstelle.
2. Klicken Sie auf **System** und dann auf das Register **Warnungsverwaltung**.
3. Aktivieren Sie auf der Plattformereignisseite **Warnungserstellung** für ein Ereignis, indem Sie auf das entsprechende Kontrollkästchen **Warnung erstellen** für dieses Ereignis klicken.

ANMERKUNG: Die Warnungserstellung kann für alle Ereignisse aktiviert oder deaktiviert werden, indem Sie auf das Kontrollkästchen neben der Spaltenüberschrift "Warnung erstellen" klicken.

4. Klicken Sie auf die Optionsschaltfläche unter der Maßnahme, die Sie für die einzelnen Ereignisse aktivieren möchten. Für jedes Ereignis kann nur eine Maßnahme eingestellt werden.
5. Klicken Sie auf **Anwenden**.

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

Plattformereignis-Traps (PET) konfigurieren

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

1. Melden Sie sich über einen unterstützten Internet-Browser am Remote- System an. Siehe Zugriff auf die Webschnittstelle.
2. Vergewissern Sie sich, dass Sie die unter Plattformereignisfilter (PEF) konfigurierenbeschriebenen Verfahren ausgeführt haben.
3. Konfigurieren Sie die PET-Ziel-IP-Adresse:
   a. Klicken Sie auf das Kontrollkästchen **Aktivieren** neben der **Ziel-IP- Adresse**, die Sie aktivieren möchten.
   b. Geben Sie eine IP-Adresse im Kästchen **Ziel-IP-Adresse** ein.

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

   c. Klicken Sie auf **Anwenden**.

   ANMERKUNG: Der Wert der **Community-Zeichenkette** muss auf der Seite **Netzwerkkonfiguration** konfiguriert werden, damit ein Trap erfolgreich gesendet werden kann. Der Wert **Community-Zeichenkette** weist auf die Community-Zeichenkette hin, die für ein SNMP-Warnungs-Trap (einfaches Netzwerkverwaltungsprotokoll) verwendet werden soll, das vom iDRAC gesendet wird. SNMP-Warnungs-Traps werden vom iDRAC übertragen, wenn ein Plattformereignis auftritt. Die Standardeinstellung für die **Community-Zeichenkette** ist **Öffentlich**.

   d. Klicken Sie auf **Senden**, um die konfigurierte Warnung zu testen (falls gewünscht).
   e. Wiederholen Sie Schritt a bis Schritt d für alle übrigen Zielnummern.

Konfiguration von E-Mail-Warnungen

1. Melden Sie sich über einen unterstützten Internet-Browser am Remote- System an.
2. Vergewissern Sie sich, dass Sie die unter Plattformereignisfilter (PEF) konfigurierenbeschriebenen Verfahren ausgeführt haben.
3. Konfigurieren Sie die E-Mail-Warnungseinstellungen.
   a. Klicken Sie im Register **Warnungsverwaltung** auf **E-Mail- Warnungseinstellungen**.
4. Konfigurieren Sie das E-Mail-Warnungsziel.
   a. Klicken Sie in der Spalte **E-Mail-Warnungsnummer** auf eine Zielnummer. Es gibt vier mögliche Ziele, die Warnungen empfangen können.
   b. Stellen Sie sicher, dass das Kontrollkästchen **Aktiviert** markiert ist.

c. Geben Sie in das **Ziel-E-Mail-Adressfeld** eine gültige E-Mail-Adresse ein.

d. Klicken Sie auf **Anwenden**.

ANMERKUNG: Für eine erfolgreiche Test-E-Mail-Versendung muss die **SMTP-Server-Adresse** auf der Seite **Netzwerkkonfiguration** konfiguriert werden. Die IP-Adresse des **SMTP-Servers** kommuniziert mit dem iDRAC, um im Falle eines Plattformereignisses E-Mail-Warnungen zu senden.

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

f. Wiederholen Sie Schritt a bis Schritt e für alle übrigen E-Mail- Warnungseinstellungen.

IPMI konfigurieren

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

2. Konfigurieren Sie IPMI über LAN.

   a. Klicken Sie auf **System**→ **Remote-Zugriff**→ iDRAC und dann auf **Netzwerk/Sicherheit**.

   b. Wählen Sie auf der Seite **Netzwerkkonfiguration** unter **IPMI-LAN- Einstellungen IPMI über LAN aktivieren** aus.

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

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

   ANMERKUNG: Die iDRAC-IPMI unterstützt das RMCP+-Protokoll.

   ANMERKUNG: Der Verschlüsselungsschlüssel muss aus einer geraden Anzahl hexadezimaler Zeichen bestehen und maximal 20 Zeichen lang sein.

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

   e. Klicken Sie auf **Anwenden**.

3. IPMI Seriell über LAN (SOL) konfigurieren.

   a. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC**.

   b. Klicken Sie auf das Register **Netzwerksicherheit** und dann auf **Seriell über LAN**.

   c. Markieren Sie auf der Seite **Seriell über LAN - Konfiguration** das Kontrollkästchen **Seriell über LAN aktivieren**, um die Funktion "Seriell über LAN" zu aktivieren.

   d. Aktualisieren Sie die IPMI-SOL-Baudrate.

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

   Klicken Sie auf das Drop-Down-Menü **Baudrate**, um eine Datengeschwindigkeit von 19,2 kbps, 57,6 kbps oder 115,2 kbps auszuwählen.

   e. Klicken Sie auf **Anwenden**.

---

iDRAC-Benutzer hinzufügen und konfigurieren

Erstellen Sie zur Verwaltung des Systems mit dem iDRAC und zur Aufrechterhaltung der Systemsicherheit eindeutige Benutzer mit spezifischen Administrationsberechtigungen (oder *rollenbasierter Autorität*).

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

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

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Netzwerk/Sicherheit**.

2. Öffnen Sie die Seite **Benutzer**, um einzelne Benutzer zu konfigurieren.

   Die Seite **Benutzer** zeigt für die einzelnen Benutzer **Benutzer-ID, Zustand, Benutzername, IPMI-LAN-Berechtigungen**, **iDRAC-Berechtigungen** sowie **Seriell über LAN** an.

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

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

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

   Tabelle 5-7 beschreibt die **allgemeinen** Einstellungen zur Konfiguration eines Benutzernamens und -kennworts für iDRAC.

   Tabelle 5-8 beschreibt die **IPMI-LAN-Berechtigungen** zum Konfigurieren der LAN-Berechtigungen des Benutzers.

   Tabelle 5-9 beschreibt die **Benutzergruppen**-Berechtigungen für die Einstellungen der **IPMI-LAN-Berechtigungen** und der **iDRAC-Benutzerberechtigungen**.

   Tabelle 5-10 beschreibt die **iDRAC-Gruppen**berechtigungen. Wenn Sie eine **iDRAC-Benutzerberechtigung** zum **Administrator**, **Hauptbenutzer** oder **Gastbenutzer** hinzufügen, verändert sich die **iDRAC-Gruppe** zur **benutzerdefinierten** Gruppe.

5. Wenn Sie fertig sind, klicken Sie auf **Anwenden**.

6. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-11.

Tabelle 5-7. Allgemeine Eigenschaften

Eigenschaft	Beschreibung
Benutzer-ID	Enthält eine von 16 voreingestellten Benutzer-ID-Nummern. Dieses Feld darf nicht bearbeitet werden.
Benutzer aktivieren	Wenn das Feld markiert ist, weist dies darauf hin, dass der Benutzerzugriff auf den iDRAC aktiviert ist. Wenn das Feld nicht markiert ist, ist der Benutzerzugriff deaktiviert.
Benutzername	Gibt einen iDRAC-Benutzernamen von bis zu 16 Zeichen an. Jeder Benutzer muss einen eindeutigen Benutzernamen besitzen. **ANMERKUNG:** Benutzernamen für den iDRAC dürfen nicht die Zeichen **/** (Schrägstrich) oder **.** (Punkt) enthalten. **ANMERKUNG:** Wenn der Benutzername geändert wird, erscheint der neue Name erst bei der nächsten Benutzeranmeldung in der Benutzeroberfläche.
Kennwort ändern	Aktiviert die Felder **Neues Kennwort** und **Neues Kennwort bestätigen**. Wenn diese Option nicht markiert ist, kann das **Kennwort** des Benutzers nicht geändert werden.
Neues Kennwort	Aktiviert die Bearbeitung des Kennworts des iDRAC-Benutzers. 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 5-8. IPMI-LAN-Benutzerberechtigungen

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

Tabelle 5-9. iDRAC-Benutzerberechtigungen

Eigenschaft	Beschreibung
iDRAC-Gruppe	Legt die maximale iDRAC-Benutzerberechtigung als eine der Folgenden fest: **Administrator**, **Hauptbenutzer**, **Gastbenutzer**, **Benutzerdefiniert** oder **Keine**. Informationen zu **DRAC-Gruppen**berechtigungen finden Sie unter Tabelle 5-10.
Bei 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, 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.

Tabelle 5-10. iDRAC-Gruppenberechtigungen

Benutzergruppe	Gewährte Berechtigungen
Administrator	**Anmeldung bei iDRAC**, **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtuellen Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Hauptbenutzer	**Anmeldung bei iDRAC**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtuellern Datenträger**, **Testwarnungen**
Gastbenutzer	**Bei iDRAC anmelden**
Benutzerdefiniert	Auswahl einer beliebigen Kombination der folgenden Berechtigungen: **Anmeldung bei iDRAC**, **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Server-Maßnahmenbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtuellern Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Keine	Keine zugewiesenen Berechtigungen

Tabelle 5-11. Schaltflächen der Seite Benutzerkonfiguration

Schaltfläche	Abhilfe
Drucken	Druckt die Werte der **Benutzerkonfiguration** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Benutzerkonfiguration** erneut.
Anwenden	Speichert alle neuen Einstellungen, die an der Benutzerkonfiguration vorgenommen wurden.
Zurück zur Benutzerseite	Wechselt zur **Benutzerseite** zurück.

---

iDRAC-Datenübertragungen anhand von SSL- und digitalen Zertifikaten sichern

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

- Secure Sockets Layer (SSL)
- Zertifikatsignierungsanforderung (CSR)
- Zugriff auf das SSL-Hauptmenü
- Ein neues CSR erstellen
- Ein Server-Zertifikat hochladen
- Ein Server-Zertifikat ansehen

Secure Sockets Layer (SSL)

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

Ein SSL-aktiviertes System kann die folgenden Tasks ausführen:

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

Das Verschlüsselungsverfahren bietet eine hohe Datensicherungsstufe. Der iDRAC verwendet den 128-Bit-SSL-Verschlüsselungsstandard, die sicherste Form der Verschlüsselung, die für Internetbrowser in Nordamerika erhältlich ist.

Der iDRAC-Web Server enthält standardmäßig ein selbstsigniertes Dell-SSL-Digitalzertifikat (Server-ID). Um für Internetübertragungen eine hohe Sicherheitsstufe zu gewährleisten, ersetzen Sie das Web Server-SSL-Zertifikat durch ein Zertifikat, das von einer bekannten Zertifizierungsstelle signiert wurde. Um das Verfahren zum Erhalt eines signierten Zertifikats einzuleiten, können Sie die iDRAC-Webschnittstelle zum Erstellen einer Zertifikatsignierungsanforderung (CSR) mit den Informationen zu Ihrer Firma verwenden. Sie können die erstellte CSR dann an eine Zertifizierungsstelle wie VeriSign oder Thawte senden.

Zertifikatsignierungsanforderung (CSR)

Eine CSR ist eine digitale Anforderung eines sicheren Serverzertifikats von einer Zertifizierungsstelle (CA). Sichere Serverzertifikate ermöglichen Clients des Servers, die Identität des Servers, zu dem sie eine Verbindung hergestellt haben, als vertrauenswürdig einzustufen und eine verschlüsselte Sitzung mit dem Server auszuhandeln.

Eine Zertifizierungsstelle ist ein Geschäftsunternehmen, das in der IT-Industrie dafür anerkannt ist, hohe Ansprüche bezüglich der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger Sicherheitskriterien zu erfüllen. Beispiele von CAs schließen Thawte und VeriSign ein. 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 Zertifizierungsstelle die Zertifikatssignierungsanforderung genehmigt und das Zertifikat gesendet hat, muss das Zertifikat zur iDRAC-Firmware

hochgeladen werden. Die in der iDRAC-Firmware gespeicherten CSR-Informationen müssen mit den Informationen im Zertifikat übereinstimmen.

Zugriff auf das SSL-Hauptmenü

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Netzwerk/Sicherheit**.
2. Klicken Sie auf **SSL**, um die Seite **SSL-Hauptmenü** zu öffnen.

Verwenden Sie die Seite **SSL-Hauptmenü** zum Erstellen einer CSR, die an eine Zertifizierungsstelle gesendet werden soll. Die CSR-Informationen werden in der iDRAC-Firmware gespeichert.

Tabelle 5-12 beschreibt die Optionen, die zum Erstellen einer CSR verfügbar sind.

Tabelle 5-13 beschreibt die auf der Seite **SSL-Hauptmenü** verfügbaren Schaltflächen.

Tabelle 5-12. SSL-Hauptmenüoptionen

Feld	Beschreibung
Eine neue Zertifikatsignierungsanforderung erstellen (CSR)	Wählen Sie die Option aus und klicken Sie auf **Weiter**, um die Seite **Zertifikatsignierungsanforderung (CSR) erstellen** zu öffnen. **ANMERKUNG:** Jede neue CSR überschreibt die vorherige CSR der Firmware. Damit eine Zertifizierungsstelle Ihre CSR annimmt, muss die CSR in der Firmware mit dem von der Zertifizierungsstelle zurückgesendeten Zertifikat übereinstimmen.
Serverzertifikat hochladen	Wählen Sie die Option aus und klicken Sie auf **Weiter**, um die Seite **Zertifikat hochladen** zu öffnen und das Zertifikat hochzuladen, das Ihnen die Zertifizierungsstelle zugesandt hat. **ANMERKUNG:** iDRAC akzeptiert lediglich X509-Base-64-kodierte Zertifikate. DER-kodierte Zertifikate werden nicht angenommen.
Serverzertifikat anzeigen	Wählen Sie die Option aus und klicken Sie auf **Weiter**, um die Seite **Serverzertifikat anzeigen** zu öffnen und ein vorhandenes Serverzertifikat anzuzeigen.

Tabelle 5-13. SSL-Hauptmenüschaltflächen

Schaltfläche	Beschreibung
Drucken	Druckt die Werte des **SSL-Hauptmenüs** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **SSL-Hauptmenü** erneut.
Weiter	Verarbeitet die Informationen auf der Seite **SSL-Hauptmenü** und fährt mit dem nächsten Schritt fort.

Neue Zertifikatsignierungsanforderung erstellen

ANMERKUNG: Jede neue Zertifikatsignierungsanforderung überschreibt alle vorangegangenen, in der Firmware gespeicherten Daten. Die Zertifikatssignierungsanforderung der Firmware muss mit dem von der Zertifizierungsstelle ausgegebenen Zertifikat übereinstimmen. Andernfalls nimmt der iDRAC das Zertifikat nicht an.

1. Wählen Sie auf der Seite **SSL-Hauptmenü** die Option **Neue Zertifikatsignierungsanforderung (CSR) erstellen** aus und klicken Sie auf **Weiter**.
2. Geben Sie auf der Seite **Zertifikatsignierungsanforderung (CSR) erstellen** jeweils einen Wert für die einzelnen CSR-Attribute ein.

   Tabelle 5-14 beschreibt die Optionen der Seite **Zertifikatsignierungsanforderung (CSR) erstellen**.
3. Klicken Sie auf **Erstellen**, um die CSR zu erstellen.
4. Klicken Sie auf **Herunterladen**, um die CSR-Datei auf Ihrem lokalen Computer zu speichern.
5. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-15.

Tabelle 5-14. 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, Unterstreichungszeichen und Punkte sind gültig. Leerstellen sind nicht gültig.
Name der Organisation	Der mit dieser Organisation assoziierte Name (zum Beispiel, XYZ Unternehmen). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Organisationseinheit	Der einer Organisationseinheit, wie z. B. einer Abteilung (z. B. Informationstechnik) zugehörige 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, wo sich das Unternehmen, das sich um Zertifikat bewirbt, befindet.
E-Mail	Die mit der CSR verbundene E-Mail-Adresse. Geben Sie die E-Mail-Adresse der Firma oder eine beliebige mit der CSR in Zusammenhang stehende E-Mail-Adresse ein. Dieses Feld ist optional.

Tabelle 5-15. Schaltflächen der Seite Zertifikatsignierungsanforderung (CSR) erstellen

Schaltfläche	Beschreibung
Drucken	Druckt die Werte **Zertifikatsignierungsanforderung erstellen** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Zertifikatsignierungsanforderung erstellen** neu.
Erstellen	Erstellt eine CSR und fordert den Benutzer dann auf, sie in einem bestimmten Verzeichnis zu speichern.
Herunterladen	Lädt das Zertifikat auf den lokalen Computer herunter.
Zurück zum SSL-Hauptmenü	Bringt den Benutzer zur Seite **SSL-Hauptmenü** zurück.

Ein Serverzertifikat hochladen

1. Auf der Seite **SSL-Hauptmenü** wählen Sie **Serverzertifikat hochladen** und klicken Sie auf **Weiter**.

   Die Seite **Zertifikat hochladen** wird eingeblendet.

2. Geben Sie in das Feld **Dateipfad** den Pfad zum Zertifikat ein oder klicken Sie auf **Durchsuchen**, um zur Zertifikatsdatei zu wechseln.

ANMERKUNG: Der Wert **Dateipfad** zeigt den relativen Dateipfad des Zertifikats an, das Sie hochladen. Sie müssen den vollständigen Dateipfad eintippen, der den vollen Pfad und den vollständigen Dateinamen mit Dateierweiterung enthält.

3. Klicken Sie auf **Anwenden**.

4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-16.

Tabelle 5-16. Schaltfläche Zertifikat hochladen-Seite

Schaltfläche	Beschreibung
Drucken	Druckt die Werte aus, die auf der Seite **Zertifikat hochladen** angezeigt werden.
Aktualisieren	Lädt die Seite **Zertifikat hochladen** erneut.
Anwenden	Wendet das Zertifikat auf die iDRAC-Firmware an.
Zurück zum SSL-Hauptmenü	Bringt den Benutzer zur Seite **SSL-Hauptmenü** zurück.

Serverzertifikat anzeigen

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

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

2. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-18.

Tabelle 5-17. Zertifikatinformationen

Feld	Beschreibung
Seriennummer	Seriennummer des Zertifikats
Bewerberinformationen	Vom Bewerber eingegebene Zertifikatsattribute
Ausstellerinformationen	Vom Aussteller zurückgegebene Zertifikatsattribute

Gültig von	Ausgabedatum des Zertifikats
Gültig bis	Ablaufdatum des Zertifikats

Tabelle 5-18. 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	Zurück zur Seite **SSL-Hauptmenü**.

Active Directory-Zertifikate konfigurieren und verwalten

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

ANMERKUNG: Weitere Informationen zur Active Directory-Konfiguration und dazu, wie Active Directory mit dem Standardschema oder einem erweiterten Schema konfiguriert wird, finden Sie unter iDRAC mit Microsoft Active Directory verwenden.

Zugriff auf das **Active Directory-Hauptmenü**:

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Netzwerk/Sicherheit**.
2. Klicken Sie auf **Active Directory**, um die Seite **Active Directory- Hauptmenü** zu öffnen.

   Tabelle 5-19 führt die Optionen der Seite **Active Directory-Hauptmenü** auf.
3. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-20.

Tabelle 5-19. Optionen der Hauptmenüseite des Active Directory

Feld	Beschreibung
Active Directory konfigurieren	Konfiguriert die Einstellungen für: **ROOT-Domänennamen** des Active Directory, **Active Directory-Authentifizierungs-Zeitüberschreitung**, **Auswahl des Active Directory-Schemas**, **iDRAC-Name**, **iDRAC-Domänenname**, **Rollengruppen**, **Gruppenname und Gruppendomäne**.
Active Directory-CA-Zertifikat hochladen	Lädt ein Active Directory-Zertifikat zum iDRAC hoch.
iDRAC-Serverzertifikat herunterladen	Über den **Windows Download Manager** können Sie ein iDRAC-Serverzertifikat auf das System herunterladen.
Active Directory-CA-Zertifikat anzeigen	Zeigt ein Active Directory-Zertifikat an, das zum iDRAC hochgeladen wurde.

Tabelle 5-20. Schaltflächen der Seite Active Directory-Hauptmenü

Schaltfläche	Definition
Drucken	Druckt die Werte des **Active Directory-Hauptmenüs** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Active Directory-Hauptmenü** erneut.
Weiter	Verarbeitet die Informationen auf der Seite **Active Directory-Hauptmenü** und fährt mit dem nächsten Schritt fort.

Active Directory konfigurieren (Standardschema und erweitertes Schema)

1. Auf der Seite **Active Directory-Hauptmenü** wählen Sie **Active Directory konfigurieren** aus und klicken dann auf **Weiter**.
2. Geben Sie auf der Seite **Active Directory-Konfiguration** die Active Directory-Einstellungen ein.

   Tabelle 5-21 beschreibt die Einstellungen der Seite **Active Directory-Konfiguration und -Verwaltung**.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-22.

5. Klicken Sie zum Konfigurieren der Rollengruppen für das Active Directory-Standardschema auf die individuelle Rollengruppe (1 - 5). Siehe Tabelle 5-23 und Tabelle 5-24.

ANMERKUNG: Klicken Sie zum Speichern der Einstellungen auf der Seite **Active Directory-Konfiguration** auf **Anwenden**, bevor Sie mit der Seite **Benutzerdefinierte Rollengruppe** fortfahren.

Tabelle 5-21. Einstellungen der Seite Active Directory-Konfiguration

Stellung	Beschreibung
Active Directory aktivieren	Wenn markiert, wird das Active Directory aktiviert. Die Standardeinstellung ist **deaktiviert**.
ROOT-Domänenname	Der ROOT-Domänenname des Active Directory. Diese Standardeinstellung ist leer. Der Name muss ein gültiger Domänenname sein und aus *x.y* bestehen, wobei *x* eine ASCII-Zeichenkette mit 1 - 254 Zeichen ohne Leerstellen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, ne oder org ist. Die Standardeinstellung ist leer.
Zeitüberschreitung	Die Wartezeit in Sekunden, bis die Active Directory-Abfragen beendet werden. Minimaler Wert ist größer/gleich 15 Sekunden. Der Standardwert ist **120**.
Standardschema verwenden	Verwendet das Standardschema mit Active Directory.
Erweitertes Schema verwenden	Verwendet das erweiterte Schema mit Active Directory.
iDRAC-Name	Der Name, der den iDRAC im Active Directory eindeutig identifiziert. Diese Standardeinstellung ist leer. Der Name muss eine ASCII-Zeichenkette mit 1 - 254 Zeichen ohne Leerstellen zwischen den Zeichen sein.
iDRAC-Domänenname	Der DNS-Name der Domäne, in der sich das Active Directory-iDRAC-Objekt befindet. Diese Standardeinstellung ist leer. Der Name muss ein gültiger Domänenname sein und aus *x.y* bestehen, wobei *x* eine ASCII-Zeichenkette mit 1 - 254 Zeichen ohne Leerstellen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, ne oder org ist.
Rollengruppen	Die Liste der Rollengruppen, die dem iDRAC zugehören. Klicken Sie zum Ändern der Einstellungen für eine Rollengruppe in der Rollengruppenliste auf eine Rollengruppennummer.
Gruppenname	Der Name, der die Rollengruppe in dem Active Directory identifiziert, das dem iDRAC zugehört. Diese Standardeinstellung ist leer.
Gruppendomäne	Der Domänentyp, bei dem sich die Rollengruppe befindet.

Tabelle 5-22. Schaltflächen der Seite Active Directory-Konfiguration

Schaltfläche	Beschreibung
Drucken	Druckt die Werte der **Active Directory-Konfiguration** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Active Directory-Konfiguration** erneut.
Anwenden	Speichert alle neuen Einstellungen, die auf der Seite der **Active Directory-Konfiguration** vorgenommen wurden.
Zurück zum Active Directory-Hauptmenü	Wechselt zur Seite **Active Directory Hauptmenü** zurück.

Tabelle 5-23. Rollengruppenberechtigungen

Stellung	Beschreibung
Zugriffsstufe der Rollengruppe	Legt die maximale iDRAC-Benutzerberechtigung als eine der Folgenden fest: **Administrator**, **Hauptbenutzer**, **Gastbenutzer**, **Keine** oder **Benutzerdefiniert**. Siehe Tabelle 5-24 zu **Rollengruppen**-Berechtigungen.
Bei iDRAC anmelden	Erlaubt der Gruppe den Anmeldezugriff auf den iDRAC.
iDRAC konfigurieren	Gibt der Gruppe die Berechtigung, den iDRAC zu konfigurieren.
Benutzer konfigurieren	Gibt der Gruppe die Berechtigung, Benutzer zu konfigurieren.
Protokolle löschen	Erlaubt der Gruppenberechtigung, Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Erlaubt der Gruppenberechtigung, Serversteuerungsbefehle auszuführen.
Auf die Konsolenumleitung zugreifen	Erlaubt der Gruppe, auf die Konsolenumleitung zuzugreifen.
Zugriff auf virtuelle Datenträger	Erlaubt der Gruppe, auf virtuelle Datenträger zuzugreifen.
Testwarnungen	Erlaubt der Gruppe, einem bestimmten Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnosebefehle ausführen	Erlaubt der Gruppenberechtigung, Diagnosebefehle auszuführen.

Tabelle 5-24. Rollengruppenberechtigungen

Eigenschaft	Beschreibung

Administrator	**Anmeldung bei iDRAC**, **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf virtuellen Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Hauptbenutzer	**Anmeldung bei iDRAC**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf virtuellen Datenträger**, **Testwarnungen**
Gastbenutzer	**Bei iDRAC anmelden**
Benutzerdefiniert	Auswahl einer beliebigen Kombination der folgenden Berechtigungen: **Anmeldung bei iDRAC**, **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Server-Maßnahmenbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf virtuellen Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Keine	Keine zugewiesenen Berechtigungen

Active Directory-CA-Zertifikat hochladen

1. Wählen Sie auf der Seite **Active Directory-Hauptmenü** die Option **Active Directory-Zertifizierungsstellenzertifikat hochladen** aus und klicken Sie auf **Weiter**.

2. Geben Sie auf der **Seite Zertifikat hochladen** den Dateipfad zum Zertifikat im Feld **Dateipfad** ein oder klicken Sie auf **Durchsuchen**, um zur Zertifikatsdatei zu wechseln.

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

Stellen Sie sicher, dass die SSL-Zertifikate des Domänen-Controllers von derselben Zertifizierungsstelle signiert wurden und dass dieses Zertifikat auf der Management Station verfügbar ist, die auf den iDRAC zugreift.

3. Klicken Sie auf **Anwenden**.

4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-25.

Tabelle 5-25. Seitenschaltflächen Zertifikat hochladen

Schaltfläche	Beschreibung
Drucken	Druckt die Werte zu **Zertifikat hochladen** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Zertifikat hochladen** erneut.
Anwenden	Wendet das Zertifikat auf die iDRAC-Firmware an.
Zurück zum Active Directory-Hauptmenü	Zurück zur Seite **Active Directory-Hauptmenü**.

iDRAC-Serverzertifikat herunterladen

1. Wählen Sie auf der Seite **Active Directory-Hauptmenü** die Option **iDRAC-Serverzertifikat herunterladen** aus und klicken Sie auf **Weiter**.

2. Speichern Sie die Datei in einem Verzeichnis Ihres Systems.

3. Klicken Sie im Fenster **Download abgeschlossen** auf **Schließen**.

Active Directory-CA-Zertifikat anzeigen

Verwenden Sie die Seite **Active Directory-Hauptmenü**, um ein Zertifizierungsstellen-Serverzertifikat für Ihren iDRAC anzuzeigen.

1. Wählen Sie auf der Seite **Active Directory-Hauptmenü** die Option **Active Directory-Zertifizierungsstellenzertifikat anzeigen** aus und klicken Sie auf **Weiter**.

   Tabelle 5-26 erläutert die Felder und zugehörigen Beschreibungen, die im **Zertifikat**-Fenster aufgeführt werden.

2. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-27.

Tabelle 5-26. Informationen zum Active Directory-CA-Zertifikat

Feld	Beschreibung
Seriennummer	Seriennummer des Zertifikats
Bewerberinformationen	Vom Bewerber eingegebene Zertifikatsattribute
Ausstellerinformationen	Vom Aussteller zurückgegebene Zertifikatsattribute.

Gültig von	Datum der Zertifikatsausstellung.
Gültig bis	Verfalldatum des Zertifikats.

Tabelle 5-27. Active Directory CA-Zertifikat-Seitenschaltflächen ansehen

Schaltfläche	Beschreibung
Drucken	Druckt die **Werte des Active Directory-Zertifizierungsstellenzertifikats, die auf dem Bildschirm angezeigt werden**, aus.
Aktualisieren	Lädt die **Seite Active Directory-Zertifizierungsstellenzertifikat neu**.
Zurück zum Active Directory-Hauptmenü	Leitet den Benutzer auf die Seite **Active Directory-Hauptmenü** zurück.

Lokalen Konfigurationszugriff aktivieren oder deaktivieren

ANMERKUNG: Die Standardeinstellung für lokalen Konfigurationszugriff ist **Aktiviert**.

Lokalen Konfigurationszugriff aktivieren

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC**→ **Netzwerk / Sicherheit**.
2. Klicken Sie unter **Lokale Konfiguration** zur Entfernung des Häkchens auf **Lokale Benutzerkonfigurationsaktualisierungen von iDRAC deaktivieren**, um den Zugriff zu aktivieren.
3. Klicken Sie auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche.

Lokalen Konfigurationszugriff deaktivieren

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC**→ **Netzwerk / Sicherheit**.
2. Klicken Sie unter **Lokale Konfiguration** zum Platzieren des Häkchens auf **Lokale Benutzerkonfigurationsaktualisierungen von iDRAC deaktivieren**, um den Zugriff zu aktivieren.
3. Klicken Sie auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche.

Seriell über LAN konfigurieren

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC**→ **Netzwerk / Sicherheit**.
2. Klicken Sie auf **Seriell über LAN**, um die Seite **Seriell über LAN - Konfiguration** zu öffnen.

   Tabelle 5-28 enthält Informationen über die Einstellungen der Seite **Seriell über LAN-Konfiguration**.
3. Klicken Sie auf **Anwenden**.
4. Konfigurieren Sie die erweiterten Einstellungen, falls erforderlich. Klicken Sie andernfalls auf die entsprechende Schaltfläche, um fortzufahren (siehe Tabelle 5-29).

   Um die erweiterten Einstellungen zu konfigurieren, führen Sie die folgenden Schritte aus:

   a. Klicken Sie auf **Erweiterte Einstellungen**.
   b. Konfigurieren Sie auf der Seite **Seriell über LAN - Konfiguration - erweiterte Einstellungen** die erweiterten Einstellungen wie erforderlich (siehe Tabelle 5-30).
   c. Klicken Sie auf **Anwenden**.
   d. Klicken Sie auf die entsprechende Schaltfläche, um fortzufahren (siehe Tabelle 5-31).

Tabelle 5-28. Einstellungen der Seite Seriell über LAN-Konfiguration

Stellung	Beschreibung
Seriell über LAN aktivieren	Wenn markiert, weist das Kontrollkästchen darauf hin, dass Seriell über LAN aktiviert ist.
Baudrate	Zeigt die Datengeschwindigkeit an. Wählen Sie eine Datengeschwindigkeit von **19,2 kbps**, **57,6 kbps** oder **115,2 kbps** aus.

Tabelle 5-29. Schaltflächen der Seite Seriell über LAN-Konfiguration

Schaltfläche	Beschreibung
Drucken	Druckt die Werte für **Seriell über LAN - Konfiguration** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Seriell über LAN - Konfiguration** erneut.
Erweiterte Einstellungen	Öffnet die Seite **Seriell über LAN-Konfiguration - Erweiterte Einstellungen**.
Anwenden	Liefert alle neuen Einstellungen, die Sie bei der Anzeige der Seite **Seriell über LAN - Konfiguration** vornehmen.

Tabelle 5-30. Einstellungen der Seite Seriell über LAN-Konfiguration - Erweiterte Einstellungen

Stellung	Beschreibung
Intervall der Zeichenakkumulation	Die Zeit, die der iDRAC wartet, bevor er ein partielles SOL-Zeichendatenpaket überträgt. Die Zeitspanne wird in Sekunden gemessen.
Schwellenwert der gesendeten Zeichen	Der iDRAC sendet ein SOL-Zeichendatenpaket mit den entsprechenden Zeichen, sobald diese Anzahl an Zeichen (oder eine höhere Anzahl) akzeptiert wurde. Der Schwellenwert wird in Zeichen gemessen.

Tabelle 5-31. Schaltflächen der Seite Seriell über LAN-Konfiguration - Erweiterte Einstellungen

Schaltfläche	Beschreibung
Drucken	Druckt die Werte für **Seriell über LAN - Konfiguration - erweiterte Einstellungen** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Seriell über LAN - Konfiguration - erweiterte Einstellungen** erneut.
Anwenden	Speichert alle neuen Einstellungen, die Sie bei der Betrachtung der Seite **Seriell über LAN - Konfiguration - erweiterte Einstellungen** vornehmen.
Zurück zur Seite Seriell über LAN - Konfiguration	Bringt den Benutzer zur Seite **Serielle über LAN - Konfiguration** zurück.

---

iDRAC-Dienste konfigurieren

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

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

ANMERKUNG: Der von Microsoft Windows bereitgestellte Telnet-Client hat bei der Kommunikation mit einer BMU ein bekanntes Problem. Verwenden Sie einen anderen Telnet-Client, wie z. B. HyperTerminal oder PuTTY.

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Netzwerk/Sicherheit**.
2. Klicken Sie auf **Dienste**, um die Seite Konfiguration von **Diensten** zu öffnen.
3. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Web Server - siehe Tabelle 5-32 für Web Server-Einstellungen
   - SSH - siehe Tabelle 5-33 für Informationen zu SSH-Einstellungen
   - Telnet - siehe Tabelle 5-34 für Informationen zu Telnet-Einstellungen
   - Automatisierter Systemwiederherstellungsagent - siehe Tabelle 5-35 für die Einstellungen des automatisierten Systemwiederherstellungsagenten
4. Klicken Sie auf **Anwenden**.
5. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-36.

Tabelle 5-32. Web Server-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert den iDRAC-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 Sitzungen, die für dieses System zulässig sind. Dieses Feld kann nicht bearbeitet werden. Es können vier Sitzungen gleichzeitig ausfgeführt werden.
Aktuelle Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich **Max. Sitzungen**. Dieses Feld kann nicht bearbeitet werden.
Zeitüberschreitung	Die Zeit in Sekunden, für die eine Verbindung ungenutzt bleiben kann. Die Sitzung wird abgebrochen, wenn das Zeitlimit erreicht wird. Änderungen an der Einstellung zur Zeitüberschreitung werden sofort wirksam und führen zu einem Reset des Web Servers. Der Zeitüberschreitungsbereich beträgt 60 bis 1920 Sekunden. Die Standardeinstellung ist **300** Sekunden.
HTTP-Anschlussnummer	Der Anschluss, an dem der iDRAC abhört, ob eine Browser-Verbindung besteht. Die Standardeinstellung ist **80.**
HTTPS-Anschlussnummer	Der Anschluss, an dem der iDRAC abhört, ob eine sichere Browser-Verbindung besteht. Die Standardeinstellung ist **443.**

Tabelle 5-33. SSH-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert SSH. Wenn markiert, weist das Kontrollkästchen darauf hin, dass SSH aktiviert ist.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger Sitzungen, die für dieses System zulässig ist. Es wird nur eine einzige Sitzung unterstützt.
Aktive Sitzungen	Die Anzahl der aktuellen Sitzungen auf dem System.
Zeitüberschreitung	Die Leerlaufzeitüberschreitung der Secure Shell, in Sekunden. Der Zeitüberschreitungsbereich beträgt 60 bis 1920 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitlimit-Funktion zu deaktivieren. Die Standardeinstellung ist **300.**
Anschlussnummer	Der Anschluss, an dem der iDRAC abhört, ob eine SSH-Verbindung besteht. Die Standardeinstellung ist **22.**

Tabelle 5-34. Telnet-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert Telnet. Wenn markiert, ist Telnet aktiviert.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger Sitzungen, die für dieses System zulässig sind. Es wird nur eine einzige Sitzung unterstützt.
Aktive Sitzungen	Die Anzahl der aktuellen Sitzungen auf dem System.
Zeitüberschreitung	Die telnet-Zeitüberschreitung wegen Leerlauf, in Sekunden. Der Zeitüberschreitungsbereich beträgt 60 bis 1920 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitlimit-Funktion zu deaktivieren. Die Standardeinstellung ist **0.**
Anschlussnummer	Der Anschluss, an dem der iDRAC abhört, ob eine Telnet-Verbindung besteht. Die Standardeinstellung ist **23.**

Tabelle 5-35. Einstellung des automatisierten Systemwiederherstellungs-Agenten

Einstellung	Beschreibung
Aktiviert	Aktiviert den automatisierten Systemwiederherstellungs-Agenten.

Tabelle 5-36. Schaltflächen der Dienste-Seite

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Dienste**.
Aktualisieren	Aktualisiert die Seite **Dienste**.
Änderungen anwenden	Wendet die Einstellungen für die Seite **Dienste** an.

---

iDRAC-Firmware aktualisieren

HINWEIS: Wenn die iDRAC-Firmware beschädigt wird, was eintreten könnte, wenn der iDRAC-Firmware-Aktualisierungsvorgang vor seinem Abschluss abgebrochen wird, können Sie den iDRAC mithilfe des CMC wiederherstellen. Anleitungen hierzu finden Sie im *CMC Firmware-Benutzerhandbuch*.

ANMERKUNG: Die Firmware-Aktualisierung behält standardmäßig die aktuellen iDRAC-Einstellungen bei. Während des Aktualisierungsvorgangs haben Sie die Möglichkeit, die iDRAC-Konfiguration auf die werkseitigen Standardeinstellungen zurückzusetzen. Wenn Sie die Konfiguration auf die Werkseinstellungen einstellen, wird der Zugriff auf das externe Netzwerk nach Abschluss der Aktualisierung deaktiviert. Das Netzwerk muss unter Verwendung des iDRAC-Konfigurationshilfsprogramms oder der CMC-Webschnittstelle aktiviert und konfiguriert werden.

1. Starten Sie die iDRAC-Webschnittstelle.
2. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Aktualisieren**.

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

3. Klicken Sie auf der Seite **Firmware-Aktualisierung** auf **Weiter**, um den Aktualisierungsvorgang zu starten.

4. Klicken Sie im Fenster **Firmware-Aktualisierung - Hochladen (Seite 1 von 4)** auf **Durchsuchen** oder geben Sie den Pfad zum heruntergeladenen Firmware-Image an.

   Zum Beispiel:

   `C:\Updates\V1.0\<Image-Name>`.

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

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

   - Die Datei wird auf den iDRAC hochgeladen. Dieser Vorgang kann mehrere Minuten beanspruchen.

     ODER

   - Sie können zu diesem Zeitpunkt auf **Abbrechen** klicken, wenn der Firmware-Aktualisierungsvorgang abgebrochen werden soll. Wenn Sie auf **Abbrechen** klicken, wird der iDRAC in den normalen Betriebsmodus zurückgesetzt.

- Im Fenster **Firmware-Aktualisierung - Validierung (Seite 2 von 4)** werden die Ergebnisse der Validierung angezeigt, die für die hochgeladene Image-Datei ausgeführt wurde.

  - Wenn die Image-Datei erfolgreich hochgeladen wurde und alle Überprüfungsvorgänge durchlaufen sind, erscheint eine Meldung mit dem Inhalt, dass das Firmware-Image überprüft wurde.

    ODER

  - Wenn das Image nicht erfolgreich hochgeladen wurde oder die Überprüfungsvorgänge nicht bestanden hat, wechselt die Firmware-Aktualisierung zum Fenster **Firmware-Aktualisierung - Hochladen (Seite 1 von 4)** zurück. Sie können versuchen, den iDRAC erneut zu aktualisieren oder auf **Abbrechen** klicken, um den iDRAC in den normalen Betriebsmodus zurückzusetzen.

ANMERKUNG: Wenn Sie die Markierung im Kontrollkästchen **Konfiguration beibehalten** entfernen, wird der iDRAC auf seine Standardeinstellungen zurückgesetzt. Das LAN ist in den Standardeinstellungen deaktiviert. Sie werden nicht in der Lage sein, sich bei der iDRAC-Webschnittstelle anzumelden. Es wird erforderlich sein, die LAN-Einstellungen unter Verwendung der CMC-Webschnittstelle oder iKVM unter Verwendung des iDRAC-Konfigurationshilfsprogramms während des BIOS-POST neu zu konfigurieren.

7. Standardmäßig ist das Kontrollkästchen **Konfiguration sichern** ausgewählt, um die aktuellen Einstellungen auf dem iDRAC nach einer Erweiterung zu sichern. Wenn die Einstellungen nicht beibehalten werden sollen, entfernen Sie die Markierung im Kontrollkästchen **Konfiguration beibehalten**.

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

9. Im Fenster **Firmware-Aktualisierung - Aktualisierung wird durchgeführt (Seite 3 von 4)** wird der Erweiterungsstatus angezeigt. Der Fortschritt des in Prozent gemessenen Firmware-Aktualisierungsvorgangs wird in der Spalte **Fortschritt** angezeigt.

10. Sobald die Firmware-Aktualisierung abgeschlossen ist, wird das Fenster **Firmware-Aktualisierung - Aktualisierungsergebnisse (Seite 4 von 4)** angezeigt und der iDRAC automatisch zurückgesetzt. Sie müssen das aktuelle Browserfenster schließen und eine neue iDRAC-Verbindung in einem neuen Browserfenster herstellen.

iDRAC-Firmware mittels CMC wiederherstellen

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

Wenn die iDRAC-Firmware beschädigt wird, was eintreten könnte, wenn der iDRAC-Firmware-Aktualisierungsvorgang vor seinem Abschluss abgebrochen wird, können Sie die CMC-Webschnittstelle zum Aktualisieren der Firmware verwenden.

Wenn der CMC die beschädigte iDRAC-Firmware ermittelt, wird der iDRAC auf der Seite **Aktualisierbare Komponenten** der CMC-Webschnittstelle aufgeführt.

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

Führen Sie zum Aktualisieren der iDRAC-Firmware folgende Schritte aus:

1. Laden Sie die neueste iDRAC-Firmware von **support.dell.com** auf den Verwaltungscomputer herunter.

2. Melden Sie sich an der webbasierten CMC-Schnittstelle an.

3. Klicken Sie in der Systemstruktur auf **Chassis (Gehäuse**.

4. Klicken Sie auf die Registerkarte **Update** (Aktualisieren). Die Seite **Updatable Components** (Aktualisierbare Komponenten) wird angezeigt. Der Server mit dem wiederherstellbaren iDRAC ist in der Liste enthalten, falls diese vom CMC wiederhergestellt werden kann.

5. Klicken Sie auf **server-*n***, wobei ***n*** die Nummer des Servers ist, dessen iDRAC Sie wiederherstellen möchten.

6. Klicken Sie auf **Durchsuchen**, um zum iDRAC-Firmware-Image zu browsen, das Sie heruntergeladen haben und klicken Sie auf **Öffnen**.
7. Klicken Sie auf **Firmware-Aktualisierung beginnen**.

Wenn die Firmware-Image-Datei zum CMC hochgeladen wurde, aktualisiert sich der iDRAC anhand des Image selbst.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC mit Microsoft Active Directory verwenden

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

Ein Verzeichnisdienst pflegt eine allgemeine Datenbank aller Informationen, die zur Steuerung von Benutzern, Computern, Druckern und weiteren Geräten in einem Netzwerk erforderlich sind. Wenn Ihre Firma die Microsoft® Active Directory® Service-Software verwendet, kann die Software so konfiguriert werden, dass sie Zugriff auf den iDRAC bietet. Sie können dann bestehenden Benutzern in der Active Directory-Software iDRAC-Benutzerberechtigungen zuteilen und diese steuern.

ANMERKUNG: Die Verwendung von Active Directory zur Erkennung von iDRAC-Benutzern wird auf den Betriebssystemen Microsoft Windows® 2000 und Windows Server® 2003 unterstützt.

Sie können Active Directory dazu verwenden, den Benutzerzugriff auf iDRAC über ein erweitertes Schema zu definieren, das die von Dell definierten Active Directory-Objekte oder ein Standardschema einsetzt, das nur Active Directory-Gruppenobjekte verwendet.

Vorteile und Nachteile des Erweiterten Schemas und Standardschemas

Wenn Sie Active Directory zur Konfiguration des Zugriffs auf den iDRAC verwenden, müssen Sie entweder das erweiterte Schema oder das Standardschema wählen.

Die Vorteile bei der Verwendung des erweiterten Schemas sind:

- Alle Zugriffssteuerungsobjekte werden im Active Directory verwahrt.
- Maximale Flexibilität bei der Konfiguration des Benutzerzugriffs auf verschiedene iDRACs mit unterschiedlichen Berechtigungsebenen.

Die Vorteile bei der Verwendung der Standardschema-Lösung:

- Es ist keine Schemaerweiterung erforderlich, da das Standardschema nur Active Directory-Objekte verwendet.
- Die Konfiguration vom Active Directory aus ist einfach.

Übersicht des Active Directory mit erweitertem Schema

Active Directory kann auf drei Arten mit dem erweiterten Schema aktiviert werden:

- Mithilfe der iDRAC-Webschnittstelle (siehe Konfiguration des iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung der Webschnittstelle).
- Mithilfe des Hilfsprogramms RACADM CLI (siehe iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung von RACADM konfigurieren).
- Mithilfe der SM-CLP-Befehlszeile (siehe iDRAC mit der Schemaerweiterung des Active Directory und SM-CLP konfigurieren).

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 bzw. darin aufgenommen werden können. Die Benutzerklasse ist ein Beispiel einer Klasse, die in der Datenbank gespeichert wird. Einige Beispiel-Attribute der Benutzerklasse sind Vorname, Nachname, Telefonnummer usw. des Benutzers. Firmen können die Active Directory-Datenbank erweitern, indem sie ihre eigenen eindeutigen Attribute und Klassen hinzufügen, um sich an umgebungsspezifische Bedürfnisse zu richten. Dell hat das Schema um die Attribute und Klassen zur Unterstützung der Remote-Verwaltungsauthentifizierung und -autorisierung erweitert.

Jedes Attribut bzw. jede Klasse, die einem vorhandenen Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert werden. Um industrieweit eindeutige ID aufrechtzuerhalten, unterhält Microsoft eine Datenbank von Active Directory Objektkennungen (OIDs), so dass Firmen beim Hinzufügen von Erweiterungen zum Schema sicher sein können, dass diese eindeutig sind und nicht miteinander in Konflikt stehen. Um das Schema im Microsoft Active Directory zu erweitern, hat Dell eindeutige OIDs, eindeutige Namenserweiterungen sowie eindeutig verknüpfte Attribut-IDs für die Attribute und Klassen erhalten, die dem Verzeichnisdienst hinzugefügt worden sind, wie in Tabelle 6-1 dargestellt.

Tabelle 6-1. Objektkennungen des Dell Active Directory

Dienstklasse des Active Directory	Active Directory-OID
Dell-Erweiterung	dell
Dell-basierte OID	1.2.840.113556.1.8000.1280
RAC-LinkID-Bereich	12070 bis 12079

Übersicht der RAC-Schema-Erweiterungen

Um in der Vielzahl von Kundenumgebungen die größte Flexibilität zu bieten, stellt Dell eine Gruppe von Objekten bereit, die, abhängig von den gewünschten Ergebnissen, vom Benutzer konfiguriert werden können. Dell hat das Schema um Zuordnungs-, Geräte- und Berechtigungseigenschaften erweitert. Die Zuordnungseigenschaft wird zur Verknüpfung der Benutzer oder Gruppen mit einem spezifischen Satz Berechtigungen an einem oder mehreren RAC-Geräten verwendet. Dieses Modell gibt dem Administrator höchste Flexibilität über die verschiedenen Kombinationen von Benutzern, RAC-Berechtigungen und RAC-Geräten auf dem Netzwerk, ohne zu viel Komplexität hinzuzufügen.

Active Directory - Objekt-Übersicht

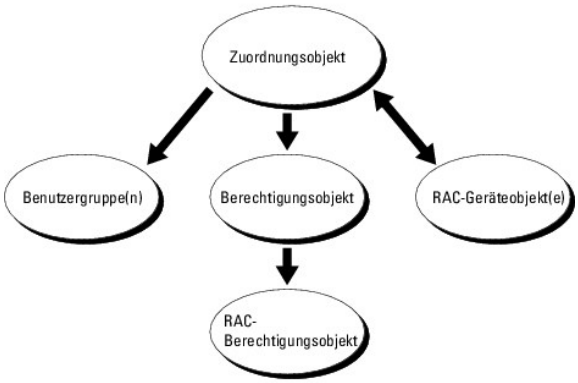
Für jedes der physischen RACs auf dem Netzwerk, das Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein RAC-Geräteobjekt erstellen. Sie können verschiedene Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt mit beliebig vielen Benutzern, Benutzergruppen, oder RAC-Geräteobjekten wie erforderlich verbunden werden kann. Die Benutzer und RAC-Geräteobjekte können Mitglieder jeder Domäne im Unternehmen sein.

Jedoch darf jedes Zuordnungsobjekt nur mit einem Berechtigungsobjekt verbunden werden bzw. darf jedes Zuordnungsobjekt Benutzer, Benutzergruppen oder RAC-Geräteobjekte nur mit einem Berechtigungsobjekt verbinden. Dieses Beispiel ermöglicht dem Administrator, die Berechtigungen jedes Benutzers auf spezifischen RACs zu steuern.

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

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

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



ANMERKUNG: Das RAC-Berechtigungsobjekt gilt sowohl für DRAC 4 als auch für iDRAC.

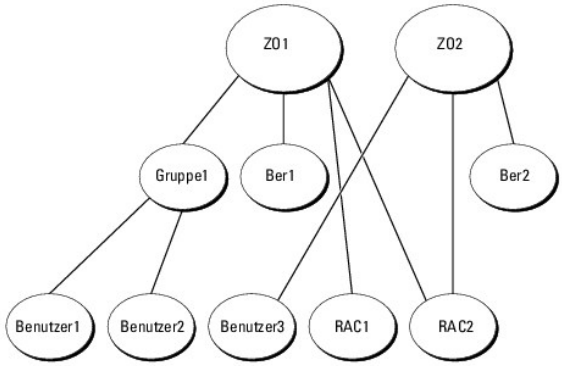
Sie können je nach Bedarf eine beliebige Anzahl von Zuordnungsobjekten erstellen. Es ist jedoch erforderlich, dass Sie mindestens ein Zuordnungsobjekt erstellen, und Sie müssen ein RAC-Geräteobjekt für jeden RAC (iDRAC) auf dem Netzwerk besitzen, das zum Zweck der Authentifizierung und Autorisierung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

Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer und/oder Gruppen sowie RAC-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die "Benutzer", die auf den RACs über "Berechtigungen" verfügen.

Active Directory-Objekte können in einer einzelnen Domäne oder in mehreren Domänen konfiguriert werden. Beispiel: Sie besitzen zwei iDRACs (RAC1 und RAC2) und drei existierende Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Sie möchten Benutzer1 und Benutzer2 ein Administratorrecht für beide iDRACs geben und Benutzer3 eine Anmeldeberechtigung für RAC2. Abbildung 6-2 zeigt, wie Sie die Active Directory-Objekte in diesem Szenario einrichten können.

Wenn Sie Universalgruppen von unterschiedlichen Domänen hinzufügen, erstellen Sie ein Zuordnungsobjekt mit Universalreichweite. Die durch das Dell Schema Extender-Dienstprogramm erstellten Standardzuordnungsobjekte sind lokale Domänengruppen und arbeiten nicht mit Universalgruppen anderer Domänen.

Abbildung 6-2. Active Directory-Objekte in einer einzelnen Domäne einrichten



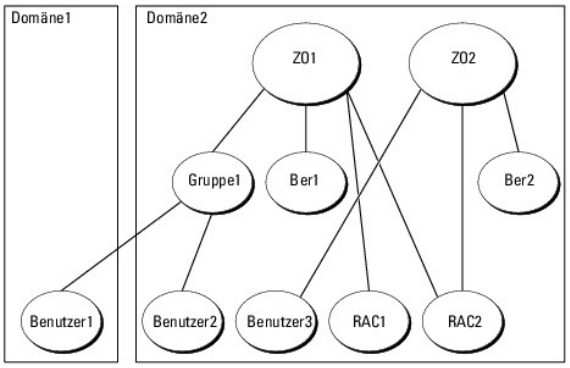
Um die Objekte für das Einzeldomänen-Szenario zu konfigurieren, führen Sie die folgenden Tasks aus:

1. Erstellen Sie zwei Zuordnungsobjekte.
2. Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die beiden iDRACs darstellen.
3. Erstellen Sie zwei Berechtigungsobjekte, Priv1 und Priv2, wobei Priv1 alle Berechtigungen (Administrator) und Priv2 Anmeldungsberechtigung besitzt.
4. user1 und user2 in Group1 gruppieren.
5. Fügen Sie Group1 als Mitglieder in Zuordnungsobjekt 1 (AO1), Priv1 als Berechtigungsobjekte in AO1 und RAC1 und RAC2 als RAC-Geräte in AO1 hinzu.
6. Fügen Sie User3 als Mitglieder im Zuordnungsobjekt 2 (AO2), Priv2 als Berechtigungsobjekte in AO2 und RAC2 als RAC-Geräte in AO2 hinzu.

Detaillierte Anleitungen hierzu finden Sie unter iDRAC-Benutzer und -Berechtigungen zum Active Directory hinzufügen.

Abbildung 6-3 enthält ein Beispiel von Active Directory-Objekten in mehreren Domänen. In diesem Szenario befinden sich zwei iDRACs (RAC1 und RAC2) und drei bestehende Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Benutzer1 ist in Domäne1 und Benutzer2 und Benutzer3 sind in Domäne2. In diesem Szenario konfigurieren Sie Benutzer1 und Benutzer2 mit Administratorrechten auf beiden iDRACs und Benutzer3 mit Anmeldeberechtigungen für RAC2.

Abbildung 6-3. Active Directory-Objekte in mehreren Domänen einrichten



Um die Objekte für das Fallbeispiel mit mehreren Domänen zu konfigurieren, führen Sie folgende Tasks aus:

1. Stellen Sie sicher, dass die Gesamtstrukturfunktionen der Domäne im einheitlichen oder im Windows 2003-Modus ist.
2. Erstellen Sie zwei Zuordnungsobjekte, ZO1 (mit der Reichweite Universell) und ZO2, in jeder Domäne.

   Abbildung 6-3 zeigt die Objekte in Domäne2.
3. Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die beiden iDRACs darstellen.
4. Erstellen Sie zwei Berechtigungsobjekte, Priv1 und Priv2, wobei Priv1 alle Berechtigungen (Administrator) und Priv2 Anmeldungsberechtigung besitzt.
5. user1 und user2 in Group1 gruppieren. Die Gruppenreichweite von Gruppe1 muss Universell sein.
6. Fügen Sie Group1 als Mitglieder in Zuordnungsobjekt 1 (AO1), Priv1 als Berechtigungsobjekte in AO1 und RAC1 und RAC2 als RAC-Geräte in AO1 hinzu.

7. Fügen Sie User3 als Mitglieder im Zuordnungsobjekt 2 (AO2), Priv2 als Berechtigungsobjekte in AO2 und RAC2 als RAC-Geräte in AO2 hinzu.

Schemaerweiterung des Active Directory zum Zugriff auf iDRAC konfigurieren

Konfigurieren Sie vor der Verwendung von Active Directory zum Zugriff auf iDRAC die Active Directory-Software und den iDRAC, indem Sie die folgenden Schritte in der vorgegebenen Reihenfolge ausführen:

1. Erweitern Sie das Active Directory-Schema (siehe Erweiterung des Active Directory-Schemas).
2. Erweitern Sie das Snap-In von Active Directory-Benutzern und - Computern (siehe Dell Erweiterung zum Active Directory-Benutzer und - Computer-Snap-In installieren).
3. Fügen Sie Active Directory iDRAC-Benutzer und ihre Berechtigungen hinzu (siehe iDRAC-Benutzer und -Berechtigungen zum Active Directory hinzufügen).
4. Aktivieren Sie SSL auf allen Domänen-Controllern (siehe SSL auf einem Domänen-Controller aktivieren).
5. Konfigurieren Sie die Active Directory-Eigenschaften des iDRAC über die iDRAC-Webschnittstelle oder das RACADM (siehe Konfiguration des iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung der Webschnittstelleoder iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung von RACADM konfigurieren).

Erweiterung des Active Directory-Schemas

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, ist sicherzustellen, dass Sie Schema-Admin-Rechte auf dem Schema Master-FSMO-Rollenbesitzer (Flexible Single Master Operation) der Domänenstruktur besitzen.

Das Schema kann anhand einer der folgenden Möglichkeiten erweitert werden:

- Dell Schema Extender-Dienstprogramm
- LDIF-Script-Datei

Die Dell-Organisationseinheit wird dem Schema nicht hinzugefügt, wenn Sie die LDIF-Skript-Datei verwenden.

Die LDIF-Dateien und Dell-Schemaerweiterung befinden sich auf Ihrer CD *Dell Systems Management Consoles* in den folgenden jeweiligen Verzeichnissen:

- *CD-Laufwerk*:**\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files**
- *CD-Laufwerk*:**\support\OMActiveDirectory Tools\RAC4-5\Schema_Extender**

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Dateien**. Zur Verwendung des Dell Schema Extender für Erweiterungen des Active Directory-Schemas siehe Dell Schema Extender verwenden.

Sie können den Schema Extender bzw. die LDIF-Dateien von einem beliebigen Standort kopieren und ausführen.

Dell Schema Extender verwenden

HINWEIS: Das Dell Schema Extender-Dienstprogramm verwendet die Datei **SchemaExtenderOem.ini**. Um sicherzustellen, dass das Dell Schemaerweiterungs-Dienstprogramm richtig funktioniert, modifizieren Sie den Namen dieser Datei nicht.

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 auf **Weiter**.
3. Wählen Sie **Aktuelle Anmeldeinformationen verwenden** aus, oder geben Sie einen Benutzernamen und ein Kennwort mit Schema-Administratorrechten ein.
4. Klicken Sie auf **Weiter**, um 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 das Vorhandensein folgender Elemente zu überprüfen:

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

   Weitere Informationen zum Aktivieren und Verwenden des Active Directory-Schema-Snap-In in der MCC stehen in Ihrer Microsoft-Dokumentation zur Verfügung.

Tabelle 6-2. Klassendefinitionen für Klassen, die dem Active Directory-Schema hinzugefügt wurden

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabelle 6-3. dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Beschreibung	Stellt das Dell RAC-Gerät dar. Das RAC-Gerät muss als dellRacDevice im Active Directory konfiguriert werden. 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 6-4. dellAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Beschreibung	Repräsentiert das Dell-Zuordnungsobjekt. Das Zuordnungsobjekt ist die Verbindung zwischen den Benutzern und den Geräten.
Klassentyp	Strukturklasse
SuperClasses	Gruppe
Attribute	dellProductMembers dellPrivilegeMember

Tabelle 6-5. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Beschreibung	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 6-6. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Beschreibung	Wird als Container-Klasse für die Dell-Berechtigungen (Autorisierungsrechte) verwendet.
Klassentyp	Strukturklasse
SuperClasses	Benutzer
Attribute	dellRAC4Privileges

Tabelle 6-7. dellProduct Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.5**
Beschreibung	Die Hauptklasse, von der alle Dell-Produkte abgeleitet werden.
Klassentyp	Strukturklasse
SuperClasses	Computer
Attribute	dellAssociationMembers

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

Attributname / Beschreibung	Zugewiesener OID / Syntax-Objektkennzeichner	Einzelbewertung
dellPrivilegeMember Die Liste von dellPrivilege-Objekten, die zu diesem Attribut gehören.	1.2.840.113556.1.8000.1280.1.1.2.1 Definierter Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Die Liste von dellRacDevices-Objekten, die zu dieser Funktion gehören. Dieses Attribut ist das Vorwärtslink zum dellAssociationMembers-Rückwärtslink. Link-ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Definierter 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-Befehls-Admin-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion Die Aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren.	1.2.840.113556.1.8000.1280.1.1.2.12 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Dieses Attribut ist der Aktuelle Rac-Typ für das dellRacDevice-Objekt und der Rückwärtslink zum dellAssociationObjectMembers-Vorwärtslink.	1.2.840.113556.1.8000.1280.1.1.2.13 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Die Liste von dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist das Rückwärtslink zum Attribut dellProductMembers. Link-ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Definierter Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

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

Wenn Sie die Systems Management Software anhand der CD *Dell Systems Management Consoles* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsverfahrens die Option **Dell-Erweiterung für das Active Directory-Benutzer und -Computer-Snap-In** auswählen. Das *Schnellinstallationshandbuch zu Dell OpenManage-Software* enthält zusätzliche Anleitungen zur Installation von Systemverwaltungssoftware.

Weitere Informationen zum 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, können Sie das Dell RAC-Objekt nicht im Container anzeigen.

Weitere Informationen finden Sie unter Active DirectoryBenutzer- und Computer-Snap-In öffnen.

Active DirectoryBenutzer- und Computer-Snap-In öffnen

Um das Active Directory-Benutzer und -Computer-Snap-In zu öffnen, führen Sie folgende Schritte aus:

1. Wenn Sie auf dem Domänen-Controller angemeldet sind, klicken Sie auf **Start**→ **Admin Tools**→ **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 auf **Eingabe**.

   Die Microsoft-Verwaltungskonsole (MMC) wird eingeblendet.

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 und klicken Sie auf **Hinzufügen**.

5. Klicken Sie auf **Schließen** und dann auf **OK**.

iDRAC-Benutzer und -Berechtigungen zum Active Directory hinzufügen

Mit dem von Dell erweiterten Active Directory-Benutzer- und Computer-Snap-In können Sie iDRAC-Benutzer und -Berechtigungen hinzuzufügen, indem Sie RAC-, Zuordnungs- und Berechtigungsobjekte erstellen. Führen Sie zum Hinzufügen der einzelnen Objektarten folgende Verfahren aus:

- RAC-Geräteobjekt erstellen
- Berechtigungsobjekt erstellen
- Zuordnungsobjekt erstellen
- Einem Zuordnungsobjekt Objekte hinzufügen

RAC-Geräteobjekt erstellen

1. Klicken Sie im Fenster MMC-**Console Root** mit der rechten Maustaste auf einen Container.

2. Wählen Sie **Neu**→ **Dell RAC-Objekt** aus.

   Das Fenster **Neues Objekt** wird geöffnet.

3. Tippen Sie einen Namen für das neue Objekt ein. Der Name muss mit dem iDRAC-Namen übereinstimmen, den Sie in Schritt a von Konfiguration des iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung der Webschnittstelle eingeben.

4. Wählen Sie **RAC-Geräteobjekt** aus.

5. Klicken Sie auf **OK**.

Berechtigungsobjekt erstellen

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

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu→ Dell RAC-Objekt** aus.

   Das Fenster **Neues Objekt** wird geöffnet.
3. Tippen 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 **RAC-Berechtigungen** und wählen Sie die Berechtigungen aus, die der Benutzer erhalten soll (weitere Informationen finden Sie unter iDRAC-Benutzerberechtigungen).

Zuordnungsobjekt erstellen

Das Zuordnungsobjekt wird von einer Gruppe abgeleitet und muss einen Gruppentyp enthalten. Die Zuordnungsreichweite legt den Sicherheitsgruppentyp für das Zuordnungsobjekt fest. Wenn Sie ein Zuordnungsobjekt erstellen, müssen Sie die Zuordnungsreichweite wählen, die sich auf den Typ der Objekte bezieht, die hinzugefügt werden sollen.

Wenn z. B. **Universal** ausgewählt wird, bedeutet dies, dass Zuordnungsobjekte nur verfügbar sind, wenn die Active Directory-Domäne im systemspezifischen Modus oder einem höheren Modus arbeitet.

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu→ Dell RAC-Objekt** aus.

   Hierdurch wird das Fenster **Neues Objekt** geöffnet.
3. Tippen Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Zuordnungsobjekt**.
5. Wählen Sie die Reichweite für das **Zuordnungsobjekt**.
6. Klicken Sie auf **OK**.

Objekte zu einem Zuordnungsobjekt hinzufügen

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und RAC-Geräte oder RAC-Gerätegruppen zuordnen. Wenn das System Windows 2000 oder höher ausführt, müssen Sie universale Gruppen verwenden, damit sich Benutzer- oder RAC-Objekte über Domänen erstrecken.

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

Benutzer oder Benutzergruppen hinzufügen

1. Klicken Sie mit der rechten Maustaste auf **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, die die Berechtigungen des Benutzers bzw. der Benutzergruppe bei Authentifizierung eines RAC-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**.

Klicken Sie auf das Register **Produkte**, um der Zuordnung ein RAC-Gerät oder mehrere RAC-Geräte hinzuzufügen. Die zugeordneten Geräte geben die an das Netzwerk angeschlossenen RAC-Geräte an, die für die festgelegten Benutzer oder Benutzergruppen verfügbar sind. Mehrere RAC-Geräte können einem Zuordnungsobjekt hinzugefügt werden.

RAC-Geräte oder RAC-Gerätegruppen hinzufügen

RAC-Geräte oder RAC-Gerätegruppen hinzufügen:

1. Wählen Sie das Register **Produkte** aus und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Namen des RAC-Geräts oder der RAC-Gerätegruppe ein und klicken Sie auf **OK**.
3. Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.

Konfiguration des iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung der Webschnittstelle

1. Öffnen Sie ein unterstütztes Web-Browser-Fenster.
2. Melden Sie sich bei der iDRAC-Webschnittstelle an.
3. Klicken Sie auf **System**→ **Remote-Zugriff**.
4. Klicken Sie auf das Register **Konfiguration** und wählen Sie **Active Directory** aus.
5. Wählen Sie auf der Seite **Active Directory-Haupmenü** die Option **Active Directory konfigurieren** aus und klicken Sie auf **Weiter**.
6. Führen Sie im Abschnitt Allgemeine Einstellungen Folgendes aus:
   e. Wählen Sie das Kontrollkästchen **Active Directory aktivieren** aus.
   f. Geben Sie den **Root-Domänennamen** ein. Der **Root-Domänenname** ist der vollständig qualifizierte Root-Domänenname der Gesamtstruktur.
   g. Geben Sie die **Zeitüberschreitung**szeit in Sekunden ein.
7. Klicken Sie im Abschnitt zur Auswahl des Active Directory-Schemas auf **Erweitertes Schema verwenden**.
8. Führen Sie im Abschnitt Einstellungen des erweiterten Schemas Folgendes aus:
   a. Geben Sie den **DRAC-Namen** ein. Dieser Name muss mit dem allgemeinen Namen des neuen RAC-Objekts übereinstimmen, das Sie im Domänen-Controller erstellt haben (siehe Schritt 3 von RAC- Geräteobjekt erstellen").
   b. Geben Sie den **DRAC-Domänennamen** ein (z. B. `iDRAC.com`). Verwenden Sie den NetBIOS-Namen nicht. Der **DRAC- Domänenname** ist der vollständig qualifizierte Domänenname der untergeordneten Domäne, in der sich das RAC-Geräteobjekt befindet.
9. Klicken Sie auf **Anwenden**, um die Active Directory-Einstellungen zu speichern.
10. Klicken Sie auf **Zurück zum Active Directory Hauptmenü**.
11. Laden Sie das Stamm-Zertifizierungsstellenzertifikat der Domänengesamtstruktur zum iDRAC hoch.
    a. Wählen Sie die Optionsschaltfläche **Active Directory- Zertifizierungsstellenzertifikat hochladen** aus und klicken Sie dann auf **Weiter**.
    b. Geben Sie auf der Seite **Zertifikat hochladen** den Dateipfad des Zertifikats ein, oder wechseln Sie zur Zertifikatsdatei.

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

    Die SSL-Zertifikate der Domänen-Controller müssen von der Stamm-CA signiert sein. Halten Sie das Stamm-CA-Zertifikat auf der Management Station bereit, die auf den iDRAC zugreift (siehe Domänen-Controller-Stamm-CA-Zertifikat exportieren).

    c. Klicken Sie auf **Anwenden**.

    Der iDRAC-Web Server startet automatisch neu, wenn Sie auf **Anwenden** klicken.
12. Melden Sie sich beim iDRAC ab und dann wieder an, um die Funktionskonfiguration für das iDRAC-Active Directory durchzuführen.
13. Klicken Sie auf **System**→ **Remote-Zugriff**.

14. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**.

15. Wenn **DHCP verwenden (für NIC-IP-Adresse)** unter **Netzwerkeinstellungen** ausgewählt ist, wählen Sie **DHCP zum Abrufen der DNS-Serveradresse verwenden** aus.

    Um die IP-Adresse eines DNS-Servers manuell einzugeben, wählen Sie **DHCP zum Abrufen der DNS-Serveradressen verwenden** ab und geben Sie die primäre und alternative IP-Adresse des DNS-Servers ein.

16. Klicken Sie auf **Änderungen übernehmen**.

    Die Funktionskonfiguration für das iDRAC-Schemaerweiterung des Active Directory wurde durchgeführt.

iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung von RACADM konfigurieren

Verwenden Sie die folgenden Befehle, um die iDRAC-Active Directory-Funktion mit der Schemaerweiterung zu konfigurieren, indem Sie das RACADM-CLI-Hilfsprogramm anstelle der Webschnittstelle 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 cfgADRacDomain <RAC-FQDN>

   racadm config -g cfgActiveDirectory -o cfgADRootDomain <Stamm-FQDN>

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

   racadm sslcertupload -t 0x2 -f <Stamm-Zeritifizierungsstellen-Zertifikat-TFTP-URI>

   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 Ihre DNS-IP- Adressen manuell eingeben möchten, 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. Drücken Sie auf **Eingabe**, um die iDRAC-Active Directory- Funktionskonfiguration durchzuführen.

iDRAC mit der Schemaerweiterung des Active Directory und SM-CLP konfigurieren

ANMERKUNG: Ein TFTP-Server muss aktiviert sein, von dem aus Sie das Stamm-Zertifizierungsstellenzertifikat abrufen und auf den Sie das iDRAC-Serverzertifikat speichern können.

Verwenden Sie die folgenden Befehle, um die iDRAC-Active Directory-Funktion mit dem erweiterten Schema unter Verwendung von SM-CLP zu konfigurieren.

1. Melden Sie sich unter Verwendung von telnet oder SSH am iDRAC an und geben Sie folgende SM-CLP-Befehle ein:

   ```
   cd /system/sp1/oemdell_adservice1

   set enablestate=1

   set oemdell_schematype=1

   set oemdell_adracdomain=<RAC-FQDN>

   set oemdell_adrootdomain=<Stamm-FQDN>

   set oemdell_adracname=<RAC-allgemeiner-Name>

   set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD

   load -source <ActiveDirectory-Zertifikat-TFTP-URI> /system1/sp1/oemdell_ssl1
   ```

```
set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL
dump -destination <DRAC-Serverzertifikat-TFTP-URI> /system1/sp1/oemdell_ssl1
```

2. Wenn DHCP auf dem iDRAC aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgenden SM-CLP- Befehl ein:

```
set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1 oemdell_serversfromdhcp=1
```

3. Wenn DHCP auf dem iDRAC deaktiviert ist oder Sie Ihre DNS-IP- Adresse manuell eingeben möchten, geben Sie folgende SM-CLP-Befehle ein:

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=0

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<primäre-DNS-IP-Adresse>

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<sekundäre-DNS-IP-Adresse>
```

Übersicht zum Standardschema des Active Directory

Wie in Abbildung 6-4 dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration unter Active Directory als auch unter iDRAC. Auf der Seite des Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der Zugriff auf den iDRAC besitzt, wird ein Mitglied der Rollengruppe sein. Um diesem Benutzer Zugriff auf einen bestimmten iDRAC zu gewähren, muss der Rollengruppenname und dessen Domänenname auf dem bestimmten iDRAC konfiguriert werden. Im Gegensatz zur Schemaerweiterungslösung wird die Rolle und die Berechtigungsebene auf jedem iDRAC und nicht im Active Directory definiert. Auf jedem iDRAC können bis zu fünf Rollengruppen konfiguriert und definiert werden. Tabelle 5-10 zeigt die Zugriffsstufe der Rollengruppen und Tabelle 6-9 zeigt die standardmäßigen Einstellungen der Rollengruppen.

Abbildung 6-4. iDRAC-Konfiguration mit Microsoft Active Directory und dem Standardschema

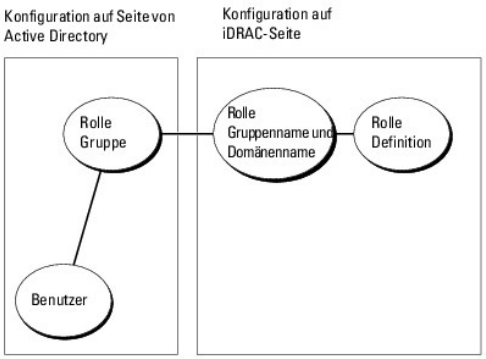


Tabelle 6-9. Standardmäßige Rollengruppenberechtigungen

Standard-Zugriffsstufe	Gewährte Berechtigungen	Bit-Maske
Administrator	Bei iDRAC **anmelden**, iDRAC **konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **auf Konsolenumleitung zugreifen**, **auf Virtuellen Datenträger zugreifen**, **Warnungen testen**, **Diagnosebefehle ausführen**	0x000001ff
Hauptbenutzer	Bei iDRAC **anmelden**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **auf Konsolenumleitung zugreifen**, **auf Virtuellen Datenträger zugreifen**, **Warnungen testen**	0x000000f9
Gastbenutzer	Bei iDRAC anmelden	0x00000001
Keine	Keine zugewiesenen Berechtigungen	0x00000000
Keine	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bit-Maskenwerte werden nur verwendet, wenn das Standardschema mit RACADM eingestellt wird.

Das Standardschema kann auf zwei Arten im Active Directory aktiviert werden:

- Mit der iDRAC-Web-Benutzeroberfläche. Siehe Konfiguration des iDRAC anhand des Standardschemas des Active Directory und der Webschnittstelle.
- Mit dem RACADM-CLI-Hilfsprogramm. Siehe Konfiguration des iDRAC anhand des Standardschemas von Active Directory und RACADM.

Standardschema von Active Directory zum Zugriff auf iDRAC konfigurieren

Bevor ein Active Directory-Benutzer auf den iDRAC zugreifen kann, müssen die folgenden Schritte zur Konfiguration des Active Directory ausgeführt werden:

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 Name der Gruppe und der Name dieser Domäne müssen auf dem iDRAC über die Webschnittstelle, RACADM oder über SM-CLP konfiguriert werden (siehe Konfiguration des iDRAC anhand des Standardschemas des Active Directory und der Webschnittstelleoder Konfiguration des iDRAC anhand des Standardschemas von Active Directory und RACADM).
3. Fügen Sie den Active Directory-Benutzer als Mitglied der Active Directory-Gruppe hinzu, um auf den iDRAC zuzugreifen.

Konfiguration des iDRAC anhand des Standardschemas des Active Directory und der Webschnittstelle

1. Öffnen Sie ein unterstütztes Web-Browser-Fenster.
2. Melden Sie sich bei der iDRAC-Webschnittstelle an.
3. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Konfiguration**.
4. Wählen Sie **Active Directory** aus, um die Seite **Active Directory- Hauptmenü** zu öffnen.
5. Wählen Sie auf der Seite **Active Directory-Haupmenü** die Option **Active Directory konfigurieren** aus und klicken Sie auf **Weiter**.
6. Führen Sie im Abschnitt Allgemeine Einstellungen Folgendes aus:
   a. Wählen Sie das Kontrollkästchen **Active Directory aktivieren** aus.
   b. Geben Sie den **Root-Domänennamen** ein. Der **Root-Domänenname** ist der vollständig qualifizierte Root-Domänenname der Gesamtstruktur.
   c. Geben Sie die **Zeitüberschreitung**szeit in Sekunden ein.
7. Klicken Sie im Abschnitt Active Directory-Schemaauswahl auf **Standardschema verwenden**.
8. Klicken Sie auf **Anwenden**, um die Active Directory-Einstellungen zu speichern.
9. Klicken Sie in der Spalte **Rollengruppen** des Abschnitts Standardschemaeinstellungen auf eine **Rollengruppe**.

   Die Seite **Rollengruppe konfigurieren** wird eingeblendet, die den **Gruppennamen**, die **Gruppendomäne** sowie die **Rollengruppenberechtigungen** einer Rollengruppe enthält.
10. Geben Sie den **Gruppennamen** ein. Der Gruppenname identifiziert die Rollengruppe in dem Active Directory, das dem iDRAC zugeordnet ist.
11. Geben Sie die **Gruppendomäne** ein. Die **Gruppendomäne** ist der vollständig qualifizierte root-Domänenname der Gesamtstruktur.
12. Richten Sie auf der Seite **Rollengruppenberechtigungen** die Gruppenberechtigungen ein.

    Tabelle 5-10 beschreibt die **Rollengruppenberechtigungen**.

    Wenn Sie eine Berechtigung modifizieren, wird die vorhandene **Rollengruppenberechtigung** (**Administrator**, **Hauptbenutzer** oder **Gastbenutzer**) auf Grundlage der modifizierten Berechtigungen entweder zur benutzerdefinierten Gruppe oder zur entsprechenden **Rollengruppenberechtigung** verändert.
13. Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern.
14. Klicken Sie auf **Zurück zur Active Directory-Konfiguration und - Verwaltung**.
15. Klicken Sie auf **Zurück zum Active Directory Hauptmenü**.
16. Laden Sie das Stamm-Zertifizierungsstellenzertifikat der Domänengesamtstruktur zum iDRAC hoch.
    a. Wählen Sie die Optionsschaltfläche **Active Directory- Zertifizierungsstellenzertifikat hochladen** aus und klicken Sie dann auf **Weiter**.
    b. Geben Sie auf der Seite **Zertifikat hochladen** den Dateipfad des Zertifikats ein oder durchsuchen Sie die Zertifikatsdatei.

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

    Die SSL-Zertifikate der Domänen-Controller müssen von der Stamm-CA signiert sein. Halten Sie das Stamm-CA-Zertifikat auf der Management Station bereit, die auf den iDRAC zugreift (siehe Domänen-Controller-Stamm-CA-Zertifikat exportieren).

    c. Klicken Sie auf **Anwenden**.

    Der iDRAC-Web Server startet automatisch neu, wenn Sie auf **Anwenden** klicken.

17. Melden Sie sich beim iDRAC ab und dann wieder an, um die Funktionskonfiguration für das iDRAC-Active Directory durchzuführen.

18. Klicken Sie auf **System**→ **Remote-Zugriff**.

19. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**.

20. Wenn **DHCP verwenden (für NIC-IP-Adresse)** unter **Netzwerkeinstellungen** ausgewählt ist, wählen Sie **DHCP zum Abrufen der DNS-Serveradresse verwenden** aus.

    Um die IP-Adresse eines DNS-Servers manuell einzugeben, wählen Sie **DHCP zum Abrufen der DNS-Serveradressen verwenden** ab und geben Sie die primäre und alternative IP-Adresse des DNS-Servers ein.

21. Klicken Sie auf **Änderungen übernehmen**.

    Die Konfiguration der Active Directory-Funktion des iDRAC-Standardschemas wurde durchgeführt.

Konfiguration des iDRAC anhand des Standardschemas von Active Directory und RACADM

Verwenden Sie die folgenden Befehle, um die iDRAC-Active Directory-Funktion mit dem Standardschema zu konfigurieren, indem Sie RACADM-CLI anstelle der Webschnittstelle 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 2

   racadm config -g cfgActiveDirectory -o cfgADRootDomain <Stamm-FQDN>

   racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupName <allgemeiner-Name-der-Rollengruppe>

   racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupDomain <RAC-FQDN>

   racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupPrivilege <Berechtigungen-Bitmaske>

   racadm sslcertupload -t 0x2 -f <Stamm-Zeritifizierungsstellen-Zertifikat-TFTP-URI>

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

   ANMERKUNG: Siehe Tabelle B-1 für Bitmaskenwerte.

2. Wenn DHCP auf dem iDRAC aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgende RACADM- Befehle ein:

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

3. Wenn DHCP auf dem iDRAC deaktiviert ist oder Sie Ihre DNS-IP- Adressen von Hand eingeben möchten, 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>
   ```

Konfiguration des iDRAC anhand des Active Directory-Standardschemas und SM-CLP

ANMERKUNG: Zertifikate können nicht mithilfe von SM-CLP hochgeladen werden. Verwenden Sie stattdessen die iDRAC-Webschnittstelle oder die Befehle des lokalen RACADM.

Verwenden Sie die folgenden Befehle, um die iDRAC-Active Directory-Funktion mit dem Standardschema unter Verwendung von SM-CLP zu konfigurieren.

1. Melden Sie sich unter Verwendung von telnet oder SSH am iDRAC an und geben Sie folgende SM-CLP-Befehle ein:

   ```
   cd /system/sp1/oemdell_adservice1

   set enablestate=1

   set oemdell_schematype=2

   set oemdell_adracdomain=<RAC-FQDN>
   ```

2. Geben Sie folgende Befehle für jede der fünf Active Directory- Rollengruppen ein:

   ```
   set /system1/sp1/groupN oemdell_groupname=<RollengruppeN-allgemeiner-Name>

   set /system1/sp1/groupN oemdell_groupdomain=<RAC-FQDN>

   set /system1/sp1/groupN oemdell_groupprivilege=<Benutzerberechtigungs-Bitmaske>
   ```

   wobei *N* eine Zahl von 1 bis 5 ist.

3. Geben Sie folgende Befehle zum Einstellen der Active Directory-SSL- Zertifizierungen ein.

   ```
   set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD
   load -source <ActiveDirectory-Zertifikat-TFTP-URI> /system1/sp1/oemdell_ssl1

   set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL

   dump -destination <iDRAC-Serverzertifikat-TFTP-URI> /system1/sp1/oemdell_ssl1
   ```

4. Wenn DHCP auf dem iDRAC aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgenden SM-CLP- Befehl ein:

   ```
   set /system1/sp1/enetport1/lanendpt1/\
   ipendpt1/dnsendpt1 oemdell_serversfromdhcp=1
   ```

5. Wenn DHCP auf dem iDRAC deaktiviert ist oder Sie Ihre DNS-IP- Adressen manuell eingeben möchten, geben Sie folgende SM-CLP-Befehle ein:

   ```
   set /system1/sp1/enetport1/lanendpt1/\
   ipendpt1/dnsendpt1 oemdell_serversfromdhcp=0

   set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
   dnsendpt1/remotesap1 dnsserveraddress=<primäre-DNS-IP-Adresse>

   set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
   dnsendpt1/remotesap1 dnsserveraddress=<sekundäre-DNS-IP-Adresse>
   ```

SSL auf einem Domänen-Controller aktivieren

Wenn Sie die Microsoft Enterprise Stamm-CA verwenden, um alle Domänen-Controller-SSL-Zertifikate automatisch zuzuweisen, müssen Sie die folgenden Schritte ausführen, um SSL auf jedem Domänen-Controller zu aktivieren.

1. Installieren Sie eine Microsoft Organisations-Stammzertifizierungsstelle auf dem Domänen-Controller.
   a. Wählen Sie **Start**→ **Systemsteuerung**→ **Software**.
   b. Wählen Sie **Windows-Komponenten hinzufügen/entfernen**.
   c. Im **Assistenten** für **Windows-Komponenten** markieren Sie das Kontrollkästchen **Zertifikatsdienste**.
   d. Wählen Sie **Stammzertifizierungsstelle der Organisation** als **Zertifizierungsstellentyp** und klicken Sie auf **Weiter**.
   e. Geben Sie einen Namen in **Allgemeiner Name dieser Zertifizierungsstelle** ein, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

2. Aktivieren Sie SSL auf jedem einzelnen Domänen-Controller, indem Sie das SSL-Zertifikat für jeden Controller installieren.
   a. Klicken Sie auf **Start**→ **Verwaltung**→ **Domänensicherheitsregeln**.
   b. Erweitern Sie den Ordner **Richtlinien öffentlicher Schlüssel** klicken Sie mit der rechten Maustaste auf **Automatische Zertifikatanforderungs-Einstellungen** und klicken Sie auf **Automatische Zertifikatanforderung**.
   c. Klicken Sie im **Setup-Assistent der automatischen Zertifikatanforderung** auf **Weiter** und wählen Sie **Domänen- Controller** aus.
   d. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Domänen-Controller-Stamm-CA-Zertifikat exportieren

ANMERKUNG: Wenn Ihr System Windows 2000 ausführt, 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** bei Windows 2000-Computern**)** und wählen Sie **Snap-In hinzufügen/entfernen** aus.

5. Klicken Sie im Fenster **Snap-In hinzufügen/entfernen** auf **Hinzufügen**.

6. Wählen Sie im Fenster **Eigenständiges Snap-In Zertifikate** aus und klicken Sie auf **Hinzufügen**.

7. Wählen Sie **Computer**-Konto und klicken Sie auf **Weiter**.

8. Wählen Sie **Lokaler Computer** und klicken Sie auf **Fertig stellen**.

9. Klicken Sie auf **OK**.

10. Erweitern Sie im Fenster **Konsole 1** den Ordner **Zertifikate**, erweitern Sie den Ordner **Persönlich** und klicken Sie auf den Ordner **Zertifikate**.

11. Suchen Sie das Stammzertifizierungsstellenzertifikat und klicken Sie mit der rechten Maustaste darauf; wählen Sie **Alle Tasks** aus und klicken Sie auf **Exportieren...**.

12. Klicken Sie im **Zertifikate exportieren-Assistenten** auf **Weiter** und wählen Sie **Privaten Schlüssel nicht exportieren** aus.

13. Klicken Sie auf **Weiter** und wählen Sie **Base-64-codiert 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 iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung der Webschnittstelle.

    Um das Zertifikat mittels der Webschnittstelle hochzuladen, führen Sie das folgende Verfahren aus:

    a. Öffnen Sie ein Fenster eines unterstützten Web-Browsers.

    b. Melden Sie sich bei der iDRAC-Webschnittstelle an.

    c. Klicken Sie auf **System**→ **Remote-Zugriff** und dann auf das Register **Konfiguration**.

    d. Klicken Sie auf **Sicherheit**, um die Seite **Hauptmenü des Sicherheitszertifikats** zu öffnen.

    e. Wählen Sie auf der Seite **Sicherheitszertifikat Hauptseite** die Option **Serverzertifikat hochladen** aus und klicken Sie auf **Weiter**.

    f. Führen Sie auf dem Bildschirm **Zertifikat hochladen** eines der folgenden Verfahren aus:

        - Klicken Sie auf **Durchsuchen** und wählen Sie das Zertifikat aus.
        - Geben Sie den Pfad zum Zertifikat in das Feld **Wert** ein.

    g. Klicken Sie auf **Anwenden**.

SSL-Zertifikat der iDRAC-Firmware importieren

Wenden Sie das folgende Verfahren an, um das SSL-Zertifikat der iDRAC-Firmware in alle vertrauenswürdigen Zertifikatlisten der Domänen-Controller zu importieren.

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

ANMERKUNG: Wenn das iDRAC-Firmware-SSL-Zertifikat von einer bekannten Zertifizierungsstelle signiert ist, müssen die in diesem Abschnitt beschriebenen Schritte nicht ausgeführt werden.

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

Für einen Zugriff auf das Zertifikat über die iDRAC-Webschnittstelle wählen Sie **Konfiguration**→ **Active Directory**→ **iDRAC-Serverzertifikat herunterladen** aus.

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 Tasks** und klicken Sie auf **Import**.

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

4. Installieren Sie das RAC-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 enthalten ist, muss sie auf allen Ihren Domänen-Controllern installiert werden.

5. Klicken Sie auf **Weiter** und wählen Sie aus, ob Windows automatisch einen Zertifikatspeicher aussuchen soll, der vom Zertifikattyp abhängt, oder ob Sie nach einem eigenen Speicher suchen wollen.

6. Klicken Sie auf **Fertig stellen** und dann auf **OK**.

Active Directory zur Anmeldung beim iDRAC verwenden

Sie können Active Directory verwenden, um sich unter Verwendung der Webschnittstelle am iDRAC anzumelden. Verwenden Sie zur Eingabe Ihres Benutzernamens eines der folgenden Formate aus:

<*Benutzername@Domäne*>

oder

<*Domäne*>\<*Benutzername*>

oder

<*Domäne*>/<*Benutzername*>

wobei *Benutzername* eine ASCII-Zeichenkette von 1 - 256 Byte ist.

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

ANMERKUNG: NetBIOS-Domänennamen wie Americas" können nicht festgelegt werden, da diese Namen nicht aufgelöst werden können.

Häufig gestellte Fragen

Tabelle 6-10 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 6-10. iDRAC mit Active Directory verwenden: Häufig gestellte Fragen

Frage	Antwort
Kann ich mich mit Active Directory über mehrfache Strukturen am iDRAC anmelden?	Ja. Der Abfragealgorithmus des iDRAC-Active Directory unterstützt mehrere Strukturen in einer einzelnen Gesamtstruktur.
Funktioniert die Anmeldung am iDRAC anhand von Active Directory im gemischten Modus (d. h. die Domänen-Controller in der Gesamtstruktur führen verschiedene Betriebssysteme aus, z. B. Microsoft Windows NT® 4.0, Windows 2000 oder Windows Server 2003)?	Ja. Im gemischten Modus müssen sich alle durch das iDRAC-Abfrageverfahren verwendeten Objekte (unter Benutzer, RAC-Geräteobjekt und Zuordnungsobjekt) in derselben Domäne befinden. Das Dell-erweiterte Active Directory-Benutzer- und -Computers-Snap-In überprüft den Modus und beschränkt Benutzer, um Objekte über Domänen hinweg zu erstellen, wenn es im Mischmodus ist.
Unterstützt die Verwendung des iDRAC mit Active Directory mehrfache Domänenumgebungen?	Ja. Die Domänen-Gesamtstrukturstufe muss im einheitlichen Modus oder Windows-2003-Modus sein. Außerdem müssen die Gruppen unter Zuordnungsobjekt, RAC-Benutzerobjekten und RAC-Geräteobjekten (einschließlich Zuordnungsobjekt) universale Gruppen sein.
Können diese Dell-erweiterten Objekte (Dell-Zuordnungsobjekt, Dell RAC-Gerät und Dell-Berechtigungsobjekt) in verschiedenen Domänen sein?	Das Zuordnungsobjekt und das Berechtigungsobjekt müssen in derselben Domäne sein. Das Dell-erweiterte Active Directory-Benutzer- und -Computers-Snap-In zwingt Sie, diese beiden Objekte in derselben Domäne zu erstellen. Andere Objekte können sich in verschiedenen Domänen befinden.
Gibt es Beschränkungen der Domänen-Controller SSL-Konfiguration?	Ja. SSL-Zertifikate aller Active Directory-Server in der Gesamtstruktur müssen von derselben Stammzertifizierungsstelle signiert werden, da iDRAC nur das Hochladen eines einzigen SSL-Zertifikats einer vertrauenswürdigen Zertifizierungsstelle zulässt.
Ich habe ein neues RAC-Zertifikat erstellt und hochgeladen und jetzt startet die Webschnittstelle nicht.	Wenn Sie zum Erstellen des RAC-Zertifikats Microsoft Certificate Services verwenden, ist eine mögliche Ursache, dass Sie bei der Erstellung des Zertifikats versehentlich **Benutzerzertifikat** statt **Internetzertifikat** ausgewählt haben. Erstellen Sie zur Wiederherstellung eine CSR und dann ein neues Webzertifikat über die Microsoft-Zertifikatdienste und laden Sie es unter Verwendung der RACADM-CLI vom verwalteten Server, indem Sie die folgenden RACADM-Befehle verwenden: racadm sslcsrgen [-g] [-u] [-f {filename}] racadm sslcertupload -t 1 -f {web_sslcert}
Was kann ich tun, wenn ich mich mit Active Directory-Authentifizierung nicht am iDRAC anmelden kann? Wie kann ich das Problem beheben?	1. Stellen Sie sicher, dass Sie während einer Anmeldung den korrekten Benutzerdomänennamen statt des NetBIOS-Namens verwenden. 2. Wenn Sie ein lokales iDRAC-Benutzerkonto besitzen, melden Sie sich mit Ihren lokalen Anmeldeinformationen am iDRAC an. Nachdem Sie angemeldet sind, die folgenden Schritte ausführen: a. Stellen Sie sicher, dass das Kästchen **Active Directory aktivieren** auf der iDRAC-Seite **Active Directory-Konfiguration** markiert ist. b. Stellen Sie sicher, dass die DNS-Einstellung auf der iDRAC-Seite **Netzwerkkonfiguration** korrekt ist.

	c. Stellen Sie sicher, dass Sie das Active Directory-Zertifikat von Ihrer Active Directory-Stammzertifizierungsstelle zum iDRAC hochgeladen haben. d. Überprüfen Sie die Domänen-Controller SSL-Zertifikate, um sicherzustellen, dass sie nicht abgelaufen sind. e. Stellen Sie sicher, dass der **DRAC-Name**, **Stammdomänenname** und **DRAC-Domänenname** mit der Active Directory-Umgebungskonfiguration übereinstimmen. f. Stellen Sie sicher, dass das iDRAC-Kennwort maximal 127 Zeichen aufweist. Während der iDRAC Kennwörter von bis zu 256 Zeichen unterstützen kann, unterstützt Active Directory nur Kennwörter, die maximal 127 Zeichen lang sind.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Anzeige der Konfiguration und des Zustands des verwalteten Servers

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

Systemübersicht

Klicken Sie auf **System**→ **Eigenschaften**→ **Zusammenfassung**, um Informationen über das Hauptsystemgehäuse und den integrierten Dell Remote Access Controller zu erhalten.

Hauptsystemgehäuse

Systeminformationen

Dieser Abschnitt der iDRAC-Webschnittstelle enthält folgende grundlegende Informationen über den verwalteten Server:

- Beschreibung - Die Modellnummer oder der Name des verwalteten Servers.
- BIOS-Version - Die BIOS-Versionsnummer des verwalteten Servers.
- Service-Tag-Nummer - Die Service-Tag-Nummer des verwalteten Servers.
- Hostname - Der mit dem verwalteten Server verbundene DNS-Hostname.
- Betriebssystemname - Der Name des auf dem verwalteten Server installierten Betriebssystems.

E/A-Mezzanine-Karte

In diesem Abschnitt der iDRAC-Webschnittstelle erhalten Sie Informationen über die folgenden E/A-Mezzanine-Karten und Speichercontroller-Karten, die auf dem verwalteten Server installiert sind:

- E/A-MEZZ-Karte - Führt die auf dem verwalteten Server installierte(n) E/A-Mezzanine-Karte(n) auf.
- Kartentyp - Der physische Typ der installierten Mezzanine-Karte/-Verbindung.
- Modellname - Modellnummer, Typ oder Beschreibung der installierten Mezzanine-Karte(n).
- Integrierte Speicherkarte - Die Modellnummer oder der Name der installierten Speichercontroller-Karte.

Automatische Wiederherstellung

In diesem Abschnitt der iDRAC-Webschnittstelle wird der aktuelle Betriebsmodus der Funktion Automatische Wiederherstellung auf dem verwalteten Server, wie zuvor von Open Manage Server Administrator eingestellt, beschrieben:

- Wiederherstellungsmaßnahme - Die Maßnahme wird durchgeführt, wenn ein Systemfehler oder *Hängen des Systems* erkannt wird. Verfügbare Maßnahmen sind **Keine Maßnahme**, **Kaltstart**, **Herunterfahren** oder **Aus- und Einschalten**.
- Anfänglicher Countdown - Der Zeitumfang (in Sekunden) nachdem ein Hängen des Systems erkannt wurde, bis der iDRAC eine Wiederherstellungsmaßnahme durchführt.
- Vorhandener Countdown - Der aktuelle Wert (in Sekunden) des Countdown-Zeitgebers.

Integrierter Dell Remote Access Controller

iDRAC-Informationen

Dieser Abschnitt der iDRAC-Webschnittstelle enthält folgende grundlegende Informationen über den iDRAC selbst:

- Datum/Uhrzeit - Das aktuelle Datum und Uhrzeit (ab Aktualisierung der letzten Seite) des iDRAC.
- Firmware-Version - Die aktuelle Version der auf dem verwalteten Server installierten iDRAC-Firmware.
- Firmware aktualisiert - Datum und Uhrzeit der letzten erfolgreichen Aktualisierung der iDRAC-Firmware.

- Hardware-Version - Die Versionsnummer der der Platine des verwalteten Servers.
- IP-Adresse - Die mit dem iDRAC (nicht dem verwalteten Server) verbundene IP-Adresse.
- Gateway - Die IP-Adresse des für den iDRAC konfigurierten Netzwerk-Gateways.
- Subnetzmaske - Die für den iDRAC konfigurierte TCP/IP-Subnetzmaske.
- MAC-Adresse - Die MAC-Adresse, die mit dem iDRAC Netzwerkschnittstellen-Controller des LAN auf der Hauptplatine (LOM) verbunden ist.
- DHCP aktiviert - Ist aktiviert, wenn der iDRAC zum Abrufen seiner IP-Adresse und von verbundenen Informationen von einem DHCP-Server eingestellt ist.
- Bevorzugte DNS-Adresse 1 - Ist auf den derzeit aktiven primären DNS-Server eingestellt.
- Alternative DNS-Adresse 2 - Ist auf die alternative DNS-Serveradresse eingestellt.

ANMERKUNG: Diese Informationen stehen auch unter **iDRAC→ Eigenschaften→ iDRAC-Informationen** zur Verfügung.

WWN/MAC-Zusammenfassung

Klicken Sie auf **System→ Eigenschaften→ WWN/MAC**, damit die aktuelle Konfiguration der installierten E/A-Mezzanine-Karten und ihrer verbundenen Netzwerkstrukturen angezeigt wird. Wenn die Funktion FlexAddress aktiviert ist, ersetzen die global zugewiesenen (Gehäuse-zugewiesen), permanent gültigen MAC-Adressen die fest verdrahteten Werte von jedem LOM.

Systemzustand

Klicken Sie auf **System→ Eigenschaften→ Zustand** , um wichtige Informationen über den Zustand des iDRAC und die von ihm überwachten Komponenten zu erhalten. Die Spalte **Schweregrad** zeigt den Status jeder Komponente. Eine Liste von Zustandssymbolen und deren Bedeutung finden Sie unter Tabelle 14-3. Klicken Sie auf den Komponentennamen in der Spalte **Komponente**, um weitere Informationen über die jeweilige Komponente zu erfahren.

ANMERKUNG: Sie können Komponenteninformationen ebenso erhalten, indem Sie im linken Fensterbereich auf den Komponentennamen klicken. Komponenten bleiben im linken Fensterbereich unabhängig vom ausgewählten Register/Bildschirm sichtbar.

iDRAC

Die iDRAC-Informationsseite führt eine Reihe wichtiger Einzelheiten über den iDRAC auf, wie z. B. Funktionszustand, Name, Firmware, Revision und Netzwerkparameter. Zusätzliche Einzelheiten stehen zur Verfügung, wenn Sie auf das entsprechende Register an der Oberseite klicken.

CMC

Die CMC-Seite zeigt den Funktionszustand, die Firmware-Version und die IP-Adresse des Gehäuseverwaltungscontrollers an. Durch Anklicken der Schaltfläche **CMC-Webschnittstelle starten** kann die CMC-Webschnittstelle auch gestartet werden.

Batterien

Die Batterie-Seite zeigt den Status und die Werte der Systemplatine-Knopfzellenbatterie an, die die Echtzeituhr (RTC) und den Datenspeicher für die CMOS-Konfiguration auf dem verwalteten System mit Strom versorgt.

Temperaturen

Die Informationsseite für die Temperatursonden zeigt den Status und die Messwerte der Außentemperatursonde auf der Platine an. Minimale und maximale Temperatur-Schwellenwerte für die Zustände *Warnung* oder *Fehler* werden zusammen mit dem aktuellen Funktionszustand der Sonde angezeigt.

Spannungen

Die Informationsseite für Spannungssonden zeigt den Status und Messwert der Spannungssonden an und liefert Informationen wie z. B. den Status der Spannungsschiene auf der Platine und CPU-Kernsensoren.

ANMERKUNG: Temperaturschwellenwerte für die Zustände *Warnung* oder *Fehler* und/oder Funktionszustände der Sonde werden, abhängig von Ihrem Servermodell, eventuell nicht angezeigt.

Stromüberwachung

Die Seite zur Stromüberwachung ermöglicht Ihnen, die folgenden Informationen zur Überwachungs- und Stromstatistik anzusehen:

- Stromüberwachung - Zeigt die Menge an Strom (in Watt) an, der gemäß des Stromüberwachungsberichts der Systemplatine vom Server verbraucht wird.

- Stromverfolgungsstatistik - Zeigt Informationen über die Menge des vom System verbrauchten Stroms an, seit die **Startzeit der Messung** zurückgesetzt wurde.
- Höchstmenge-Statistik - Zeigt Informationen über die vom System aufgenommene Stromspitze an, seit die **Startzeit der Messung** zurückgesetzt wurde.

CPU

Die CPU-Informationsseite erstattet Bericht über den Zustand jeder CPU auf dem verwalteten Server. Dieser Funktionszustand stellt eine Abwicklung zahlreicher individueller Wärme-, Strom- und Funktionstests dar.

POST

Die POST-Code-Seite zeigt den letzten POST-Code des Systems (hexadezimal) an, bevor das Betriebssystem des verwalteten Servers gestartet wird.

Sonstige Zustände

Die Seite Sonstige Zustände bietet Zugriff auf die folgenden Systemprotokolle:

System-Ereignisprotokoll - Zeigt systemkritische Ereignisse an, die auf dem verwalteten System vorkommen.

POST-Code-Seite - Zeigt den letzten POST-Code des Systems (hexadezimal) an, bevor das Betriebssystem des verwalteten Servers gestartet wird.

Letzter Absturz - Zeigt den Bildschirm und die Zeit des letzten Absturzes an.

Start-Capture - Gibt die letzten drei Startbildschirme wieder.

ANMERKUNG: Diese Informationen stehen auch unter **System**→ **Eigenschaften**→ **Protokolle** zur Verfügung.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

GUI-Konsolenumleitung verwenden

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

Dieser Abschnitt enthält Informationen über die Anwendung der iDRAC-Konsolenumleitungsfunktion.

Übersicht

Mit der iDRAC-Konsolenumleitungsfunktion können Sie im Remote-Zugriff im grafischen Modus oder Textmodus auf die lokale Konsole zugreifen. Mittels der Konsolenumleitung können Sie ein oder mehrere iDRAC-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.

Die Seite **Konsolenumleitung** ermöglicht Ihnen, das Remote-System zu verwalten, indem Sie Tastatur, Video und Maus auf Ihrer lokalen Verwaltungsstation verwenden, um die entsprechenden Geräte auf einem verwalteten Remote-Server zu steuern. Diese Funktion kann in Verbindung mit der Virtuellen Datenträger-Funktion verwendet werden, um Remote-Software-Installationen auszuführen.

Die folgenden Regeln gelten für eine Konsolenumleitungssitzung:

- Es können maximal zwei gleichzeitige Konsolenumleitungssitzungen unterstützt werden. Beide Sitzungen zeigen dieselbe Konsole des verwalteten Servers gleichzeitig an.
- Eine Konsolenumleitungssitzung darf nicht über einen Webbrowser auf dem verwalteten System gestartet werden.
- Die erforderliche verfügbare Netzwerk-Mindestbandbreite beträgt 1 MB/s.

Wenn ein zweiter Benutzer eine Konsolenumleitungssitzung anfordert, wird der erste Benutzer benachrichtigt, und er erhält die Option, den Zugriff abzulehnen, nur Video zu erlauben oder vollständig freigegebenen Zugriff zu erlauben. Der zweite Benutzer wird benachrichtigt, dass ein anderer Benutzer die Steuerung übernommen hat. Wenn der erste Benutzer dann nicht innerhalb von 30 Sekunden antwortet, wird dem zweiten Benutzer automatisch voller Zugriff gewährt. Während der Zeit, in der zwei Sitzungen gleichzeitig aktiv sind, erhält jeder Benutzer eine Meldung in der rechten, oberen Ecke des Bildschirms, die den jeweils anderen Benutzer mit einer aktiven Sitzung identifiziert. Eine dritte aktive Sitzung ist nicht erlaubt. Wenn ein dritter Benutzer eine Konsolenumleitungssitzung anfordert, wird der Zugriff ohne Unterbrechung des ersten oder zweiten Benutzers verweigert.

Wenn weder der erste noch der zweite Benutzer über Administratorberechtigungen verfügt, wird die Sitzung des zweiten Benutzers automatisch beendet, wenn der erste Benutzer seine aktive Sitzung beendet.

Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

Tabelle 8-1 listet die unterstützten Bildschirmauflösungen und entsprechenden Bildwiederholfrequenzen für eine Konsolenumleitungssitzung auf, die auf dem verwalteten Server ausgeführt wird.

Tabelle 8-1. 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

Management Station konfigurieren

Zur Verwendung der Konsolenumleitung auf der Management Station führen Sie die folgenden Verfahren aus:

1. Installieren und konfigurieren Sie einen unterstützten Internet-Browser. Weitere Informationen finden Sie in den folgenden Abschnitten:
   - Unterstützte Webbrowser
   - Einen unterstützten Web-Browser konfigurieren
2. Wenn Sie Firefox verwenden oder den Java Viewer mit Internet Explorer verwenden möchten, installieren Sie eine Java-Laufzeitumgebung (JRE). Siehe Java-Laufzeitumgebung (JRE) installieren.
3. Es wird empfohlen, die Bildschirmauflösung auf 1280x1024 Pixel oder höher einzustellen.

HINWEIS: Wenn eine aktive Konsolenumleitungssitzung vorhanden ist und ein Monitor mit niedriger Auflösung an der iKVM angeschlossen wird, wird die Serverkonsolenauflösung eventuell zurückgesetzt, wenn der Server auf der lokalen Konsole ausgewählt wird. Wenn der Server ein Linux-Betriebssystem ausführt, kann eine X11-Konsole auf dem lokalen Monitor eventuell nicht angezeigt werden. Durch Drücken auf <Strg><Alt><F1> auf der iKVM wird Linux auf eine Textkonsole geschaltet.

Konfiguration der Konsolenumleitung auf der iDRAC-Webschnittstelle

Um auf der iDRAC-Webschnittstelle eine Konsolenumleitung zu konfigurieren, führen Sie folgende Schritte aus:

1. Klicken Sie auf **System** und dann auf das Register **Konsole**.
2. Klicken Sie auf **Konfiguration**, um die Seite **Konsolenumleitungskonfiguration** zu öffnen.
3. Konfigurieren Sie die Konsolenumleitungseigenschaften. Tabelle 8-2 beschreibt die Einstellungen für die Konsolenumleitung.
4. Wenn Sie fertig sind, klicken Sie auf **Anwenden**.
5. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 8-3.

Tabelle 8-2. Konfigurationseigenschaften der Konsolenumleitung

Eigenschaft	Beschreibung
Aktiviert	Anklicken, um die Konsolenumleitung zu aktivieren oder zu deaktivieren. **Markiert** zeigt an, dass die Konsolenumleitung aktiviert ist. **Nicht markiert** zeigt an, dass die Konsolenumleitung deaktiviert ist. Die Standardeinstellung ist **aktiviert**.
Max. Sitzungen	Zeigt die Anzahl der maximal möglichen Konsolenumleitungssitzungen an - **1** oder **2**. Verwenden Sie das Drop-Down-Menü, um die maximal zulässigen Konsolenumleitungs-Sitzungen zu ändern. Die Standardeinstellung ist **2.**
Aktive Sitzungen	Zeigt die Anzahl der Sitzungen Aktiver Konsolen an. Dieses Feld ist schreibgeschützt.
Tastatur- und Mausanschlussnummer	Die 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.**
Videoanschlussnummer	Die Netzwerkanschlussnummer, die zur Verbindung mit dem Konsolenumleitungs-Bildschirmdienst verwendet wird. Diese Einstellung muss eventuell geändert werden, wenn ein anderes Programm den Standardanschluss verwendet. Die Standardeinstellung ist **5901.**
Videoverschlüsselung aktiviert	**Markiert** zeigt an, dass die Videoverschlüsselung aktiviert ist. Der zum Videoanschluss übertragene Datenverkehr ist verschlüsselt. **Nicht markiert** zeigt an, dass die Videoverschlüsselung deaktiviert ist. Der zum Videoanschluss übertragene Datenverkehr ist nicht verschlüsselt. Die Standardeinstellung ist **Verschlüsselt. Ein Deaktivieren der Verschlüsselung kann die Leistung auf langsameren Netzwerken verbessern.**
Mausmodus	Wählen Sie **Windows**, wenn der verwaltete Server auf einem Windows-Betriebssystem ausführt. Wählen Sie **Linux** aus, wenn Ihr Server auf Linux ausgeführt wird. Wählen Sie **Kein**, wenn der Server weder auf einem Windows- noch auf einem Linux-Betriebssystem ausführt. Die Standardeinstellung ist **Windows**.
Konsolen-Plugin-Typ für IE	Wenn der Internet Explorer auf einem Windows-Betriebssystem verwendet wird, können die folgenden Viewer ausgewählt werden: *ActiveX* - Der *ActiveX-Konsolenumleitungs*-Viewer Java - *Java-Konsolenumleitungs*-Viewer. **ANMERKUNG:** Abhängig von Ihrer Internet Explorer-Version müssen eventuell zusätzliche Sicherheitseinschränkungen ausgeschaltet werden (siehe Virtuellen Datenträger konfigurieren und verwenden).

	ANMERKUNG: Auf dem Client-System muss die Java-Laufzeitumgebung installiert sein, damit der Java-Viewer verwendet werden kann.
Lokale Konsole deaktivieren	Die Markierung weist darauf hin, dass die Ausgabe an den iKVM-Monitor während der Konsolenumleitung deaktiviert wird. Hierdurch wird sichergestellt, dass die unter Verwendung der **Konsolenumleitung** ausgeführten Tasks auf dem lokalen Monitor des verwalteten Servers nicht sichtbar sind.

ANMERKUNG: Informationen zur Verwendung des virtuellen Datenträgers mit Konsolenumleitung finden Sie unter Virtuellen Datenträger konfigurieren und verwenden.

Die Schaltflächen in Tabelle 8-5 sind auf der Seite **Konsolenumleitungskonfiguration** verfügbar.

Tabelle 8-3. Schaltflächen der Seite Konsolenumleitungskonfiguration

Schaltfläche	Definition
Drucken	Druckt die Seite **Konsolenumleitungskonfiguration**
Aktualisieren	Lädt die Seite **Konsolenumleitungskonfiguration** neu
Anwenden	Speichert alle neuen Einstellungen, die an der Konsolenumleitung vorgenommen wurden.

Konsolenumleitung auf der SM-CLP-Befehlszeilenoberfläche konfigurieren

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 Verwaltungsstation aus gesteuert werden.

Führen Sie folgende Schritte aus, um auf der Webschnittstelle eine Konsolenumleitungssitzung zu öffnen:

1. Klicken Sie auf **System** und dann auf das Register **Konsole**.
2. Verwenden Sie auf der Seite **Konsolenumleitung** die Informationen unter, Tabelle 8-4 um sicherzustellen, dass eine Konsolenumleitungssitzung verfügbar ist

   Sollten Sie einige der angezeigten Eigenschaftenwerte neu konfigurieren wollen, finden Sie entsprechende Informationen unter Konfiguration der Konsolenumleitung auf der iDRAC-Webschnittstelle.

Tabelle 8-4. Informationen zur Seite Konsolenumleitung

Eigenschaft	Beschreibung
Aktivierte Konsolenumleitung	Ja/Nein
Videoverschlüsselung aktiviert	Ja/Nein
Max. Sitzungen	Zeigt die maximale Anzahl unterstützter Konsolenumleitungssitzungen an
Aktuelle Sitzungen	Zeigt die aktuelle Anzahl aktiver Konsolenumleitungssitzungen an
Mausmodus	Zeigt die aktuell geltende Mausbeschleunigung an. Der Modus **Mausbeschleunigung** sollte auf der Grundlage des auf dem verwalteten Server installierten Betriebssystems ausgewählt werden.
Konsolen-Plugin-Typ	Zeigt den aktuell konfigurierten Plugin-Typ. **ActiveX** - Ein Active-X-Viewer wird gestartet. Der Active-X-Viewer funktioniert nur im Internet Explorer bei der Ausführung auf einem Windows-Betriebssystem. **Java** - Ein Java-Viewer wird gestartet. Der Java-Viewer kann in jedem Browser, einschließlich Internet Explorer, verwendet werden. Wenn Ihr Client auf einem anderen Betriebssystem als Windows ausgeführt wird, müssen Sie den Java-Viewer verwenden. Wenn Sie mit dem Internet Explorer im Windows-Betriebssystem auf den iDRAC zugreifen, können Sie entweder Active-X oder Java als Plugin-Typ auswählen.
Lokale Konsole	Nicht markiert, wenn die lokale Konsole nicht deaktiviert wurde. Wenn markiert, kann keine Person über die iKVM-Verbindung auf dem Gehäuse auf die Konsole zugreifen.

ANMERKUNG: Informationen zur Verwendung des virtuellen Datenträgers mit Konsolenumleitung finden Sie unter Virtuellen Datenträger konfigurieren und verwenden.

Die Schaltflächen in Tabelle 8-5 sind auf der Seite **Konsolenumleitungskonfiguration** verfügbar.

Tabelle 8-5. Schaltflächen der Seite Konsolenumleitung

Schaltfläche	Definition
Aktualisieren	Lädt die Seite **Konsolenumleitungskonfiguration** neu
Viewer starten	Öffnet eine Konsolenumleitungssitzung auf dem Remote-Ziel-System.
Drucken	Druckt die Seite **Konsolenumleitungskonfiguration**

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 innerhalb drei Minuten durch diese Dialogfelder wechseln. Ansonsten werden Sie aufgefordert, die Anwendung erneut zu starten.

   ANMERKUNG: Wenn in den folgenden Schritten ein Fenster oder mehrere Fenster zur **Sicherheitswarnung** eingeblendet werden, lesen Sie die Informationen im jeweiligen Fenster, und klicken Sie auf **Ja**, um fortzufahren.

   Die Verwaltungsstation wird mit dem iDRAC verbunden und der Desktop des Remote-Systems wird in der Dell Digital KVM Viewer-Anwendung angezeigt.

4. Zwei Mauszeiger erscheinen im Viewer-Fenster: einer für das Remote- System und einer für das lokale System. Die beiden Mauszeiger müssen synchronisiert werden, damit der Remote-Mauszeiger dem lokalen Mauszeiger folgt. Siehe Synchronisieren der Mauszeiger.

Video Viewer verwenden

Der Video Viewer ist eine Benutzerschnittstelle zwischen der Verwaltungsstation und dem verwalteten Server, wodurch der Desktop des verwalteten Servers sichtbar wird und die Maus-und Tastaturfunktionen von der Verwaltungsstation aus gesteuert werden können. Wenn Sie eine Verbindung zum Remote-System herstellen, wird der Video Viewer in einem separaten Fenster gestartet.

Der Video Viewer bietet die Möglichkeit verschiedener Steuerungseinsellungen wie Farbmodus, Maussynchronisation, Snapshots, Tastaturmakros und Zugriff auf den virtuellen Datenträger. Klicken Sie auf **Hilfe**, um weitere Informationen über diese Funktionen zu erhalten.

Wenn Sie eine Konsolenumleitungssitzung starten und der Video Viewer erscheint, ist es eventuell notwendig, den Farbmodus einzustellen und die Mauszeiger zu synchronisieren.

Tabelle 8-6 beschreibt die Menüoptionen, die im Viewer zum Gebrauch verfügbar sind.

Tabelle 8-6. Auswahlmöglichkeiten auf der Viewer-Menüleiste

Menüelement	Artikel	Beschreibung
Bildschirm	Anhalten	Hält die Konsolenumleitung vorübergehend an.
	Wieder aufnehmen	Nimmt die Konsolenumleitung wieder auf.
	Aktualisieren	Zeichnet die Bildschirmanzeige des Viewers neu.
	Aktuellen Bildschirminhalt erfassen	Erfasst den aktuellen Remote-Systembildschirm in einer **.bmp**-Datei auf Windows oder in einer **.png**-Datei auf Linux. Ein Dialogfeld wird angezeigt, in dem Sie die Datei zu einem angegebenen Standort speichern können.
	Vollbildschirm	Um den Video Viewer auf Vollbildschirmmodus zu erweitern, wählen Sie **Vollbildschirm** im **Video**menü aus.
	Beenden	Wenn Sie die Konsole nicht mehr verwenden und sich abgemeldet haben (durch Verwendung des Abmeldevorgangs des Remote-Systems), wählen Sie im **Video**menü **Beenden**, um das Fenster **Video Viewer** zu schließen.
Keyboard (Tastatur)	Rechte Alt-Taste halten	Wählen Sie dieses Element aus, bevor Sie Tasten verwenden, die mit der rechten <Alt>-Taste kombiniert werden sollen.
	Linke Alt-Taste halten	Wählen Sie dieses Element, bevor Sie Tasten verwenden, die mit der linken <Alt>-Taste kombiniert werden sollen.
	Linke Windows-Taste	Wählen Sie **Gedrückt halten** aus, bevor Sie Zeichen eingeben, die mit der linken Windows-Taste kombiniert werden sollen. Wählen Sie **Drücken und loslassen** aus, um einen Tastenanschlag der linken Windows-Taste zu senden.
	Rechte Windows-Taste	Wählen Sie **Gedrückt halten** aus, bevor Sie Zeichen eingeben, die mit der rechten Windows-Tate kombiniert werden sollen. Wählen Sie **Drücken und loslassen** aus, um einen Tastenanschlag der rechten Windows-Taste zu senden.
	Makros	Wenn Sie ein Makro auswählen oder den für das Makro angegebenen Hotkey eingeben, wird die Maßnahme auf dem Remote-System ausgeführt. Der Video Viewer enthält die folgenden Makros: • Strg-Alt-Entf • Alt-Tab • Alt-Esc • Strg-Esc • Alt-Leerzeichen • Alt-Eingabe • Alt-Bindestrich • Alt-F4 • Druck • Alt-Druck • F1 • Anhalten • Alt+m
	Tastaturdurchgang	Im Modus Tastaturdurchgang können alle Tastaturfunktionen auf dem Client zum Server umgeleitet werden.
Maus	Cursor synchronisieren	Im **Maus**menü können Sie den Cursor synchronisieren, damit die Maus auf dem Client zur Maus auf dem Server

		umgeleitet wird.
Optionen	Farbmodus	Ermöglicht Ihnen, zur Verbesserung der Leistung über das Netzwerk eine Farbtiefe auszuwählen. Wenn Sie z. B. Software vom virtuellen Datenträger installieren, können Sie die niedrigste Farbtiefe auswählen (3-Bit grau), damit der Konsolen-Viewer weniger Netzwerkbandbreite verwendet und mehr Bandbreite verbleibt, um Daten vom Datenträger zu übertragen. Der Farbmodus kann auf 15-Bit Farbe, 7-Bit Farbe, 4-Bit Farbe, 4-Bit grau und 3-Bit grau eingestellt werden.
Datenträger	Virtueller Datenträger-Assistent	Das **Datenträger**menü bietet Zugriff auf den Virtueller Datenträger-Assistenten, wodurch Sie zu einem Gerät oder einem Image umleiten können, wie z. B.: • Diskettenlaufwerk • CD • DVD • Image im ISO-Format • USB-Flash-Laufwerk Informationen zur Funktion virtueller Datenträger finden Sie unter Virtuellen Datenträger konfigurieren und verwenden. Wenn Sie den virtuellen Datenträger verwenden, muss das Konsolen-Viewer-Fenster aktiv sein.
Hilfe	NZ	Aktiviert das **Hilfe**-Menü.

Synchronisieren der Mauszeiger

Wenn Sie mittels Konsolenumleitung eine Verbindung zu einem Remote-PowerEdge-System herstellen, kann die Geschwindigkeit der Mausbeschleunigung auf dem Remote-System eventuell nicht mit dem Mauszeiger auf der Verwaltungsstation synchronisiert werden, was dazu führt, dass zwei Mauszeiger im Video Viewer-Fenster erscheinen.

Zum Synchronisieren der Mauszeiger klicken Sie auf **Maus**→ **Cursor synchronisieren** oder drücken Sie auf <Alt><M>.

Das Menü zum Synchronisieren des Cursors lässt sich umschalten. Stellen Sie sicher, dass sich neben dem Menüelement ein Häkchen befindet, damit die Maussynchronisation aktiv ist.

Stellen Sie bei der Verwendung von Red Hat® Linux® oder Novell® SUSE® Linux sicher, dass der Mausmodus für Linux konfiguriert ist, bevor Sie den Viewer starten. Hilfe bei der Konfiguration steht unter Konfiguration der Konsolenumleitung auf der iDRAC-Webschnittstelle zur Verfügung. Die Standardmauseinstellungen des Betriebssystems werden zur Steuerung des Mauspfeils auf dem Bildschirm der iDRAC-Konsolenumleitung verwendet.

Lokale Konsole deaktivieren oder aktivieren

Sie können den iDRAC so konfigurieren, dass iKVM-Verbindungen über die iDRAC-Webschnittstelle unzulässig sind. Wenn die lokale Konsole deaktiviert ist, wird in der Liste der Server (OSCAR) ein gelber Statuspunkt angezeigt, um darauf hinzuweisen, dass die Konsole im iDRAC geschlossen ist. Wenn die lokale Konsole aktiviert ist, ist der Statuspunkt grün.

Wenn Sie sicherstellen möchten, dass Sie exklusiven Zugriff auf die Konsole des verwalteten Servers haben, müssen Sie die lokale Konsole deaktivieren *und die* **Max. Sitzungen** auf der **Seite Konsolenumleitung** auf 1 konfigurieren.

ANMERKUNG: Die Funktion der lokalen Konsole wird auf allen x9xx PowerEdge-Systemen außer PowerEdge SC1435 und 6950 unterstützt.

ANMERKUNG: Das Deaktivieren (Ausschalten) des lokalen Videos auf dem Server führt dazu, dass der Monitor, die Tastatur und die Maus, die an die iKVM angeschlossen sind, deaktiviert werden.

Wenden Sie zum Deaktivieren oder Aktivieren der lokalen Konsole das folgende Verfahren an:

1. Öffnen Sie auf Ihrer Verwaltungsstation einen unterstützten Webbrowser, und melden Sie sich am iDRAC an. Weitere Informationen finden Sie unter Zugriff auf die Webschnittstelle.
2. Klicken Sie auf **System**, dann auf das Register **Konsole** und dann auf **Konfiguration**.
3. Wenn auf dem Server lokales Video deaktiviert (ausgeschaltet) werden soll, wählen Sie auf der Seite **Konsolenumleitungskonfiguration** das Kontrollkästchen **Lokale Konsole deaktivieren** aus, und klicken Sie dann auf **Anwenden**. Der Standardwert lautet **AUS**.
4. Wenn auf dem Server lokales Video aktiviert (eingeschaltet) werden soll, wählen Sie auf der Seite **Konsolenumleitungskonfiguration** das Kontrollkästchen **Lokale Konsole deaktivieren** ab, und klicken Sie dann auf **Anwenden**.

Die Seite **Konsolenumleitung** zeigt den Status des lokalen Servervideos an.

Häufig gestellte Fragen

Tabelle 8-7 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 8-7. Konsolenumleitung verwenden: Häufig gestellte Fragen

Frage	Antwort

Kann eine neue Remote-Konsolen-Videositzung gestartet werden, wenn das lokale Video auf dem Server ausgeschaltet ist?	Ja.
Warum dauert es 15 Sekunden, um das lokale Video auf dem Server auszuschalten, nachdem eine Aufforderung zum Ausschalten des lokalen Vidoes erteilt wurde?	Hierdurch wird einem lokalen Benutzer die Gelegenheit gegeben, Maßnahmen durchzuführen, bevor das Video ausgeschaltet wird.
Gibt es beim Einschalten des lokalen Videos eine Zeitverzögerung?	Nein. Sobald der iDRAC eine Aufforderung zum **EIN**schalten des lokalen Videos erhält, wird das Video sofort eingeschaltet.
Kann der lokale Benutzer das Video auch ausschalten?	Ja, ein lokaler Benutzer kann die lokale RACADM-CLI verwenden, um das VIdeo auszuschalten.
Kann der lokale Benutzer das Video auch einschalten?	Nein Wenn die lokale Konsole deaktiviert ist, sind auch die Tastatur und die Maus des lokalen Benutzers deaktiviert und Einstellungsänderungen sind nicht möglich.
Werden beim Ausschalten des lokalen Videos auch die lokale Tastatur und Maus ausgeschaltet?	Ja.
Wird durch das Ausschalten der lokalen Konsole auch das Video der Remote-Konsolensitzung ausgeschaltet?	Nein, das Ein- oder Ausschalten des lokalen Videos ist unabhängig von der Remote-Konsolensitzung.
Welche Berechtigungen sind für einen iDRAC-Benutzer erforderlich, um das lokale Server-Video ein- oder auszuschalten?	Jeder Benutzer mit iDRAC-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 iDRAC-Webschnittstelle angezeigt. Der RACADM-CLI-Befehl **racadm getconfig -g cfgRacTuning** zeigt den Status im Objekt **cfgRacTuneLocalServerVideo** an. Der Status wird auch auf der iKVM-OSCAR-Anzeige sichtbar. Wenn die lokale Konsole aktiviert ist, erscheint neben dem Servernamen eine grüne Statusanzeige. Wenn sie deaktiviert ist, weist ein gelber Punkt darauf hin, dass die lokale Konsole vom iDRAC gesperrt ist.
Ich kann vom Konsolenumleitungsfenster aus den unteren Teil des Systembildschirms nicht sehen.	Stellen Sie sicher, dass die Bildschirmauflösung der Management Station auf 1280 x 1024 eingestellt ist.
Das Konsolenfenster ist entstellt.	Für den Konsolen-Viewer auf Linux ist ein UTF-8-Zeichensatz erforderlich. Überprüfen Sie Ihr Gebietsschema und setzen Sie den Zeichensatz ggf. zurück. Weitere Informationen finden Sie unter Gebietsschema in Linux einstellen.
Warum wird auf dem verwalteten Server ein leerer Bildschirm eingeblendet, wenn das Windows 2000-Betriebssystem lädt?	Auf dem verwalteten Server befindet sich nicht der richtige ATI-Videotreiber. Es ist erforderlich, den Videotreiber unter Verwendung der CD *Dell PowerEdge Installation and Server Management* zu aktualisieren.
Warum synchronisiert die Maus nicht in DOS, wenn die Konsolenumleitung ausgeführt wird?	Das Dell-BIOS emuliert den Maustreiber als PS/2-Maus. Die PS/2-Maus ist so konzipiert, dass sie die Relativposition für den Mauszeiger verwendet, was die Verzögerung in der Synchronisation verursacht. Der iDRAC enthält einen USB-Maustreiber, der eine absolute Position und ein genaueres Verfolgen des Mauszeigers ermöglicht. Selbst wenn der iDRAC die absolute USB-Mausposition auf das Dell-BIOS überträgt, würde die BIOS-Emulation sie auf die relative Position zurücksetzen, und das Verhalten würde unverändert bleiben. Um dieses Problem zu beheben, stellen Sie in der Konsolenumleitungskonfiguration den Mausmodus auf **KEINE** ein.
Warum synchronisiert die Maus nicht unter der Linux-Textkonsole?	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 Maussynchronisation.	Stellen Sie sicher, dass vor dem Beginn einer Konsolenumleitungssitzung die richtige Maus für das Betriebssystem ausgewählt ist. Stellen Sie sicher, dass im **Maus**-Menü **Maus synchronisieren** markiert ist. Drücken Sie auf <Alt><M>, oder wählen Sie **Maus**→ **Maus synchronisieren** aus, um die Maussynchronisation umzuschalten. Wenn die Synchronisation aktiviert wird, wird neben der Auswahl im **Maus**-Menü ein Häkchen eingeblendet.
Warum kann ich keine Tastatur oder Maus verwenden, während ich ein Microsoft®-Betriebssystem mithilfe einer iDRAC-Konsolenumleitung im Remote-Zugriff installiere?	Wenn Sie im Remote-Zugriff auf 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?	Wenn über den iDRAC auf die Num-Taste zugegriffen wird, stimmt die Num-Taste auf der Verwaltungsstation 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 Sie beide Kontrolle über das System.
Welche Bandbreite benötige ich, um eine Konsolenumleitungssitzung auszuführen?	Zum Erzielen einer guten Leistung empfiehlt Dell eine 5 MB/s-Verbindung. Eine 1 MB/s-Verbindung ist zum Erzielen der Mindestleistung vorgeschrieben.
Was sind die Mindestsystemanforderungen für meine Management Station zum Ausführen der Konsolenumleitung?	Die Verwaltungsstation erfordert einen Intel Pentium III 500-MHz-Prozessor mit mindestens 256 MB RAM.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

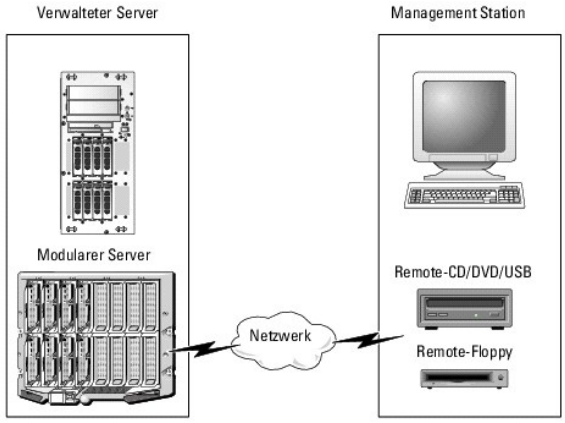
Virtuellen Datenträger konfigurieren und verwenden

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

Übersicht

Die Funktion **Virtueller Datenträger**, auf die über den Konsolenumleitungs-Viewer zugegriffen werden kann, bietet dem verwalteten Server Zugriff auf Datenträger, die mit einem Remote-System auf dem Netzwerk verbunden sind. Abbildung 9-1 zeigt die gesamte Architektur des **virtuellen Datenträgers**.

Abbildung 9-1. 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 Disketten-Laufwerken installieren.

ANMERKUNG: Virtuelle Datenträger erfordern eine minimale verfügbare Netzwerkbandbreite von 128 kbps.

Virtueller Datenträger definiert zwei Geräte für das Betriebssystem und das BIOS des verwalteten Servers: ein Diskettenlaufwerk und ein optisches Festplattenlaufwerk.

Die Management Station liefert die physischen Datenträger oder Bilddatei über das Netzwerk. Wenn eine Verbindung zum **virtuellen Datenträger** hergestellt wirdt, werden alle Zugriffs-Anforderungen der Verwaltungsstation auf das virtuelle CD-/Disketten-Laufwerk über das Netzwerk an die Verwaltungsstation geleitet. Das Verbinden des **virtuellen Datenträgers** scheint identisch mit dem Einsetzen von Datenträgern in physische Geräte zu sein. Wenn keine Verbindung zum virtuellen Datenträger hergestellt ist, verhalten sich virtuelle Geräte auf dem verwalteten Server wie zwei Laufwerke ohne Datenträger.

Tabelle 9-1 führt die unterstützten Laufwerkverbindungen für virtuelle Floppy-Laufwerke und virtuelle optische Laufwerke auf.

ANMERKUNG: Werden **virtuelle Datenträger** geändert, während sie verbunden sind, kann dies die System-Startsequenz anhalten.

Tabelle 9-1. Unterstützte Laufwerkverbindungen

Unterstützte Verbindungen virtueller Floppy-Laufwerke	Unterstützte Verbindungen virtueller optischer Laufwerke
Legacy 1,44 Zoll-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-Image-Datei im Format ISO9660
1,44 Zoll-Floppy-Abbild	USB-CD-ROM-Laufwerk mit CD-ROM-Datenträger
USB-Wechselplatte	

Windows-basierte Management Station

Um die Funktion des **virtuellen Datenträgers** auf einer Verwaltungsstation mit dem Betriebssystem Microsoft® Windows® auszuführen, installieren Sie eine unterstützte Internet Explorer-Version mit dem ActiveX-Steuerungs-Plugin (siehe Unterstützte Webbrowser). Stellen Sie die Browser-Sicherheit auf **Mittel** oder auf eine niedrigere Einstellung ein, damit Internet Explorer signierte ActiveX-Steuerungen herunterladen und installieren kann.

Abhängig von Ihrer Internet Explorer-Version ist eventuell eine benutzerdefinierte Sicherheitseinstellung für ActiveX erforderlich:

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf **Extras**→ **Internetoptionen** und dann auf die Registerkarte **Sicherheit**.
3. Klicken Sie unter **Wählen Sie eine Webinhaltszone, um deren Sicherheitseinstellungen festzulegen**, um die gewünschte Zone auszuwählen.
4. Klicken Sie dann unter **Sicherheitsstufe dieser Zone** auf **Stufe anpassen**.

   Das Fenster **Sicherheitseinstellungen** wird angezeigt.
5. Stellen Sie unter **ActiveX-Steuerelemente und Plugins** sicher, dass die folgenden Einstellungen auf **Aktivieren** eingestellt sind.
   - Scriptlets erlauben
   - Automatische Eingabeaufforderung für ActiveX-Steuerelemente
   - Download von signierten ActiveX-Steuerelementen
   - Download von unsignierten ActiveX-Steuerelementen
6. Klicken Sie auf **OK**, um die Änderungen zu speichern, und schließen Sie das Fenster **Sicherheitseinstellungen**.
7. Klicken Sie auf **OK**, um das Fenster **Internetoptionen** zu schließen.
8. Starten Sie den Internet Explorer neu.

Zum Installieren von ActiveX müssen Sie über Administratorrechte verfügen. Vor der Installation der ActiveX-Steuerung zeigt Internet Explorer eventuell eine Sicherheitswarnung an. Um das Installationsverfahren für ActiveX Control abzuschließen, akzeptieren Sie die ActiveX Control, wenn Internet Explorer Sie mit einer Sicherheitswarnung dazu auffordert.

Linux-basierte Management Station

Um die Funktion des virtuellen Datenträgers auf einer Verwaltungsstation mit Linux-Betriebssystem auszuführen, installieren Sie eine unterstützte Version von Firefox. Weitere Informationen finden Sie unter Unterstützte Webbrowser.

Zum Ausführen des Konsolenumleitungs-Plugin ist eine Java-Laufzeitumgebung (JRE) erforderlich. Sie können eine JRE von **java.sun.com** herunterladen. JRE-Version 1.6 oder höher wird empfohlen.

Virtuellen Datenträger konfigurieren

1. Melden Sie sich bei der iDRAC-Webschnittstelle an.
2. Wählen Sie in der Navigationsstruktur **System** aus und klicken Sie auf das Register **Konsole**.
3. Klicken Sie auf **Konfiguration**→ **Virtueller Datenträger**, um die Einstellungen des virtuellen Datenträgers zu konfigurieren.

   Tabelle 9-2 beschreibt die Konfigurationswerte des **virtuellen Datenträgers**.
4. Wenn Sie mit den Einstellungen fertig sind, klicken Sie auf **Anwenden**.
5. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 9-3.

Tabelle 9-2. Konfigurationswerte des virtuellen Datenträgers

Attribut	Wert
Virtuellen Datenträger anschließen	**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 am Server an, wenn eine Sitzung des virtuellen Datenträgers gestartet wird.
Maximale Sitzungen	Zeigt die maximale Anzahl zulässiger **Virtueller Datenträger**-Sitzungen an. Diese beträgt immer 1.
Aktive Sitzungen	Zeigt die aktuelle Anzahl von Sitzungen des virtuellen Datenträgers an.
Virtueller Datenträger-Verschlüsselung aktiviert	Klicken Sie auf das Kontrollkästchen, um die Verschlüsselung auf Verbindungen des **Virtuellen Datenträgers** zu aktivieren oder zu deaktivieren. Markieren aktiviert die Verschlüsselung; das Aufheben der Markierung deaktiviert die Verschlüsselung.
Anschlussnummer des virtuellen Datenträgers	Die Netzwerkanschlussnummer, die zur Verbindung mit dem Dienst des **virtuellen Datenträgers** ohne Verschlüsselung verwendet wird. Zwei hintereinander liegende Anschlüsse, beginnend mit der festgelegten Anschlussnummer, werden zur

	Verbindung mit dem Dienst **Virtueller Datenträger** verwendet. Die Anschlussnummer, die dem festgelegten Anschluss folgt, darf für keinen anderen iDRAC-Dienst konfiguriert werden. Die Standardeinstellung ist **3668**.
SSL-Anschlussnummer des virtuellen Datenträgers	Die Netzwerkanschlussnummer, die für verschlüsselte Verbindungen zum **Virtueller Datenträger**-Dienst verwendet wird. Zwei hintereinander liegende Anschlüsse, beginnend mit der festgelegten Anschlussnummer, werden zur Verbindung mit dem Dienst **Virtueller Datenträger** verwendet. Die Anschlussnummer, die dem festgelegten Anschluss folgt, darf für keinen anderen iDRAC-Dienst konfiguriert werden. Die Standardeinstellung ist **3670**.
Diskettenemulation	Zeigt an, ob der **virtuelle Datenträger** dem Server als Diskettenlaufwerk oder USB-Schlüssel angezeigt wird. Wenn **Diskettenemulation** markiert ist, wird das **virtuelle Datenträger**-Gerät auf dem Server als Diskettengerät angezeigt. Wenn es nicht ausgewählt ist, wird es als USB-Schlüssellaufwerk angezeigt.
Einmal Starten aktivieren	Wählen Sie dieses Kästchen aus, um die Option Einmal Starten zu aktivieren. Diese Option beendet die Sitzung des **Virtuellen Datenträgers** automatisch, nachdem der Server einmal gestartet wurde. Diese Option ist nützlich für automatische Bereitstellungen.

Tabelle 9-3. Schaltflächen der Konfigurationsseite des virtuellen Datenträgers

Schaltfläche	Beschreibung
Drucken	Druckt die Werte der **Konsolenkonfiguration** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Konsolenkonfiguration** erneut.
Anwenden	Speichert alle neuen Einstellungen, die auf der Seite **Konsolenkonfiguration** vorgenommen wurden.

Virtuellen Datenträger ausführen

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

HINWEIS: Die Anwendung des Konsolen-Viewer-Fensters muss während des Zugriffs auf den virtuellen Datenträger aktiv bleiben.

1. Öffnen Sie einen unterstützten Internet-Browser auf der Management Station. Siehe Unterstützte Webbrowser.

2. Starten Sie die iDRAC-Webschnittstelle. Zugriff auf die Webschnittstelle.

3. Wählen Sie in der Navigationsstruktur **System** aus und klicken Sie auf das Register **Konsole**.

   Die Seite **Konsolenumleitung** wird eingeblendet. Wenn Sie die Werte angezeigter Attribute ändern möchten, finden Sie entsprechende Informationen unter Virtuellen Datenträger konfigurieren.

   ANMERKUNG: Die **Floppy-Abbilddatei** unter **Floppy-Laufwerk** (falls zutreffend) kann angezeigt werden, da diese Komponente als virtuelle Floppy virtualisiert werden kann. Sie können ein optisches Laufwerk und eine Floppy gleichzeitig oder ein einzelnes Laufwerk auswählen.

   ANMERKUNG: Die Laufwerksbuchstaben des virtuellen Geräts auf dem verwalteten Server entsprechen nicht den Buchstaben des physischen Laufwerks auf der Management Station.

   ANMERKUNG: Der **virtuelle Datenträger** funktioniert eventuell nicht ordnungsgemäß auf Clients des Windows-Betriebssystems, die mit Internet Explorer Enhanced Security konfiguriert wurden. Um dieses Problem zu lösen, ziehen Sie die Dokumentation zu Ihrem Microsoft-Betriebssystem zurate oder setzen sich mit Ihrem Administrator in Verbindung.

4. Klicken Sie auf **Viewer starten**.

   ANMERKUNG: Bei Linux wird die Datei **jviewer.jnlp** auf den Desktop heruntergeladen und in einem ein Dialogfeld wird gefragt, welche Maßnahme auf die Datei angewendet werden soll. Wählen Sie die Option **Mit Programm öffnen** aus und dann die Anwendung **javaws**, die sich im Unterverzeichnis **bin** des JRE-Installationsverzeichnisses befindet.

   Die Anwendung **iDRACView** wird in einem separaten Fenster gestartet.

5. Klicken Sie auf **Datenträger→ Assistent des virtuellen Datenträgers...**.

   Der Assistent zur Datenträgerumleitung wird eingeblendet.

6. Zeigen Sie das Statusfenster an. Wenn eine Datenträgerverbindung besteht, muss diese vor dem Verbinden mit einer anderen Datenträgerquelle zuerst unterbrochen werden. Klicken Sie auf die Schaltfläche **Trennen**, die sich rechts neben dem Datenträger befindet, dessen Verbindung Sie unterbrechen möchten.

7. Wählen Sie die Optionsschaltfläche neben den Datenträgertypen aus, zu denen eine Verbindung hergestellt werden soll.

   Sie können eine Optionsschaltfläche im Abschnitt **Disketten-/USB-Laufwerk** und eine im Abschnitt **CD-/DVD-Laufwerk** auswählen.

   Wenn Sie eine Verbindung zu einem Disketten-Image oder einem ISO-Image herstellen möchten, geben Sie (auf Ihrem lokalen Computer) den Pfad zum Image ein, oder klicken Sie auf die Schaltfläche **Durchsuchen**, um zum Image zu browsen.

8. Klicken Sie **neben jedem ausgewählten Datenträgertyp auf die Schaltfläche Verbinden.**

   Die Verbindung zum Datenträger wird hergestellt und das Statusfenster aktualisiert.

9. Klicken Sie auf die **Schaltfläche Schließen.**

Verbindung des virtuellen Datenträgers unterbrechen

1. Klicken Sie auf **Datenträger→ Virtueller Datenträger-Assistent...**.
2. Klicken Sie neben dem Datenträger, dessen Verbindung unterbrochen werden soll, auf **Trennen**.

   Die Verbindung zum Datenträger wird unterbrochen und das Statusfenster aktualisiert.
3. Klicken Sie auf **Schließen**.

Starten vom virtuellen Datenträger

Das System-BIOS ermöglicht Ihnen, von virtuellen optischen Laufwerken oder virtuellen Diskettenlaufwerken 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 werden.

Um die BIOS-Einstellung zu ändern, führen Sie die folgenden Schritte aus:

1. Starten Sie den verwalteten Server.
2. Drücken Sie auf <F2>, um das BIOS-Setup-Fenster aufzurufen.
3. Rollen Sie zur Startsequenz und drücken Sie auf die Eingabetaste.

   Im Popup-Fenster werden die virtuellen optischen Laufwerke und virtuellen Floppy-Laufwerke mit den Standardstartkomponenten aufgeführt.
4. Stellen Sie sicher, dass das virtuelle Laufwerk aktiviert und als erste Komponente mit startfähigem Datenträger aufgeführt 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 wird und startfähige Datenträger vorhanden sind, startet das System zum virtuellen Gerät. Ansonsten ignoriert das System die Komponente - ähnlich wie einer physischen Komponente ohne startfähigen Datenträger.

Installation von Betriebssystemen mittels virtueller Datenträger

In diesem Abschnitt wird eine manuelle, interaktive Methode zum Installieren des Betriebssystems auf der Management Station beschrieben, die mehrere Stunden in Anspruch nehmen kann. 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, die im Abschnitt "Starten vom virtuellen Datenträger" enthalten sind, um sicherzustellen, dass das BIOS so eingestellt ist, dass es von dem CD- Laufwerk aus startet, von dem aus Sie die Installation vornehmen.
3. Folgen Sie den Bildschirmanleitungen, um die Installation abzuschließen.

Virtuelle Datenträger verwenden, wenn das Betriebssystem des Servers ausgeführt wird

Windows-basierte Systeme

Auf Windows-Systemen werden die Laufwerke der virtuellen Datenträger automatisch geladen, wenn sie angeschlossen und mit einem Laufwerkbuchstaben konfiguriert werden.

Die Verwendung der virtuellen Laufwerke innerhalb Windows ist der Verwendung der physischen Laufwerke ähnlich. Wenn Sie über den Assistenten des virtuellen Datenträgers eine Verbindung zum Datenträger herstellen, ist der Datenträger am System verfügbar, wenn Sie auf das Laufwerk klicken und dessen

Inhalt durchsuchen.

Linux-basierte Systeme

Abhängig von der Konfiguration der Software auf Ihrem System dürfen die virtuellen Datenträgerlaufwerke nicht automatisch geladen werden. Wenn Ihre Laufwerke nicht automatisch geladen werden, laden Sie sie unter Verwendung des Linux-Befehls **Laden** manuell.

Häufig gestellte Fragen

Tabelle 9-4 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 9-4. Virtuelle Datenträger verwenden: Häufig gestellte Fragen

Frage	Antwort
Manchmal bemerke ich, dass die Client-Verbindung meines virtuellen Datenträgers unterbrochen wird. Warum ist das so?	Wenn eine Netzwerk-Zeitüberschreitung eintritt, trennt die iDRAC-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Wenn die Konfigurationseinstellungen des virtuellen Datenträgers in der iDRAC-Webschnittstelle oder durch Befehle des lokalen RACADM geändert werden, wird die Verbindung aller verbundener Datenträger bei Übernahme der Konfigurationsänderung unterbrochen. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie den Virtueller Datenträger-Assistenten.
Welche Betriebssysteme unterstützen den iDRAC?	Eine Liste unterstützter Betriebssysteme finden Sie unter Unterstützte Betriebssysteme.
Welche Webbrowser unterstützen den iDRAC?	Eine Liste unterstützter Webbrowser finden Sie unter Unterstützte Webbrowser.
Warum bricht meine Client-Verbindung manchmal ab?	• Ihre Client-Verbindung kann manchmal abbrechen, 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 verloren gehen, wenn das Client-System zu viel Zeit in Anspruch nimmt, bevor es 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, trennt die iDRAC-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Es ist auch möglich, dass jemand die Konfigurationseinstellungen des virtuellen Datenträgers in der Webschnittstelle oder durch Eingabe von RADACM-Befehlen verändert hat. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie die Funktion **Virtueller Datenträger**.
Eine Installation des Windows-Betriebssystems scheint zu lange zu dauern. Warum ist das so?	Wenn Sie das Windows-Betriebssystem über die CD *Dell PowerEdge Installation and Server Management* und über eine langsame Netzwerkverbindung installieren, ist für das Installationsverfahren auf Grund der Netzwerklatenzzeit eventuell ein höherer Zeitaufwand erforderlich, um auf die iDRAC-Webschnittstelle zuzugreifen. Obwohl das Installationsfenster den Installationsfortschritt nicht anzeigt, wird das Installationsverfahren dennoch durchgeführt.
Ich sehe den Inhalt eines Floppy-Laufwerks oder eines USB-Speicherschlüssels an. Wenn ich versuche, über das gleiche Laufwerk eine Verbindung zum virtuellen Datenträger herzustellen, erhalte ich eine Verbindungs-Fehlermeldung und werde gebeten, den Vorgang zu wiederholen. Warum ist das so?	Ein gleichzeitiger Zugriff auf virtuelle Floppy-Laufwerke ist nicht zulässig. Vor dem Versuch, das Laufwerk zu virtualisieren, ist die Anwendung zum Anzeigen des Laufwerkinhalts zu schließen.
Wie konfiguriere ich meine virtuelle Komponente als startfähige Komponente?	Greifen Sie auf dem verwalteten Server auf das BIOS-Setup zu und wechseln Sie zum Startmenü. Machen Sie die virtuelle CD, die virtuelle Floppy oder den Virtual Flash ausfindig und ändern Sie die Komponenten-Startreihenfolge wie erforderlich. 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 iDRAC können Sie von den folgenden startfähigen Datenträgern aus starten: • CDROM/DVD-Datenträger • ISO 9660-Abbild • 1,44 Zoll-Diskette oder Floppy-Abbild • USB-Schlüssel, der vom Betriebssystem als Wechselplatte erkannt wird • Ein USB-Schlüsselabbild
Wie kann ich meinen USB-Schlüssel startfähig machen?	Suchen Sie unter **support.dell.com** nach dem Dell-Startdienstprogramm, einem Windows-Programm, mit dem Sie den Dell-USB-Schlüssel startfähig machen können. Sie können auch über eine Windows 98-Startdiskette starten und Systemdateien von der Startdiskette auf Ihren 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. Sie können auch das Startdienstprogramm von Dell verwenden, um einen startfähigen USB-Schlüssel zu erstellen. Dieses Dienstprogramm ist nur mit USB-Schlüsseln der Marke Dell kompatibel. Um das Dienstprogramm herunterzuladen, öffnen Sie einen Webbrowser, wechseln Sie zu Dells Support-Website unter **support.dell.com** und suchen Sie nach der Datei R122672.exe.
Ich kann mein virtuelles Floppy-Gerät auf einem	Bei einigen Linux-Versionen erfolgt die automatische Ladung des virtuellen Floppy-Laufwerks und des

System, das Red Hat® Enterprise Linux® oder SUSE® Linux ausführt, nicht finden. Mein virtueller Datenträger ist angeschlossen und ich bin mit meiner Remote-Floppy verbunden. Was soll ich tun?	virtuellen CD-Laufwerks auf unterschiedliche Weise. 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 Floppy-Laufwerk 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 gemeldet wurde. 4. Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls und finden Sie den Gerätenamen, der der virtuellen Dell-Diskette gegeben wurde. 5. Stellen Sie sicher, dass das virtuelle Floppy-Laufwerk angeschlossen ist und dass 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 ausfindig gemachte Name der Komponente ist. /mnt/floppy ist der Bereitstellungspunkt.
Welche Dateisystemtypen werden auf meinem virtuellen Diskettenlaufwerk unterstützt?	Ihr virtuelles Diskettenlaufwerk unterstützt FAT16- oder FAT32-Dateisysteme.
Als ich im Remote-Zugriff anhand der iDRAC-Webschnittstelle eine Firmware-Aktualisierung ausgeführt habe, wurden meine virtuellen Laufwerke vom Server entfernt. Warum ist das so?	Firmware-Aktualisierungen führen zu einem Reset des iDRAC, einem Abbruch der Remote-Verbindung sowie zum Entladen der virtuellen Laufwerke. Die Laufwerke erscheinen wieder, wenn der iDRAC-Reset abgeschlossen ist.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Befehlszeilenoberfläche des lokalen RACADM verwenden

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

Die Befehlszeilenoberfläche (CLI) des lokalen RACADM bietet Zugriff auf die iDRAC-Verwaltungsfunktionen vom verwalteten Server aus. RACADM bietet Zugriff auf dieselben Funktionen wie die iDRAC-Webschnittstelle. RACADM kann jedoch in Skripts verwendet werden, um die Konfiguration mehrfacher Server und iDRACs zu erleichtern, bei denen die Webschnittstelle nützlicher für die interaktive Verwaltung ist.

Befehle des lokalen RACADM verwenden zum Zugriff auf den iDRAC vom verwalteten Server aus keine Netzwerkverbindungen. Dies bedeutet, dass Sie Befehle des lokalen RACADM verwenden können, um den anfänglichen iDRAC-Netzwerkbetrieb zu konfigurieren.

Weitere Informationen zur gleichzeitigen Konfiguration mehrerer iDRACs finden Sie unter Mehrere iDRACs gleichzeitigkonfigurieren.

Dieser Abschnitt enthält die folgenden Informationen:

- RACADM von einer Eingabeaufforderung aus verwenden
- iDRAC mit dem Befehl **racadm** konfigurieren
- RACADM-Konfigurationsdatei zur Konfiguration mehrerer iDRACs verwenden

---

RACADM-Befehl verwenden

RACADM-Befehle werden lokal (auf dem verwalteten Server) über eine Befehlseingabeaufforderung oder eine Shell-Eingabeaufforderung ausgeführt.

Melden Sie sich am verwalteten Server an, starten Sie eine Befehlsshell und geben Sie Befehle des lokalen RACADM im folgenden Format ein:

```
racadm <Unterbefehl> -g <Gruppe> -o <Objekt> <Wert>
```

Ohne Optionen zeigt der Befehl RACADM Informationen zum allgemeinen Gebrauch an. Geben Sie zur Anzeige des RACADM-Unterbefehls Folgendes ein:

```
r Acadm-Hilfe
```

Die Liste der Unterbefehle enthält alle Befehle, die durch den iDRAC unterstützt werden.

Um für einen Unterbefehl Hilfe zu erhalten, geben Sie Folgendes ein:

```
racadm help-<Unterbefehl>
```

Der Befehl zeigt die Syntax- und Befehlszeilenoptionen für den Unterbefehl an.

RACADM-Unterbefehle

Tabelle 10-1 enthält eine Beschreibung der einzelnen RACADM-Unterbefehle, die Sie in RACADM ausführen können. Eine ausführliche Auflistung von RACADM-Unterbefehlen einschließlich der Syntax und gültiger Einträge finden Sie unter Übersicht der RACADM-Unterbefehle.

Tabelle 10-1. RACADM-Unterbefehle

Befehl	Beschreibung
clrraclog	Löscht das iDRAC-Protokoll. Nach dem Löschvorgang wird ein einzelner Eintrag vorgenommen, um den Benutzer anzuzeigen sowie die Uhrzeit, zu der das Protokoll gelöscht wurde.
clrsel	Löscht die Einträge des Systemereignisprotokolls des verwalteten Servers.
config	Konfiguriert den iDRAC.
getconfig	Zeigt die aktuellen iDRAC-Konfigurationseigenschaften an.
getniccfg	Zeigt die derzeitige IP-Konfiguration für den Controller an.
getraclog	Zeigt das iDRAC-Protokoll an.
getractime	Zeigt die iDRAC-Zeit an.
getssninfo	Zeigt Informationen über aktive Sitzungen an
getsvctag	Zeigt Service-Tag-Nummern an.
getsysinfo	Zeigt Informationen zu iDRAC und verwaltetem Server, einschließlich IP-Konfiguration, Hardwaremodell, Firmware-Versionen und Betriebssystem an.
gettracelog	Zeigt das Ablaufverfolgungsprotokoll des iDRAC an. Bei Verwendung mit -i zeigt der Befehl die Anzahl von Einträgen im iDRAC-

	Ablaufverfolgungsprotokoll an.
Hilfe	Führt iDRAC-Unterbefehle auf.
Hilfe - *<Unterbefehl>*	Listet die Verwendungsaussage für den angegebenen Unterbefehl auf.
racreset	Setzt den iDRAC zurück.
racresetcfg	Setzt den iDRAC auf die Standardkonfiguration zurück.
serveraction	Führt Stromverwaltungsvorgänge auf dem verwalteten Server aus.
setniccfg	Stellt die IP-Konfiguration für den Controller ein.
sslcertdownload	Lädt ein CA-Zertifikat herunter.
sslcertupload	Lädt ein Zertifizierungsstellenzertifikat oder Serverzertifikat zum iDRAC hoch.
sslcertview	Zeigt ein Zertifizierungsstellenzertifikat oder Serverzertifikat im iDRAC an.
sslcsrgen	Erstellt die SSL-CSR und lädt sie herunter.
testemail	Zwingt den iDRAC, eine E-Mail über den iDRAC zu senden.
testtrap	Zwingt den iDRAC, eine SNMP-Warnung über die iDRAC-NIC zu senden.

RACADM-Dienstprogramm zum Konfigurieren des iDRAC verwenden

In diesem Abschnitt wird beschrieben, wie RACADM zum Ausführen verschiedener iDRAC-Konfigurations-Tasks verwendet wird.

Aktuelle iDRAC-Einstellungen anzeigen

Der RACADM-Unterbefehl **getconfig** ruft aktuelle Konfigurationseinstellungen vom iDRAC ab. Die Konfigurationswerte werden in *Gruppen* organisiert, die ein oder mehrere *Objekt(e)* enthalten, wobei die Objekte *Werte* haben.

Eine vollständige Beschreibung der Gruppen und Objekte finden Sie unter Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank.

Geben Sie zum Anzeigen einer Liste aller iDRAC-Gruppen den folgenden Befehl ein:

```
racadm getconfig -h
```

Geben Sie zum Anzeigen der Objekte und Werte für eine bestimmte Gruppe den folgenden Befehl ein:

```
racadm getconfig -g <Gruppe>
```

Beispiel: Um eine Liste aller **cfgLanNetworking**-Gruppenobjekteinstellungen anzuzeigen, geben Sie den folgenden Befehl ein:

```
racadm getconfig -g cfgLanNetworking
```

iDRAC-Benutzer mit RACADM verwalten

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

ANMERKUNG: Wenn Sie einen neuen iDRAC konfigurieren oder den Befehl **racadm racresetcfg** ausgeführt haben, ist der einzige aktuelle Benutzer **root** mit dem Kennwort **calvin**.

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

Sie können in der iDRAC-Eigenschaftendatenbank bis zu 15 Benutzer konfigurieren. (Ein 16. Benutzer ist für den IPMI-LAN-Benutzer reserviert.) Überprüfen Sie, ob bereits aktuelle Benutzer vorhanden sind, bevor Sie einen iDRAC-Benutzer manuell aktivieren.

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 bis 16 ein:

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

ANMERKUNG: Sie können auch racadm getconfig -f *<Dateiname>* eingeben und die erstellte Datei *<Dateiname>* anzeigen, die alle Benutzer sowie alle anderen iDRAC-Konfigurationsparameter einschließt.

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

```
# cfgUserAdminIndex=nn

cfgUserAdminUserName=
```

Wenn das Objekt **cfgUserAdminUserName** keinen Wert besitzt, steht diese Indexnummer, die durch das Objekt **cfgUserAdminIndex** angezeigt wird, zur Verfügung. Wenn hinter dem = ein Name erscheint, ist dieser Index diesem Benutzernamen zugewiesen.

iDRAC-Benutzer hinzufügen

Führen Sie zum Hinzufügen eines neuen Benutzers zum iDRAC folgende Schritte aus:

1. Legen Sie den Benutzernamen fest.
2. Legen Sie das Kennwort fest.
3. Stellen Sie die Benutzerberechtigung zum Anmelden am iDRAC ein.
4. Aktivieren Sie den Benutzer.

Beispiel

Das folgende Beispiel beschreibt, wie man dem iDRAC einen neuen Benutzer namens "John" mit dem Kennwort "123456" und Anmeldeberechtigung hinzufügt.

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

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

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

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

Verwenden Sie zum Verifizieren des neuen Benutzers einen der folgenden Befehle:

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 2
```

iDRAC-Benutzer mit Berechtigungen aktivieren

Um einem Benutzer bestimmte administrative (rollenbasierte) Berechtigungen zu erteilen, stellen Sie die Eigenschaft **cfgUserAdminPrivilege** auf eine Bitmaske ein, die aus den unter Tabelle 10-2 gezeigten Werten konstruiert ist:

Tabelle 10-2. Bit-Masken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
Bei iDRAC anmelden	0x0000001
iDRAC konfigurieren	0x0000002
Benutzer konfigurieren	0x0000004
Protokolle löschen	0x0000008
Serversteuerungsbefehle ausführen	0x0000010
Auf die Konsolenumleitung zugreifen	0x0000020
Zugriff auf virtuelle Datenträger	0x0000040
Testwarnungen	0x0000080
Debug-Befehle ausführen	0x0000100

Um dem Benutzer z. B. die Berechtigungen **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen** und **Zugriff auf Konsolenumleitung** zu erteilen, fügen Sie die Werte 0x00000002, 0x00000004, 0x00000008 und 0x00000010 hinzu, um die Bitmap 0x0000002E zu konstruieren. Geben Sie dann den folgenden Befehl zum Einstellen der Berechtigung ein:

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x0000002E
```

iDRAC-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 RAC-Benutzers verwendet werden kann:

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

Eine Null-Kette doppelter Anführungszeichen ("") weist den iDRAC an, die Benutzerkonfiguration am angegebenen Index zu entfernen und die Benutzerkonfiguration auf die ursprünglichen Werkseinstellungen zurückzusetzen.

Testen von E-Mail-Warnmeldungen

Mit der iDRAC-E-Mail-Warnungsfunktion können Benutzer E-Mail-Warnungen erhalten, wenn auf dem verwalteten Server ein kritisches Ereignis auftritt. Das folgende Beispiel zeigt, wie man die E-Mail-Warnungsfunktion testet, um sicherzustellen, dass der iDRAC ordnungsgemäß E-Mail-Warnungen über das Netzwerk senden kann.

```
racadm testemail -i 2
```

ANMERKUNG: Stellen Sie sicher, dass die SMTP- und E-Mail-Warnungseinstellungen konfiguriert sind, bevor Sie die E-Mail-Warnungsfunktion testen. Weitere Informationen finden Sie unter Konfiguration von E-Mail-Warnungen.

iDRAC-SNMP-Trap-Warnungsfunktion testen

Die iDRAC-SNMP-Trap-Warnungsfunktion ermöglicht den SNMP-Trap-Abhörkonfigurationen, Traps für Systemereignisse zu empfangen, die auf dem verwalteten Server auftreten.

Das folgende Beispiel zeigt, wie ein Benutzer die SNMP-Trap-Warnungsfunktion testen kann.

```
racadm testtrap -i 2
```

ANMERKUNG: Stellen Sie vor dem Testen der iDRAC-SNMP-Trap-Warnungsfunktion sicher, dass die SNMP- und Trap-Einstellungen ordnungsgemäß konfiguriert sind. Diese Einstellungen können anhand der Beschreibungen zu den Unterbefehlen **testtrap** und **testemail** konfiguriert werden.

iDRAC-Netzwerkeigenschaften konfigurieren

Geben Sie Folgendes ein, um eine Liste verfügbarer Netzwerkeigenschaften zu erstellen:

```
racadm getconfig -g cfgLanNetworking
```

Wenn DHCP zum Erhalt einer IP-Adresse verwendet werden soll, kann der folgende Befehl zum Schreiben des Objekts **cfgNicUseDhcp** und zum Aktivieren dieser Funktion verwendet werden:

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

Die Befehle enthalten dieselbe Konfigurationsfunktionalität wie das iDRAC-Konfigurationsdienstprogramm, wenn Sie dazu aufgefordert werden, <Strg><E> zu drücken. Weitere Informationen zum Konfigurieren von Netzwerkeigenschaften mit dem iDRAC-Konfigurationshilfsprogramm finden Sie unter LAN.

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 iDRAC-LAN selbst dann deaktiviert, wenn DHCP aktiviert ist.

IPMI konfigurieren

1. Konfigurieren Sie IPMI über LAN, indem Sie folgenden Befehl eingeben:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
   ```

ANMERKUNG: Diese Einstellung bestimmt die IPMI-Befehle, die von der IPMI-über-LAN-Schnittstelle ausgeführt werden können. Weitere Informationen finden Sie in den IPMI 2.0-Angaben.

a. Aktualisieren Sie die IPMI-Kanalberechtigungen, indem Sie folgenden Befehl eingeben:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <Klasse>
```

wobei <*Klasse*> eine der Folgenden ist:

- 2 (**Benutzer**)
- 3 (**Operator**)
- 4 (**Administrator**)

Beispiel: Um die IPMI-LAN-Kanalberechtigung auf 2 (Benutzer) einzustellen, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
```

b. Stellen Sie, falls erforderlich, den Verschlüsselungsschlüssel des IPMI- LAN-Kanals ein, indem Sie einen Befehl wie den folgenden eingeben:

ANMERKUNG: Die iDRAC-IPMI unterstützt das RMCP+-Protokoll. Die IPMI 2.0-Spezifikationen enthalten weitere Informationen.

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <Schlüssel>
```

wobei <*Schlüssel*> ein aus 20 Zeichen bestehender Verschlüsselungsschlüssel in einem gültigen Hexadezimal-Format ist.

2. Konfigurieren Sie IPMI Seriell über LAN (SOL), indem Sie folgenden Befehl verwenden:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

ANMERKUNG: Die IPMI-SOL-Mindestzugriffsstufe bestimmt die Mindestberechtigung, die zum Aktivieren von IPMI SOL erforderlich ist. Weitere Informationen enthält die IPMI 2.0-Spezifikation.

a. Aktualisieren Sie die IPMI-SOL-Mindestberechtigungsebene mit folgendem Befehl:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <Klasse>
```

wobei <*Klasse*> eines von Folgendem darstellt:

- 2 (**Benutzer**)
- 3 (**Operator**)
- 4 (**Administrator**)

Beispiel: Um die IPMI-Berechtigungen für 2 (Benutzer) zu konfigurieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

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

b. Aktualisieren Sie die IPMI-SOL-Baudrate mit folgendem Befehl:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <Baud-Rate>
```

wobei <*Baud-Rate*> 19200, 57600 oder 115200 Bit/s ist.

Zum Beispiel:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. Aktivieren Sie SOL, indem Sie an der Eingabeaufforderung folgenden Befehl eingeben.

ANMERKUNG: SOL kann für jeden einzelnen Benutzer aktiviert oder deaktiviert werden.

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <ID> 2
```

wobei <*ID*> die eindeutige Benutzer-ID ist.

PEF konfigurieren

Sie können die Maßnahme konfigurieren, die iDRAC bei den einzelnen Plattformwarnungen ergreifen soll. Tabelle 10-3 führt die möglichen Maßnahmen sowie den Wert auf, mithilfe derer sie in RACADM identifiziert werden können.

Tabelle 10-3. Plattformereignismaßnahme

Abhilfe	Wert
Keine Maßnahme	0
Stromversorgung aus	1
Neustarten	2
Aus- und einschalten	3

1. Konfigurieren Sie PEF-Maßnahmen mit folgendem Befehl:

   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i <*Index*> <*Maßnahme-Wert*>

   wobei <*Index*> der PEF-Index ist (siehe Tabelle 5-6 und <*Maßnahmenwert*> ein Wert von Tabelle 10-3.

   Um beispielsweise PEF zum Neustarten des Systems und zum Senden einer IPMI-Warnung zu aktivieren, wenn auf dem Prozessor ein kritisches Ereignis festgestellt wird, geben Sie den folgenden Befehl ein:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2
   ```

PET konfigurieren

1. Aktivieren Sie globale Warnungen mit folgendem Befehl:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Aktivieren Sie PET mit folgendem Befehl:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <Index> <0|1>
   ```

   wobei <*Index*> der PET-Zielindex ist und 0 oder 1 PET deaktivieren bzw. PET aktivieren.

   Beispiel: Um PET mit dem Index 4 zu aktivieren, geben Sie den folgenden Befehl ein:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
   ```

3. Konfigurieren Sie Ihre PET-Regel mit folgendem Befehl:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <Index> <IP-Adresse>
   ```

   wobei <*Index*> der PET-Zielindex und <*IP-Adresse*> die Ziel-IP-Adresse des Systems ist, das die Plattformereigniswarnungen empfängt.

4. Konfigurieren Sie die Community-Namenzeichenkette.

   Geben Sie in der Befehlszeile Folgendes ein:

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

   wobei <*Name*> der PET-Community-Name ist.

Konfiguration von E-Mail-Alarmen

1. Aktivieren Sie globale Warnungen mit folgendem Befehl:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Aktivieren Sie E-Mail-Warnungen mit folgendem Befehl:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <Index> <0|1>
   ```

   wobei <*Index*> der E-Mail-Zielindex ist und 0 die E-Mail-Warnung deaktiviert oder 1 den Wert aktiviert. Der E-Mail-Zielindex kann ein Wert von 1 bis 4 sein.

   Beispiel: Um E-Mail mit dem Index 4 zu aktivieren, geben Sie den folgenden Befehl ein:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. Konfigurieren Sie Ihre E-Mail-Einstellungen mit folgendem Befehl:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <E-Mail-Adresse>
   ```

   wobei 1 der E-Mail-Zielindex und <*E-Mail-Adresse*> die Ziel-E-Mail-Adresse ist, die die Plattformereigniswarnungen empfängt.

4. Geben Sie zum Konfigurieren einer benutzerdefinierten Meldung den folgenden Befehl ein:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <Index> <Benutzerdefinierte-Meldung>
   ```

   wobei <*Index*> der E-Mail-Zielindex und <*benutzerdefinierte Meldung*> die benutzerdefinierte Meldung ist.

5. Testen Sie die konfigurierte E-Mail-Warnung, falls gewünscht, mit folgendem Befehl:

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

   wobei <*Index*> der zu testende E-Mail-Zielindex ist.

IP-Filterung konfigurieren (IpBereich)

Die IP-Adressenfilterung (oder *IP-Bereichsüberprüfung*) gestattet den iDRAC-Zugriff nur von Clients oder Verwaltungsstationen, deren IP-Adressen innerhalb eines vom Benutzer angegebenen Bereiches liegen. Alle anderen Anmeldeaufforderungen werden abgewiesen.

Die IP-Filterung vergleicht die IP-Adresse einer eingehenden Anmeldung mit dem IP-Adressenbereich, der in den folgenden **cfgRacTuning**-Eigenschaften angegeben ist:

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

Die Eigenschaft **cfgRacTuneIpRangeMask** wird sowohl auf die eingehende IP-Adresse als auch auf die **cfgRacTuneIpRangeAddr**-Eigenschaften angewendet. Sind die Ergebnisse identisch, wird für die eingehende Anmeldeaufforderung der Zugriff auf den iDRAC zugelassen. Anmeldungen von IP-Adressen außerhalb dieses Bereichs erhalten eine Fehlermeldung.

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

```
cfgRacTuneIpRangeMask & (<eingehende-IP-Adresse> ^ cfgRacTuneIpRangeAddr)
```

wobei & das binäre UND der Mengen und ^ das binäre ausschließliche ODER ist.

Eine vollständige Liste der **cfgRacTuning**-Eigenschaften finden Sie unter cfgRacTuning.

Tabelle 10-4. Eigenschaften der IP-Adressenfilterung (IpRange)

Eigenschaft	Beschreibung
cfgRacTuneIpRangeEnable	Aktiviert die IP-Bereichs-Überprüfungsfunktion.
cfgRacTuneIpRangeAddr	Bestimmt das akzeptable IP-Adressen-Bitmuster, abhängig von den Einsen (1) in der Subnetzmaske. Diese Eigenschaft wird bitweise mit **cfgRacTuneIpRangeMask** "g*eund*et", um den oberen Teil der zugelassenen IP-Adresse zu bestimmen. Die Anmeldung wird für alle IP-Adressen, die dieses Bit-Muster in den oberen Bits aufweisen, zugelassen. Anmeldungen von IP-Adressen, die außerhalb dieses Bereiches stattfinden, schlagen fehl. Für die Standardwerte der einzelnen Eigenschaften ist für die Anmeldung ein Adressenbereich von 192.168.1.0 bis 192.168.1.255 zulässig.
cfgRacTuneIpRangeMask	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Maske muss in der Form einer Netzmaske sein, wobei die bedeutenderen Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu Nullen (0) in den niederwertigeren Bits.

IP-Filterung konfigurieren

Führen Sie zur Konfiguration der IP-Filterung in der Webschnittstelle folgende Schritte aus:

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC**→ **Netzwerk / Sicherheit**.
2. Klicken Sie auf der Seite **Netzwerkkonfiguration** auf **Erweiterte Einstellungen**.
3. Markieren Sie das Kontrollkästchen **IP-Bereich aktiviert** und geben Sie die **IP-Bereichsadresse** und die **IP-Bereichs-Subnetzmaske** ein.
4. Klicken Sie auf **Anwenden**.

Im Folgenden sind Beispiele zur Verwendung des lokalen RACADM zum Einstellen der IP-Filterung aufgeführt.

ANMERKUNG: Unter Befehlszeilenoberfläche des lokalen RACADM verwendenfinden Sie weitere Informationen zu RACADM- und RACADM-Befehlen.

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

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

   racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57
   ```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

2. Zur Beschränkung von Anmeldungen auf einen kleinen Satz von vier angrenzenden IP-Adressen (z. B. 192.168.0.212 bis 192.168.0.215) wählen Sie alle außer den niederwertigsten zwei Bit 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
```

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

Richtlinien zu IP-Filtern

Verwenden Sie die folgenden Richtlinien, wenn Sie den IP-Filter aktivieren:

- Stellen Sie sicher, dass **cfgRacTuneIpRangeMask** in Form einer Netzmaske konfiguriert ist, wobei alle höchstwertigen Bits Einsen (1) sind (was das Subnetz in der Maske definiert), mit einem Übergang zu nur Nullen (0) in den niederwertigeren Bits.
- Verwenden Sie die Basisadresse des gewünschten Bereichs als Wert von **cfgRacTuneIpRangeAddr**. Der binäre 32-Bit-Wert dieser Adresse sollte Nullen in allen niederwertigen Bits haben, wo Nullen in der Maske sind.

IP-Blockierung konfigurieren

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

Die Funktionen der IP-Blockierung schließen ein:

- Die Anzahl zulässiger Anmeldefehlschläge (**cfgRacTuneIpBlkFailcount**)
- Die Zeitspanne in Sekunden, während der diese Fehler auftreten müssen (**cfgRacTuneIpBlkFailWindow**)
- Die Zeitdauer in Sekunden, während der die blockierte IP-Adresse daran gehindert wird, eine Sitzung herzustellen, nachdem die zulässige Anzahl von Fehlern überschritten wurde (**cfgRacTuneIpBlkPenaltyTime**)

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

ANMERKUNG: Wenn Anmeldungsversuche von der Client-IP-Adresse abgelehnt werden, können einige SSH-Clients die folgende Meldung anzeigen: ssh exchange identification: Verbindung vom Remote-Host geschlossen.

Eine vollständige Liste der **cfgRacTune**-Eigenschaften finden Sie unter Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank.

Anmeldungswiederholungs-Beschränkungseigenschaften führt die vom Benutzer definierten Parameter auf.

Tabelle 10-5. Anmeldungswiederholungs-Beschränkungseigenschaften

Eigenschaft	Definition
cfgRacTuneIpBlkEnable	Aktiviert die IP-Blockierungsfunktion. Wenn innerhalb eines bestimmten Zeitraums aufeinander folgende Fehler (**cfgRacTuneIpBlkFailCount**) von einer einzelnen IP-Adresse aus festgestellt werden (**cfgRacTuneIpBlkFailWindow**), werden alle weiteren Versuche, von dieser Adresse aus eine Sitzung herzustellen, während eines bestimmten Zeitraums zurückgewiesen (**cfgRacTuneIpBlkPenaltyTime**).
cfgRacTuneIpBlkFailCount	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche zurückgewiesen werden.
cfgRacTuneIpBlkFailWindow	Die Zeitspanne in Sekunden, während der die fehlgeschlagenen Versuche gezählt werden. Wenn die Fehlversuche diese Grenze überschreiten, werden sie aus dem Zähler gelöscht.
cfgRacTuneIpBlkPenaltyTime	Definiert den Zeitraum in Sekunden, während dessen Anmeldeversuche von einer IP-Adresse aus auf Grund übermäßiger Fehler zurückgewiesen werden.

IP-Blockierung aktivieren

Das folgende Beispiel hindert eine Client-IP-Adresse fünf Minuten lang daran, eine Sitzung zu beginnen, wenn dieser Client innerhalb einer Minute fünf fehlerhafte Anmeldeversuche durchführt.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

Das folgende Beispiel verhindert mehr als drei Fehlversuche innerhalb einer Minute und verhindert eine Stunde lang zusätzliche Anmeldungsversuche.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 360
```

iDRAC-Telnet- und SSH-Dienste mittels lokalem RACADM konfigurieren

Die Telnet-/SSH-Konsole kann lokal (auf dem verwalteten Server) unter Verwendung von RACADM-Befehlen konfiguriert werden.

ANMERKUNG: Um die Befehle in diesem Abschnitt ausführen zu können, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.

ANMERKUNG: Eine Neukonfiguration von Telnet- oder SSH-Einstellungen im iDRAC führt dazu, dass alle aktuellen Sitzungen ohne Warnung beendet werden.

Um Telnet und SSH vom lokalen RACADM zu aktivieren, melden Sie sich am verwalteten Server an und geben Sie auf eine entsprechende Eingabeaufforderung hin die folgenden Befehle ein:

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

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

Ändern Sie zum Deaktivieren des Telnet- oder SSH-Diensts den Wert von `1` zu `0`:

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

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

Geben Sie den folgenden Befehl ein, um die Telnet-Schnittstellennummer auf dem iDRAC zu ändern.

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <neue Anschlussnummer>
```

Geben Sie z. B. zum Ändern der Telnet-Schnittstelle von der Standardeinstellung 22 auf 8022 den folgenden Befehl ein:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

Eine vollständige Liste verfügbarer RACADM-CLI-Befehle finden Sie unter Befehlszeilenoberfläche des lokalen RACADM verwenden.

---

iDRAC-Konfigurationsdatei verwenden

Eine iDRAC-Konfigurationsdatei ist eine Textdatei, die eine Darstellung der Werte in der iDRAC-Datenbank enthält. Der RACADM-Unterbefehl **getconfig** kann zum Erstellen einer Konfigurationsdatei verwendet werden, die die aktuellen Werte des iDRAC enthält. Sie können dann die Datei bearbeiten und den RACADM-Unterbefehl **config -f** zum Zurückladen der Datei in den iDRAC verwenden, oder die Konfiguration auf andere iDRACs kopieren.

iDRAC-Konfigurationsdatei erstellen

Die Konfigurationsdatei ist eine (unformatierte) Textdatei. Es können alle gültigen Dateinamen verwendet werden; die gebräuchliche Dateierweiterung **.cfg** wird empfohlen.

Die Konfigurationsdatei kann:

- Mit einem Textbearbeitungsprogramm erstellt werden
- Über den RACADM-Unterbefehl **getconfig** vom iDRAC abgerufen werden
- Über den RACADM-Unterbefehl **getconfig** vom iDRAC abgerufen und dann bearbeitet werden

Geben Sie zum Abrufen einer Konfigurationsdatei unter Verwendung des RACADM-Befehls **getconfig** den folgenden Befehl an einer Eingabeaufforderung auf dem verwalteten Server ein:

```
racadm getconfig -f myconfig.cfg
```

Anhand dieses Befehls wird die Datei **myconfig.cfg** im aktuellen Verzeichnis erstellt.

Syntax der Konfigurationsdatei

HINWEIS: Bearbeiten Sie die Konfigurationsdatei mit einem Klartext-Bearbeitungsprogramm, z. B. **Notepad** (Windows) oder **vi** (Linux). Das Dienstprogramm **racadm** parst nur ASCII-Text. Formatierung verwirrt den Parser, wodurch die iDRAC-Datenbank beschädigt werden kann.

In diesem Abschnitt wird das Format der Konfigurationsdatei beschrieben.

- Zeilen, die mit einem # beginnen, sind Kommentare.

  Ein Kommentar *muss* in der ersten Spalte der Zeile beginnen. Ein #-Zeichen wird in jeder anderen Spalte als normales #-Zeichen behandelt.

  Beispiel:

  ```
  #

  # Dies ist eine Anmerkung

  [cfgUserAdmin]

  cfgUserAdminPrivilege=4
  ```

- Alle Gruppeneinträge müssen sich zwischen den Zeichen **[** und **]** befinden.

  Das Anfangszeichen **[**, das einen Gruppennamen anzeigt, *muss* in Spalte eins 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)
  ```

- Parameter werden als *Objekt*=*Wert*-Paare ohne Leerzeichen zwischen Objekt, = und Wert angegeben.

  Auf den Wert folgende Leerzeichen werden ignoriert. Ein Leerzeichen innerhalb einer Wertezeichenkette bleibt unverändert. Alle Zeichen rechts neben = werden unverändert übernommen (z. B. ein zweites = oder ein #, *[*, *]* usw.).

- Der Parser ignoriert einen Index-Objekteintrag.

  Benutzer können *nicht* angeben, welcher Index verwendet werden soll. Wenn der Index bereits vorhanden ist, wird dieser entweder verwendet, oder es wird ein neuer Eintrag im ersten verfügbaren Index für diese Gruppe erstellt.

  Der Befehl `racadm getconfig -f <Dateiname>` setzt einen Kommentar vor die Index-Objekte, wodurch ermöglicht wird, die enthaltenen Kommentare zu sehen.

ANMERKUNG: Sie können eine indizierte Gruppe mit folgendem Befehl manuell erstellen:
`racadm config -g <Gruppenname> -o <verankertes-Objekt> -i <Index> <eindeutiger-Ankername>`

- Die Zeile für eine indizierte Gruppe *kann nicht* aus einer Konfigurationsdatei gelöscht werden.

  Benutzer müssen ein indiziertes Objekt manuell mit folgendem Befehl entfernen:

  ```
  racadm config -g <Gruppenname> -o <Objektname> -i <Index> ""
  ```

ANMERKUNG: Eine NULL-Zeichenkette (durch die beiden Zeichen "" gekennzeichnet) weist iDRAC 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>
```

- Bei indizierten Gruppen *muss* der Objektanker das erste Objekt nach dem *[ ]*-Paar sein. Im Folgenden finden Sie Beispiele für aktuelle indizierte Gruppen:

  ```
  [cfgUserAdmin]

  cfgUserAdminUserName=<Benutzername>
  ```

- 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 aus dem iDRAC für diese Gruppe. Alle Objekte innerhalb dieser Gruppe sind einfache Modifizierungen, wenn der iDRAC konfiguriert wird. Wenn ein modifiziertes Objekt einen neuen Index darstellt, wird der Index während der Konfiguration auf dem iDRAC erstellt.

- Es ist nicht möglich, einen gewünschten Index in einer Konfigurationsdatei zu bestimmen.

  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 geändert. Wenn kein Index vorhanden ist, wird der erste verfügbare Index verwendet. Diese Methode sorgt für Flexibilität, wenn indizierte Einträge hinzugefügt werden, wobei der Benutzer keine genauen Index-Übereinstimmungen zwischen allen verwalteten RACs vorzunehmen braucht. Neue Benutzer werden dem ersten verfügbaren Index hinzugefügt. Eine Konfigurationsdatei, die auf einem iDRAC korrekt parst und ausgeführt wird, kann auf einem anderen iDRAC möglicherweise nicht korrekt ausgeführt werden, falls alle Indizes belegt sind und ein neuer Benutzer hinzugefügt werden muss.

iDRAC-IP-Adresse in einer Konfigurationsdatei modifizieren

Wenn Sie die iDRAC-IP-Adresse in der Konfigurationsdatei modifizieren, entfernen Sie alle unnötigen **<***variabel***>**=<*Wert*>-Einträge. Es verbleibt nur die tatsächliche Bezeichnung der variablen Gruppe mit "[" und "]" einschließlich der beiden **<***Variable***>**=<*Wert*>-Einträge, die sich auf die Änderung der IP-Adresse beziehen.

Zum Beispiel:

```
#

# Objektgruppe "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Die Datei wird wie folgt aktualisiert:

```
#

# Objektgruppe "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# Anmerkung, der Rest dieser Zeile wird ignoriert

cfgNicGateway=10.35.9.1
```

Konfigurationsdatei in den iDRAC laden

Der Befehl `racadm config -f <Dateiname>` parst die Konfigurationsdatei, um zu überprüfen, ob gültige Gruppen- und Objektnamen vorhanden sind und Syntaxregeln befolgt werden. Weist die Datei keine Fehler auf, aktualisiert der Befehl die iDRAC-Datenbank mit dem Dateiinhalt.

ANMERKUNG: Wenn Sie nur die Syntax überprüfen, jedoch nicht die iDRAC-Datenbank aktualisieren möchten, fügen Sie dem Unterbefehl **config** die Option **-c** hinzu.

Fehler in der Konfigurationsdatei werden mit der Zeilennummer sowie einer Meldung markiert, die das Problem beschreibt. Bevor die Konfigurationsdatei den iDRAC aktualisieren kann, müssen alle Fehler korrigiert worden sein.

HINWEIS: Verwenden Sie den Unterbefehl **racresetcfg**, um die Datenbank und die iDRAC-NIC-Einstellungen auf die ursprünglichen Standardeinstellungen zurückzusetzen und alle Benutzer und Benutzerkonfigurationen zu entfernen. Während der Stammbenutzer verfügbar ist, werden die Einstellungen anderer Benutzer ebenfalls auf die Standardeinstellungen zurückgesetzt.

Bevor Sie den Befehl `racadm config -f <Dateiname>` ausführen, können Sie den Unterbefehl **racreset** ausführen, um den iDRAC auf seine Standardeinstellungen zurückzusetzen. Stellen Sie sicher, dass die zu ladende Konfigurationsdatei alle gewünschten Objekte, Benutzer, Indizes und anderen Parameter enthält.

Um den iDRAC mit der Konfigurationsdatei zu aktualisieren, führen Sie an der Eingabeaufforderung des verwalteten Servers folgenden Befehl aus:

```
racadm config -f <Dateiname>
```

Nachdem der Befehl abgeschlossen wurde, können Sie den RACADM-Unterbefehl **getconfig** ausführen, um zu bestätigen, dass die Aktualisierung erfolgreich verlaufen ist.

Mehrere iDRACs gleichzeitigkonfigurieren

Anhand einer Konfigurationsdatei können Sie andere iDRACs mit identischen Eigenschaften konfigurieren. Führen Sie zur Konfiguration mehrfacher iDRACs die folgenden Schritte aus:

1. Erstellen Sie die Konfigurationsdatei von dem iDRAC aus, dessen Einstellungen Sie auf den anderen replizieren möchten. Geben Sie an der Eingabeaufforderung des verwalteten Servers folgenden Befehl ein:

   ```
   racadm getconfig -f <Dateiname>
   ```

   wobei <*Dateiname*> der Name einer Datei zum Speichern der iDRAC-Eigenschaften ist, wie z. B. **myconfig.cfg**.

   Weitere Informationen finden Sie unter iDRAC-Konfigurationsdatei erstellen.

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

2. Bearbeiten Sie die im vorherigen Schritt erstellte Konfigurationsdatei und entfernen Sie alle Einstellungen oder kommentieren Sie alle Einstellungen aus, die Sie *nicht* replizieren möchten.

3. Kopieren Sie die bearbeitete Konfigurationsdatei auf ein Netzlaufwerk, auf dem alle verwalteten Server, deren iDRAC konfiguriert werden soll, auf sie zugreifen können.

4. Führen Sie für jeden iDRAC, den Sie konfigurieren möchten, Folgendes aus:

   a. Melden Sie sich am verwalteten Server an und öffnen Sie eine Eingabeaufforderung.

   b. Wenn Sie den iDRAC von den Standardeinstellungen aus neu konfigurieren möchten, geben Sie folgenden Befehl ein:

      ```
      racadm racreset
      ```

   c. Laden Sie die Konfigurationsdatei mit folgendem Befehl in den iDRAC:

      ```
      racadm config -f <Dateiname>
      ```

      wobei <*Dateiname*> der Name der von Ihnen erstellten Konfigurationsdatei ist. Schließen Sie den vollständigen Pfad mit ein, wenn sich die Datei nicht im Arbeitsverzeichnis befindet.

   d. Setzen Sie den konfigurierten iDRAC mit folgendem Befehl zurück:

      ```
      racadm reset
      ```

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC-SM-CLP-Befehlszeilenoberfläche verwenden

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

Dieser Abschnitt enthält Informationen zum SMWG-SM-CLP (Serververwaltungs-Workgroup, Serververwaltungs-Befehlszeilenprotokoll), das im iDRAC integriert ist.

ANMERKUNG: Für diesen Abschnitt wird angenommen, dass Sie mit der SMASH-Initiative (Systemverwaltungsarchitektur für Serverhardware) und den SMWG SM-CLP-Angaben vertraut sind. Weitere Information zu diesen Angaben finden Sie auf der Website zur Distributed Management Task Force (DMTF) unter **www.dmtf.org**.

Das iDRAC-SM-CLP ist ein Protokoll, das von der DMTF und der SMWG betrieben wird, um für Systemverwaltungs-CLI-Umsetzungen Standards zu bieten. Viele Ansätze basieren auf einer definierten SMASH-Architektur, die als Fundament für mehr genormte Systems Management-Komponentensätze dienen soll. Der SMWG SM-CLP ist eine Unterkomponente der gesamten von DMTF verfolgten SMASH-Bemühungen.

SM-CLP enthält einen Teilsatz der Funktionalität, die von der Befehlszeilenoberfläche des lokalen RACADM zur Verfügung gestellt wird, jedoch über einen unterschiedlichen Zugriffspfad. SM-CLP wird innerhalb des iDRAC ausgeführt und RACADM auf dem verwalteten Server. Bei RACADM handelt es sich außerdem um eine Dell-proprietäre Schnittstelle, wobei SM-CLP eine Industriestandardschnittstelle ist. Eine Zuweisung der RACADM- und SM-CLP-Befehle finden Sie unter RACADM- und SM-CLP-Äquivalenzen.

Systemverwaltung mit SM-CLP

Das iDRAC-SM-CLP ermöglicht Ihnen die Verwaltung der folgenden Systemfunktionen über eine Befehlszeile oder ein Skript:

- Serverstromverwaltung - System einschalten, herunterfahren oder neu starten
- Verwaltung des Systemereignisprotokolls (SEL) - SEL-Datensätze anzeigen oder löschen
- iDRAC-Benutzerkontoverwaltung
- Active Directory-Konfiguration
- iDRAC-LAN-Konfiguration
- Erstellung einer SSL-Zertifikatsignaturanforderung (CSR)
- Konfiguration des virtuellen Datenträgers
- SOL-Umleitung (Seriell über LAN) über Telnet oder SSH

---

iDRAC-SM-CLP-Support

SM-CLP wird von der iDRAC-Firmware gehostet und unterstützt Telnet- und SSH-Verbindungen. Die iDRAC-SM-CLP-Schnittstelle basiert auf der SM-CLP-Spezifikation Version 1.0, bereitgestellt von der DMTF-Organisation.

Die folgenden Abschnitte enthalten eine Übersicht der SM-CLP-Funktion, die vom iDRAC gehostet wird.

SM-CLP-Funktionen

Die SM-CLP-Spezifikation enthält einen allgemeinen Satz von SM-CLP-Standardverben, die für das einfache Systems Management über CLI verwendet werden können.

SM-CLP fördert das Konzept von Verben und Zielen, um Systemkonfigurationsfähigkeiten über die CLI bereitzustellen. Das Verb zeigt den auszuführenden Vorgang an und das Ziel bestimmt die Einheit (oder das Objekt), die den Vorgang ausführt.

Im Folgenden wird die Syntax der SM-CLP-Befehlszeile dargestellt:

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

Tabelle 11-1 enthält eine Liste der Verben, die die iDRAC-CLI unterstützt, die Syntax der einzelnen Befehle sowie eine Liste der Optionen, die das Verb unterstützt.

Tabelle 11-1. Unterstützte SM-CLP-CLI-Verben

Verb	Beschreibung	Optionen
CD	Navigiert mithilfe der Shell durch den Adressbereich des verwalteten Systems. Syntax: cd [*Optionen*] [*Ziel*]	-default, -examine, -help, -output, -version
delete	Löscht eine Objektinstanz. Syntax: delete [*Optionen*] *Ziel*	-examine, -help, -output, -version
dump	Bewegt ein Binärbild von MAP zu URI. dump -Ziel <*URI*> [*Optionen*] [*Ziel*]	-destination, -examine, -help, -output, -version
exit	Beendet die SM-CLP-Shell-Sitzung. Syntax: exit [*Optionen*]	-help, -output, -version
Hilfe	Zeigt Hilfe für SM-CLP-Befehle an. help	-examine, -help, -output, -version
load	Bewegt ein Binärbild zu MAP von URI. Syntax: load -source <*URI*> [*Optionen*] [*Ziel*]	-examine, -help, -output, -source, -version
reset	Setzt das Ziel zurück. Syntax: reset [*Optionen*] [*Ziel*]	-examine, -help, -output, -version
set	Stellt die Eigenschaften eines Ziels ein Syntax: set [*Optionen*] [*Ziel*] <*Eigenschaftenname*>=<*Wert*>	-examine, -help, -output, -version
show	Zeigt die Zieleigenschaften, Verben und Unterziele an. Syntax: show [*Optionen*] [*Ziel*] <*Eigenschaftenname*>=<*Wert*>	-all, -default, -display, -examine, -help, -level, -output, -version
start	Startet ein Ziel. Syntax: start [*Optionen*] [*Ziel*]	-examine, -force, -help, -output, -version
stop	Fährt ein Ziel herunter. Syntax: stop [*Optionen*] [*Ziel*]	-examine, -force, -help, -output, -state, -version, -wait
version	Zeigt die Versionsattribute eines Ziels an. Syntax: version [*Optionen*]	-examine, -help, -output, -version

Tabelle 11-2 beschreibt die SM-CLP-Optionen. Einige Optionen haben abgekürzte Formen, wie in der Tabelle gezeigt.

Tabelle 11-2. Unterstützte SM-CLP-Optionen

SM-CLP-Option	Beschreibung
-all, -a	Beauftragt das Verb, alle Funktionen auszuführen, die möglich sind.
-destination	Bestimmt den Speicherort, an dem ein Image im Dump-Befehl gespeichert wird. Syntax: -destination <URI>
-display, -d	Filtert die Befehlsausgabe. Syntax: -displaz <Eigenschaften | Ziele | Verben>[, <Eigenschaften | Ziele | Verben>]*

-examine, -x	Weist den Befehlsprozessor an, die Befehlssyntax zu validieren, ohne den Befehl auszuführen.
-help, -h	Zeigt Hilfe für das Verb an.
-level, -l	Weist das Verb an, an Zielen auf zusätzlichen Stufen unterhalb des festgelegten Ziels zu arbeiten. Syntax: `-level <n | alle>`
-output, -o	Legt das Format für die Ausgabe fest. Syntax: `-output <Text | clpcsv | clpxml>`
-source	Legt den Speicherort eines Image in einem Ladebefehl fest. Syntax: `-source <URI>`
-version, -v	Zeigt die SMASH-CLP-Versionsnummer an.

MAP-Adressbereich navigieren

ANMERKUNG: Auf SM-CLP-Adresspfaden können der Schrägstrich (/) und der umgekehrte Schrägstrich (\) miteinander vertauscht werden. Ein umgekehrter Schrägstrich am Ende einer Befehlszeile führt jedoch den Befehl in der nächsten Zeile fort und wird ignoriert, wenn der Befehl geparst wird.

Objekte, die mit dem SM-CLP verwaltet werden können, werden durch Ziele repräsentiert, die in einem hierarchischen Bereich, Adressbereich des Verwaltungszugriffspunkts (Manageability Access Point = MAP) genannt, angeordnet sind. Ein Adresspfad legt den Pfad vom Adressbereichsstamm zu einem Objekt im Adressbereich fest.

Das Stammziel wird durch einen Schrägstrich (/) oder einen umgekehrten Schrägstrich (\) dargestellt. Es ist der standardmäßige Ausgangspunkt, wenn Sie sich am iDRAC anmelden. Wechseln Sie vom Stamm herunter, indem Sie das Verb cd verwenden. Wenn Sie z. B. zum dritten Eintrag des Systemereignisprotokolls (SEL) wechseln möchten, geben Sie den folgenden Befehl ein:

```
->cd /system1/sp1/logs1/record3
```

Geben Sie das Verb cd ohne Ziel ein, um Ihren aktuellen Standort im Adressbereich zu finden. Die `..` und `.` Abkürzungen funktionieren auf dieselbe Weise wie unter Windows und Linux: `..` bezieht sich auf die übergeordnete Ebene und `.` bezieht sich auf die aktuelle Ebene.

Ziele

Tabelle 11-3 enthält eine Liste von Zielen, die über das SM-CLP zur Verfügung stehen.

Tabelle 11-3. SM-CLP-Ziele

Ziel	Definition
/system1/	Das Ziel des verwalteten Systems.
/system1/sp1	Der Dienstprozessor.
/system1/sol1	Ziel Seriell über LAN.
/system1/sp1/account1 through /system1/sp1/account16	Die 16 lokalen iDRAC-Benutzerkonten. account1 ist das Stammkonto.
/system1/sp1/enetport1	Die iDRAC-NIC-MAC-Adresse.
/system1/sp1/enetport1/lanendpt1/ ipendpt1	Die Einstellungen für iDRAC-IP, Gateway und Netzmaske.
/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1	Die Einstellungen des iDRAC-DNS-Servers.
/system1/sp1/group1 through /system1/sp1/group5	Die Active Directory-Standardschemagruppen.
/system1/sp1/logs1	Das Protokollsammlungsziel.
/system1/sp1/logs1/record1	Eine einzelnes SEL-Datensatzinstanz auf dem Managed System.
/system1/sp1/logs1/records	Das SEL-Ziel auf dem verwalteten System.
/system1/sp1/oemdell_racsecurity1	Speicher für Parameter, die zum Erstellen einer Zertifikatsignierungsanforderung verwendet werden.
/system1/sp1/oemdell_ssl1	Status der SSL-Zertifikatanforderung.
/system1/sp1/oemdell_vmservice1	Konfiguration und Zustand des virtuellen Datenträgers.

Verb Anzeigen verwenden

Um mehr über ein Ziel zu erfahren, verwenden Sie das Verb show. Dieses Verb zeigt die Eigenschaften des Ziels, untergeordnete Ziele sowie eine Liste der SM-CLP-Verben an, die an diesem Ort zulässig sind.

Option -display verwenden

Anhand der Option **show -display** können Sie die Befehlsausgabe auf eines oder mehrere der folgenden Elemente einschränken: Eigenschaften, Ziele, Verben. Wenn Sie z. B. nur die Eigenschaften und Ziele des aktuellen Orts anzeigen möchten, verwenden Sie den folgenden Befehl:

```
show -d properties,targets /system1/sp1/account1
```

Wenn Sie nur bestimmte Eigenschaften aufführen möchten, qualifizieren Sie sie, wie im folgenden Befehl gezeigt:

```
show -d properties=(userid,username) /system1/sp1/account1
```

Wenn Sie nur eine Eigenschaft anzeigen möchten, können Sie die Klammern auslassen.

Option -level verwenden

Die Option **show -level** führt **show** über zusätzliche Ebenen unterhalb des festgelegten Ziels aus. Wenn Sie z. B. die Eigenschaften **username** und **userid** der Ziele **account1** bis **account16** unterhalb von **/system1/sp1** anzeigen möchten, könnten Sie den folgenden Befehl eingeben:

```
show -l 1 -d properties=(userid,username) /system1/sp1/account*
```

Wenn Sie alle Ziele und Eigenschaften im Adressbereich anzeigen möchten, verwenden Sie die Option **-l all**, wie im folgenden Befehl:

```
show -l all -d properties /
```

-output-Option verwenden

Die Option **-output** legt eines von vier Formaten für die Ausgabe von SM-CLP-Verben fest: **text**, **clpcsv**, **keyword** und **clpxml**.

Das Standardformat ist **text**, die am einfachsten lesbare Ausgabe. Das Format **clpcsv** ist ein Format, bei dem Werte durch Kommas getrennt werden. Es eignet sich dazu, in ein Tabellenkalkulationsprogramm geladen zu werden. Das Format **keyword** gibt Informationen als eine Liste von keyword=value-Paaren (eines pro Zeile) aus. Das Format **clpxml** ist ein XML-Dokument, das ein **response**-XML-Element enthält. Die DMTF hat die Formate **clpcsv** und **clpxml** festgelegt und ihre Bestimmungen können auf der DMTF-Website unter **www.dmtf.org** eingesehen werden.

Das folgende Beispiel zeigt, wie der Inhalt des SEL in XML ausgegeben werden kann:

```
show -l all -output format=clpxml /system1/sp1/logs1
```

Beispiele des iDRAC-SM-CLP

Die folgenden Unterabschnitte enthalten Beispiele zur Verwendung des SM-CLP, um folgende Vorgänge auszuführen:

- Serverstromverwaltung
- SEL-Verwaltung
- MAP-Zielnavigation
- Eigenschaften des Anzeigesystems
- iDRAC-IP-Adresse, Subnetzmaske und Gateway-Adresse einstellen

Informationen zur Verwendung der iDRAC SM-CLP-Schnittstellen finden Sie unter iDRAC SMCLP-Eigenschaftendatenbank.

Server-Stromverwaltung

Tabelle 11-4 enthält Beispiele für die Verwendung des SM-CLP zum Ausführen von Stromverwaltungsvorgängen auf einem verwalteten Server.

Tabelle 11-4. Server-Stromverwaltungsvorgänge

Operation	Syntax

Anmeldung am iDRAC über die SSH-Schnittstelle	`>ssh 192.168.0.120`
	`>Anmeldung: root`
	`>Kennwort:`

Schalten Sie den Server aus.	`->stop /system1` `system1 wurde erfolgreich angehalten`
Server aus dem ausgeschalteten Zustand hochfahren	`->start /system1` `system1 wurde erfolgreich gestartet`

Server neu starten	->reset /system1 system1 wurde erfolgreich zurückgesetzt

SEL-Verwaltung

Tabelle 11-5 enthält Beispiele für die Verwendung des SM-CLP zum Ausführen von SEL-bezogenen Vorgängen auf dem Managed System.

Tabelle 11-5. SEL-Verwaltungsvorgänge

Operation	Syntax
SEL anzeigen	->show /system1/sp1/logs1 Targets: record1 record2 record3 record4 record5 Properties: Description=IPMI SEL MaxNumberOfRecords=512 CurrentNumberOfRecords=5 Verbs: CD delete exit help show version
SEL-Datensatz anzeigen	->show /system1/sp1/logs1/record4 ufip=/system1/sp1/logs1/log1/record4 Properties: Caption=Not Fefined Description=Backplane Drive 0: drive slot sensor for Backplane, drive presence was asserted Elementname=Not Supported LogCreationClassName=CIM_RecordLog LogName=IPMI-SEL CreationClassName=CIM_LogRecord RecordID-ID=4 MessageTimeStamp=16:37:10,January 13,2007 Verbe: CD exit help show version
SEL löschen	->delete /system1/sp1/logs1 All records deleted successfully

MAP-Zielnavigation

Tabelle 11-6 enthält Beispiele für die Verwendung des Verbs **cd**, um innerhalb des MAP zu navigieren. In allen Beispielen wird angenommen, dass das ausgängliche Standardziel '/' ist.

Tabelle 11-6. Map-Zielnavigationsvorgänge

Operation	Syntax
Wechseln Sie zum Systemziel und führen Sie einen Neustart durch.	->cd system1 ->reset **ANMERKUNG:** Das aktuelle Standardziel ist '/'.
Wechseln Sie zum SEL-Ziel und zeigen Sie die Protokolldatensätze an.	->cd system1 ->cd sp1 ->cd logs1 ->show
	->cd system1/sp1/logs1 ->show
Aktuelles Ziel anzeigen	->cd .

Eine Stufe höher gehen	`->cd ..`
Shell beenden	`->exit`

iDRAC-IP-Adresse, Subnetzmaske und Gateway-Adresse einstellen

Die Verwendung des SM-CLP zum Aktualisieren der iDRAC-Netzwerkeigenschaften wird über zwei Verfahren ausgeführt:

1. Stellen Sie unter **/system1/sp1/enetport1/lanendpt1/ipendpt1** neue Werte für die NIC-Eigenschaften ein:
   - **oemdell_nicenable** - auf 1 einstellen, um iDRAC-Netzwerkbetrieb zu aktivieren, auf 0, um zu deaktivieren
   - **ipaddress** - die IP-Adresse
   - **subnetmask** - die Subnetzmaske
   - **oemdell_usedhcp** - auf 1 einstellen, um die Verwendung von DHCP zum Einstellen der Eigenschaften **ipaddress** und **subnetmask** zu aktivieren, auf 0 einstellen, um statische Werte einzustellen
2. Übernehmen Sie die neuen Werte, indem Sie die Eigenschaft **committed** auf 1 einstellen.

Immer wenn die Eigenschaft **commit** den Wert 1 hat, sind die aktuellen Einstellungen der Eigenschaften aktiv. Wenn Sie eine Eigenschaft ändern, wird die Eigenschaft **commit** auf 0 zurückgesetzt, um darauf hinzuweisen, dass die Werte nicht übernommen wurden.

ANMERKUNG: Die Eigenschaft **commit** wirkt sich nur auf die Eigenschaften am MAP-Ort **/system1/sp1/enetport1/lanendpt1/ipendpt1** aus. Alle anderen SM-CLP-Befehle werden sofort wirksam.

ANMERKUNG: Wenn Sie ein lokales RACADM zum Einstellen der iDRAC-Netzwerkeigenschaften verwenden, werden Ihre Änderungen sofort wirksam, da ein lokales RACADM nicht auf eine Netzwerkverbindung angewiesen ist.

Wenn Sie die Änderungen übernehmen, werden die neuen Netzwerkeinstellungen wirksam, was dazu führt, dass Ihre Telnet- oder ssh-Sitzung abgebrochen wird. Indem Sie den Schritt commit einführen, können Sie die Beendigung Ihrer Sitzung so lange verzögern, bis Sie alle SM-CLP-Befehle ausgeführt haben.

Tabelle 11-7 zeigt Beispiele zum Einstellen der iDRAC-Eigenschaften unter Verwendung des SM-CLP.

Tabelle 11-7. iDRAC-Netzwerkeigenschaften mit SM-CLP einstellen

Operation	Syntax
Wechseln Sie zum Speicherort der iDRAC-NIC-Eigenschaften	`->cd /system1/sp1/enetport1/lanendpt1/ipendpt1`
Stellen Sie die neue IP-Adresse ein	`->set ipaddress=10.10.10.10`
Stellen Sie die Subnetzmaske ein	`->set subnetmask=255.255.255.255`
Schalten Sie das DHCP-Flag ein	`->set oemdell_usedhcp=1`
Aktivieren Sie die NIC	`->set oemdell_nicenable=1`
Übernehmen Sie die Änderungen	`->set committed=1`

iDRAC-Firmware mittels SM-CLP aktualisieren

Um die iDRAC-Firmware unter Verwendung des SM-CLP zu aktualisieren, müssen Sie den TFTP-URI des Dell Update Package kennen.

Führen Sie zum Aktualisieren der Firmware unter Verwendung des SM-CLP die folgenden Schritte aus:

1. Melden Sie sich über telnet oder SSH am iDRAC an.
2. Überprüfen Sie die aktuelle Firmware-Version mit folgendem Befehl:

   ```
   version
   ```

3. Geben Sie folgenden Befehl ein:

   ```
   load -source tftp://<tftp-Server>/<Aktualisierungspfad> /system1/sp1
   ```

   wobei <*tftp-Server*> der DNS-Name oder die IP-Adresse des TFTP-Servers ist und <*Aktualisierungspfad*> der Pfad zum Aktualisierungspaket auf dem TFTP-Server.

   Ihre Telnet- oder SSH-Sitzung wird abgebrochen werden. Sie müssen eventuell mehrere Minuten abwarten, bis die Firmware-Aktualisierung abgeschlossen ist.

4. Starten Sie eine neue Telnet- oder SSH-Sitzung und geben Sie den Versionsbefehl erneut ein, um zu prüfen, ob die neue Firmware geschrieben wurde.

Seriell über LAN (SOL) mit Telnet oder SSH verwenden

Verwenden Sie eine Telnet- oder SSH-Konsole auf Ihrer Verwaltungsstation, um zum iDRAC eine Verbindung herzustellen, und leiten Sie dann die serielle Schnittstelle des verwalteten Servers in Ihre Konsole um. Diese Funktion stellt eine Alternative zu IPMI SOL dar, für die ein Dienstprogramm wie **solproxy** zum Übersetzen des seriellen Stroms an und von Netzwerkpakete(n) erforderlich ist. Die iDRAC SOL-Implementierung macht ein zusätzliches Dienstprogramm überflüssig, da die seriell-zu-Netzwerk-Übersetzung innerhalb des iDRAC stattfindet.

Die verwendete Telnet- oder SSH-Konsole sollte in der Lage sein, die Daten zu interpretieren, die von dem seriellen Anschluss des verwalteten Servers eingehen und auf diese Daten zu reagieren. Der serielle Anschluss wird normalerweise an eine Shell angeschlossen, die ein ANSI- oder VT100-Terminal emuliert.

Sie können unter Verwendung von Telnet eine Verbindung zum IPMI LAN-SOL-Anschluss - Anschluss 2100 - herstellen. Die serielle Konsole wird automatisch auf Ihre Telnet-Konsole umgeleitet.

Mit SSH oder Telnet können Sie zum iDRAC auf die gleiche Weise wie zum SM-CLP eine Verbindung herstellen. Die SOL-Umleitung kann dann vom Ziel **/system1/sol1** aus gestartet werden.

Informationen zur Verwendung von Telnet und SSH-Clients bei iDRAC finden Sie unter Telnet- oder SSH-Clients installieren.

SOL über Telnet mit HyperTerminal auf Microsoft Windows verwenden

1. Wählen Sie **Start**→ **Alle Programme**→ **Zubehör**→ **Kommunikation**→ **HyperTerminal** aus.
2. Geben Sie für die Verbindung einen Namen ein, wählen Sie ein Symbol aus und klicken Sie auf **OK**.
3. Wählen Sie im Feld **Verbindung herstellen über** aus der Liste **TCP/IP (Winsock)** aus.
4. Geben Sie in das Feld **Host-Adresse** den DNS-Namen oder die IP-Adresse des iDRAC ein.
5. Geben Sie in das Feld **Schnittstellennummer** die Telnet- Schnittstellennummer ein.
6. Klicken Sie auf **OK**.

Klicken Sie zum Beenden der SOL-Sitzung auf das Symbol zum Abbrechen der HyperTerminal-Verbindung.

SOL über Telnet mit Linux verwenden

Um auf einer Linux-Verwaltungsstation SOL von Telnet aus zu starten, führen Sie folgende Schritte aus:

1. Starten Sie eine Shell.
2. Stellen Sie mit folgendem Befehl eine Verbindung zum iDRAC her:

   ```
   telnet <iDRAC-IP-Adresse>
   ```

   ANMERKUNG: Wenn Sie die Standard-Anschlussnummer für den Telnet-Dienst, 23, geändert haben, fügen Sie die Anschlussnummer am Ende des **telnet**-Befehls hinzu.

3. Geben Sie zum Starten von SOL folgenden Befehl ein:

   ```
   start /system1/sol1
   ```

   Sie werden nun mit der seriellen Schnittstelle des verwalteten Servers verbunden.

Wenn Sie bereit sind, SOL zu beenden, geben Sie <Strg>+] ein (halten Sie Strg gedrückt, geben Sie eine rechte eckige Klammer ein und lassen Sie dann die Tasten los). Eine Telnet-Eingabeaufforderung wird angezeigt. Geben Sie quit ein, um Telnet zu beenden.

SOL über SSH verwenden

Anhand des Ziels **/system1/sol1** können Sie dene seriellen Anschluss des verwalteten Servers in Ihre SSH-Konsole umleiten.

1. Stellen Sie anhand von OpenSSH oder PuTTY eine Verbindung zum iDRAC her.
2. Geben Sie zum Starten von SOL folgenden Befehl ein:

   ```
   start /system1/sol1
   ```

Sie werden nun mit dem seriellen Anschluss des verwalteten Servers verbunden. Die SM-CLP-Befehle stehen Ihnen nicht mehr zur Verfügung.

Wenn Sie bereit sind, die SOL-Umleitung zu beenden, drücken Sie auf die Eingabetaste, auf <Esc> und dann auf <T> (drücken Sie auf eine Taste nach der

anderen, der Reihenfolge nach). Die SSH-Sitzung wird geschlossen.

Sobald SOL gestartet ist, können Sie nicht zum SM-CLP zurückkehren. Sie müssen die SSH-Sitzung beenden und eine neue starten, um das SM-CLP verwenden zu können.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Betriebssystem mithilfe von iVM-CLI bereitstellen

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

Das Dienstprogramm Befehlszeilenoberfläche des virtuellen Datenträgers (iVM-CLI) ist eine Befehlszeilenoberfläche, die die Funktionen des virtuellen Datenträgers von der Verwaltungsstation zum iDRAC im Remote-System bereitstellt. Mit iVM-CLI und geskripteten Methoden können Sie Ihr Betriebssystem auf mehreren Remote-Systemen in Ihrem Netzwerk einsetzen.

Dieser Abschnitt gibt Auskunft über die Integration des iVM-CLI-Dienstprogramms in Ihrem Betriebsnetz.

Bevor Sie beginnen

Stellen Sie vor dem Einsatz des iVM-CLI-Dienstprogramms sicher, dass die gewünschten Remote-Systeme und das Betriebsnetz den in den folgenden Abschnitten aufgeführten Anforderungen entsprechen.

Remote-System-Anforderungen

- Der iDRAC ist auf jedem Remote-System konfiguriert.

Netzwerkanforderungen

Eine Netzwerkfreigabe muss die folgenden Komponenten enthalten:

- Betriebssystemdateien
- Erforderliche Treiber
- Startabbilddatei(en) des Betriebssystems

  Die Image-Datei muss das ISO-Image einer Betriebssystem-CD oder einer CD/DVD mit einem dem Industriestandard entsprechenden startfähigen Format sein.

Startfähige Abbilddatei erstellen

Bevor Sie die Abbilddatei für die Remote-Systeme bereitstellen, ist sicherzustellen, dass ein unterstütztes System von der Datei starten kann. Um die Image-Datei zu prüfen, übertragen Sie sie mithilfe der iDRAC-Webbenutzeroberfläche auf ein Testsystem und führen Sie dann einen Neustart des Systems durch.

Die folgenden Abschnitte enthalten spezifische Informationen über das Erstellen von Abbilddateien für Linux- und Windows-Systeme.

Abbilddatei für Linux-Systeme erstellen

Verwenden Sie das Datenvervielfältigungs-Dienstprogramm (dd), um eine startfähige Image-Datei für das Linux-System zu erstellen.

Um das Dienstprogramm auszuführen, öffnen Sie eine Eingabeaufforderung und geben Sie Folgendes ein:

```
dd if=<Eingabekomponente> of=<Ausgabedatei>
```

Zum Beispiel:

```
dd if=/dev/sdc0 of=mycd.img
```

Abbilddatei für Windows-Systeme erstellen

Achten Sie bei der Auswahl eines Daten-Replicator-Dienstprogramms für Windows-Abbilddateien darauf, dass es sich um ein Dienstprogramm handelt, das die Abbilddatei 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 eine startfähige, vorkonfigurierte Bereitstellungs-Abbilddatei zur Bereitstellung des Betriebssystems an die Remote-Systeme haben, können Sie diesen Schritt überspringen.

   Wenn Sie keine startfähige, vorkonfigurierte Bereitstellungs-Abbilddatei haben, erstellen Sie die Datei. Schließen Sie alle für die Betriebssystem-Bereitstellungsverfahren zu verwendenden Programme und/oder Skripts ein.

   Zum Bereitstellen eines Microsoft® Windows®-Betriebssystems kann die Image-Datei z. B. Programme enthalten, die den von Microsoft Systems Management Server (SMS) verwendeten Bereitstellungsmethoden ähnlich sind.

   Wenn Sie die Abbilddatei erstellen, führen Sie folgendes aus:

   - Die netzwerkbasierten Standardinstallationsverfahren befolgen.
   - Das Bereitstellungs-Abbild als "schreibgeschützt" kennzeichnen, um sicherzustellen, dass jedes Zielsystem startet und dasselbe Bereitstellungsverfahren ausführt.

- Eines der folgenden Verfahren ausführen:
  - Integrieren Sie **ipmitool** und die Befehlszeilenoberfläche des virtuellen Datenträgers (iVM-CLI) in Ihre bestehende Betriebssystem-Bereitstellungsanwendung. Verwenden Sie das Beispielskript **ivmdeploy** als Orientierungshilfe beim Verwenden des Dienstprogramms.
  - Verwenden Sie das vorhandene **ivmdeploy**-Script, um das Betriebssystem bereitzustellen.

Betriebssystem bereitstellen

Verwenden Sie das iVM-Dienstprogramm und das im Dienstprogramm enthaltene **ivmdeploy**-Skript, um das Betriebssystem Ihren Remote-Systemen bereitzustellen.

Sehen Sie sich, bevor Sie beginnen, das **ivmdeploy**-Beispielskript an, das mit dem iVM-CLI-Dienstprogramm enthalten ist. Das Skript zeigt die detaillierten Schritte auf, die zur Bereitstellung des Betriebssystems an Remote-Systemen in Ihrem Netzwerk erforderlich sind.

Das folgende Verfahren enthält eine hochstufige Übersicht zur Bereitstellung des Betriebssystems auf Remote-Zielsystemen.

1. Führen Sie die iDRAC-IP-Adressen der Remote-Systeme auf, die in der Textdatei **ip.txt** bereitgestellt werden (eine IP-Adresse pro Zeile).

2. Legen Sie eine startfähige Betriebssystem-CD oder -DVD in das Laufwerk des Client-Datenträgers ein.

3. Führen Sie an der Befehlszeile **ivmdeploy** aus.

Geben Sie zum Ausführen des ivmdeploy-Skripts den folgenden Befehl an der Befehlszeile ein:

```
ivmdeploy -r ip.txt -u <idrac-Benutzer> -p <idrac-Kennwt> -c {<iso9660-img> | <Pfad>}
```

wobei

- *<idrac-Benutzer>* ist der iDRAC-Benutzername, z. B. **root**
- *<idrac-Kennwt>* ist das Kennwort für den iDRAC-Benutzer, z. B. **calvin**
- *<iso9660-img>* ist der Pfad zu einem ISO9660-Image der Betriebssystem-Installations-CD-ROM oder -DVD
- *<Pfad>* ist der Pfad zu dem Gerät, das die Betriebssystem-Installations-CD-ROM oder -DVD enthält

Das Skript **ivmdeploy** leitet seine Befehlszeilenoptionen an das Dienstprogramm **iVMCLI** weiter. Einzelheiten zu diesen Optionen finden Sie unter Befehlszeilenoptionen. Das Skript verarbeitet die Option **-r** auf leicht unterschiedliche Weise als die Option **iVMCLI -r**. Wenn das Argument der Option **-r** der Name einer vorhandenen Datei ist, liest das Skript iDRAC-IP-Adressen aus der festgelegten Datei und führt das Dienstprogramm **iVMCLI** einmal pro Zeile aus. Ist das Argument der Option **-r** kein Dateiname, sollte es die Adresse eines einzelnen iDRAC sein. In diesem Fall arbeitet die Option **-r** wie für das Dienstprogramm **iVMCLI** beschrieben.

Das ivmdeploy-Skript unterstützt die Installation nur über eine CD/DVD oder ein CD/DVD-ISO9660-Image. Wenn Sie die Installation über eine Diskette oder ein Diskettenimage vornehmen müssen, können Sie das Skript zur Verwendung der Option **iVMCLI -f** modifizieren.

Befehlszeilenoberflächen-Dienstprogramm des virtuellen Datenträgers verwenden

Das Dienstprogramm Befehlszeilenoberfläche des virtuellen Datenträgers (iVM-CLI) ist eine scriptfähige Befehlszeilenoberfläche, die die Funktionen des virtuellen Datenträgers von der Verwaltungsstation zum iDRAC bereitstellt.

Das iVM-CLI-Dienstprogramm bietet die folgenden Funktionen:

ANMERKUNG: Beim Virtualisieren von schreibgeschützten Abbilddateien können sich mehrere Sitzungen dieselben Abbilddatenträger teilen. Beim Virtualisieren von physischen Laufwerken kann zu einem bestimmten Zeitpunkt jeweils nur eine Sitzung auf ein gegebenes physisches Laufwerk zugreifen.

- Wechselmedienkomponenten oder Abbilddateien, die mit den Plug-ins des virtuellen Datenträgers übereinstimmen
- Automatische Terminierung, wenn die Einmal-Startoption der iDRAC-Firmware aktiviert ist.
- Sichere Datenübertragung zum iDRAC mittels SSL-Verschlüsselung

Stellen Sie vor dem Ausführen des Dienstprogramms sicher, dass Sie für den iDRAC über Benutzerberechtigungen des virtuellen Datenträgers verfügen.

Wenn das Betriebssystem Administratorrechte oder eine betriebssystemspezifische Berechtigung oder Gruppenmitgliedschaft unterstützt, sind Administratorrechte auch zum Ausführen des iVM-CLI-Befehls erforderlich.

Der Administrator des Client-Systems steuert Benutzergruppen und -berechtigungen und dadurch auch die Benutzer, die das Dienstprogramm ausführen können.

Für Windows-Systeme müssen Sie über Hauptbenutzerberechtigungen verfügen, um das iVM-CLI-Dienstprogramm auszuführen.

Für Linux-Systeme können Sie ohne Administratorrechte auf das iVM-CLI-Dienstprogramm zugreifen, indem Sie den **sudo**-Befehl verwenden. Dieser Befehl enthält ein zentrales Mittel zur Bereitstellung von Nicht-Administrator-Zugriff und protokolliert alle Benutzerbefehle. Um Benutzer in der iVM-CLI-Gruppe hinzuzufügen oder zu bearbeiten, verwendet der Administrator den **visudo**-Befehl. Benutzer ohne Administratorrechte können den Befehl **sudo** als Präfix zur iVM-CLI-Befehlszeile (oder zum iVM-CLI Skript) hinzufügen, um Zugriff auf den iDRAC im Remote-System zu erhalten und das Dienstprogramm auszuführen.

iVM-CLI-Dienstprogramm installieren

Das iVM-CLI-Dienstprogramm befindet sich auf der CD *Dell OpenManage™ Systems Management Consoles*, die im Systemverwaltungssoftware-Kit zu Dell OpenManage enthalten ist. Legen Sie zur Installation des Dienstprogramms die CD *System Management Consoles* in das CD-Laufwerk des Systems ein und folgen Sie den Bildschirmanleitungen.

Die CD *Systems Management Consoles* enthält die neuesten System Management-Softwareprodukte, einschließlich Diagnose, Speicherverwaltung, RAS-Dienst und RACADM-Dienstprogramm. Diese CD enthält auch Infodateien mit den neuesten Produktinformationen über die Systemverwaltungssoftware.

Die CD *Systems Management Consoles* enthält **ivmdeploy**, ein Beispielskript, das illustriert, wie man die iVM-CLI- und RACADM-Dienstprogramme zur Bereitstellung von Software an verschiedene Remote-Systeme verwendet.

ANMERKUNG: Das **ivmdeploy**-Script hängt bei seiner Installation von den anderen, in seinem Verzeichnis vorhandenen, Dateien ab. Wenn Sie das Skript von einem anderen Verzeichnis aus verwenden möchten, müssen Sie alle Dateien mit ihm installieren.

Befehlszeilenoptionen

Die iVM-CLI-Schnittstelle ist auf Windows- und Linux-Systemen identisch. Das Dienstprogramm verwendet Optionen, die mit den RACADM-Dienstprogramm-Optionen übereinstimmen. Eine Option zur Angabe der iDRAC-IP-Adresse erfordert z. B. dieselbe Syntax für die RACADM- und iVM-CLI-Dienstprogramme.

Das Format eines iVM-CLI-Befehls lautet:

`iVMCLI [Parameter] [Betriebssystem_Shell-Optionen]`

Bei der Befehlszeilensyntax wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter iVM-CLI-Parameter".

Wenn das Remote-System die Befehle akzeptiert und der iDRAC die Verbindung genehmigt, wird der Befehl weiterhin ausgeführt, bis eine der folgenden Situationen zutrifft:

- Die iVM-CLI-Verbindung wird aus einem beliebigen Grund abgebrochen.
- Das Verfahren wird mit einer Betriebssystemsteuerung manuell abgebrochen. Beispiel: In Windows können Sie den Task-Manager verwenden, um das Verfahren abzubrechen.

iVM-CLI-Parameter

iDRAC-IP-Adresse

`-r <iDRAC-IP-Adresse>[:<iDRAC-SSL-Port>]`

Dieser Parameter bietet die iDRAC-IP-Adresse und die SSL-Schnittstelle, die das Dienstprogramm zum Herstellen einer Verbindung des virtuellen Datenträgers zum Ziel-iDRAC benötigt. Wenn Sie eine ungültige IP-Adresse oder einen ungültigen DDNS-Namen eingeben, wird eine Fehlermeldung angezeigt, und der Befehl wird abgebrochen.

wobei *<iDRAC-IP-Adresse>* eine gültige, eindeutige IP-Adresse oder der iDRAC-DDNS-Name (dynamisches Domänennamenssystem) ist, falls unterstützt. Wenn *<iDRAC-SSL-Anschluss>* ausgelassen wird, wird die Anschluss 443 (Standard-Anschluss) verwendet. Solange der iDRAC-Standard-SSL-Anschluss nicht geändert wird, ist der optionale SSL-Anschluss nicht erforderlich.

iDRAC-Benutzername

`-u <iDRAC-Benutzername>`

Dieser Parameter enthält den iDRAC-Benutzernamen, der den virtuellen Datenträger ausführen wird.

Der *<iDRAC-Benutzername>* muss die folgenden Attribute aufweisen:

- Gültiger Benutzername
- iDRAC - Benutzerberechtigung für den virtuellen Datenträger

Wenn die iDRAC-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt, und der Befehl wird terminiert.

iDRAC-Benutzerkennwort

`-p <iDRAC-Benutzerkennwort>`

Dieser Parameter enthält das Kennwort für den angegebenen iDRAC-Benutzer.

Wenn die iDRAC-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt, und der Befehl wird terminiert.

Floppy/Festplatten-Komponente oder Abbilddatei

`-f {<Gerätename> | <Abbilddatei>}`

wobei *<Gerätename>* ein gültiger Laufwerkbuchstabe (bei Windows-Systemen) oder ein gültiger Gerätekomponentenname ist, einschließlich der Partitionsnummer des bereitstellbaren Dateisystems, falls zutreffend (bei Linux-Systemen), und wobei *<Image-Datei>* der Dateiname und Pfad einer gültigen Image-Datei ist.

Dieser Parameter bestimmt die Komponente oder die Datei, die den virtuellen Floppy-/Festplatten-Datenträger liefern.

Beispiel: Eine Abbilddatei 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 zur Abbilddatei schreiben. Konfigurieren Sie das Betriebssystem so, dass eine Floppy-Abbilddatei, die nicht überschrieben werden soll, mit einem Schreibschutz versehen wird.

Beispiel: Ein Komponente wird wie folgt angegeben:

`-f a:\` (Windows-System)

`-f /dev/sdb4 # 4th partition on device /dev/sdb` (Linux-System)

Wenn die Komponente eine Schreibschutzfunktion bietet, können Sie diese Funktion verwenden, um sicherzustellen, dass der virtuelle Datenträger nicht zum Datenträger schreibt.

Lassen Sie diesen Parameter aus der Befehlszeile aus, wenn Sie keine Diskettendatenträger virtualisieren. Wenn ein ungültiger Wert festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.

CD/DVD-Komponente oder -Abbilddatei

`-c {<Gerätename> | <Image-Datei>}`

wobei *<Gerätename>* ein gültiger CD/DVD-Laufwerkbuchstabe (bei Windows-Systemen) oder ein gültiger CD/DVD-Gerätedateiname (bei Linux-Systemen) ist, und wobei *<Image-Datei>* der Dateiname und Pfad einer gültigen ISO-9660-Image-Datei ist.

Dieser Parameter bestimmt die Komponente oder Datei, die die virtuellen CD/DVD-ROM-Datenträger liefert:

Beispiel: Eine Abbilddatei wird wie folgt angegeben:

`-c c:\temp\mydvd.img` (Windows-Systeme)

`-c /tmp/mydvd.img` (Linux-Systeme)

Beispiel: Ein Komponente wird wie folgt angegeben:

`-c d:\` (Windows-Systeme)

`-c /dev/cdrom` (Linux-Systeme)

Lassen Sie diesen Parameter aus der Befehlszeile aus, wenn Sie keine CD/DVD-Datenträger virtualisieren. Wenn ein ungültiger Wert festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.

Geben Sie mit dem Befehl mindestens einen Datenträgertyp (Floppy oder CD/DVD-Laufwerk) an, es sei denn, es werden nur Switch-Optionen vorgegeben. Andernfalls wird eine Fehlermeldung angezeigt und der Befehl mit einem Fehler abgebrochen.

Versionsanzeige

-v

Dieser Parameter wird zur Anzeige der iVM-CLI-Dienstprogrammversion verwendet. Wenn keine anderen Nicht-Switch-Optionen geboten werden, wird der Befehl ohne Fehlermeldung abgebrochen.

Hilfeanzeige

-h

Dieser Parameter zeigt eine Zusammenfassung der iVM-CLI-Dienstprogrammparameter an. Wenn keine anderen Nicht-Switch-Optionen geboten werden, wird der Befehl ohne Fehler abgebrochen.

Manuelle Anzeige

-m

Dieser Parameter zeigt eine detaillierte man-Seite" für das iVM-CLI-Dienstprogramm an, einschließlich Beschreibungen aller möglicher Optionen.

Verschlüsselte Daten

-e

Wenn dieser Parameter in der Befehlszeile enthalten ist, verwendet die iVM-CLI einen SSL-verschlüsselten Kanal zur Übertragung von Daten zwischen der Verwaltungsstation und dem iDRAC im Remote-System. Wenn dieser Parameter nicht in der Befehlszeile enthalten ist, wird die Datenübertragung nicht verschlüsselt.

iVM-CLI-Betriebssystem, Shell-Optionen

Die folgenden Betriebssystemfunktionen können in der iVM-CLI-Befehlszeile verwendet werden:

- stderr/stdout-Umleitung - Leitet jede gedruckte Dienstprogrammausgabe zu einer Datei um.

  Die Verwendung des "größer als"-Zeichens (>), gefolgt von einem Dateinamen, überschreibt z. B. die angegebene Datei mit der gedruckten Ausgabe des iVM-CLI-Dienstprogramms.

  ANMERKUNG: Das iVM-CLI-Dienstprogramm liest nicht von der Standardeingabe (**stdin**). Infolgedessen ist keine **stdin**-Umleitung erforderlich.

- Ausführung im Hintergrund - Standardmäßig wird das iVM-CLI-Dienstprogramm im Vordergrund ausgeführt. Verwenden Sie die Befehlsshell-Funktionen des Betriebssystems, um zu veranlassen, dass das Dienstprogramm im Hintergrund ausgeführt wird. Unter einem Linux-Betriebssystem wird z. B. durch das auf den Befehl folgende Et-Zeichen (&) veranlasst, dass das Programm als neues Hintergrundverfahren erzeugt wird.

Diese letztere Methode ist bei Skriptprogrammen nützlich, da dem Skript nach dem Starten eines neuen Vorgangs für den iVM-CLI-Befehl ermöglicht wird, fortzufahren (andernfalls würde das Skript blockieren, bis das iVM-CLI-Programm beendet ist). Wenn auf diese Weise mehrere iVM-CLI-Instanzen gestartet werden und eine oder mehrere Befehlsinstanzen manuell beendet werden müssen, sind die betriebssystemspezifischen Einrichtungen zum Auflisten und Beenden von Verfahren zu verwenden.

iVM-CLI-Rückmeldecodes

0 = Kein Fehler

1 = Kann keine Verbindung herstellen

2 = iVM-CLI-Befehlszeilenfehler

3 = RAC-Firmware-Verbindung abgebrochen

Immer wenn Fehler auftreten, werden neben der Standardfehlerausgabe auch Textmeldungen auf Englisch ausgegeben.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC-Konfigurations-Dienstprogramm verwenden

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

Übersicht

Das iDRAC-Konfigurationshilfsprogramm ist eine Vorstart-Konfigurationsumgebung, die Ihnen ermöglicht, Parameter für den iDRAC und den verwalteten Server anzuzeigen und einzustellen. Genauer gesagt können Sie:

- die Firmware-Revisionsnummern für die Firmware des iDRAC und der primären Rückwandplatine anzeigen
- das lokale Netzwerk des iDRAC konfigurieren, aktivieren oder deaktivieren
- IPMI über LAN aktivieren oder deaktivieren
- ein LAN-PET-Ziel (Plattformereignis-Trap) aktivieren
- die Geräte des virtuellen Datenträgers verbinden oder abtrennen
- den administrativen Benutzernamen bzw. das administrative Kennwort ändern
- die iDRAC-Konfiguration auf die Werkseinstellungen zurücksetzen
- SEL-Meldungen (Systemereignisprotokoll) anzeigen oder Meldungen aus dem Protokoll löschen

Die Tasks, die Sie anhand des iDRAC-Konfigurationshilfsprogramms ausführen können, können auch unter Verwendung anderer Dienstprogramme ausgeführt werden, die durch den iDRAC oder die OpenManage-Software zur Verfügung gestellt werden. Diese Dienstprogramme schließen die Webschnittstelle, die SM-CLP-Befehlszeilenoberfläche, die Befehlszeilenoberfläche des lokalen RACADM und, im Falle einfacher Netzwerkkonfiguration während der erstmaligen CMC-Konfiguration, das CMC-LCD ein.

---

iDRAC-Konfigurationsdienstprogramm starten

Zum erstmaligen Zugreifen auf das iDRAC-Konfigurationshilfsprogramm oder nach dem Zurücksetzen des iDRAC auf seine Standardeinstellungen muss eine iKVM-verbundene Konsole verwendet werden.

1. Geben Sie auf der Tastatur, die mit der iKVM-Konsole verbunden ist, <Druck> ein, um das Menü für iKVM-Onscreen-Konfiguration und - Berichterstattung (OSCAR) anzuzeigen. Verwenden Sie die Taste <Nach oben> und <Nach unten>, um den Steckplatz zu markieren, der den Server enthält und drücken Sie dann auf <Eingabe>.
2. Schalten Sie den Server ein oder starten Sie ihn neu, indem Sie an seiner Vorderseite auf den Netzschalter drücken.
3. Wenn Sie die Meldung **Drücken Sie für das Remote-Zugriffs-Setup innerhalb von 5 Sek. auf <Strg-E>.....** sehen,drücken Sie sofort auf <Strg><E>.

ANMERKUNG: Wenn das Betriebssystem zu laden beginnt, bevor Sie auf <Strg><E> drücken, lassen Sie das System den Startvorgang beenden, starten Sie dann den Server erneut und wiederholen Sie den Vorgang.

Das iDRAC-Konfigurationshilfsprogramm wird angezeigt. Die ersten beiden Zeilen enthalten Informationen zur iDRAC-Firmware und zu den Firmware-Revisionen der primären Rückwandplatine. Die Revisionsstufen können nützlich sein, wenn Sie bestimmen möchten, ob ein Firmware-Upgrade erforderlich ist.

Die iDRAC-Firmware ist der Teil der Firmware, der für externe Schnittstellen zuständig ist, wie z. B. die Webschnittstellen oder das SM-CLP. Die Firmware der primären Rückwandplatine ist der Teil der Firmware, der mit der Serverhardware-Umgebung gekoppelt wird und diese überwacht.

---

iDRAC-Konfigurationshilfsprogramm verwenden

Unterhalb der Firmware-Revisionsmeldungen besteht der Rest des iDRAC-Konfigurationshilfsprogramms aus einem Menü von Elementen, auf die Sie über die Tasten <Nach oben> und <Nach unten> zugreifen können.

- Wenn ein Menüelement zu einem Untermenü oder einem bearbeitbaren Textfeld führt, drücken Sie auf <Eingabe>, um auf das Element zuzugreifen und auf <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 auf <Nach links>, <Nach rechts> oder auf die <Leertaste>, um einen Wert auszuwählen.
- Kann ein Element nicht bearbeitet werden, wird es blau angezeigt. Einige Elemente werden abhängig von anderen getroffenen Auswahlen bearbeitbar.
- In der unteren Zeile des Bildschirms werden Anleitungen zum aktuellen Element angezeigt. Sie können auf <F1> drücken, um bzgl. des aktuellen Elements Hilfe aufzurufen.
- Wenn Sie mit der Verwendung des iDRAC-Konfigurationshilfsprogramms fertig sind, drücken Sie auf <Esc>, um das Beenden-Menü anzuzeigen. Wählen Sie dort, ob Sie Ihre Änderungen speichern oder verwerfen möchten oder ob Sie zum Hilfsprogramm zurückkehren möchten.

In den folgenden Abschnitten werden die Menüelemente des iDRAC-Konfigurationshilfsprogramms beschrieben.

LAN

Verwenden Sie die Tasten <Nach links> und <Nach rechts> sowie die Leertaste, um zwischen **Aktiviert** und **Deaktiviert** auszuwählen.

Das iDRAC-LAN ist in der Standardkonfiguration deaktiviert. Das LAN muss aktiviert sein, damit der Gebrauch der iDRAC-Einrichtungen, wie z. B. der Webschnittstelle, des Telnet/SSH-Zugriffs auf die SM-CLP-Befehlszeilenoberfläche, der Konsolenumleitung und des virtuellen Datenträgers, gestattet wird.

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

`iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF. (iDRAC-bandexterne Schnittstelle wird deaktiviert, wenn der LAN-Kanal AUS ist.)`

`Press any key to clear the message and continue. (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 iDRAC-HTTP-, HTTPS-, Telnet- oder SSH-Schnittstellen zugreifen, der bandexterne Verwaltungsnetzwerkdatenverkehr (wie z. B. IPMI-Meldungen, die von einer Verwaltungsstation aus an den iDRAC gesendet werden) nicht empfangen werden kann, wenn das LAN deaktiviert ist. Die Schnittstelle des lokalen RACADM bleibt verfügbar und kann zur Neukonfiguration des iDRAC-LAN verwendet werden.

IPMI über LAN (Ein/Aus)

Verwenden Sie die Tasten <Nach links> und <Nach rechts> sowie die Leertaste, um zwischen **Ein** und **Aus** zu wählen. Wenn **Aus** ausgewählt ist, akzeptiert der iDRAC keine IPMI-Meldungen, die über die LAN-Schnittstelle eingehen.

Wenn Sie **Aus** auswählen, wird die folgende Warnung angezeigt:

`iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF. (iDRAC-bandexterne Schnittstelle wird deaktiviert, wenn der LAN-Kanal AUS ist.)`

Drücken Sie auf eine beliebige Taste, um die Meldung zu löschen und fortzufahren. Unter LAN finden Sie eine Erklärung der Meldung.

LAN-Parameter

Drücken Sie auf <Eingabe>, um das Untermenü der LAN-Parameter anzuzeigen. Wenn Sie die Konfiguration der LAN-Parameter abgeschlossen haben, drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln.

Tabelle 13-1. LAN-Parameter

Artikel	Beschreibung
Verschlüsselungsschlüssel RMCP+	Drücken Sie auf <Eingabe>, um den Wert zu bearbeiten, und auf <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 der IPMI Authentifizierung und Verschlüsselung 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 werden konnte, werden die Felder auf Null eingestellt. Wenn **Statisch** ausgewählt ist, werden die Elemente **Ethernet-IP-Adresse**, **Subnetzmaske** und **Standard-Gateway** bearbeitbar**.**
Ethernet-IP-Adresse	Wenn die **IP-Adressenquelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse ein, die dem iDRAC zugewiesen werden soll. Die Standardeinstellung ist **192.168.0.120** plus die Nummer des Steckplatzes, in dem sich der Server befindet.
MAC-Adresse	Dies ist die nicht bearbeitbare MAC-Adresse der iDRAC-Netzwerkschnittstelle.
Subnetzmaske	Wenn die **IP-Adressenquelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene Subnetzmaskenadresse an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die Subnetzmaske für den iDRAC ein. Die Standardeinstellung ist **255.255.255.0.**
Standard-Gateway	Wenn die **IP-Adressenquelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse des Standard-Gateways an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse des Standard-Gateways ein. Die Standardeinstellung ist **192.168.0.1.**
LAN-Warnung aktiviert	Wählen Sie **Ein** aus, um die PET-LAN-Warnung (Plattformereignis-Trap) zu aktivieren.
Warnungsregel, Eintrag 1	Wählen Sie Aktivieren oder Deaktivieren aus, um das erste Warnungsziel zu aktivieren.

Warnungsziel 1	Geben Sie die IP-Adresse ein, an die PET-LAN-Warnungen weitergeleitet werden sollen.
Zeichenkette des Host-Namens	Drücken Sie zur Bearbeitung auf <Eingabe>. Geben Sie den Namen des Hosts für PET-Warnungen ein.
DNS-Server von DHCP	Wählen Sie **Ein** aus, um DNS-Server-Adressen von einem DHCP-Dienst auf dem Netzwerk abzurufen. Wählen Sie **Aus** aus, um die unten stehenden DNS-Server-Adressen zu bestimmen.
DNS-Server 1	Wenn **DNS-Server von DHCP Aus** ist, geben Sie die IP-Adresse des ersten DNS-Servers ein.
DNS-Server 2	Wenn **DNS-Server von DHCP Aus** ist, geben Sie die IP-Adresse des zweiten DNS-Servers ein.
iDRAC-Name registrieren	Wählen Sie **Ein**, um den iDRAC-Namen im DNS-Dienst zu registrieren. Wählen Sie **Aus**, wenn Sie nicht möchten, dass Benutzer in der Lage sein sollen, den iDRAC-Namen im DNS zu finden.
iDRAC-Name	Wenn **iDRAC-Name registrieren** auf **Ein** eingestellt ist, drücken Sie auf <Eingabe>, um das Textfeld **Aktueller DNS-iDRAC-Name** zu bearbeiten. Drücken Sie auf <Eingabe>, wenn Sie den iDRAC-Namen fertig bearbeitet haben. Drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln. Der iDRAC-Name muss ein gültiger DNS-Host-Name sein.
Domänenname von DHCP	Wählen Sie **Ein** aus, 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 auf <Eingabe>, um das Textfeld **Aktueller Domänenname** zu bearbeiten. Drücken Sie auf <Eingabe>, 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, wie z. B. `meinefirma.com`.

Virtueller Datenträger

Verwenden Sie die Tasten <Nach links> und <Nach rechts>, um **Verbunden** oder **Abgetrennt** auszuwählen. Wenn Sie **Verbunden** auswählen, werden die virtuellen Datenträgergeräte mit dem USB-Bus verbunden. Hierdurch werden sie während **Konsolenumleitungs**-Sitzungen verfügbar gemacht.

Wenn Sie **Abgetrennt** auswählen, können Benutzer während **Konsolenumleitungs**-Sitzungen nicht auf virtuelle Datenträgergeräte zugreifen.

ANMERKUNG: Um ein USB-Flashlaufwerk mit der Funktion **Virtueller Datenträger** zu verwenden, muss der **Emulationstyp des USB-Flashlaufwerks** im BIOS-Setup-Dienstprogramm auf **Festplatte** eingestellt sein. Sie können auf das BIOS-Setup-Dienstprogramm zugreifen, indem Sie während des Serverstarts auf <F2> drücken. Wenn der **Emulationstyp des USB-Flashlaufwerks** auf **Automatisch** eingestellt ist, erscheint das Flashlaufwerk dem System als Diskettenlaufwerk.

LAN-Benutzerkonfiguration

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

Tabelle 13-2. LAN-Benutzerkonfigurationsseite

Artikel	Beschreibung
Kontozugriff	Wählen Sie **Aktiviert** aus, um das Administratorkonto zu aktivieren. Wählen Sie **Deaktiviert** aus, um das Administratorkonto zu deaktivieren.
Kontoberechtigung	Wählen Sie zwischen **Admin**, **Benutzer**, **Operator** und **Kein Zugriff** aus.
Kontobenutzername	Drücken Sie auf <Eingabe>, um den Benutzernamen zu bearbeiten, und dann auf <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 iDRAC-Konfigurationselemente auf die Werkseinstellungen zurückzusetzen. Dies ist eventuell z. B. dann erforderlich, wenn Sie das Kennwort des administrativen Benutzers vergessen haben oder den iDRAC von den Standardeinstellungen neu konfigurieren möchten.

ANMERKUNG: In der Standardkonfiguration ist der iDRAC-Netzwerkbetrieb deaktiviert. Sie können den iDRAC erst dann über das Netzwerk neu konfigurieren, wenn Sie das iDRAC-Netzwerk im iDRAC-Konfigurationshilfsprogramm aktiviert haben.

Drücken Sie auf <Eingabe>, um das Element auszuwählen. Die folgende Warnungsmeldung wird eingeblendet:

```
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 auf <Eingabe>, um den iDRAC auf die Standardeinstellungen zurückzusetzen.

Menü des Systemereignisprotokolls

Das Menü **Systemereignisprotokoll** ermöglicht Ihnen, Meldungen des Systemereignisprotokolls (SEL) anzuzeigen und die Protokollmeldungen zu löschen. Drücken Sie auf <Eingabe>, um das **Menü des Systemereignisprotokolls** anzuzeigen. Das System zählt die Protokolleinträge und zeigt dann die Gesamtanzahl von Einträgen sowie die aktuellste Meldung an. Das SEL speichert maximal 512 Meldungen.

Um SEL-Meldungen anzuzeigen, wählen Sie **Systemereignisprotokoll anzeigen** aus und drücken Sie auf <Eingabe>. Verwenden Sie die Taste <Nach links>, um die vorhergehende (ältere) Meldung zu verschieben, und die Taste <Nach rechts>, um die nächste (neuere) Meldung zu verschieben. Geben Sie eine Eintragsnummer an, um zu diesem Eintrag zu wechseln. Drücken Sie auf <Esc>, wenn Sie mit dem Anzeigen von SEL-Meldungen fertig sind.

ANMERKUNG: Sie können das SEL nur im iDRAC-Konfigurationsdienstprogramm oder in der iDRAC-Webschnittstelle löschen.

Wählen Sie zum Löschen des SEL **Systemereignisprotokoll löschen** aus und drücken Sie auf <Eingabe>.

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

iDRAC-Konfigurationshilfsprogramm beenden

Wenn Sie mit den Änderungen der iDRAC-Konfiguration fertig sind, drücken Sie auf die Taste <Esc>, um das Menü Beenden anzuzeigen.

Wählen Sie **Änderungen speichern und beenden** aus und drücken Sie dann auf <Eingabe>, um Ihre Änderungen beizubehalten.

Wählen Sie **Änderungen ablehnen und beenden** aus und drücken Sie auf <Eingabe>, um alle vorgenommenen Änderungen zu ignorieren.

Wählen Sie **Zu Setup zurückwechseln** aus und drücken Sie auf <Eingabe>, um zum iDRAC-Konfigurationshilfsprogramm zurückzuwechseln.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Wiederherstellung und Fehlerbehebung des verwalteten Servers

Integrated Dell™ Remote Access Controller Firmware Version 1.2-
Benutzerhandbuch

In diesem Abschnitt wird erklärt, wie Tasks mithilfe der iDRAC-Einrichtungen ausgeführt werden, die sich auf die Diagnose und die Fehlerbehebung eines im Remote-Zugriff verwalteten Servers beziehen. Er enthält die folgenden Unterabschnitte:

- Problemanzeigen - hilft Ihnen, Meldungen und andere Systemanzeigen zu finden, die zu einer Problemdiagnose führen können
- Hilfsprogramme zur Problemlösung - beschreibt iDRAC-Hilfsprogramme, die Sie zur Fehlerbehebung des Systems verwenden können
- Fehlerbehebung und häufig gestellte Fragen - Antworten zu typischen Situationen, denen Sie begegnen könnten

---

Sicherheit geht vor - für Sie und Ihr System

Um bestimmte Verfahren in diesem Abschnitt ausführen zu können, müssen Sie mit dem Gehäuse, dem PowerEdge-Server oder anderen Hardwaremodulen arbeiten. Versuchen Sie nicht, die Hardware des Systems zu warten, es sei denn, Sie befolgen die Erklärungen in diesem Handbuch und an anderer Stelle in Ihrer Systemdokumentation.

△ **VORSICHT: Viele Reparaturarbeiten dürfen nur von qualifizierten Servicetechnikern durchgeführt werden. Sie dürfen nur Fehlerbehebungsmaßnahmen ausführen und einfache Reparaturen vornehmen, wenn dies in Ihrer Produktdokumentation genehmigt ist oder wenn Sie online bzw. telefonisch von einem Service- und Support-Team entsprechende Anleitungen erhalten. Schäden infolge von Reparaturarbeiten, die nicht von Dell autorisiert sind, werden nicht von der Garantie abgedeckt. Lesen und befolgen Sie die zusammen mit dem Produkt gelieferten Sicherheitshinweise.**

Problemanzeigen

Die in diesem Abschnitt beschriebenen Anzeichen weisen darauf hin, dass im System ein Problem vorliegen könnte.

LED-Anzeigen

Das anfängliche Anzeichen eines Systemproblems könnte über die LEDs am Gehäuse oder an den im System installierten Komponenten angezeigt werden. Die folgenden Komponenten und Module besitzen Status-LEDs:

- Gehäuse-LCD-Anzeige
- Server
- Lüfter
- CMCs
- E/A-Module
- Netzteile

Die einzelne LED des Gehäuse-LCD fasst den Status aller Komponenten im System zusammen. Eine ständig leuchtende blaue LED des LCD zeigt an, dass auf dem System keine Fehlerzustände festgestellt wurden. Eine blinkende gelbe LED des LCD zeigt an, dass ein bzw. mehrere Fehlerzustände festgestellt wurden.

Wenn am Gehäuse-LCD eine gelbe LED blinkt, können Sie über das LCD-Menü herausfinden, welche Komponente fehlerhaft ist. Hilfe zur Verwendung des LCD finden Sie im *Dell CMC- Firmware-Benutzerhandbuch*.

Tabelle 14-1 beschreibt die Bedeutungen der LED-Anzeigen des PowerEdge-Servers:

Tabelle 14-1. Server-LED-Anzeigen

LED-Anzeige	Bedeutung
ständig grün	Der Server ist eingeschaltet. Ein Fehlen der grünen LED bedeutet, dass der Server nicht eingeschaltet ist.
ständig blau	Der iDRAC ist fehlerfrei.
blinkt gelb	Der iDRAC hat einen Fehlerzustand festgestellt oder aktualisiert gerade die Firmware.
blinkt blau	Ein Benutzer hat die Locator-ID für diesen Server aktiviert.

Anzeigen für Hardwareprobleme

Anzeichen dafür, dass bei einem Modul ein Hardwareproblem vorliegt, schließen folgende ein:

- Gerät kann nicht hochgefahren werden
- Laute Lüfter
- Verlust der Netzwerkkonnektivität
- Warnungen zu Batterie, Temperatur, Spannung oder Stromüberwachungssensor
- Festplattenfehler
- Fehler des USB-Datenträgers
- Physischer Schaden durch Fallenlassen, Wasser oder andere äußerliche Einwirkung

Sollte ein solches Problem auftreten, können Sie versuchen, es folgendermaßen zu beheben:

- Setzen Sie das Modul noch einmal ein und starten Sie es erneut
- Versuchen Sie, das Modul in einem anderen Schacht des Gehäuses einzusetzen
- Versuchen Sie, Festplatten oder USB-Schlüssel auszutauschen
- Schließen Sie die Strom- und Netzwerkkabel erneut an, oder tauschen Sie sie aus

Wenn das Problem mit diesen Schritten nicht behoben werden kann, ziehen Sie das *Hardware-Benutzerhandbuch* zurate, um spezifische Fehlerbehebungsinformationen für das Hardwaregerät zu erhalten.

Weitere Problemanzeigen

Tabelle 14-2. Problemanzeigen

Achten Sie auf Folgendes:	**Aktion:**
Warnmeldungen der Systemverwaltungssoftware	Weitere Informationen finden Sie in der Dokumentation zur Systemverwaltungssoftware.
Meldungen im Systemereignisprotokoll	Siehe Systemereignisprotokoll (SEL) überprüfen.
Meldungen der POST-Codes beim Start	Siehe POST-Codes überprüfen.
Meldungen auf dem Bildschirm Letzter Absturz	Siehe Bildschirm Letzter Systemabsturz anzeigen.
Alarmmeldungen auf dem Serverstatusbildschirm des LCD	Siehe Serverstatusbildschirm auf Fehlermeldungen überprüfen.
Meldungen im iDRAC-Protokoll	Siehe iDRAC-Protokoll anzeigen.

Hilfsprogramme zum Lösen von Problemen

In diesem Abschnitt werden iDRAC-Einrichtungen beschrieben, die Sie zur Diagnose von Problemen auf dem System verwenden können, besonders wenn Probleme im Remote-Zugriff gelöst werden sollen.

- Überprüfen des Systemzustands
- Systemereignisprotokoll auf Fehlermeldungen überprüfen
- POST-Codes überprüfen
- Bildschirm des letzten Systemabsturzes anzeigen
- Serverstatusbildschirm auf dem LCD auf Fehlermeldungen überprüfen
- iDRAC-Protokoll anzeigen
- Zugriff auf Systeminformationen
- Verwalteten Server im Gehäuse identifizieren
- Diagnosekonsole verwenden
- Netzstrom auf einem Remote-System verwalten

Überprüfen des Systemzustands

Wenn Sie sich an der iDRAC-Webschnittstelle anmelden, beschreibt die erste angezeigte Seite den Zustand der Systemkomponenten. Tabelle 14-3 beschreibt die Bedeutung der Systemzustandsanzeigen.

Tabelle 14-3. Systemzustandsanzeigen

Anzeige	Beschreibung
	Eine grüne Markierung zeigt eine gesunde (normale) Status-Bedingung an.
	Ein gelbes Dreieck, das ein Ausrufezeichen enthält, zeigt eine (nichtkritische) Warnungsstatus-Bedingung an.
	Ein rotes X zeigt eine kritische (Ausfall) Status-Bedingung an.
	Ein Fragezeichen-Symbol zeigt an, dass der Status unbekannt ist.

Klicken Sie auf der Seite **Funktionszustand** auf eine beliebige Komponente, um Informationen zur Komponente anzuzeigen. Sensormesswerte werden für Batterien, Temperaturen, Spannungen und Stromüberwachung angezeigt, was bei der Diagnose gewisser Problemtypen hilfreich ist. Die Informationsseiten zu iDRAC und CMC enthalten nützliche Informationen zu aktuellem Status und Konfiguration.

Systemereignisprotokoll (SEL) überprüfen

Auf der Seite **SEL-Protokoll** werden Meldungen zu Ereignissen angezeigt, die auf dem verwalteten Server auftreten.

Führen Sie zum Anzeigen des **Systemereignisprotokolls** folgende Schritte aus:

1. Klicken Sie auf **System** und dann auf das Register **Protokolle**.
2. Klicken Sie auf **Systemereignisprotokoll**, um die Seite **Systemereignisprotokoll** anzuzeigen.

   Die Seite **Systemereignisprotokoll** blendet eine Systemzustandsanzeige (siehe Tabelle 14-3), einen Zeitstempel sowie eine Beschreibung des Ereignisses ein.
3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Systemereignisprotokoll**, um fortzufahren (siehe Tabelle 14-4).

Tabelle 14-4. Schaltflächen der SEL-Seite

Schaltfläche	Maßnahme:
Drucken	Druckt **SEL in der Sortierreihenfolge, in der es im Fenster erscheint.**
Protokoll löschen	Löscht das **SEL**. **ANMERKUNG:** Die Schaltfläche **Protokoll löschen** erscheint nur, wenn Sie die Berechtigung **Protokolle löschen** besitzen.
Speichern unter	Öffnet ein Pop-Up-Fenster, das Ihnen ermöglicht, das **SEL** zu 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 herunter, die auf der Support-Website von Microsoft® unter support.microsoft.com verfügbar ist.
Aktualisieren	Lädt die Seite **SEL** hoch.

POST-Codes überprüfen

Die Seite **POST-Code** zeigt den letzten POST-Code des Systems vor dem Start des Betriebssystems an. POST-Codes zeigen den Fortschritt des System-BIOS an, kennzeichnen verschiedene Phasen der Startsequenz von Power-on-Reset und ermöglichen Ihnen, Fehler bezüglich des Systemstarts zu diagnostizieren.

ANMERKUNG: Den Text für die Nummern der POST-Code-Meldungen auf der LCD-Anzeige oder machen im *Hardwarebenutzerhandbuch* nachsehen.

Führen Sie zum Anzeigen der POST-Codes folgende Schritte aus:

1. Klicken Sie auf **System**, das Register **Protokolle** und dann auf **POST- Codes**.

   Die Seite **POST-Codes** blendet eine Systemzustandsanzeige (siehe Tabelle 14-3), einen Hexadezimalcode sowie eine Beschreibung des Codes ein.
2. Klicken Sie auf die entsprechende Schaltfläche der Seite **POST-Codes**, um fortzufahren (siehe Tabelle 14-5).

Tabelle 14-5. POST-Code-Schaltflächen

Schaltfläche	Maßnahme:
Drucken	Druckt die Seite **POST-Codes aus.**
Aktualisieren	Lädt die Seite **POST-Codes** neu.

Bildschirm Letzter Systemabsturz anzeigen

HINWEIS: Die Funktion Bildschirm Letzter Absturz muss in Server Administrator und in der iDRAC-Webschnittstelle konfiguriert werden. Anleitungen zum Konfigurieren dieser Funktion finden Sie unter Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz.

Auf der Seite **Bildschirm Letzter Absturz** wird der letzte Absturzbildschirm mit Informationen über die Ereignisse vor dem Systemabsturz angezeigt. Das Image des letzten Systemabsturzes ist im Dauerspeicher des iDRAC gespeichert und steht im Remote-Zugriff zur Verfügung.

Zur Ansicht der Seite **Bildschirm Letzter Absturz** führen Sie die folgenden Schritte aus:

- Klicken Sie auf **System**, das Register **Protokolle** und dann auf **Letzter Absturz**.

Die Seite **Bildschirm Letzter Absturz** führt die in Tabelle 14-6 gezeigten Schaltflächen auf:

ANMERKUNG: Die Schaltflächen **Speichern** und **Löschen** werden nicht angezeigt, wenn kein gespeicherter Absturzbildschirm vorhanden ist.

Tabelle 14-6. Schaltflächen der Seite Bildschirm Letzter Absturz

Schaltfläche	Maßnahme:
Drucken	Druckt die Seite **Bildschirm Letzter Absturz**.
Speichern	Öffnet ein Popup-Fenster, über das Sie die Seite **Bildschirm Letzter Absturz** in einem Verzeichnis Ihrer Wahl speichern können.
Löschen	Löscht die Seite **Bildschirm Letzter Absturz**.
Aktualisieren	Lädt die Seite **Bildschirm Letzter Absturz** neu.

ANMERKUNG: Aufgrund von Schwankungen im Zeitgeber für Autom. Wiederherstellung kann der **Bildschirm Letzter Absturz** eventuell nicht erfasst werden, wenn der System-Reset-Zeitgeber mit einem zu hohen Wert konfiguriert ist. Die Standardeinstellung ist 480 Sekunden. Stellen Sie den System-Reset-Zeitgeber mit dem Server Administrator oder IT Assistant auf 60 Sekunden ein und vergewissern Sie sich, dass der **Bildschirm Letzter Absturz** korrekt funktioniert. Weitere Informationen hierzu finden Sie unter Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz.

Die letzten Startsequenzen anzeigen"

Wenn Sie Startprobleme bemerken, können Sie sich die Bildschirmaktivität der Geschehnisse während der letzten drei Startsequenzen auf der Start-Capture-Seite ansehen. Die Wiedergabe der Startbildschirme tritt mit einer Rate von 1 Frame pro Sekunde auf. Tabelle 14-7 führt die verfügbaren Steuerungsmaßnahmen auf.

ANMERKUNG: Sie müssen über Administratorrechte verfügen, um die Wiedergabe der Start-Capture-Sequenzen anzuzeigen.

Tabelle 14-7. Start-Capture-Optionen

Schaltfläche/Option	Beschreibung
Startreihenfolge auswählen	Ermöglicht Ihnen, die Startreihenfolge zum Laden und Abspielen auszuwählen. - Start-Capture 1 - Lädt die letzte Startsequenz. - Start-Capture 2 - Lädt die (vorletzte) Startsequenz, die vor dem Start-Capture 1 aufgetreten ist. - Start-Capture 3 - Lädt die (drittletzte) Startsequenz, die vor dem Start-Capture 2 aufgetreten ist.
Speichern unter	Erstellt eine komprimierte .zip-Datei, die alle Start-Capture-Images der aktuellen Sequenz enthält. Der Benutzer muss über Administratorrechte verfügen, um diese Maßnahme durchzuführen.
Vorhergehender Bildschirm	Bringt Sie zum vorhergehenden Bildschirm, falls vorhanden, in der Wiedergabekonsole.
Wiedergabe	Startet die Bildschirmwiedergabe vom aktuellen Bildschirm in der Wiedergabekonsole.
Anhalten	Hält die Bildschirmwiedergabe auf dem aktuellen in der Wiedergabekonsole angezeigten Bildschirm an.
Beenden	Beendet die Bildschirmwiedergabe und lädt den ersten Bildschirm dieser Startsequenz.
Nächster Bildschirm	Bringt Sie zum nächsten Bildschirm, falls vorhanden, in der Wiedergabekonsole.
Drucken	Druckt das Start-Capture-Image, das auf dem Bildschirm eingeblendet wird.
Aktualisieren	Lädt die Start-Capture-Seite neu.

Serverstatusbildschirm auf Fehlermeldungen überprüfen

Wenn eine gelbe LED zu blinken beginnt und ein bestimmter Server einen Fehler aufweist, kennzeichnet der Hauptserverstatusbildschirm auf dem LCD den betroffenen Server in orange. Verwenden Sie die Navigationsschaltflächen des LCD, um den betroffenen Server zu kennzeichnen und klicken Sie dann auf die Schaltfläche in der Mitte. Fehler- und Warnmeldungen werden jetzt in der zweiten Zeile angezeigt. In der folgenden Tabelle werden alle Fehlermeldungen sowie die Schweregrade der Fehler aufgeführt.

Tabelle 14-8. Serverstatusbildschirm

Schweregrad	Meldung	Ursache
Warnung	Umgebungstemperatur der Systemplatine: Temperatursensor für Systemplatine, Warnungsereignis	Umgebungstemperatur des Servers hat eine Warnungsschwelle überschritten
Kritisch	Umgebungstemperatur der Systemplatine: Temperatursensor für Systemplatine, Fehlerereignis	Umgebungstemperatur des Servers hat eine Fehlerschwelle überschritten
Kritisch	CMOS-Batterie der Systemplatine: Batteriesensor der Systemplatine, Ausfall bestätigt	CMOS-Batterie nicht vorhanden oder weist keine Spannung auf
Warnung	Systemebene der Systemplatine: Stromsensor für Systemplatine, Warnungsereignis	Strom hat eine Warnungsschwelle überschritten
Kritisch	Systemebene der Systemplatine: Stromsensor für Systemplatine, Fehlerereignis	Strom hat eine Fehlerschwelle überschritten
Kritisch	CPU<Nummer> <Name des Spannungssensors>: Spannungssensor für CPU<Nummer>, bestätigter Zustand wurde bestätigt	Spannung außerhalb des Bereichs
Kritisch	Systemplatine <Name des Spannungssensors>: Spannungssensor für Systemplatine, bestätigter Zustand wurde bestätigt	Spannung außerhalb des Bereichs
Kritisch	CPU<Nummer> <Name des Spannungssensors>: Spannungssensor für CPU<Nummer>, bestätigter Zustand wurde bestätigt	Spannung außerhalb des Bereichs
Kritisch	CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, IERR wurde bestätigt	CPU-Fehler
Kritisch	CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, thermische Auslösung wurde bestätigt	CPU überhitzt
Kritisch	CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, Konfigurationsfehler wurde bestätigt	Falscher Prozessortyp oder an falschem Ort
Kritisch	CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, Bestätigung des Vorhandenseins wurde aufgehoben	Erforderliche CPU fehlt oder nicht vorhanden
Kritisch	Video-Riser-Karte der Systemplatine: Modulsensor der Systemplatine, Entfernen des Geräts wurde bestätigt	Erforderliches Modul wurde entfernt
Kritisch	Mezz B<Steckplatznummer> Status: Add-In-Kartensensor für Mezz B<Steckplatznummer>, Installationsfehler wurde bestätigt	Falsche Mezzaninkarte für E/A-Architektur installiert
Kritisch	Mezz C<Steckplatznummer> Status: Add-In-Kartensensor für Mezz C<Steckplatznummer>, Installationsfehler wurde bestätigt	Falsche Mezzaninkarte für E/A-Architektur installiert
Kritisch	Rückwandplatine, Laufwerk <Nummer>: Laufwerksteckplatzsensor für Rückwandplatine, Laufwerk entfernt	Speicherlaufwerk wurde entfernt
Kritisch	Rückwandplatine, Laufwerk <Nummer>: Laufwerksteckplatzsensor für Rückwandplatine, Laufwerkfehler wurde bestätigt	Speicherlaufwerk fehlerhaft
Kritisch	Systemplatine, PFault störsicher: Spannungssensor für Systemplatine, bestätigter Zustand wurde bestätigt	Dieses Ereignis wird erstellt, wenn sich die Systemplatinenspannungen nicht auf normalen Ebenen befinden.
Kritisch	Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, abgelaufener Zeitgeber wurde bestätigt	Der iDRAC-Watchdog-Zeitgeber ist abgelaufen und es wurde keine Maßnahme festgelegt.
Kritisch	Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, Neustart wurde bestätigt	Der iDRAC-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist), und die Maßnahme wurde auf Neustart festgelegt.
Kritisch	Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, Ausschalten des Stroms wurde bestätigt	Der iDRAC-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist), und die Maßnahme wurde auf Ausschalten des Stroms festgelegt.
Kritisch	Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, Aus- und Einschalten des Stroms wurde bestätigt	Der iDRAC-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist) und die Maßnahme wurde auf Aus- und Einschalten des Stroms festgelegt.
Kritisch	Systemplatinen-SEL: Ereignisprotokollsensor für Systemplatine, volles Protokoll wurde bestätigt	Das SEL-Gerät stellt fest, dass dem SEL nur ein Eintrag hinzugefügt werden kann, bevor es voll ist.
Warnung	ECC, korrigierbarer Fehler: Speichersensor, korrigierbarer ECC (<DIMM-Position>) wurde bestätigt	Korrigierbare ECC-Fehler haben eine kritische Rate erreicht.
Kritisch	ECC, nicht korrigierbarer Fehler: Speichersensor, nicht korrigierbarer ECC (<DIMM-Position>) wurde bestätigt	Ein nicht korrigierbarer ECC-Fehler wurde festgestellt.
Kritisch	E/A-Kanalüberprüfung: Sensor für kritische Ereignisse, E/A-Kanalüberprüfungs-NMI wurde bestätigt	Im E/A-Kanal wird ein kritischer Interrupt erstellt.
Kritisch	PCI-Paritätsfehler: Sensor für kritische Ereignisse, PCI PERR wurde bestätigt	Auf dem PCI-Bus wurde ein Paritätsfehler festgestellt.
Kritisch	PCI-Systemfehler: Sensor für kritische Ereignisse, PCI SERR (<Steckplatznummer oder PCI-Geräte-ID>) wurde bestätigt	PCI-Fehler durch Gerät festgestellt
Kritisch	SBE-Protokoll deaktiviert: Ereignisprotokollsensor, Deaktivierung der Protokollierung korrigierbarer Speicherfehler wurde bestätigt	Einzelbitfehler-Protokollierung wird deaktiviert, wenn zu viele SBE protokolliert werden
Kritisch	Protokollierung deaktiviert: Ereignisprotokollsensor, Deaktivierung der gesamten Ereignisprotokollierung wurde bestätigt	Die gesamte Fehlerprotokollierung ist deaktiviert

Nicht wiederherstellbar	CPU-Protokollfehler: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt	Das Prozessorprotokoll ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht wiederherstellbar	CPU-Bus-PERR: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt	Der Prozessor-Bus-PERR ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht wiederherstellbar	CPU-Initialisierungsfehler: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt	Die Prozessorinitialisierung ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht wiederherstellbar	CPU-Maschinenüberprüfung: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt	Die Prozessormaschinenüberprüfung ist in einen nicht wiederherstellbaren Zustand übergegangen.
Kritisch	Speicher reserviert: Speichersensor, Redundanz verloren (<DIMM-Position>) wurde bestätigt	Speicherreserve ist nicht mehr redundant.
Kritisch	Speicher gespiegelt: Speichersensor, Redundanz verloren (<DIMM-Position>) wurde bestätigt	Gespiegelter Speicher ist nicht mehr redundant.
Kritisch	Speicher-RAID: Speichersensor, Redundanz verloren (<DIMM-Position>) wurde bestätigt	RAID-Speicher ist nicht mehr redundant
Warnung	Speicher hinzugefügt: Speichersensor, Bestätigung des Vorhandenseins (<DIMM-Position>) wurde aufgehoben	Hinzugefügtes Speichermodul wurde entfernt.
Warnung	Speicher entfernt: Speichersensor, Bestätigung des Vorhandenseins (<DIMM-Position>) wurde aufgehoben	Speichermodul wurde entfernt.
Kritisch	Speicherkonfigurationsfehler: Speichersensor, Konfigurationsfehler (<DIMM-Position>) wurde bestätigt	Speicherkonfiguration für das System ist falsch.
Warnung	Speicherredundanz-Zunahme: Speichersensor, Redundanz herabgesetzt (<DIMM-Position>) wurde bestätigt	Speicherredundanz ist herabgesetzt aber nicht verloren
Kritisch	Schwerwiegender PCIE-Fehler: Sensor für kritische Ereignisse, schwerwiegender Busfehler wurde bestätigt	Schwerwiegender Fehler auf dem PCIE-Bus festgestellt.
Kritisch	Chipset-Fehler: Sensor für kritische Ereignisse, PCI-PERR wurde bestätigt	Chip-Fehler wurde festgestellt.
Warnung	Speicher-ECC-Warnung: Speichersensor, Übergang zu nicht kritisch von OK (<DIMM-Position>) wurde bestätigt	Die Rate der korrigierbaren ECC-Fehler gehen über eine normale Rate hinaus.
Kritisch	Speicher-ECC-Warnung: Speichersensor, Übergang zu kritisch von weniger schwer (<DIMM-Position>) wurde bestätigt	Korrigierbare ECC-Fehler haben kritische Rate erreicht.
Kritisch	POST-Fehler: POST-Sensor, Kein Speicher installiert	Kein Speicher auf Platine festgestellt
Kritisch	POST-Fehler: POST-Sensor, Speicherkonfigurationsfehler	Speicher wurde erkannt, kann jedoch nicht konfiguriert werden.
Kritisch	POST-Fehler: POST-Sensor, Fehler durch unbrauchbaren Speicher	Speicher wurde konfiguriert, ist jedoch unbrauchbar.
Kritisch	POST-Fehler: POST-Sensor, Shadow-BIOS fehlerhaft	System-BIOS, Shadow-Fehler
Kritisch	POST-Fehler: POST-Sensor, CMOS fehlerhaft	CMOS-Fehler
Kritisch	POST-Fehler: POST-Sensor, DMA-Controller fehlerhaft	DMA-Controller-Fehler
Kritisch	POST-Fehler: POST-Sensor, Interrupt-Controller fehlerhaft	Interrupt-Controller-Fehler
Kritisch	POST-Fehler: POST-Sensor, Zeitgeberaktualisierung fehlerhaft	Fehler bei der Zeitgeberaktualisierung
Kritisch	POST-Fehler: POST-Sensor, Fehler bei programmierbarem Intervallzeitgeber	Fehler beim programmierbaren Intervallzeitgeber
Kritisch	POST-Fehler: POST-Sensor, Paritätsfehler	Paritätsfehler
Kritisch	POST-Fehler: POST-Sensor, SIO fehlerhaft	SIO-Fehler
Kritisch	POST-Fehler: POST-Sensor, Tastatur-Controller fehlerhaft	Tastatur-Controllerfehler
Kritisch	POST-Fehler: POST-Sensor, Interrupt-Initialisierung der Systemverwaltung fehlerhaft	Initialisierungsfehler bei Systemverwaltungs-Interrupt
Kritisch	POST-Fehler: POST-Sensor, Test zum Herunterfahren des BIOS fehlerhaft	Fehler beim BIOS-Herunterfahren-Test
Kritisch	POST-Fehler: POST-Sensor, BIOS-POST-Speichertest fehlerhaft	BIOS-POST-Speicherüberprüfungsfehler
Kritisch	POST-Fehler: POST-Sensor, Konfiguration des Dell Remote Access Controller fehlerhaft	Konfigurationsfehler bei Dell Remote Access Controller
Kritisch	POST-Fehler: POST-Sensor, CPU-Konfiguration fehlerhaft	CPU-Konfigurationsfehler
Kritisch	POST-Fehler: POST-Sensor, Falsche Speicherkonfiguration	Falsche Speicherkonfiguration
Kritisch	POST-Fehler: POST-Sensor, POST-Fehler	Allgemeiner Fehler nach Video
Kritisch	Hardwareversions-Fehler: Sensor für Versionsänderung, Hardware-Inkompatibilität wurde bestätigt	Inkompatible Hardware wurde festgestellt
Kritisch	Hardwareversions-Fehler: Sensor für Versionsänderung, Hardware-Inkompatibilität (BMC-Firmware) wurde bestätigt	Hardware ist inkompatibel mit Firmware
Kritisch	Hardwareversions-Fehler: Sensor für Versionsänderung, Hardware-Inkompatibilität (BMC-Firmware und CPU-Übereinstimmungsfehler) wurde bestätigt	CPU und Firmware nicht kompatibel
Kritisch	Speicherübertemperatur: Speichersensor, korrigierbarer ECC <DIMM-Position> wurde bestätigt	Überhitzung des Speichermoduls
Kritisch	Speicher, SB-CRC schwerwiegend: Speichersensor, nicht korrigierbarer ECC wurde bestätigt	Southbridge-Speicher fehlerhaft
Kritisch	Speicher, NB-CRC schwerwiegend: Speichersensor, nicht korrigierbarer ECC wurde bestätigt	Northbridge-Speicher fehlerhaft

Kritisch	Watchdog-Zeitgeber: Watchdog-Sensor, Neustart wurde bestätigt	Watchdog-Zeitgeber verursachte Systemneustart
Kritisch	Watchdog-Zeitgeber: Watchdog-Sensor, Ablaufen des Zeitgebers wurde bestätigt	Watchdog-Zeitgeber abgelaufen, jedoch keine Maßnahme ergriffen
Warnung	Link-Tuning: Sensor für Versionsänderung, Bestätigung der erfolgreichen Software- oder F/W-Änderung wurde aufgehoben	Link-Tuning-Einstellung für ordnungsgemäßen NIC-Betrieb konnte nicht aktualisiert werden
Warnung	Link-Tuning: Sensor für Versionsänderung, Bestätigung der erfolgreichen Hardwareänderung <Gerätesteckplatznummer> wurde aufgehoben	Link-Tuning-Einstellung für ordnungsgemäßen NIC-Betrieb konnte nicht aktualisiert werden
Kritisch	Link-T/Flex-Adr: Link-Tuning-Sensor, Bestätigung, dass die virtuelle MAC-Adresse (Bus-Nr. Geräte-Nr. Funktions-Nr.) nicht programmiert werden konnte	Flex-Adresse konnte für dieses Gerät nicht programmiert werden
Kritisch	Link-T/Flex-Adr: Link-Tuning-Sensor, Bestätigung, dass Geräte-Options-ROM Link-Tuning oder Flex-Adresse (Mezz <Position>) nicht unterstützen konnte	Options-ROM unterstützt Flex-Adresse oder Link-Tuning nicht
Kritisch	Link-T/Flex-Adr: Link-Tuning-Sensor, Bestätigung, dass Daten zu Link-Tuning oder Flex-Adresse nicht vom BMC/iDRAC abgerufen werden konnten	Informationen zu Link-Tuning oder Flex-Adresse konnten nicht vom BMC/iDRAC abgerufen werden
Kritisch	Link-T/Flex-Adr: Link-Tuning-Sensor, Bestätigung, dass Geräte-Options-ROM Link-Tuning oder Flex-Adresse (Mezz <Position>) nicht unterstützen konnte	Diese Ereignis wird erstellt, wenn PCI-Geräte-Options-ROM für einen NIC weder die Link-Tuning- noch die Flex-Adresse-Funktion unterstützt.
Kritisch	LinkT/FlexAddr: Link-Tuning-Sensor, Bestätigung, dass die virtuelle MAC-Adresse (<Position>) nicht programmiert werden konnte	Dieses Ereignis wird erstellt, wenn das BIOS die virtuelle MAC-Adresse, die auf dem NIC-Gerät vorgegeben ist, nicht programmieren kann.
Kritisch	I/O Fatal Err: Unbehebbarer E/A-Gruppensensor, unbehebbarer E/A-Fehler (<Position>)	Dieses Ereignis wird in Verbindung mit einem CPU-IERR erstellt und zeigt an, welches Gerät diesen CPU-IERR verursacht hat.
Warnung	PCIE NonFatal Er: Behebbarer E/A-Gruppensensor, PCIe-Fehler (<Position>)	Dieses Ereignis wird in Verbindung mit einem CPU-IERR erstellt.

iDRAC-Protokoll anzeigen

Das **iDRAC-Protokoll** ist ein beständiges Protokoll, das in der iDRAC-Firmware geführt wird. Das Protokoll enthält eine Liste von Benutzermaßnahmen (wie z. B. An- und Abmelden, Änderungen der Sicherheitsregeln) und Warnungen, die vom iDRAC ausgegeben werden. Die ältesten Einträge werden überschrieben, wenn das Protokoll voll wird.

Während das **Systemereignisprotokoll** (SEL) Einträge von Ereignissen enthält, die auf dem verwalteten Server auftreten, enthält das **iDRAC-Protokoll** Einträge von Ereignissen, die im iDRAC auftreten.

Führen Sie zum Zugriff auf das **iDRAC**-Protokoll folgende Schritte aus:

- Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf **iDRAC-Protokoll**.

Das **iDRAC-Protokoll** stellt die in Tabelle 14-9 aufgeführten Informationen zur Verfügung.

Tabelle 14-9. Informationen der iDRAC-Protokollseite

Feld	Beschreibung
Uhrzeit/Datum	Datum und Uhrzeit (z. B. 19. Dez. 16:55:47). Der iDRAC stellt seine Uhr nach der Uhr des verwalteten Servers. Wenn der iDRAC beim anfänglichen Start nicht mit dem verwalteten Server kommunizieren kann, wird die Zeit als die Zeichenkette Systemstart angezeigt.
Source	Die Schnittstelle, die das Ereignis verursacht hat.
Beschreibung	Eine kurze Beschreibung des Ereignisses und der Name des Benutzers, der sich am iDRAC angemeldet hat.

Verwendung der Schaltflächen auf der iDRAC-Anmeldeseite

Die Seite **iDRAC-Protokoll** enthält folgende Schaltflächen (siehe Tabelle 14-10).

Tabelle 14-10. 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** wird nur angezeigt, wenn Sie über die Berechtigung **Protokolle löschen** verfügen.
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 herunter, die auf der Support-Website von Microsoft unter **support.microsoft.com** verfügbar ist.
Aktualisieren	Lädt die Seite **iDRAC-Protokoll** neu.

Systeminformationen anzeigen

Die Seite **Systemzusammenfassung** enthält Informationen über die folgenden Systemkomponenten:

- Hauptsystemgehäuse
- Integrierter Dell Remote Access Controller

Klicken Sie zum Zugreifen auf die Systeminformationen auf **System→ Eigenschaften**.

Hauptsystemgehäuse

Tabelle 14-11 und Tabelle 14-12 beschreiben die Eigenschaften des Hauptsystemgehäuses.

Tabelle 14-11. Systeminformationsfelder

Feld	Beschreibung
Beschreibung	Gibt eine Systembeschreibung.
BIOS-Version	Führt die System-BIOS-Version auf.
Service-Kennnummer	Führt die Service-Tag-Nummer des Systems an.
Host-Name	Stellt den Namen des Host-Systems zur Verfügung.
Betriebssystemname	Führt das auf dem System ausgeführte Betriebssystem an.

Tabelle 14-12. Felder der Autom. Wiederherstellung

Feld	Beschreibung
Wiederherstellungsmaßnahme	Wenn festgestellt wird, dass das *System hängt*, kann der iDRAC zum Ausführen der folgenden Maßnahmen konfiguriert werden: **Keine Maßnahme**, **Hardware-Reset**, **Herunterfahren** oder **Aus- und einschalten**.
Anfänglicher Countdown	Die Anzahl der Sekunden nach Feststellung eines *hängenden Systems*, nach denen der iDRAC eine Wiederherstellungsmaßnahme ausführt.
Vorhandener Countdown	Der aktuelle Wert, in Sekunden, des Countdown-Zeitgebers.

Integrierter Dell Remote Access Controller

Tabelle 14-13 beschreibt die iDRAC-Eigenschaften.

Tabelle 14-13. iDRAC-Informationsfelder

Feld	Beschreibung
Uhrzeit/Datum	Zeigt das aktuelle Datum bzw. die aktuelle Uhrzeit auf dem iDRAC in MGZ an.
Firmware-Version	Führt die Version der iDRAC-Firmware an.
Aktualisierte Firmware	Führt das Datum der letzten Firmware-Aktualisierung auf. Das Datum wird im UTC-Format angezeigt, z. B.: Tue, 8 May 2007, 22:18:21 UTC.
IP-Adresse	Die 32-Bit-Adresse, die die Netzwerkschnittstelle identifiziert. Der Wert wird im *Punkttrennungs*-Format angezeigt, z. B. 143.166.154.127.
Gateway	Die IP-Adresse des Gateways, die als Brücke zu anderen Netzwerken dient. Dieser Wert wird im *Punkttrennungs*-Format angegeben, z. B. 143.166.150.5.
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.
MAC-Adresse	Die MAC-Adresse (Medienzugriffssteuerung), die jede NIC im Netzwerk eindeutig identifiziert, z. B. 00-00-0c-ac-08. Hierbei handelt es sich um eine von Dell zugewiesene ID, die nicht bearbeitet werden kann.
DHCP aktiviert	**Aktiviert** weist darauf hin, dass das dynamische Host-Konfigurationsprotokoll (DHCP) aktiviert ist. **Deaktiviert** weist darauf hin, dass DHCP *nicht* aktiviert ist.

Verwalteten Server im Gehäuse identifizieren

In das PowerEdge M1000e-Gehäuse können bis zu 16 Server eingebaut werden. Um einen bestimmten Server im Gehäuse aufzufinden, können Sie die iDRAC-Webschnittstelle verwenden, um auf dem Server eine blaue, blinkende LED einzuschalten. Wenn Sie die LED einschalten, können Sie die Anzahl von Sekunden festlegen, während denen die LED blinken soll, um sicherzustellen, dass Sie das Gehäuse erreichen können, während die LED noch blinkt. Durch die Eingabe von 0 blinkt die LED so lange weiter, bis Sie sie deaktivieren.

Führen Sie zum Identifizieren des Servers Folgendes aus:

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC**→ **Störungen beheben**.
2. Markieren Sie auf der Seite **Identifizieren** das Wertekästchen neben **Server identifizieren**.
3. Geben Sie im Feld **Server-Zeitüberschreitung identifizieren** die Anzahl von Sekunden ein, während denen die LED blinken soll. Geben Sie 0 ein, wenn die LED so lange blinken soll, bis Sie sie deaktivieren.
4. Klicken Sie auf **Anwenden**.

Eine blaue LED auf dem Server wird während der festgelegten Anzahl von Sekunden blinken.

Wenn Sie 0 eingegeben haben, damit die LED weiterblinkt, führen Sie die folgenden Schritte aus, um Sie zu deaktivieren:

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC**→ **Störungen beheben**.
2. Heben Sie auf der Seite **Identifizieren** die Markierung des Wertekästchens neben **Server identifizieren** auf.
3. Klicken Sie auf **Anwenden**.

Diagnosekonsole verwenden

Der iDRAC bietet einen Standardsatz von Netzwerkdiagnose-Hilfsprogrammen (siehe Tabelle 14-14), die den mit Microsoft® Windows®- oder Linux-basierten Systemen gelieferten Hilfsprogrammen ähnlich sind. Mit der iDRAC-Webschnittstelle können Sie auf die Hilfsprogramme zum Netzwerk-Debuggen zugreifen.

Führen Sie zum Zugriff auf die Seite **Diagnosekonsole** folgende Schritte aus:

1. Klicken Sie auf **System**→ **iDRAC**→ **Störungen beheben**.
2. Klicken Sie auf das Register **Diagnose**.

Tabelle 14-14 beschreibt die Befehle, die auf der Seite **Diagnosekonsole** eingegeben werden können. Geben Sie einen Befehl ein und klicken Sie auf **Senden**. Die Debug-Ergebnisse werden auf der Seite **Diagnosekonsole** angezeigt.

Klicken Sie auf die Schaltfläche **Löschen**, um die durch den vorhergehenden Befehl angezeigten Ergebnisse zu löschen.

Zum Aktualisieren der Seite **Diagnosekonsole** klicken Sie auf **Aktualisieren**.

Tabelle 14-14. 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 Netzschnittstellentabelle an.
netstat	Druckt den Inhalt der Routingtabelle aus.
ping *<IP-Adresse>*	Überprüft, ob die Ziel-IP-Adresse unter Verwendung des Inhalts der aktuellen Routing-Tabelle vom iDRAC aus erreichbar ist. Im Feld rechts von dieser Option muss eine Ziel-IP-Adresse eingegeben werden. Ein ICMP-Echo-Paket (Internetsteuerungsmeldungsprotokoll) wird basierend auf dem aktuellen Inhalt der Routingtabelle zur Ziel-IP-Adresse gesendet.
gettracelog	Zeigt das Ablaufverfolgungsprotokoll des iDRAC an. Weitere Informationen finden Sie unter gettracelog.

Netzstrom auf einem Remote-System verwalten

Mit dem iDRAC können im Remote-Zugriff mehrere Stromverwaltungsmaßnahmen auf dem verwalteten Server durchgeführt werden. Verwenden Sie die Seite Stromverwaltung, um während eines Neustarts und beim System-Ein- und Ausschalten ein ordentliches Herunterfahren durch das Betriebssystem durchzuführen.

ANMERKUNG: Sie müssen über die Berechtigung **Server-Maßnahmenbefehle ausführen** verfügen, um Stromverwaltungsmaßnahmen ausführen zu können. Unter iDRAC-Benutzer hinzufügen und konfigurieren finden Sie Hilfeanleitungen zum Konfigurieren von Benutzerberechtigungen.

1. Klicken Sie auf **System** und dann auf das Register **Stromverwaltung**.

2. Wählen Sie eine **Stromsteuerungsmaßnahme** aus, z. B. **System zurücksetzen (Softwareneustart)**.

   Tabelle 14-15 bietet Informationen zu Stromregelungsmaßnahmen

3. Klicken Sie auf **Anwenden**, um die ausgewählte Maßnahme auszuführen.

4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 14-16.

Tabelle 14-15. Stromsteuerungsmaßnahmen

System einschalten	Schaltet den Systemstrom ein (äquivalent zum Drücken des Netzschalters, wenn der Serverstrom ausgeschaltet ist).
System ausschalten	Schaltet den Systemstrom ein (äquivalent zum Drücken des Netzschalters, wenn der Serverstrom eingeschaltet ist).
NMI (nicht-maskierbarer Interrupt)	Sendet einen Interrupt hoher Stufe ans Betriebssystem, was dazu führt, dass das System den Vorgang unterbricht, um kritische Diagnose- und Fehlerbehebungsaktivitäten zu ermöglichen.
Ordentliches Herunterfahren	Versucht, das Betriebssystem ordentlich herunterzufahren und schaltet dann das System aus. Hierfür ist ein ACPI-abhängiges Betriebssystem (Advanced Configuration and Power Interface) erforderlich, das systemgesteuerte Stromverwaltung ermöglicht.
System zurücksetzen (Softwareneustart)	Startet das System neu, ohne es auszuschalten (Softwareneustart).
System aus- und wieder einschalten (Power Cycle)	Schaltet das System aus und startet es dann neu (Hardwareneustart).

Tabelle 14-16. Schaltflächen der Stromverwaltungs-Seite

Schaltfläche	**Maßnahme:**
Drucken	Druckt die Werte der **Stromverwaltung** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Stromverwaltung** erneut.
Anwenden	Speichert alle neuen Einstellungen, die Sie bei der Betrachtung der Seite Stromverwaltung vornehmen.

Fehlerbehebung und häufig gestellte Fragen

Tabelle 14-17 enthält häufig gestellte Fragen zu Problemen bei der Störungsbehebung.

Tabelle 14-17. Häufig gestellte Fragen/Störungsbehebung

Frage	**Antwort**
Die LED auf dem Server blinkt gelb.	Überprüfen Sie das SEL auf Meldungen und löschen Sie das SEL dann, um die blinkende LED zu stoppen. Von der iDRAC-Webschnittstelle: • Siehe Systemereignisprotokoll (SEL) überprüfen Vom SM-CLP: • Siehe SEL-Verwaltung Vom iDRAC-Konfigurationshilfsprogramm: • Siehe Menü des Systemereignisprotokolls
Auf dem Server ist eine blaue blinkende LED.	Ein Benutzer hat die Locator-ID für den Server aktiviert. Dies ist ein Signal, das zum Identifizieren des Servers im Gehäuse behilflich ist. Informationen zu dieser Funktion finden Sie unter Verwalteten Server im Gehäuse identifizieren.
Wie kann ich die IP-Adresse des iDRAC finden?	Von der CMC-Webschnittstelle: 1. Klicken Sie auf **Gehäuse**→ **Server** und dann auf das Register **Setup**. 2. Klicken Sie auf **Bereitstellen**. 3. Lesen Sie die IP-Adresse für Ihren Server aus der angezeigten Tabelle ab. Von der iKVM: • Starten Sie den Server neu und geben Sie das iDRAC-Konfigurationshilfsprogramm durch Drücken auf <Strg><E> ein ODER • Warten Sie darauf, dass die IP-Adresse während des BIOS-POST angezeigt wird. ODER • Wählen Sie im OSCAR die "Dell CMC"-Konsole aus, um sich über eine lokale serielle

	Verbindung am CMC anzumelden. CMC-RACADM-Befehle können über diese Verbindung ausgegeben werden. Eine vollständige Liste der CMC-RACADM-Unterbefehle finden Sie im *CMC Firmware-Benutzerhandbuch*.
Wie kann ich die IP-Adresse des iDRAC finden? *(Fortsetzung)*	Zum Beispiel: $ racadm getniccfg -m server-1 DHCP Aktiviert = 1 IP-Adresse = 192.168.0.1 Subnetzmaske = 255.255.255.0 Gateway = 192.168.0.1 Von lokalem RACADM: 1. Geben Sie den folgenden Befehl an einer Eingabeaufforderung ein: racadm getsysinfo Vom LCD: 1. Markieren Sie im Hauptmenü das Element **Server** und drücken Sie auf die Schaltfläche mit dem Häkchen. 2. Wählen Sie den Server aus, dessen IP-Adresse Sie suchen und drücken Sie auf die Schaltfläche mit dem Häkchen.
Wie kann ich die IP-Adresse des CMC finden?	Von der iDRAC-Webschnittstelle: - Klicken Sie auf **System**→ **Remote-Zugriff**→ **CMC**. Die CMC-IP-Adresse wird auf der Seite **Zusammenfassung** angezeigt. ODER - Wählen Sie im OSCAR die "Dell CMC"-Konsole aus, um sich über eine lokale serielle Verbindung am CMC anzumelden. CMC-RACADM-Befehle können über diese Verbindung ausgegeben werden. Eine vollständige Liste der CMC-RACADM-Unterbefehle finden Sie im *CMC Firmware-Benutzerhandbuch*. $ racadm getniccfg -m chassis NIC Aktiviert = 1 DHCP Aktiviert = 1 Statische IP-Adresse = 192.168.0.120 Statische Subnetzmaske = 255.255.255.0 Statisches Gateway = 192.168.0.1 Aktuelle IP-Adresse = 10.35.155.151 Aktuelle Subnetzmaske = 255.255.255.0 Aktuelles Gateway = 10.35.155.1 Geschwindigkeit = Automatische Aushandlung Duplex = Automatische Aushandlung
Die iDRAC-Netzwerkverbindung funktioniert nicht.	- Stellen Sie sicher, dass das LAN-Kabel am CMC angeschlossen ist. - Stellen Sie sicher, dass das iDRAC-LAN aktiviert ist.
Ich habe den Server in das Gehäuse eingesetzt und den Netzschalter gedrückt, aber nichts ist passiert.	- Der iDRAC braucht etwa 30 Sekunden, um initialisiert zu werden, bevor der Server hochfahren kann. Warten Sie 30 Sekunden und drücken Sie dann den Netzschalter noch einmal. - Überprüfen Sie das Strombudget des CMC. Das Strombudget für das Gehäuse wurde möglicherweise überschritten.
Ich habe den Benutzernamen und das Kennwort für den iDRAC-Administrator vergessen.	Sie müssen den iDRAC auf seine Standardeinstellungen wiederherstellen. 1. Starten Sie den Server neu und drücken Sie auf <Strg><E>, wenn Sie zur Eingabe des iDRAC-Konfigurationshilfsprogramms aufgefordert werden. 2. Markieren Sie im Menü des Konfigurationshilfsprogramms **Auf Standardeinstellung zurücksetzen** und drücken Sie auf <Eingabe>. Weitere Informationen finden Sie unter Auf Standardeinstellung zurücksetzen.
Wie kann ich den Namen des Steckplatzes für meinen Server ändern?	1. Melden Sie sich bei der CMC-Webschnittstelle an. 2. Öffnen Sie die **Gehäuse**struktur und klicken Sie auf **Server**. 3. Klicken Sie auf das Register **Setup**. 4. Geben Sie den neuen Namen für den Steckplatz in die Zeile für den Server ein. 5. Klicken Sie auf **Anwenden**.
Wenn eine Konsolenumleitungssitzung von der iDRAC-Webschnittstelle aus gestartet wird, wird ein ActiveX-Sicherheits-Popup eingeblendet.	Der iDRAC ist möglicherweise keine vertrauenswürdige Site für den Client-Browser. Um zu verhindern, dass jedes Mal, wenn Sie eine Konsolenumleitungssitzung beginnen, ein Sicherheits-Popup eingeblendet wird, fügen Sie den iDRAC einfach der Liste vertrauenswürdiger Sites hinzu: 1. Klicken Sie auf **Extras**→ **Internetoptionen...**→ **Sicherheit**→ **Vertrauenswürdige Sites**. 2. Klicken Sie auf **Sites**, und geben Sie die IP-Adresse oder den DNS-Namen des iDRAC ein. 3. Klicken Sie auf **Hinzufügen**.
Wenn ich eine Konsolenumleitungssitzung starte, ist der Viewer-Bildschirm leer.	Wenn Sie die Berechtigung **Virtueller Datenträger** besitzen, jedoch nicht die Berechtigung **Konsolenumleitung,** können Sie den Viewer starten und so auf die Funktion des virtuellen Datenträgers zugreifen. Jedoch wird hierbei die Konsole des verwalteten Servers nicht angezeigt.

Der iDRAC startet nicht.	Enfernen Sie den Server und setzen Sie ihn erneut ein. Überprüfen Sie die CMC-Webschnittstelle, um zu sehen, ob der iDRAC als aktualisierbare Komponente erscheint. Ist dies der Fall, befolgen Sie die Anleitungen unter iDRAC-Firmware mittels CMC wiederherstellen. Wird das Problem hierdurch nicht gelöst, setzen Sie sich mit dem technischen Support in Verbindung.
Beim Versuch, den verwalteten Server zu starten, ist die Betriebsanzeige grün, aber es ist überhaupt kein POST bzw. kein Video vorhanden.	Dies kann eintreten, wenn beliebige der folgenden Zustände zutreffen: • Speicher ist nicht installiert oder ist unzugänglich. • Die CPU ist nicht installiert oder ist unzugänglich. • Die Video-Riser-Karte fehlt oder ist falsch verbunden. Sehen Sie außerdem nach Fehlermeldungen im iDRAC-Protokoll, von der iDRAC-Webschnittstelle oder vom LCD.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Glossar

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Active Directory

Active Directory ist ein zentralisiertes, standardisiertes System zur Automatisierung der Netzwerkverwaltung von Benutzerdaten, Sicherheit und verteilten Ressourcen und macht die Zusammenarbeit mit anderen Verzeichnissen möglich. Active Directory richtet sich speziell auf dezentrale Netzwerkumgebungen aus.

ARP

Akronym für Address Resolution Protocol (Adressenauflösungsprotokoll). Eine Methode, die Ethernet-Adresse eines Hosts aus seiner Internet-Adresse zu ermitteln.

ASCII

Akronym für American Standard Code for Information Interchange (US-Standardcode für Informationsaustausch). Eine Codedarstellung zur Anzeige oder zum Drucken von Buchstaben, Zahlen und anderen Zeichen.

BIOS

Akronym für Basic Input/Output System (Grundlegendes Eingabe-/Ausgabesystem). Der Teil der Systemsoftware, der die Schnittstelle unterster Ebene zu Peripheriegeräten darstellt und der die erste Stufe des Systemstartprozesses steuert, einschließlich des Ladens des Betriebssystems in den Speicher.

Bus

Eine Reihe von Leitern, über die verschiedene Funktionseinheiten in einem Computer verbunden sind. Busse werden nach der Art der transportierten Daten benannt, wie z. B. Datenbus, Adressbus oder PCI-Bus.

CA

Eine Zertifizierungsstelle ist ein Geschäftsunternehmen, das in der IT-Industrie dafür anerkannt ist, hohe Standards der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger Sicherheitskriterien einzuhalten. Beispiele von CAs schließen Thawte und VeriSign ein. 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.

CD

Abkürzung für Compact Disc.

CHAP

Akronym für Challenge Handshake Authentication Protocol (Challenge Handshake-Authentifizierungsprotokoll), wobei es sich um eine Authentifizierungsmethode handelt, die von PPP-Servern zur Überprüfung der Identität des Herstellers einer Verbindung verwendet wird.

CIM

Akronym für das Allgemeine Informationsmodell, das ein für das Verwalten von Betriebssystemen auf einem Netzwerk bestimmtes Protokolle ist.

CLI

Abkürzung für Command-Line Interface (Befehlszeilenoberfläche).

CLP

Abkürzung für Command-Line Protocol (Befehlszeilenprotokoll).

CSR

Abkürzung für Certificate Signing Request (Zertifikatssignierungsanforderung).

DDNS

Abkürzung für Dynamic Domain Name System (Dynamisches Domänennamenssystem).

DHCP

Abkürzung für Dynamic Host Configuration Protocol (Dynamisches Host-Konfigurationsprotokoll), wobei es sich um ein Protokoll handelt, mit dem IP-Adressen für Computer in einem lokalen Netzwerk dynamisch zugewiesen werden können.

DLL

Abkürzung für Dynamic Link Library (Dynamische Bibliothek). Eine Bibliothek von kleinen Programmen, die beliebig aufgerufen werden können, wenn sie von einem größeren Programm benötigt werden, das auf dem System ausgeführt wird. Das kleine Programm, das das größere Programm mit einem spezifischen Gerät wie einem Drucker oder Scanner kommunizieren lässt, wird oft als ein DLL-Programm (oder eine DLL-Datei) präsentiert.

DMTF

Abkürzung für Distributed Management Task Force.

DNS

Abkürzung für Domain Name System (Domänennamenssystem).

DSU

Abkürzung für Disk Storage Unit (Festplattenspeichereinheit).

erweitertes Schema

Eine mit Active Directory verwendete Lösung zum Bestimmen von Benutzerzugriffen auf den iDRAC 6; verwendet Dell-definierte Active Directory-Objekte.

FQDN

Akronym für Fully Qualified Domain Names (Vollständig qualifizierte Domänennamen). Microsoft® Active Directory® unterstützt nur FQDN mit 64 Byte oder weniger.

FSMO

Flexible Single Master Operation (Flexibler einzelner übergeordneter Vorgang). Dies ist die Art und Weise von Microsoft, die Atomarität des Erweiterungsvorgangs zu garantieren.

GMT

Abkürzung für Greenwich Mean Time (Mittlere Greenwich-Zeit). Standarduhrzeit an jedem Ort der Welt. GMT ist normalerweise die mittlere Sonnenzeit entlang des Nullmeridians (0-Längengrad), der durch das Greenwich Observatory außerhalb von London, Großbritannien, verläuft.

GPIO

Abkürzung für General Purpose Input/Output (Allgemeine Eingabe/Ausgabe).

GRUB

Akronym für GRand Unified Bootloader, ein neuer und allgemein verwendeter Linux-Lader.

GUI

Abkürzung für Graphical User Interface (Graphische Benutzeroberfläche). Eine Anzeigenoberfläche eines Computers, in der Elemente wie z. B. Fenster, Dialogfelder und Schaltflächen verwendet werden, im Gegensatz zu einer Befehlsaufforderungsschnittstelle, in der alle Benutzerinteraktionen als Text dargestellt und eingegeben werden.

Hardwareprotokoll

Zeichnet vom iDRAC 6 erstellte Ereignisse auf.

iAMT

Intel® Active Management Technology - Liefert sicherere Systemverwaltungsfähigkeiten, egal, ob der Computer ein- oder ausgeschaltet ist, und auch dann, wenn das System nicht reagiert.

ICMB

Abkürzung für Intelligent Enclosure Management Bus (Intelligenter Gehäuseverwaltungsbus).

ICMP

Abkürzung für Internet Control Message Protocol (Internet-Steuerungsmeldungsprotokoll).

ID

Abkürzung für Identifier (Bezeichner). Wird normalerweise als Bezeichnung für einen Benutzer-Bezeichner (Benutzer-ID) oder Objekt-Bezeichner (Objekt-ID) verwendet.

iDRAC6

Akronym für Integrated Dell Remote Access Controller, das integrierte System-auf-Chip-Überwachungs-/Steuerungssystem für die Dell 11G-PowerEdge-Server.

IP

Abkürzung für Internet Protocol (Internet-Protokoll). Die Netzwerkschicht für TCP/IP. IP ermöglicht Paket-Routing, Fragmentierung und Reorganisation.

IPMB

Abkürzung für Intelligent Platform Management Bus (intelligenter Plattformverwaltungsbus), der ein in der Systemverwaltungstechnologie verwendeter Bus ist.

IPMI

Abkürzung für Intelligent Platform Management Interface (Intelligente Plattformverwaltungsschnittstelle). Ein Teil der Systemverwaltungstechnologie.

kBit/s

Abkürzung für Kilobits per Second (Kilobit pro Sekunde). Eine Datentransferrate.

Konsolenumleitung

Konsolenumleitung ist eine Funktion, die den Anzeigebildschirm sowie die Maus- und Tastaturfunktionen eines verwalteten Servers an die entsprechenden Komponenten einer Management Station weiterleitet. Die Systemkonsole der Management Station kann zur Steuerung des verwalteten Servers verwendet werden.

LAN

Abkürzung für Local Area Network (Lokales Netzwerk).

LDAP

Abkürzung für Lightweight Directory Access Protocol.

LED

Akronym für Light-Emitting Diode (Leuchtdiode).

LOM

Abkürzung für Local Area Network On Motherboard (Lokales Netz auf der Hauptplatine).

LUN

Akronym für Logical Unit Number (Logische Einheitennummer).

MAC

Akronym für Media Access Control (Medienzugriffssteuerung). Eine Netzwerkunterschicht zwischen einem Netzwerkknoten und der physikalischen Netzwerkschicht.

MAC-Adresse

Akronym für Media Access Control Address (Datenträgerzugriffssteuerungsadresse). Eine spezielle Adresse, die in den physischen Komponenten eines NIC integriert ist.

Management Station

Die Management Station ist das System, von dem aus ein Administrator ein Dell-System mit iDRAC 6 im Remote-Zugriff verwaltet.

MAP

Abkürzung für Manageability Access Point (Verwaltungsfunktionen-Zugriffspunkt).

MBit/s

Abkürzung für Megabits per Second (Megabit pro Sekunde). Eine Datentransferrate.

MIB

Abkürzung für Management Information Base (Verwaltungsinformationsbasis).

MII

Abkürzung für Media Independent Interface (Datenträgerunabhängige Schnittstelle).

NAS

Abkürzung für Network Attached Storage (Dem Netzwerk beigefügter Speicher).

NIC

Abkürzung für Network Interface Card (Netzwerkschnittstellenkarte). Eine in einem Computer installierte Adapterplatine, die eine physische Verbindung zu einem Netzwerk bietet.

OID

Abkürzung für Object Identifiers (Objektbezeichner).

PCI

Abkürzung für Peripheral Component Interconnect (Verbindung peripherer Komponenten). Eine Standardschnittstellen- und Bustechnologie zum Anschluss von Peripheriegeräten an ein System und zur Kommunikation mit diesen Peripheriegeräten.

POST

Akronym für Power-On Self-Test (Einschaltselbsttest). Eine Sequenz diagnostischer Tests, die automatisch von einem System ausgeführt werden, wenn es eingeschaltet ist.

PPP

Abkürzung für Point-to-Point Protocol (Punkt-zu-Punkt-Protokoll). Ein Standardinternetprotokoll zur Übertragung von Netzwerkschicht-Datagrammen (wie z.B. IP-Pakete) über serielle Punkt-zu-Punkt-Verknüpfungen.

RAC

Abkürzung für Remote Access Controller (Remote Access Controller).

RAM

Akronym für Random Access Memory (Speicher mit wahlfreiem Zugriff). RAM ist der allgemeine lesbare und beschreibbare Speicher in Systemen und im iDRAC 6.

RAM-Platte

Ein speicherresidentes Programm, das ein Festplattenlaufwerk emuliert. Der iDRAC 6 besitzt eine RAM-Platte im Speicher.

ROM

Akronym für Read-Only Memory (Nur-Lese-Speicher). Speicher, von dem Daten gelesen werden können, auf den jedoch keine Daten geschrieben werden können.

RPM

Abkürzung für Red Hat® Package Manager, der ein Paketverwaltungssystem für das Red Hat Enterprise Linux®-Betriebssystem ist, das bei der Installation von Softwarepaketen hilft. Es ist einem Installationsprogramm ähnlich.

SAC

Akronym für Microsoft Special Administration Console.

SAP

Abkürzung für Service Access Point (Service-Zugriffspunkt).

SEL

Akronym für System Event Log (Systemereignisprotokoll).

SM-CLP

Abkürzung für Server Management Command Line Protocol (Serververwaltungs-Befehlszeilenprotokoll). SM-CLP ist eine Unterkomponente der DMTF SMASH-Initiative zum Rationalisieren der Serververwaltung auf mehreren Plattformen. Die SM-CLP-Spezifikation beschreibt die standardisierten Verben und Ziele zum

Ausführen verschiedener Verwaltungsaufgaben in Verbindung mit den Spezifikationen zur verwalteten Elementadressierung und zahlreichen Profilen zur SM-CLP-Zuordnungsspezifikation.

SMI

Abkürzung für Systems Management Interrupt.

SMTP

Abkürzung für Simple Mail Transfer Protocol (Einfaches Mail-Übertragungsprotokoll). Ein Protokoll, das dazu verwendet wird, elektronische Post zwischen Systemen zu übertragen, normalerweise über ein Ethernet.

SMWG

Abkürzung für Systems Management Working Group (Systemverwaltungs-Arbeitsgruppe).

SNMP-Trap

Eine vom iDRAC 6 erzeugte Meldung (Ereignis), die Informationen über Statusänderungen auf dem verwalteten System oder über mögliche Hardwarestörungen enthält.

SSH

Abkürzung für Secure Shell (Sichere Shell).

SSL

Abkürzung für Secure Sockets Layer (Sichere Sockelschicht).

Standardschema

Eine mit Active Directory verwendete Lösung zum Bestimmen von Benutzerzugriffen auf den iDRAC 6; verwendet Dell-definierte Active Directory-Objekte.

TAP

Abkürzung für Telelocator Alphanumeric Protocol (Alphanumerisches Telelocator-Protokoll). Ein Protokoll zum Senden von Anfragen an einen Funkrufdienst.

TCP/IP

Abkürzung für Transmission Control Protocol/Internet Protocol (Übertragungssteuerungsprotokoll/Internetprotokoll). Stellt den Satz an Standard-Ethernetprotokollen dar, der die Netzwerkschicht- und Übertragungsschichtprotokolle enthält.

TFTP

Abkürzung für Trivial File Transfer Protocol (Trivial-Dateiübertragungsprotokoll). Ein einfaches Dateiübertragungsprotokoll, das zum Herunterladen von Startcode auf datenträgerlose Geräte oder Systeme verwendet wird.

Unified Server Configurator

Der Dell Unified Server Configurator (USC) ist ein integriertes Konfigurationsdienstprogramm, das System- und Speicherverwaltungsaufgaben aus einer eingebetteten Umgebung im gesamten Lebenszyklus des Servers ermöglicht.

USB

Akronym für Universal Serial Bus (Universeller serieller Bus).

USC

Abkürzung für Unified Server Configurator.

USV

Akronym für unterbrechungsfreie Stromversorgung.

UTC

Abkürzung für Universal Coordinated Time (Koordinierte Weltzeit). *Siehe* GMT.

verwalteter Server

Der verwaltete Server ist das System, in dem der iDRAC 6 integriert ist.

verwaltetes System

Ein von einer Management Station überwachtes System wird verwaltetes System genannt.

VLAN

Abkürzung für Virtual Local Area Network (Virtuelles lokales Netzwerk).

VNC

Abkürzung für Virtual Network Computing (Virtueller Netzwerkbetrieb).

VT-100

Abkürzung für Video Terminal 100. Wird von den gebräuchlichsten Terminalemulationsprogrammen verwendet.

WAN

Abkürzung für Wide Area Network (Weitbereichsnetzwerk).

WS-MAN

Abkürzung für Web Services for Management (WS-MAN)-Protokoll (Webdienste zur Verwaltung). WS-MAN ist ein Übertragungsmechanismus für den Informationsaustausch. WS-MAN bietet eine universelle Sprache für Geräte zur Freigabe von Daten, damit diese einfacher verwaltet werden können.

Zurücksetzen

Um zu einer vorherigen Software- oder Firmwareversion zurückzukehren.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Übersicht der RACADM-Unterbefehle

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

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

---

help

ANMERKUNG: Um diesen Befehl verwenden zu können, 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, und enthält eine kurze Beschreibung der einzelnen Befehle.

Zusammenfassung

```
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/serial-RACADM

---

arp

ANMERKUNG: Um diesen Befehl verwenden zu können, 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.

Zusammenfassung

```
racadm arp
```

Unterstützte Schnittstellen

- Remote-RACADM
- telnet/ssh/serial-RACADM

---

clearasrscreen

ANMERKUNG: Um diesen Befehl verwenden zu können, 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.

Zusammenfassung

```
racadm clearasrscreen
```

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-RACADM

---

config

ANMERKUNG: Um den Befehl **getconfig** verwenden zu können, 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 iDRAC 6.
getconfig	Ruft die iDRAC 6-Konfigurationsdaten ab.

Zusammenfassung

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

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

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-RACADM

Beschreibung

Mit dem Unterbefehl **config** kann der Benutzer die Konfigurationsparameter des iDRAC 6 einzeln oder stapelweise als Teil einer Konfigurationsdatei einrichten. Wenn sich die Daten unterscheiden, wird das iDRAC 6-Objekt mit dem neuen Wert geschrieben.

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*>** kann **config** den Inhalt der durch **<*Dateiname*>** festgelegten Datei lesen und den iDRAC 6 konfigurieren. Die Datei muss Daten enthalten, die dem unter "Parsen-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 dezimale Ganzzahl 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 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 kommen keine Schreibvorgänge beim iDRAC 6 vor. Diese Option ist nur eine Kontrolle.

Ausgabe

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

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

Dieser Unterbefehl zeigt an, wie viele geschriebene Konfigurationsobjekte sich von wie vielen Objekten insgesamt in der **.cfg**-Datei befanden.

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 den iDRAC 6 oder konfiguriert ihn neu. Die Datei **myrac.cfg** kann aus dem Befehl **getconfig** erstellt werden. Die Datei **myrac.cfg** kann auch manuell bearbeitet werden, solange die Analyse-Richtlinien 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 **myrac.cfg**-Datei entfernen möchten, verwenden Sie die Option **-p**.

---

getconfig

Beschreibung des Unterbefehls getconfig

Mit dem Unterbefehl **getconfig** kann der Benutzer iDRAC 6-Konfigurationsparameter einzeln abrufen oder alle iDRAC 6-Konfigurationsgruppen abrufen und sie in einer Datei speichern.

Eingabe

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

ANMERKUNG: Die Option **-f** ohne Dateiangabe wird den Dateiinhalt an den Terminal-Bildschirm ausgeben.

Tabelle A-6. Optionen des Unterbefehls getconfig

Option	Beschreibung
-f	Die Option **-f <*Dateiname*>** weist getconfig an, die gesamte iDRAC 6-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 einstellen, um die **cfgIpmiPet**-Gruppe zur Datei zu erfassen.
-g	Die Option **-g <*Gruppenname*>** bzw. die **Gruppe**noption kann verwendet werden, um die Konfiguration für eine einzelne Gruppe anzuzeigen. Der **Gruppenname** ist der Name der Gruppe, der 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 vorhandener Konfigurationsgruppen an, die Sie verwenden können. Diese Option ist nützlich, wenn die genauen Gruppennamen nicht bekannt sind.
-i	Die Option **-i <*Index*>** bzw. die **Index**option ist nur für indizierte Gruppen gültig und kann zur Bestimmung einer eindeutigen Gruppe verwendet werden. Der <*Index*> ist eine dezimale Ganzzahl 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 "Benennungs"wert.
-o	Der -o **<*Objektname*>** bzw. die Objektoption gibt den Objektnamen an, 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 **Benutzername**noption kann zur Anzeige der Konfiguration des angegebenen Benutzers verwendet werden. Die Option **<*Benutzername*>** ist der Anmeldename des Benutzers.
-v	Die Option **-v** zeigt zusätzliche Details mit der Anzeige der Eigenschaften an und wird mit der Option **-g** verwendet.

Ausgabe

Dieser Unterbefehl erzeugt eine Fehlerausgabe, wenn einer der folgenden Punkte 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 iDRAC 6 in **myrac.cfg**.

- `racadm getconfig -h`

Zeigt eine Liste der verfügbaren Konfigurationsgruppen auf dem iDRAC 6 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 an Index 2 mit ausführlichen Informationen für die Eigenschaftswerte an.

Zusammenfassung

```
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/serial-RACADM

---

coredump

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 Coredump des iDRAC 6 an.

Zusammenfassung

```
racadm coredump
```

Beschreibung

Mit dem Unterbefehl **coredump** werden detaillierte Informationen bezüglich kritischer Probleme am RAC angezeigt, die vor Kurzem aufgetreten sind. Die coredump-Informationen können zur Diagnose dieser kritischen Probleme eingesetzt werden.

Wenn verfügbar, sind die Coredump-Informationen beständig über Betriebszyklen des iDRAC 6 und werden verfügbar bleiben, bis eine der folgenden Bedingungen eintritt:

- Die coredump-Informationen werden mit dem Unterbefehl **coredumpdelete** gelöscht.
- Auf dem RAC tritt eine weitere kritische Bedingung 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/serial-RACADM

---

coredumpdelete

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 iDRAC 6 gespeicherten Coredump.

Zusammenfassung

```
racadm coredumpdelete
```

Beschreibung

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

ANMERKUNG: Wenn der Befehl **coredumpdelete** ausgegeben 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 im Unterbefehl **coredump**.

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-RACADM

---

fwupdate

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **iDRAC 6 konfigurieren** verfügen.

ANMERKUNG: Lesen Sie die zusätzlichen Informationen unter "Erweiterte Konfiguration des iDRAC 6", 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 iDRAC 6.

Zusammenfassung

```
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 iDRAC 6 aktualisieren. Der Benutzer kann:

- Den Status des Firmware-Aktualisierungsverfahrens prüfen

- iDRAC 6-Firmware von einem TFTP-Server durch Angabe einer IP-Adresse und eines optionalen Pfads aktualisieren.
- iDRAC 6-Firmware vom lokalen Dateisystem mittels lokalem RACADM aktualisieren.
- Auf die Standby-Firmware zurücksetzen.

Unterstützte Schnittstellen

- lokaler RACADM
- telnet/ssh/serial-RACADM

Eingabe

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

ANMERKUNG: Die Option **-p** wird nur in lokalem RACADM unterstützt, nicht jedoch bei der Remote- oder seriellen/Telnet/SSH-Konsole.

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 Optionen **-g** oder **-p** verwendet werden. Nach der Aktualisierung führt der iDRAC 6 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. Da 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** oder **directory** bestimmt das Verzeichnis auf dem TFTP-Server oder auf dem Hostserver des iDRAC 6, in dem sich die Firmware-Aktualisierungsdatei befindet.
-p	Die Option **-p** bzw. **put** wird zum Aktualisieren der Firmware-Datei vom verwalteten System zum iDRAC 6 verwendet. Die Option **-u** muss zusammen mit der Option **-p** verwendet werden.
-r	Die Option **Zurücksetzen** 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** angegeben) auf dem TFTP-Server unter einer bestimmten IP-Adresse (durch die Option **-a** angegeben) herunterzuladen. Nachdem die Abbilddatei vom TFTP-Server heruntergeladen wurde, beginnt der Aktualisierungsvorgang. Wenn dieser abgeschlossen ist, wird der iDRAC 6 zurückgesetzt.

- `racadm fwupdate -s`

  Diese Option liest den derzeitigen Status der Firmware-Aktualisierung.

- `racadm fwupdate -p -u -d <Pfad>`

  In diesem Beispiel wird das Firmware-Image für die Aktualisierung vom Dateisystem des Hosts geliefert.

ANMERKUNG: Die Option **-p** wird in der Remote-RACADM-Schnittstelle für den Unterbefehl fwupdate nicht unterstützt.

---

getssninfo

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 pausierende Sitzungen der Sitzungstabelle des Sitzungs-Managers abrufen.

Zusammenfassung

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

Beschreibung

Über den Befehl **getssninfo** wird eine Liste der Benutzer ausgegeben, die mit dem iDRAC 6 verbunden sind. Die zusammenfassenden Informationen geben die folgende Auskunft:

- Benutzername
- IP-Adresse (wenn anwendbar)
- Sitzungstyp (Beispiel: seriell oder Telnet)
- Konsolen in Gebrauch (Beispiel: Virtueller Datenträger oder Virtuelle KVM)

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-RACADM

Eingabe

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

Tabelle A-12. Optionen des Unterbefehls getssninfo

Option	Beschreibung
-A	Die Option **-A** eliminiert 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 ausgedruckt, 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	Virtual 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 verwenden zu können, 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 iDRAC 6, System und Watchdog-Status an.

Zusammenfassung

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

Beschreibung

Mit dem Unterbefehl **getsysinfo** werden Informationen bezüglich der Konfiguration von RAC, verwaltetem System und Watchdog angezeigt.

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-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 iDRAC 6-Informationen an.
-s	Zeigt Systeminformationen an
-w	Zeigt Watchdog-Informationen an
-A	Unterdrückt das Drucken von Kopfzeilen und Beschriftungen.

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

Ausgabe

Mit dem Unterbefehl **getsysinfo** werden Informationen bezüglich der Konfiguration von RAC, verwaltetem System und Watchdog angezeigt.

Beispielausgabe

```
RAC Information:
RAC Date/Time = 10/01/2008 09:39:53
Firmware Version = 0.32
Firmware Build = 55729
Last Firmware Update = 09/25/2008 18:08:31
Hardware Version = 0.01
MAC Address = 00:1e:c9:b2:c7:1f

Common settings:
Register DNS RAC Name = 0
```

```
DNS RAC Name = iDRAC6
Current DNS Domain =
Domain Name from DHCP = 0

IPv4 settings:
Enabled = 1
Current IP Address = 192.168.0.120
Current IP Gateway = 192.168.0.1
Current IP Netmask = 255.255.255.0
DHCP Enabled = 0
Current DNS Server 1 = 0.0.0.0
Current DNS Server 2 = 0.0.0.0
DNS Servers from DHCP = 0

IPv6 settings:
Enabled = 0
Current IP Address 1 = 2002:0000:0000::0001
Current IP Gateway = ::
Prefix Length = 64
Autoconfig              = 1
DNS Server from DHCPv6  = 0
Current DNS Server 1    = ::
Current DNS Server 2    = ::

System Information:
System Model = PowerEdge R610
System BIOS Version = 0.2.4
BMC Firmware Version = 0.32
Service Tag = AC056
Host Name =
OS Name =
Power Status = ON

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 und BS-Name in der **getsysinfo**-Ausgabe zeigen nur genaue Informationen an, wenn Dell™ OpenManage™-Systemsoftware auf dem verwalteten System installiert ist. Wenn OpenManage nicht auf dem verwalteten System installiert ist, können diese Felder leer oder fehlerhaft sein.

---

getractime

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 aus an.

Zusammenfassung

```
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/serial-RACADM

---

ifconfig

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 Netzschnittstellentabelle an.

Zusammenfassung

```
racadm ifconfig
```

---

netstat

ANMERKUNG: Um diesen Befehl verwenden zu können, 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.

Zusammenfassung

```
racadm netstat
```

Unterstützte Schnittstellen

- Remote-RACADM
- telnet/ssh/serial-RACADM

---

ping

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 Routing-Tabelle vom iDRAC 6 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.

Zusammenfassung

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

Unterstützte Schnittstellen

- Remote-RACADM
- telnet/ssh/serial-RACADM

---

setniccfg

ANMERKUNG: Um den Befehl **setniccfg** verwenden zu können, 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 gegeneinander ausgetauscht werden.

Zusammenfassung

```
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/serial-RACADM

---

getniccfg

ANMERKUNG: Um den Befehl **getniccfg** verwenden zu können, 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.

Zusammenfassung

```
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. Bei erfolgreicher Ausführung wird andernfalls 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/serial-RACADM

---

getsvctag

ANMERKUNG: Um diesen Befehl verwenden zu können, 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.

Zusammenfassung

`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/serial-RACADM

---

racdump

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 iDRAC 6 an.

Zusammenfassung

```
racadm racdump
```

Beschreibung

Der Unterbefehl **racdump** ist ein einziger Befehl, mit dem ein Speicherabbild, der Status und allgemeine iDRAC 6-Platineninformationen bezogen werden können.

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

- Allgemeine System-/RAC-Informationen
- Core Dump
- Sitzungsinformationen
- Verfahrensinformationen
- Firmware-Build-Informationen

Unterstützte Schnittstellen

- Remote-RACADM
- telnet/ssh/serial-RACADM

---

racreset

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

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

Tabelle A-24. racreset

Unterbefehl	Definition
racreset	Setzt den iDRAC 6 zurück.

ANMERKUNG: Wenn Sie einen racreset-Unterbefehl ausgeben, kann der iDRAC 6 bis zu eine Minute in Anspruch nehmen, um in einen einsatzfähigen Zustand zurückzukehren.

Zusammenfassung

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

Beschreibung

Der Unterbefehl **racreset** gibt einen Reset an den iDRAC 6 aus. Das Reset-Ereignis wird in das iDRAC 6-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 Kaltstart des iDRAC 6 neu gestartet werden, wie in Tabelle A-25 beschrieben.

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 iDRAC 6-Controller zu Wiederherstellungszwecken zurückzusetzen.
soft	Ein *Software*-Reset führt einen ordentlichen Neustart auf dem RAC aus.

Beispiele

- `racadm racreset`

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

- `racadm racreset hard`

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

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-RACADM

---

racresetcfg

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 iDRAC 6-Konfiguration auf die werkseitigen Standardwerte zurück.

Zusammenfassung

`racadm racresetcfg`

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-RACADM

Beschreibung

Der Befehl **racresetcfg** entfernt alle Eigenschaften-Einträge der Datenbank, die vom Benutzer konfiguriert wurden. Die Datenbank besitzt Standard-Eigenschaften für alle Einträge, die zur Wiederherstellung der ursprünglichen Standardeinstellungen der Karte verwendet werden. Nach dem Zurücksetzen der Datenbank-Eigenschaften wird der iDRAC 6 automatisch zurückgesetzt.

ANMERKUNG: Mit diesem Befehl wird die aktuelle iDRAC 6-Konfiguration gelöscht und der iDRAC 6 und die serielle Konfiguration werden auf die ursprünglichen Standardeinstellungen zurückgesetzt. Nach dem Reset sind Standardname und -kennwort **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 Internet-Browser, telnet/ssh oder Remote-RACADM) ausgeben, müssen Sie die Standard-IP-Adresse verwenden.

ANMERKUNG: Bestimmte iDRAC 6-Firmware-Prozesse müssen zum Zurücksetzen auf die Standardeinstellungen angehalten und neu gestartet werden, um den Vorgang abzuschließen. iDRAC 6 wird dann für ca. 30 Sekunden nicht antworten, während der Vorgang abgeschlossen wird.

---

serveraction

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 Einschalten/Ausschalten-Zyklus durch.

Zusammenfassung

```
racadm serveraction <Maßnahme>
```

Beschreibung

Der Unterbefehl serveraction ermöglicht Benutzern, Stromverwaltungsvorgänge auf dem Host-System auszuführen. Tabelle A-28 beschreibt die Stromregelungsoptionen zu **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** - Leitet einen Ein-/Ausschaltvorgang auf dem verwalteten System ein. 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 aus.

Ausgabe

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

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-RACADM

---

getraclog

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 iDRAC 6-Protokoll an.
getraclog	Zeigt die iDRAC 6-Protokolleinträge an.

Zusammenfassung

```
racadm getraclog -i

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

Beschreibung

Der Befehl **getraclog -i** zeigt die Anzahl der Einträge im iDRAC 6-Protokoll an.

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

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

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

Ausgabe

Die Anzeige der Standardausgabe gibt Folgendes an: Datensatznummer, Zeitstempel, Quelle und Beschreibung. Der Zeitstempel beginnt um Mitternacht, dem 1. Januar, 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/serial-RACADM

---

clrraclog

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

Zusammenfassung

```
racadm clrraclog
```

Beschreibung

Mit dem Unterbefehl **clrraclog** werden alle vorhandenen Einträge aus dem iDRAC 6-Protokoll entfernt. Ein neuer Einzeldatensatz wird erstellt, um Datum und Uhrzeit des Löschens des Protokolls aufzuzeichnen.

---

getsel

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 SEL-Einträge an.

Zusammenfassung

```
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 SEL 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 Etiketten fest.

-c - Zeigt die Höchstanzahl der zurückzugebenden Einträge an.

-o - Zeigt die Ausgabe auf einer einzelnen Zeile an.

-s - Gibt den für die Anzeige verwendeten Startdatensatz an

-E - Legt die 16 Byte des Roh-SEL am Ende jeder Ausgabezeile als Sequenz von hexadezimalen Werten ab.

-R - Es werden nur die Rohdaten ausgedruckt.

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

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

Ausgabe

Die Anzeige der Standardausgabe gibt Folgendes an: Datensatznummer, Zeitstempel, Schweregrad und Beschreibung.

Zum 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/serial-RACADM

---

clrsel

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

Zusammenfassung

```
racadm clrsel
```

Beschreibung

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

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-RACADM

---

gettracelog

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 iDRAC 6-Ablaufverfolgungsprotokoll an.
gettracelog	Zeigt das iDRAC 6-Ablaufverfolgungsprotokoll an.

Zusammenfassung

```
racadm gettracelog -i

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

Beschreibung

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

-i - Zeigt die Anzahl der Einträge im iDRAC 6-Ablaufverfolgungsprotokoll an

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

-o - Zeigt die Ausgabe auf einer einzelnen Zeile an.

-c - Gibt die Anzahl der anzuzeigenden Datensätze an

-s - Gibt den anzuzeigenden Startdatensatz an

-A - Zeigt Kopfzeilen oder Etiketten nicht an

Ausgabe

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

Zum 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/serial-RACADM

---

sslcsrgen

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 herunter (vom RAC).

Zusammenfassung

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

racadm sslcsrgen -s
```

Beschreibung

Der Unterbefehl **sslcsrgen** kann verwendet werden, um eine CSR zu erstellen und die Datei zum lokalen 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>*), an den die CSR heruntergeladen wird.

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

Wenn keine Optionen angegeben werden, wird eine CSR erstellt und standardmäßig als **sslcsr** zum lokalen 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/serial-RACADM

---

sslcertupload

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 CA-Zertifikat vom Client zum RAC hoch.

Zusammenfassung

```
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 hochzuladenden Zertifikatstyp an, entweder ein CA-Zertifikat oder ein Server-Zertifikat. 1 = Server-Zertifikat 2 = CA-Zertifikat
-f	Gibt den Dateinamen des hochzuladenden Zertifikats an. Wenn die Datei nicht festgelegt wird, wird die Datei **sslcert** im aktuellen Verzeichnis ausgewählt.

Der Befehl **sslcertupload** gibt bei Erfolg `0` und bei Nichterfolg einen anderen Wert als Null zurück.

Einschränkungen

Der Unterbefehl **sslcertupload** kann nur von einem lokalen oder einem Remote-RACADM-Client aus ausgeführt werden. Der Unterbefehl **sslcsrgen** kann nicht in 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 verwenden zu können, 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 iDRAC 6 auf das Dateisystem des Clients herunter.

Zusammenfassung

```
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 Zertifikats an, entweder das Microsoft® Active Directory®-Zertifikat oder das Serverzertifikat. 1 = Server-Zertifikat 2 = Microsoft Active Directory-Zertifikat
-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 Nichterfolg einen anderen Wert als Null zurück.

Einschränkungen

Der Unterbefehl **sslcertdownload** kann nur von einem lokalen oder einem Remote-RACADM-Client aus ausgeführt werden. Der Unterbefehl **sslcsrgen** kann nicht in 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 verwenden zu können, 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, der bzw. das auf dem RAC vorhanden ist.

Zusammenfassung

```
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 das Microsoft Active Directory-Zertifikat oder das Serverzertifikat. 1 = Server-Zertifikat 2 = Microsoft Active Directory-Zertifikat
-A	Gibt keine Kopfzeilen/Bezeichnungen aus.

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/serial-RACADM

---

sslkeyupload

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 iDRAC 6 hoch.

Zusammenfassung

```
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 Nichterfolg einen anderen Wert als 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 RAC

Zusammenfassung

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

Beschreibung

Sendet eine Test-E-Mail vom iDRAC 6 an ein festgelegtes Ziel.

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

Tabelle A-43. testemail-Konfiguration

Abhilfe	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 -i 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/serial-RACADM

---

testtrap

ANMERKUNG: Um diesen Befehl verwenden zu können, 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.

Zusammenfassung

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

Beschreibung

Mit dem Unterbefehl **testtrap** wird die Trap-Warnungsfunktion des RAC-SNMP getestet, indem ein Test-Trap vom iDRAC 6 an einen festgelegten Ziel-Trap-Hörer auf dem 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

Abhilfe	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 sind zwischen 1 und 4.

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-RACADM

---

vmdisconnect

ANMERKUNG: Um diesen Befehl verwenden zu können, 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 iDRAC 6-Verbindungen des virtuellen Datenträgers von Remote Clients aus.

Zusammenfassung

```
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 durch den Gebrauch von lokalem oder Remote-RACADM zur Verfügung.

Mit dem Unterbefehl **vmdisconnect** wird einem iDRAC 6-Benutzer ermöglicht, alle aktiven Sitzungen des virtuellen Datenträgers zu unterbrechen. Die aktiven Sitzungen des virtuellen Datenträgers können auf der webbasierten iDRAC 6-Schnittstelle oder durch Verwendung des Unterbefehls RACADM **getsysinfo** angezeigt werden.

Unterstützte Schnittstellen

- lokaler RACADM

- Remote-RACADM
- telnet/ssh/serial-RACADM

---

vmkey

ANMERKUNG: Um diesen Befehl verwenden zu können, 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.

Zusammenfassung

```
racadm vmkey <Maßnahme>
```

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

Beschreibung

Wenn ein benutzerdefiniertes Schlüsselabbild des virtuellen Datenträgers zum RAC hochgeladen wird, wird die Schlüsselgröße zur Abbildgröße. Der vmkey-Unterbefehl kann verwendet werden, um den Schlüssel auf seine ursprüngliche Standardgröße zurückzusetzen, d. h. 256 MB auf dem iDRAC 6.

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-RACADM

---

usercertupload

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

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

Tabelle A-50. usercertupload

Unterbefehl	Beschreibung
usercertupload	Lädt ein Benutzerzertifikat oder ein Benutzer-CA-Zertifikat vom Client auf den iDRAC 6 hoch.

Zusammenfassung

```
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 CA-Zertifikat oder ein Server-Zertifikat. 1 = Benutzerzertifikat 2 = Benutzer-CA-Zertifikat
-f	Gibt den Dateinamen des hochzuladenden Zertifikats an. Wenn die Datei nicht festgelegt 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 Nichterfolg einen anderen Wert als 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 verwenden zu können, 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-CA-Zertifikat an, das auf dem iDRAC 6 vorhanden ist.

Zusammenfassung

```
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-CA-Zertifikat. 1 = Benutzerzertifikat 2 = Benutzer-CA-Zertifikat
-A	Gibt keine Kopfzeilen/Bezeichnungen aus.
-i	Indexnummer des Benutzers. Gültige Werte sind 1 - 16.

Unterstützte Schnittstellen

- lokaler RACADM
- Remote-RACADM
- telnet/ssh/serial-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.

Zusammenfassung

`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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC 6-Definitionen für Eigenschafts-Datenbankgruppen und Objekte

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Die iDRAC 6-Eigenschaftendatenbank enthält die Konfigurationsinformationen für den iDRAC 6. Daten werden nach assoziiertem Objekt organisiert und Objekte werden nach der Objektgruppe organisiert. Die IDs für die Gruppen und Objekte, die von der Datenbank der Eigenschaften unterstützt werden, sind in diesem Abschnitt aufgeführt.

Verwenden Sie die Gruppen- und Objekt-IDs mit dem RACADM-Dienstprogramm, um den iDRAC 6 zu konfigurieren. Die folgenden Abschnitte beschreiben jedes Objekt und zeigen an, ob das Objekt schreibbar, lesbar oder beides ist.

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 iDRAC 6.

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

idRacProductInfo (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 63 ASCII-Zeichen.

Standardeinstellung

Integrierter Dell Remote Access Controller

Beschreibung

Eine Textzeichenkette, die das Produkt identifiziert.

idRacDescriptionInfo (schreibgeschützt)

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 (schreibgeschützt)

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 (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 16 ASCII-Zeichen.

Standardeinstellung

Die aktuelle Build-Version der iDRAC 6-Firmware.

Beschreibung

Eine Zeichenkette mit der aktuellen Build-Version des Produkts.

idRacName (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 15 ASCII-Zeichen.

Standardeinstellung

iDRAC

Beschreibung

Ein vom Benutzer vergebener Name zur Identifizierung dieses Controllers.

idRacType (schreibgeschützt)

Zulässige Werte

Produkt-ID

Standardeinstellung

10

Beschreibung

Identifiziert den Remote Access Controller-Typ als den iDRAC 6.

---

cfgLanNetworking

Diese Gruppe enthält Parameter zum Konfigurieren des iDRAC 6-NIC.

Es ist eine Instanz der Gruppe zulässig. Für alle Objekte in dieser Gruppe ist ein Reset des iDRAC 6-NIC erforderlich, wodurch ein kurzzeitiger Verlust der Konnektivität auftreten kann. Objekte, die die iDRAC 6-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 iDRAC 6-IPv4-Stapel.

cfgNicSelection (Lesen/Schreiben)

Zulässige Werte

0 = Freigegeben

1 = Freigegeben mit Failover: LOM2

2 = Dediziert

3 = Freigegeben mit Failover: Alle LOMs (nur iDRAC 6 Enterprise)

Standardeinstellung

0 (iDRAC 6 Express)

2 (iDRAC 6 Enterprise)

Beschreibung

Legt den aktuellen Verfahrensmodus für den RAC-Netzwerkschnittstellen-Controller (NIC) 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 auf dem Netzwerk dieselbe IP-Adresse auf dem Host-Server und dem RAC verwenden.
Freigegeben mit 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 mit Failover: Alle LOMs	Aktiviert Teaming-Fähigkeiten zwischen allen LOMs auf den integrierten Netzwerkschnittstellen-Controllern des Host-Servers. Die Remote-Zugriffs-Gerätenetzschnittstelle ist vollständig funktionsfähig, wenn das Host-Betriebssystem für das 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-Fähigkeiten von 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 iDRAC 6-DNS-Domänenname vom Netzwerk-DHCP-Server aus zugewiesen werden muss.

cfgDNSDomainName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette mit 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 mit 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 iDRAC 6-Namen an, der standardmäßig die RAC-*Service-Tag-Nummer* ist. 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 iDRAC 6-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 darstellt. 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 darstellt. 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 iDRAC 6-Netzwerkschnittstellen-Controller. Wenn der NIC deaktiviert ist, kann nicht mehr auf die Remote-Netzwerkschnittstellen über den iDRAC 6 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 darstellt. Beispiel: 192.168.0.20.

Standardeinstellung

192.168.0.120

Beschreibung

Gibt die dem iDRAC 6 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 darstellt. Beispiel: 255.255.255.0.

Standardeinstellung

255.255.255.0

Beschreibung

Die für die iDRAC 6-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 darstellt. Beispiel: 192.168.0.1.

Standardeinstellung

192.168.0.1

Beschreibung

Die iDRAC 6-Gateway-IPv4-Adresse.

cfgNicUseDhcp (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Gibt an, ob DHCP zum Zuweisen der iDRAC 6-IPv4-Adresse verwendet wird. Wenn diese Eigenschaft auf 1 (TRUE) eingestellt wird, werden die iDRAC 6-IPv4-Adresse, die Subnetzmaske sowie der Gateway vom DHCP-Server auf dem Netzwerk zugewiesen. Wenn diese Eigenschaft auf **0** (FALSE) eingestellt ist, kann der Benutzer die Eigenschaften von **cfgNicIpAddress**, **cfgNicNetmask** und **cfgNicGateway** konfigurieren.

cfgNicMacAddress (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette, die die iDRAC 6-NIC-MAC-Adresse darstellt.

Standardeinstellung

Die aktuelle MAC-Adresse des iDRAC 6-NIC. Beispiel: 00:12:67:52:51:A3.

Beschreibung

Die iDRAC 6-NIC-MAC-Adresse.

---

cfgRemoteHosts

Diese Gruppe enthält Eigenschaften, die 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 iDRAC 6-Firmware-Aktualisierung über einen Netzwerk-TFTP-Server.

cfgRhostsFwUpdateIpAddr (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

0.0.0.0

Beschreibung

Gibt die IPv4-Adresse des Netzwerk-TFTP-Servers an, die für TFTP-iDRAC 6-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 iDRAC 6-Firmware-Imagedatei auf dem TFTP-Server an. Der TFTP-Pfad ist relativ zum TFTP-Stammpfad 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 darstellt. 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 iDRAC 6, wenn die Warnungen konfiguriert und aktiviert sind. Der TFTP-Server überträgt Dateien zum und vom iDRAC 6.

---

cfgUserAdmin

Diese Gruppe bietet Konfigurationsinformationen über die Benutzer, denen erlaubt wird, über die verfügbaren Remote-Schnittstellen auf den iDRAC 6 zuzugreifen.

Es sind bis zu 16 Beispiele der Benutzergruppe gestattet. Jedes Beispiel vertritt die Konfiguration für einen einzelnen Benutzer.

cfgUserAdminIndex (schreibgeschützt)

Zulässige Werte

1 - 16

Standardeinstellung

<instance>

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 zu 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 werden. Tabelle B-2 beschreibt die Benutzerberechtigungs-Bitwerte, die zum Erstellen von Bitmasken kombiniert werden können.

Tabelle B-2. Bit-Masken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
Bei iDRAC anmelden	0x0000001
iDRAC konfigurieren	0x0000002
Benutzer konfigurieren	0x0000004
Protokolle löschen	0x0000008
Serversteuerungsbefehle ausführen	0x0000010
Auf die Konsolenumleitung zugreifen	0x0000020
Zugriff auf virtuelle Datenträger	0x0000040
Testwarnungen	0x0000080
Debug-Befehle ausführen	0x0000100

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 Serverkonfigurations-Informationen 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 der Zeichenkette von doppelten Notierungen ("") 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 sind 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 Seriell über LAN (SOL)-Benutzerzugriff auf 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 iDRAC 6-E-Mail-Warnmeldungsfähigkeiten.

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

cfgEmailAlertIndex (schreibgeschützt)

Zulässige Werte

1 - 4

Standardeinstellung

<instance>

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, für die eine Verbindung zum iDRAC 6 hergestellt werden kann.

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 während der angegebenen Sitzungen inaktiv bleibt, wird die Sitzung geschlossen.

cfgSsnMgtConsRedirMaxSessions (Lesen / Schreiben)

Zulässige Werte

1 - 4

Standardeinstellung

2

Beschreibung

Gibt die maximale Anzahl von Konsolenumleitungssitzungen an, die auf dem iDRAC 6 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 im Leerlauf 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. Es ist erforderlich, dass Sie sich ab- und wieder anmelden, damit die neuen Einstellungen wirksam werden können.

cfgSsnMgtSshIdleTimeout (Lesen / Schreiben)

Zulässige Werte

0 (Kein Zeitlimit)

60 - 1920

Standardeinstellung

300

Beschreibung

Bestimmt die Leerlaufzeitüberschreitung für Secure Shell. Diese Eigenschaft legt die Zeitspanne in Sekunden fest, während der eine Verbindung im Leerlauf 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. Es ist erforderlich, dass Sie sich ab- und wieder anmelden, damit die neuen Einstellungen wirksam werden können.

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 hatte.

cfgSsnMgtTelnetTimeout (Lesen/Schreiben)

Zulässige Werte

0 (Kein Zeitlimit)

60 - 1920

Standardeinstellung

300

Beschreibung

Definiert die Leerlaufzeitüberschreitung von Telnet. Diese Eigenschaft legt die Zeitspanne in Sekunden fest, während der eine Verbindung im Leerlauf 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 wirksam werden können).

Eine abgelaufene Telnet-Sitzung zeigt die folgende Fehlermeldung an:

```
Connection timed out

(Zeitüberschreitung der Verbindung)
```

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

---

cfgSerial

Diese Gruppe enthält Konfigurationsparameter für die iDRAC 6-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 an der seriellen iDRAC 6-Schnittstelle 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-Tasten-Codes dargestellt werden:

(a) ^ gefolgt von einem beliebigen alphabetischen 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 iDRAC 6.

cfgSerialTelnetEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Telnet-Konsolenschnittstelle auf dem iDRAC 6.

---

cfgOobSnmp

Die Gruppe enthält Parameter zur Konfiguration des SNMP-Agenten und der Trap-Fähigkeiten des iDRAC 6.

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 iDRAC 6.

---

cfgRacTuning

Diese Gruppe wird verwendet, um verschiedene iDRAC 6-Konfigurationseigenschaften, wie z. B. gültige Schnittstellen und Schnittstellensicherheits-Beschränkungen 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 Schnittstellennummer an, die für die HTTP-Netzwerkkommunikation mit dem iDRAC 6 zu verwenden ist.

cfgRacTuneHttpsPort (Lesen/Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

443

Beschreibung

Gibt die Schnittstellennummer an, die für die HTTP-Netzwerkkommunikation mit dem iDRAC 6 zu verwenden ist.

cfgRacTuneIpRangeEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Funktion zur Überprüfung des iDRAC 6-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 iDRAC 6-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 sie 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 iDRAC 6-SSH-Schnittstelle verwendete Schnittstellennummer an.

cfgRacTuneTelnetPort (Lesen/Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

23

Beschreibung

Gibt die für die iDRAC 6-Telnet-Schnittstelle verwendete Schnittstellennummer 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 iDRAC 6-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 iDRAC 6.

cfgRacTuneLocalServerVideo (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert das lokale Servervideo (schaltet es ein) oder deaktiviert es (schaltet es aus).

cfgRacTuneLocalConfigDisable (Lesen / Schreiben)

Zulässige Werte

0 (TRUE)

1 (FALSE)

Standardeinstellung

0

Beschreibung

Deaktiviert Schreibzugriff auf die iDRAC 6-Konfigurationsdaten durch Einstellen auf 1.

cfgRacTuneWebserverEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert den iDRAC 6-Web Server. Wird diese Eigenschaft deaktiviert, ist der Zugriff auf den iDRAC 6 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 (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 255 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Der Host-Name des verwalteten Servers.

ifcRacMnOsOsName (schreibgeschützt)

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 iDRAC 6-SSL-CSR-Funktion (Zertifikatsignierungsanforderung) in Beziehung stehen. Die Eigenschaften in dieser Gruppe müssen konfiguriert werden, bevor vom iDRAC 6 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 allgemeinen Namen (CN) der CSR an, der ein IP- oder der iDRAC-Name, wie im Zertifikat festgelegt, 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-Zustandsnamen (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 iDRAC 6-Datenträgers. Es ist eine Instanz der Gruppe zulässig. In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben.

cfgVirMediaAttached (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-/Disketten-Laufwerks 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 Komponenten veranlasst, die Verbindung zum USB-Bus abzutrennen.

cfgVirtualBootOnce (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Einmal-Start-Funktion des virtuellen iDRAC 6-Datenträgers.

cfgVirMediaFloppyEmulation (Lesen / Schreiben)

ANMERKUNG: Der virtuelle Datenträger muss neu verbunden werden (mittels cfgVirMediaAttached), damit die Änderungen wirksam werden.

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 Floppy-Laufwerk von Windows-Betriebssystemen als Floppy-Laufwerk 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.

cfgActiveDirectory

Diese Gruppe enthält Parameter zum Konfigurieren der iDRAC 6-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 iDRAC 6 befindet.

cfgADRacName (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette von bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

<leer>

Beschreibung

Name des iDRAC 6, 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 iDRAC 6. Ist diese Eigenschaft deaktiviert, wird nur die Authentifizierung des lokalen iDRAC 6 für Benutzeranmeldungen verwendet.

cfgADDomainController1 (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

<leer>

Beschreibung

Der iDRAC 6 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 Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) darstellen.

Standardeinstellung

<leer>

Beschreibung

Der iDRAC 6 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 Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) darstellen.

Standardeinstellung

<leer>

Beschreibung

Der iDRAC 6 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 sollen, 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 Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) darstellen.

Standardeinstellung

<leer>

Beschreibung

iDRAC 6 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 Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) darstellen.

Standardeinstellung

<leer>

Beschreibung

iDRAC 6 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 Zeichen, die eine gültige IP-Adresse oder einen FQDN (vollständig qualifizierter Domänenname) darstellen.

Standardeinstellung

<leer>

Beschreibung

iDRAC 6 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-Zertifikatsvalidierung als Teil des Active Directory-Konfigurationsvorgangs.

---

cfgStandardSchema

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

cfgSSADRoleGroupIndex (schreibgeschützt)

Zulässige Werte

Eine ganze Zahl zwischen 1 und 5.

Standardeinstellung

<instance>

Beschreibung

Index der Rollengruppe, wie im Active Directory verzeichnet.

cfgSSADRoleGroupName (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette von bis zu 254 Zeichen ohne Leerzeichen.

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. Bit-Masken für Berechtigungen der Rollengruppe

Rollengruppenberechtigung	Bit-Maske
Bei 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 der der iDRAC 6 vor dem Übertragen eines teilweisen SOL-Zeichen-Datenpakets wartet. Dieser Wert besteht aus 1-basierten 5-ms-Stufen.

cfgIpmiSolSendThreshold (Read/Write)

Zulässige Werte

1 - 255

Standardeinstellung

255

Beschreibung

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

---

cfgIpmiLan

Diese Gruppe wird zur Konfiguration der IPMI-über-LAN-Fähigkeiten 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 einzelnen E-Mail-Warnmeldungs-Eigenschaften des Typs aktivieren/deaktivieren.

cfgIpmiEncryptionKey (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von Hexadezimalziffern von 0 bis 20 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 zum Konfigurieren von IPv6-Plattformereignis-Traps auf dem verwalteten Server verwendet.

cfgIpmiPetIPv6Index (schreibgeschützt)

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 zum Konfigurieren 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.

cfgIpmiPefName (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 255 Zeichen.

Standardeinstellung

Der Name des Index-Filters.

Beschreibung

Gibt den Namen des Plattformereignisfilters an.

cfgIpmiPefIndex (Lesen/Schreiben)

Zulässige Werte

1 - 19

Standardeinstellung

Der Indexwert eines Plattformereignisfilter-Objekts.

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 (schreibgeschützt)

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 darstellt. 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 zum Konfigurieren der Active Directory-Benutzerdomänennamen verwendet. Es können maximal 40 Domänenamen zu jeder gegeben Zeit konfiguriert werden.

cfgUserDomainIndex (schreibgeschützt)

Zulässige Werte

1 - 40

Standardeinstellung

Der Indexwert.

Beschreibung

Stellt eine spezifische Domäne dar.

cfgUserDomainName (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 255 ASCII-Zeichen.

Standardeinstellung

<leer>

Beschreibung

Gibt den Active Directory-Benutzerdomänennamen an.

---

cfgServerPower

Diese Gruppe bietet verschiedene Energieverwaltungsfunktionen.

cfgServerPowerStatus (schreibgeschützt)

Zulässige Werte

1 (EIN)

0 (AUS)

Standardeinstellung

<aktueller Serverstromzustand>

Beschreibung

Stellt den Serverstromzustand als entweder EIN oder AUS dar.

cfgServerPowerAllocation (schreibgeschützt)

ANMERKUNG: Wenn mehr als ein Netztzeil benötigt wird, sorgt diese Eigenschaft für einen Anstieg der minimalen Netzteilkapazität.

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<leer>

Beschreibung

Stellt die verfügbare zugewiesene Stromversorgung zur Verwendung des Servers dar.

cfgServerActualPowerConsumption (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<leer>

Beschreibung

Stellt den vom Server verbrauchten Strom zur aktuellen Zeit dar.

cfgServerMinPowerCapacity (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<leer>

Beschreibung

Stellt die minimale Serverstromkapazität dar.

cfgServerMaxPowerCapacity (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<leer>

Beschreibung

Stellt die maximale Serverstromkapazität dar.

cfgServerPeakPowerConsumption (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

<aktuelle Spitzenleistungsaufnahme des Servers>

Beschreibung

Stellt den maximalen vom Server verbrauchten Strom bis zur aktuellen Zeit dar.

cfgServerPeakPowerConsumptionTimestamp (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 32 Zeichen

Standardeinstellung

Zeitmarke der maximalen Leistungsaufnahme

Beschreibung

Zeitpunkt, an dem die maximale Leistungsaufnahme aufgezeichnet wurde.

cfgServerPowerConsumptionClear (Nur Schreibzugriff)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

****

Beschreibung

Setzt die cfgServerPeakPowerConsumption-Eigenschaft auf 0 und die cfgServerPeakPowerConsumptionTimestamp-Eigenschaft 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 zum Konfigurieren der IPv6-über-LAN-Netzwerkbetrieb-Fähigkeiten verwendet.

cfgIPv6Enable

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert den iDRAC 6-IPv6-Stapel.

cfgIPv6Address1 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

::

Beschreibung

Eine iDRAC 6-IPv6-Adresse.

cfgIPv6Gateway (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

::

Beschreibung

Die iDRAC 6-Gateway-IPv6-Adresse.

cfgIPv6PrefixLength (Lesen/Schreiben)

Zulässige Werte

1 - 128

Standardeinstellung

64

Beschreibung

Die Präfixlänge für die iDRAC 6-IPv6-Adresse 1.

cfgIPv6AutoConfig (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die IPv6-Option automatische Konfiguration.

cfgIPv6LinkLocalAddress (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

::

Beschreibung

Die lokale iDRAC 6-IPv6-Link-Adresse.

cfgIPv6Address2 (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

::

Beschreibung

Eine iDRAC 6-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 darstellt.

Standardeinstellung

::

Beschreibung

Eine IPv6-DNS-Server-Adresse.

cfgIPv6DNSServer2 (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die einen gültigen IPv6-Eintrag darstellt.

Standardeinstellung

::

Beschreibung

Eine IPv6-DNS-Server-Adresse.

---

cfgIPv6URL

Diese Gruppe legt Eigenschaften, die zum Konfigurieren der iDRAC 6-IPv6-URL verwendet werden, fest.

cfgIPv6URLstring (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von bis zu 80 Zeichen.

Standardeinstellung

<leer>

Beschreibung

Die iDRAC 6-IPv6-URL

---

cfgIpmiSerial

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

cfgIpmiSerialConnectionMode (Lesen/Schreiben)

Zulässige Werte

0 (Terminal)

1 (Basic)

Standardeinstellung

1

Beschreibung

Wenn die iDRAC 6-Eigenschaft **cfgSerialConsoleEnable** auf 0 (deaktiviert) gesetzt wird, wird die serielle iDRAC 6-Schnittstelle zur seriellen IPMI-Schnittstelle. Diese Eigenschaft bestimmt den definierten IPMI- Modus der seriellen Schnittstelle.

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

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 die serielle IPMI-Schnittstelle 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

Gibt die Spezifikation der Zeilenumbruchssequenz für die serielle IPMI-Schnittstelle an.

cfgIpmiSerialInputNewLineSequence (Lesen/Schreiben)

Zulässige Werte

0 (<EINGABE>)

1 (NULL)

Standardeinstellung

1

Beschreibung

Gibt die Spezifikation der Eingabe-Zeilenumbruchssequenz für die serielle IPMI-Schnittstelle an.

---

cfgSmartCard

Diese Gruppe legt Eigenschaften fest, die zur Unterstützung des Zugriffs auf den iDRAC 6 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 zum Zugriff auf den iDRAC 6 mithilfe 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 Aushandlung von physikalischer Verbindungsgeschwindigkeit und Duplex. Wenn aktiviert, hat die automatische Aushandlung 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 iDRAC 6-NIC verwendet wird.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Unterstützte RACADM-Schnittstellen

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Die folgende Tabelle enthält eine Übersicht über RACADM-Unterbefehle und ihre entsprechende Schnittstellenunterstützung.

Tabelle C-1. Schnittstellenunterstützung für RACADM-Unterbefehle

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

usercertview	✔	✔	✔
localConRedirDisable	✘	✔	✘
✔ = Unterstützt; ✘ = Nicht unterstützt			

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC 6-Übersicht

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Der Integrated Dell™ Remote Access Controller 6 (iDRAC 6) ist eine Systemverwaltungs-Hardware- und Software-Lösung, die Remote-Verwaltungsfähigkeiten, Wiederherstellung für abgestürzte Systeme sowie Stromsteuerungsfunktionen für Dell PowerEdge™-Systeme bietet.

Der iDRAC 6 verwendet einen integrierten System-auf-Chip-Mikroprozessor für das Remote-Überwachungs-/Steuerungssystem. Der iDRAC 6 und der verwaltete PowerEdge-Server koexistieren auf der Systemplatine. Das Betriebssystem des Servers befasst sich mit der Ausführung von Anwendungen und der iDRAC 6 mit der Überwachung und Verwaltung der Serverumgebung und des Serverstatus außerhalb des Betriebssystems.

Der iDRAC 6 kann so konfiguriert werden, dass er Ihnen bei Warnungen oder Fehlern eine E-Mail oder eine Trap-Warnung des einfachen Netzwerk-Verwaltungsprotokolls (SNMP) sendet. Um Ihnen bei der Diagnose der wahrscheinlichen Ursache eines Systemabsturzes behilflich zu sein, kann der iDRAC 6 Ereignisdaten protokollieren und einen Screenshot erstellen, wenn er einen Systemabsturz feststellt.

Die iDRAC 6-Netzwerkschnittstelle ist standardmäßig mit der statischen IP-Adresse 192.168.0.120 aktiviert. Sie muss konfiguriert werden, bevor ein Zugriff auf den iDRAC 6 möglich ist. Nachdem der iDRAC 6 auf dem Netzwerk konfiguriert wurde, kann auf ihn an seiner zugewiesenen IP-Adresse über die iDRAC 6-Webschnittstelle, Telnet oder SSH (Secure Shell) sowie unterstützte Netzwerkverwaltungsprotokolle wie die IPMI (intelligente Plattform-Verwaltungsschnittstelle) zugegriffen werden.

---

iDRAC 6 Express-Verwaltungsfunktionen

iDRAC 6 Express bietet die folgenden Verwaltungsfunktionen:

- Registrierung des dynamischen Domänennamensystems (DDNS)
- Remote-Systemverwaltung und -überwachung mithilfe einer Webschnittstelle und der SM-CLP-Befehlszeile über eine serielle, Telnet- oder SSH-Verbindung.
- Unterstützung für Microsoft® Active Directory®-Authentifizierung - Fasst iDRAC 6-Benutzer-IDs und -kennwörter unter Verwendung eines erweiterten oder Standardschemas in Active Directory zusammen
- Überwachung - Zugriff auf Systeminformationen und Komponentenstatus
- Zugriff auf Systemprotokolle - Bietet Zugriff auf das Systemereignisprotokoll, das iDRAC 6-Protokoll und den Bildschirm Letzter Absturz des abgestürzten oder nicht reagierenden Systems, unabhängig vom Zustand des Betriebssystems
- Dell OpenManage™ Software-Integration - Ermöglicht Ihnen, die iDRAC 6-Webschnittstelle vom Dell OpenManage Server Administrator oder IT Assistent zu starten
- iDRAC 6-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 von einer Verwaltungskonsole aus
- Unterstützung für die intelligente Plattform-Verwaltungsschnittstelle (IPMI)
- SSL (Secure Sockets Layer)-Verschlüsselung - 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 Systemverwaltungs-Tasks
- IPv6-Support - Bietet zusätzliche Unterstützung für z. B.: Zugriff auf die iDRAC 6-Webschnittstelle mithilfe einer IPv6-Adresse, legt die IPv6-Adresse für den iDRAC-NIC fest und bestimmt eine Zielnummer zum Konfigurieren eines IPv6-SNMP-Warnungsziels
- WS-MAN-Support - Bietet mithilfe des Protokolls Webdienste zur Verwaltung (WS-MAN) Verwaltung zum Zugriff auf das Netzwerk.
- SM-CLP-Support - Fügt SM-CLP (Serververwaltungs-Befehlszeilenprotokoll)-Support hinzu, um Standards für Systemverwaltungs-CLI-Implementierungen zu bieten.
- Zurücksetzen und Wiederherstellung der Firmware - Ermöglicht Ihnen, von einem Firmware-Image ihrer Wahl aus zu starten (oder zu einem zurückzusetzen).

Weitere Informationen zu iDRAC 6 Express finden Sie im *Hardware-Benutzerhandbuch* unter **support.dell.com\manuals**.

---

iDRAC6 Enterprise

Bietet zusätzliche Unterstützung für RACADM, virtuelle KVM, virtuelle Datenträgerfunktionen, einen dedizierten NIC und virtuellen Flash (mit einer optianalen Dell vFlash-Medienkarte). Weitere Informationen zu iDRAC 6 Express finden Sie im *Hardware-Benutzerhandbuch* unter **support.dell.com\manuals**.

---

iDRAC 6-Sicherheitsfunktionen

Der iDRAC 6 enthält die folgenden Sicherheitsfunktionen:

- Benutzerauthentifizierung durch Active Directory (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- and Webschnittstellen, die 128-Bit- und 40-Bit-Verschlüsselung unterstützen (für Länder, in denen 128-Bit nicht zulässig sind), verwenden den SSL 3.0-Standard
- Konfiguration der Sitzungszeitüberschreitung (in Sekunden) über die Webschnittstelle oder SM-CLP
- Konfigurierbare IP-Schnittstellen (wo anwendbar)

  ANMERKUNG: Telnet unterstützt SSL-Verschlüsselung nicht.

- 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
- Die Fähigkeit, den IP-Adressenbereich für Clients, die eine Verbindung zum iDRAC 6 herstellen, zu beschränken.
- Smart Card-Authentifizierung

Unterstützte Plattformen

Der iDRAC 6 unterstützt die folgenden PowerEdge-Systeme:

- PowerEdge R710
- PowerEdge R610
- PowerEdge T610

Informationen zu den neuesten unterstützten Plattformen finden Sie in der Infodatei zum iDRAC 6 und im *Dell OpenManage Server Administrator-Kompatibilitätshandbuch* unter **support.dell.com\manuals** und auf der DVD *Dell Systems Management Tools and Documentation*, die mit Ihrem System geliefert wurde.

Unterstützte Betriebssysteme

Tabelle 1-1 führt die Betriebssysteme auf, die den iDRAC 6 unterstützen.

Aktuelle Informationen hierzu erhalten Sie im *Dell OpenManage Server Administrator-Kompatibilitätshandbuch* auf der Dell Support-Website unter **support.dell.com\manuals** und auf der DVD *Dell Systems Management Tools and Documentation*, die mit Ihrem System geliefert wurde.

Tabelle 1-1. Unterstützte Betriebssysteme für den verwalteten Server

Betriebssystem-Familie	Betriebssystem
Microsoft Windows	Windows Server® 2003-Familie mit folgendem Inhalt: Windows Server 2003 R2 (Web, Standard und Enterprise Editions) mit SP2 (x86) Windows Server 2003 R2 (Standard, Enterprise und DataCenter Editions) mit SP2 (x64) Windows Server 2003 (SBS, Standard und Premium Editions) mit SP2 **ANMERKUNG:** Achten Sie beim Installieren des Windows Server 2003 mit Service Pack 1 auf Änderungen an den DCOM-Sicherheitseinstellungen. Weitere Informationen finden Sie in Artikel 903220 auf der Support-Website von Microsoft unter **support.microsoft.com/kb/903220**. Windows Server 2008 Core (Web, Standard und Enterprise Editions) (x86) Windows Server 2008 Core (Standard, Enterprise und DataCenter Editions (x64) Windows Server 2008 SBS, EBS, Standard und Premium Editions
SUSE® Linux	Enterprise Server 10 SP2
Red Hat® Linux®	Enterprise Linux 4.7 (x86_32, x86_64) Enterprise Linux 5 U2 (x86_32, x86_64)
VMware®	ESX 3.5 U4 ESXi 3.5 U4 Flash

Unterstützte Webbrowser

Tabelle 1-2 führt die als iDRAC 6-Clients unterstützten Webbrowser auf.

Neueste Informationen hierzu finden Sie in der iDRAC 6-Infodatei und dem *Dell OpenManage Server Administrator-Kompatibilitätshandbuch* auf der Dell Support-Website unter **support.dell.com\manuals**.

ANMERKUNG: Aufgrund von ernsthaften Sicherheitslücken wird SSL 2.0 nicht mehr unterstützt. Ihr Browser muss so konfiguriert sein, dass SSL 3.0 für eine einwandfreie Arbeitsweise aktiviert werden kann.

Tabelle 1-2. Unterstützte Web-Browser

Unterstützte Web-Browser
Microsoft Internet Explorer 6.0 mit SP2 für Windows XP, Windows 2000 Server, Windows 2000 Pro, Windows 2003 Server Gold, Windows 2003 Server SP1 und Windows 2003 Server SP2
Microsoft Internet Explorer 7.0 für Windows 2003 Server Gold, Windows 2003 Server SP1, Windows 2003 Server SP2, Windows Server 2008 und Windows Vista
Mozilla Firefox 2.0 auf SUSE Linux Enterprise Server (SLES) 10 SP1
Mozilla Firefox 3.0 auf Windows 2003 Server Gold, Windows 2003 Server SP1, Windows 2003 Server SP2, Windows 2000 Pro, Windows XP, Windows Server 2008, Windows Vista, Red Hat Enterprise Linux 4 und 5, SLES 9 und 10 und SLES 10 SP1

Unterstützte Remote-Zugriffsverbindungen

Tabelle 1-3 führt die Verbindungsfunktionen auf.

Tabelle 1-3. Unterstützte Remote-Zugriffs-Verbindungen

Verbindung	Funktionen
iDRAC 6-NIC	• 10 MBit/s/100 MBit/s/Ethernet • DHCP-Unterstützung • SNMP-Traps und E-Mail-Ereignis-Benachrichtigung • Unterstützung für SM-CLP-Befehlsshell (Telnet oder SSH) und für Verfahren wie iDRAC 6-Konfigurations-, Systemstart-, Reset-, Einschalt- und Herunterfahren-Befehle • Unterstützung für IPMI-Dienstprogramme wie IPMItool und ipmish • Serielle Verbindungen

iDRAC 6-Anschlüsse

Tabelle 1-4 führt die Anschlüsse auf, die der iDRAC 6 auf Verbindungen abhört. Tabelle 1-5 kennzeichnet die Anschlüsse, die der iDRAC 6 als Client verwendet. Diese Informationen sind erforderlich, wenn Firewalls für den Remote-Zugriff auf einen iDRAC 6 geöffnet werden.

Tabelle 1-4. iDRAC 6-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 1-5. iDRAC 6-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 iDRAC 6 auf dem System. Diese Dateien sind auf der Dell Support-Website unter **support.dell.com\manuals** verfügbar.

- Die iDRAC 6-Online-Hilfe enthält genaue Informationen zur Verwendung der webbasierten Schnittstelle.
- Weitere Informationen zur Konfiguration der iDRAC-Hardware und Systemdienste finden Sie im *Dell Unified Server Configurator-Benutzerhandbuch*.
- Das *Dell OpenManage IT Assistant-Benutzerhandbuch* enthält Informationen zur Verwendung des IT Assistant.
- Informationen zum Installieren eines iDRAC 6 finden Sie im *Hardware-Benutzerhandbuch*.
- Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen über die Installation und Verwendung von Server Administrator.
- Informationen über die neuesten unterstützten Plattformen finden Sie in der iDRAC 6-Infodatei und im *Dell OpenManage Server Administrator-Kompatibilitätshandbuch*.
- Das *Benutzerhandbuch zu Dell Update Packages* enthält Informationen zum Abrufen und Verwenden von Dell Update Packages als Teil Ihrer Systemaktualisierungsstrategie.
- Informationen zur iDRAC 6- und IPMI-Schnittstelle erhalten Sie im *Dell OpenManage Baseboard-Verwaltungs-Controller-Dienstprogramm-Benutzerhandbuch*.

Die folgenden Systemdokumente sind außerdem erhältlich, um weitere Informationen über das System zur Verfügung zu stellen, auf dem Ihr iDRAC 6 installiert ist:

- 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, Einrichtung des Systems und technische Daten.
- Im *Hardware-Benutzerhandbuch* erhalten Sie Informationen über Systemfunktionen, zur Fehlerbehebung am System und zum Installieren oder Austauschen von Systemkomponenten.
- In der Dokumentation zur Systemverwaltungssoftware sind die Merkmale, die Anforderungen, die Installation und der grundlegende Einsatz der Software beschrieben.
- In der Dokumentation zum Betriebssystem ist beschrieben, wie das Betriebssystem installiert (sofern erforderlich), konfiguriert und verwendet wird.
- Dokumentationen für alle separat erworbenen Komponenten enthalten Informationen zur Konfiguration und zur Installation dieser Zusatzgeräte.
- Möglicherweise sind auch aktualisierte Dokumente beigelegt, in denen Änderungen am System, an der Software und/oder an der Dokumentation beschrieben sind.

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

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Virtuellen Datenträger konfigurieren und verwenden

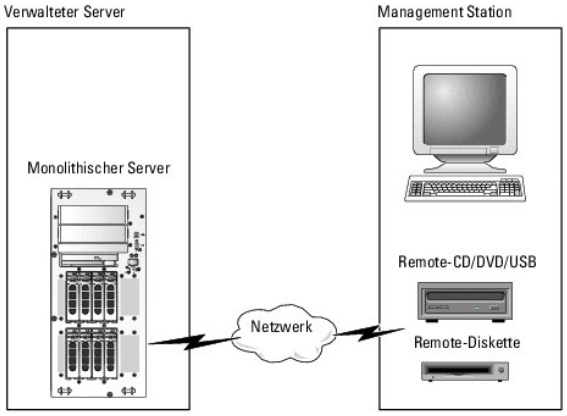
Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

---

Übersicht

Die Funktion **Virtueller Datenträger**, auf die über den Konsolenumleitungs-Viewer zugegriffen werden kann, bietet dem verwalteten Server Zugriff auf Datenträger, die mit einem Remote-System auf dem Netzwerk verbunden sind. Abbildung 10-1 zeigt die gesamte Architektur des **virtuellen Datenträgers**.

Abbildung 10-1. 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 Disketten-Laufwerken installieren.

ANMERKUNG: Virtuelle Datenträger erfordern eine minimale verfügbare Netzwerkbandbreite von 128 kbps.

Virtueller Datenträger definiert zwei Geräte für das Betriebssystem und das BIOS des verwalteten Servers: ein Diskettenlaufwerk und ein optisches Festplattenlaufwerk.

Die Management Station liefert die physischen Datenträger oder Bilddatei über das Netzwerk. Wenn ein **virtueller Datenträger** angeschlossen oder automatisch angeschlossen wird, werden alle Zugriffsanforderungen der Management Station auf das virtuelle CD-/Disketten-Laufwerk über das Netzwerk an die Verwaltungsstation geleitet. Das Verbinden des **virtuellen Datenträgers** scheint identisch mit dem Einsetzen von Datenträgern in physische Geräte zu sein. Ist der virtuelle Datenträger nicht angeschlossen, werden die virtuellen Geräte nicht beim verwalteten Server angezeigt.

Tabelle 10-1 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 10-1. Unterstützte Laufwerkverbindungen

Unterstützte Verbindungen virtueller Disketten-Laufwerke	Unterstützte Verbindungen virtueller optischer Laufwerke
Legacy 1,44 Zoll-Disketten-Laufwerk mit 1,44 Zoll-Diskette	CD-ROM, DVD, CDRW, Kombinationslaufwerk mit CD-ROM-Datenträger
USB-Disketten-Laufwerk mit 1,44 Zoll-Diskette	CD-ROM/DVD-Image-Datei im Format ISO9660
1,44 Zoll-Floppy-Abbild	USB-CD-ROM-Laufwerk mit CD-ROM-Datenträger
USB-Wechselplatte	

Windows-basierte Management Station

Um die Funktion des **virtuellen Datenträgers** auf einer Verwaltungsstation mit dem Betriebssystem Microsoft® Windows® auszuführen, installieren Sie eine unterstützte Internet Explorer- oder Firefox-Version mit Java Runtime Environment (JRE). Näheres erfahren Sie im Abschnitt "Unterstützte Webbrowser".

Linux-basierte Management Station

Um die Funktion des virtuellen Datenträgers auf einer Verwaltungsstation mit Linux-Betriebssystem auszuführen, installieren Sie eine unterstützte Version von Firefox. Weitere Informationen finden Sie unter "Unterstützte Webbrowser".

Zum Ausführen des Konsolenumleitungs-Plugin ist eine Java-Laufzeitumgebung (JRE) erforderlich. Sie können eine JRE von **java.sun.com** herunterladen. JRE-Version 1.6 oder höher wird empfohlen.

Virtuellen Datenträger konfigurieren

1. Melden Sie sich bei der iDRAC6-Webschnittstelle an.
2. Wählen Sie **System**→ **Konsole/Datenträger** aus.
3. Klicken Sie auf **Konfiguration**→ **Virtueller Datenträger**, um die Einstellungen des virtuellen Datenträgers zu konfigurieren.

   Tabelle 10-2 beschreibt die Konfigurationswerte des **virtuellen Datenträgers**.
4. Wenn Sie mit den Einstellungen fertig sind, klicken Sie auf **Anwenden**.
5. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 10-3.

Tabelle 10-2. Konfigurationseigenschaften für virtuelle Datenträger

Attribut	Wert
Zustand Remote-Datenträger angeschlossen	**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 am Server an, wenn eine Sitzung des virtuellen Datenträgers gestartet wird.
Max. Sitzungen	Zeigt die maximale Anzahl an zulässigen **Virtueller Datenträger-Sitzungen** an, die immer 1 ist.
Aktive Sitzungen	Zeigt die aktuelle Anzahl von Sitzungen des virtuellen Datenträgers an.
Virtueller Datenträger-Verschlüsselung 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 Diskettenlaufwerk oder USB-Schlüssel angezeigt wird. Wenn **Diskettenemulation** markiert ist, wird das **virtuelle Datenträger**-Gerät auf dem Server als Diskettengerät angezeigt. Wenn es nicht ausgewählt ist, wird es als USB-Schlüssellaufwerk angezeigt.
Einmal Starten aktivieren	Wählen Sie dieses Kästchen aus, um die Option Einmal Starten zu aktivieren. Diese Option beendet die Sitzung des **Virtuellen Datenträgers** automatisch, nachdem der Server einmal gestartet wurde. Diese Option ist nützlich für automatische Bereitstellungen.

Tabelle 10-3. Schaltflächen der Konfigurationsseite

Schaltfläche	Beschreibung
Drucken	Druckt die Werte der **Konfiguration**, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Konfiguration** erneut.
Änderungen 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: Die Anwendung des Konsolen-Viewer-Fensters muss während des Zugriffs auf den virtuellen Datenträger aktiv 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. Server neu starten

3. Führen Sie die folgenden Befehle aus, um die virtuelle CD/DVD und/oder die virtuelle Diskette anzuzeigen:

   cat /proc/scsi/scsi

ANMERKUNG: Mit 'Virtueller Datenträger' können Sie nur ein(e) Diskette/USB-Laufwerk/Image/Schlüssel und ein optisches Laufwerk von Ihrer Management Station virtualisieren, die als (virtuelles) Laufwerk auf dem verwalteten Server verfügbar sind.

Unterstützte Konfigurationen des virtuellen Datenträgers

Sie können den virtuellen Datenträger für ein Floppy-Laufwerk und ein optisches Laufwerk aktivieren. Es kann für jeden Datenträgertyp nur ein einziges Laufwerk auf einmal 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 zum Ausführen von 'Virtueller Datenträger' aus:

1. Öffnen Sie einen unterstützten Internet-Browser auf der Management Station. Weitere Informationen finden Sie unter "Unterstützte Webbrowser".

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

3. Wählen Sie **System**→ **Konsole/Datenträger** aus.

   Die Seite **Konsolenumleitung und virtueller Datenträger** wird angezeigt. Wenn Sie die Werte angezeigter Attribute ändern möchten, finden Sie entsprechende Informationen unter "Virtuellen Datenträger konfigurieren".

   ANMERKUNG: Die Disketten**-Abbilddatei** unter Disketten**-Laufwerk** (falls zutreffend) kann angezeigt werden, da diese Komponente als virtuelle Diskette virtualisiert werden kann. Sie können ein optisches Laufwerk und eine Diskette/ein USB-Flashlaufwerk 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 eventuell nicht ordnungsgemäß auf Clients des Windows-Betriebssystems, die mit Internet Explorer Enhanced Security konfiguriert wurden. Um dieses Problem zu lösen, ziehen Sie die Dokumentation zu Ihrem Microsoft-Betriebssystem zurate oder setzen sich mit Ihrem Systemadministrator in Verbindung.

4. Klicken Sie auf **Viewer starten**.

   ANMERKUNG: Bei Linux wird die Datei **jviewer.jnlp** auf den Desktop heruntergeladen und 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 **iDRAC KVM Agent** wird in einem separaten Fenster gestartet.

5. Klicken Sie auf **Extras**→ **Virtuellen Datenträger starten**.

   Der Assistent zur Datenträgerumleitung wird eingeblendet.

   ANMERKUNG: Schließen Sie diesen Assistenten nur, wenn Sie die Sitzung des virtuellen Datenträgers beenden möchten.

6. Wenn eine Datenträgerverbindung besteht, muss diese vor dem Verbinden mit einer anderen Datenträgerquelle zuerst unterbrochen werden. Wählen Sie das Kästchen links vom Datenträger, der abgetrennt werden soll, ab.

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

   Wenn Sie eine Verbindung zu einem Disketten-Image oder einem ISO-Image herstellen möchten, geben Sie (auf Ihrem lokalen Computer) den Pfad zum Image ein, oder klicken Sie auf die Schaltfläche **Image hinzufügen...**, um zum Image zu navigieren**.**

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

Verbindung des virtuellen Datenträgers unterbrechen

1. Klicken Sie auf **Extras**→ **Virtuellen Datenträger starten**.

2. Wählen Sie das Kästchen neben dem Datenträger, den Sie abtrennen möchten, ab.

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

3. Klicken Sie auf **Beenden, um den Datenträgerumleitungs assistenten zu beenden**.

Starten vom virtuellen Datenträger

Das System-BIOS ermöglicht Ihnen, von virtuellen optischen Laufwerken oder virtuellen Diskettenlaufwerken 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 werden.

Um die BIOS-Einstellung zu ändern, führen Sie die folgenden Schritte aus:

1. Starten Sie den verwalteten Server.
2. Drücken Sie auf <F2>, um das BIOS-Setup-Fenster aufzurufen.
3. Rollen Sie zur Startsequenz und drücken Sie auf die Eingabetaste.

   Im Popup-Fenster werden die virtuellen optischen Laufwerke und virtuellen Disketten-Laufwerke mit den Standardstartkomponenten aufgeführt.

4. Stellen Sie sicher, dass das virtuelle Laufwerk aktiviert und als erste Komponente mit startfähigem Datenträger aufgeführt 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 wird und startfähige Datenträger vorhanden sind, startet das System zum virtuellen Gerät. Ansonsten ignoriert das System die Komponente - ähnlich wie einer physischen Komponente ohne startfähigen Datenträger.

Installation von Betriebssystemen mittels virtueller Datenträger

In diesem Abschnitt wird eine manuelle, interaktive Methode zum Installieren des Betriebssystems auf der Management Station beschrieben, die mehrere Stunden in Anspruch nehmen kann. 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, die im Abschnitt "Starten vom virtuellen Datenträger" enthalten sind, um sicherzustellen, dass das BIOS so eingestellt ist, dass es von dem CD- Laufwerk aus startet, von dem aus Sie die Installation vornehmen.
3. Folgen Sie den Bildschirmanleitungen, um die Installation abzuschließen.

Es ist wichtig, diese Schritte für die Mehrfach-Disk-Installation 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 kann fehlschlagen.

Funktion 'Einmal starten'

Mit der Funktion 'Einmal starten' können Sie die Startreihenfolge zeitweise ändern, um von einem virtuellen Remote-Datenträgergerät 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 nutzen zu können.

Verwenden der 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 **Boot Once Enabled ('Einmal starten' aktiviert)** unter Virtueller Datenträger aus.
5. Schalten Sie den Server aus und dann wieder ein.

   Der Server startet vom Remote-Gerät des virtuellen Datenträgers. Wenn der Server beim nächsten Mal neu startet, wird die Verbindung des virtuellen Datenträgers abgetrennt.

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 werden.

Die Verwendung der virtuellen Laufwerke innerhalb Windows ist der Verwendung der physischen Laufwerke ähnlich. Wenn Sie über den Assistenten des virtuellen Datenträgers eine Verbindung zum Datenträger herstellen, ist der Datenträger am System verfügbar, wenn Sie auf das Laufwerk klicken und dessen Inhalt durchsuchen.

Linux-basierte Systeme

Abhängig von der Konfiguration der Software auf Ihrem System dürfen die virtuellen Datenträgerlaufwerke nicht automatisch geladen werden. Wenn Ihre Laufwerke nicht automatisch geladen werden, laden Sie sie unter Verwendung des Linux-Befehls **Laden** manuell.

Häufig gestellte Fragen

Tabelle 10-4 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 10-4. Virtuelle Datenträger verwenden: Häufig gestellte Fragen

Frage	Antwort
Manchmal bemerke ich, dass die Client-Verbindung meines virtuellen Datenträgers unterbrochen wird. Warum?	Wenn bei einem Netzwerk eine Zeitüberschreitung eintritt, trennt die iDRAC6-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Wenn die Konfigurationseinstellungen des virtuellen Datenträgers in der iDRAC6-Webschnittstelle oder durch Befehle des lokalen RACADM geändert werden, wird die Verbindung aller verbundener Datenträger bei Übernahme der Konfigurationsänderung unterbrochen. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie den Virtuellen Datenträger-Assistenten.
Welche Betriebssysteme unterstützen den iDRAC6?	Eine Liste unterstützter Betriebssysteme finden Sie unter "Unterstützte Betriebssysteme".
Welche Webbrowser unterstützen den iDRAC6?	Eine Liste unterstützter Internet-Browser erhalten Sie unter "Unterstützte Webbrowser".
Warum bricht meine Client-Verbindung manchmal ab?	• Ihre Client-Verbindung kann manchmal abbrechen, 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 verloren gehen, wenn das Client-System zu viel Zeit in Anspruch nimmt, bevor es 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, trennt die iDRAC6-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Es ist auch möglich, dass jemand die Konfigurationseinstellungen des virtuellen Datenträgers in der Webschnittstelle oder durch Eingabe von RADACM-Befehlen verändert hat. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie die Funktion **Virtueller Datenträger**.
Eine Installation des Windows-Betriebssystems über virtuelle 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 Netzwerklatenzzeit mehr Zeit in Anspruch nimmt, um auf die iDRAC6-Webschnittstelle zuzugreifen. Obwohl das Installationsfenster den Installationsfortschritt nicht anzeigt, wird das Installationsverfahren dennoch durchgeführt.
Wie konfiguriere ich meine virtuelle Komponente als startfähige Komponente?	Greifen Sie auf dem verwalteten Server auf das BIOS-Setup zu und wechseln Sie zum Startmenü. Machen Sie die virtuelle CD, die virtuelle Diskette oder den Virtual Flash ausfindig und ändern Sie die Komponenten-Startreihenfolge wie erforderlich. 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: • CDROM/DVD-Datenträger • ISO 9660-Abbild • 1,44 Zoll-Diskette oder Diskette-Abbild • USB-Schlüssel, der vom Betriebssystem als Wechselplatte erkannt wird • Ein USB-Schlüsselabbild
Wie kann ich meinen USB-Schlüssel startfähig machen?	Suchen Sie unter **support.dell.com** nach dem Dell-Startdienstprogramm, einem Windows-Programm, mit dem Sie den Dell-USB-Schlüssel startfähig machen können. Sie können auch über eine Windows 98-Startdiskette starten und Systemdateien von der Startdiskette auf Ihren 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 Floppy-Komponente/virtuelle CD auf einem System, das das Red Hat Enterprise Linux- oder SUSE® Linux-Betriebssystem ausführt, nicht finden. Mein virtueller Datenträger ist angeschlossen und ich bin mit meiner Remote-Diskette verbunden. Was soll ich tun?	Bei einigen Linux-Versionen erfolgt die automatische Ladung des virtuellen Floppy-Laufwerks und des virtuellen CD-Laufwerks auf unterschiedliche Weise. 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 Disketten-Laufwerk 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 gemeldet wurde. 4. Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls und finden Sie den Gerätenamen, der der virtuellen Dell-Diskette gegeben wurde. 5. Stellen Sie sicher, dass das virtuelle Disketten-Laufwerk angeschlossen ist und dass 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 ausfindig gemachte Name der Komponente ist. /mnt/floppy ist der Bereitstellungspunkt.
Ich kann meine virtuelle Floppy-Komponente/virtuelle CD auf einem System, das das Red Hat® Enterprise Linux®- oder SUSE® Linux-Betriebssystem ausführt, nicht finden. Mein virtueller Datenträger ist angeschlossen und ich bin mit meiner Remote-Diskette verbunden. Was soll 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 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 Hierfür gilt hh:mm:ss der Zeitstempel der Meldung ist, die von grep in Schritt 1 gemeldet wurde. 4. Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls, und machen Sie den Komponentennamen ausfindig, den die "virtuelle Dell-CD" trägt. 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 ausfindig gemachte Name der Komponente 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 führen zu einem Reset des iDRAC6, einem Abbruch der Remote-Verbindung sowie zum Entladen der virtuellen Laufwerke.
Warum werden alle meine USB-Geräte abgetrennt, nachdem ich ein USB-Gerät angeschlossen habe?	Virtuelle Datenträgergeräte und virtuelle Flash-Geräte werden als gemeinsames USB-Gerät am Host-USB-BUS angeschlossen, und sie verwenden einen gemeinsamen USB-Anschluss. Wann immer 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 zeitweise vom Host-USB-Bus

	abgetrennt und danach wieder verbunden. Wenn ein virtuelles Datenträger-Gerät vom Host-Betriebssystem verwendet wird, müssen Sie das Verbinden oder 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

WS-MAN-Schnittstelle verwenden

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Die iDRAC 6-Firmware bietet Verwaltung zum Zugriff auf das Netzwerk über das WS-MAN-Protokoll (Web Services für die Vewaltung). WS-MAN ist ein Übertragungsmechanismus für den Informationsaustausch. WS-MAN bietet eine universelle Sprache für Geräte zur Freigabe von Daten, damit diese einfacher verwaltet werden können. WS-MAN stellt einen wesentlichen Teil der Remote-System-Verwaltungslösung dar, jedoch ist es nicht der einzige Teil.

WS-MAN verwendet HTTPS, um sicheren Veraltungsdatenverkehr zu gewährleisten. Der Client muss sich mithilfe der lokalen oder der Microsoft® Active Directory®-Benutzerberechtigungen anmelden, um die Sitzung zu authentifizieren. HTTPS verwendet SSL (Secure Socket Layer) am IP-Anschluss 443, um Datenübertragungen zu sichern.

Die durch WS-MAN zur Verfügung gestellten Daten sind eine Teilmenge der Daten, die von der iDRAC 6-Instrumentierungsschnittstelle geliefert werden, die den DMTF-Profilen (Distributed Management Task Force) und den Dell-Erweiterungsprofilen zugewiesen sind.

WS-MAN ist die gebräuchlichste Anwendung zum Übertragen von DMTF-CIM-basierten Verwaltungsinformationen. CIM bestimmt die Typen zur Informationsverwaltung, die in einem verwalteten System verändert werden können. Darin sind die Objekte enthalten, über die sich der Client und der Dienst über die Leitung verständigen. WS-MAN legt einige Standardmaßnahmen fest, die auf Verwaltungsobjekten ausgeführt werden können. Beispiel: Ein Client-System kann durch Verwendung von WS-MAN eine Sammlung von Verwaltungsobjekten auffinden, den Inhalt eines Verwaltungsobjekts abrufen und dessen Inhalt auf neue Werte einstellen. WS-MAN enthält Verben zur Verwaltungskonversation; CIM-Klassen und -Eigenschaften stellen die Nomen und zwar Objekte dar, auf denen Maßnahmen durch die Verben ausgeführt werden.

Um Kompatibilität zwischen Clients und Diensten zu gewährleisten, legen DMTF und Dell weiterhin ein minimales Standard-*Vokabular* von CIM-Klassen, Eigenschaften und Verhaltensweisen fest, die jeder Teil verstehen muss. Diese DMTF- und Dell-spezifischen Profile bestimmen ein Set an Konventionen, die von allen dem Standard entsprechenden Diensten umgesetzt werden müssen. Aus diesem Grund können sich alle Clients darauf verlassen, dass diese Konventionen ordnungsgemäß funktionieren.

Unterstützte CIM-Profile

Tabelle 11-1. Unterstützte CIM-Profile

Standard-DMTF
1. Basisserver Bestimmt CIM-Klassen zum Darstellen des Host-Servers.
2. Serviceprozessor: Enthält die Definition von CIM-Klassen zum Darstellen des iDRAC 6. **ANMERKUNG:** Das Profil des Basisservers (oben) und des Serviceprozessors sind hinsichtlich der sie beschreibenden Objekte autonom, die alle anderen in den Komponentenprofilen definierten CIM-Objekte zusammenfassen.
3. Physische Anlagen: Bestimmen CIM-Klassen zum Darstellen der physischen Aspekte der verwalteten Elemente. iDRAC 6 verwendet dieses Profil, um die FRU-Informationen des Hostservers und seiner Komponenten sowie die physische Topologie darzustellen.
4. SM-CLP-Administrator-Domäne Bestimmt CIM-Klassen zum Darstellen der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für eigene Umsetzung von CLP.
5. Stromzustandsverwaltung Bestimmt CIM-Klassen für Stromsteuerungsvorgänge. iDRAC 6 verwendet dieses Profil für die Stromsteuerungsvorgänge des Hostservers.
6. Netzteil (Version 1.1) Bestimmt CIM-Klassen zum Darstellen von Netzteilen. iDRAC 6 verwendet dieses Profil zum Darstellen der Netzteile des Hostservers, um den Stromverbrauch, wie z. B. Wasserzeichen eines hohen und niedrigen Stromverbrauchs, zu beschreiben.
7. CLP-Dienst Bestimmt CIM-Klassen zum Darstellen der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für eigene Umsetzung von CLP.
8. IP-Schnittstelle 9. DHCP-Client 10. DNS-Client 11. Ethernet-Anschluss Die zuvor erwähnten Profile bestimmen CIM-Klassen zum Darstellen von Netzwerkstapeln. iDRAC 6 verwendet diese Profile, um die Konfiguration des iDRAC 6-NIC darzustellen.
12. Datensatzprotokoll Bestimmt CIM-Klassen zum Darstellen unterschiedlicher Protokolltypen. iDRAC 6 verwendet dieses Profil, um das Systemereignisprotokoll (SEL) und das iDRAC 6-RAC-Protokoll darzustellen.
13. Software-Bestandsaufnahme Bestimmt CIM-Klassen zur Bestandsaufnahme von installierter oder verfügbarer Software. iDRAC 6 verwendet dieses Profil zur Bestandsaufnahme von kürzlich installierten iDRAC 6-Firmwareversionen über das TFTP-Protokoll.

14. Rollenbasierte Authentifizierung Bestimmt CIM-Klassen zum Darstellen von Rollen. iDRAC 6 verwendet dieses Profil zum Konfigurieren von iDRAC 6-Kontoberechtigungen.
15. Software-Aktualisierung Bestimmt CIM-Klassen zur Bestandsaufnahme von verfügbaren Software-Aktualisierungen. iDRAC 6 verwendet dieses Profil zur Bestandsaufnahme von Firmware-Aktualisierungen über das TFTP-Protokoll.
16. SMASH-Sammlung Bestimmt CIM-Klassen zum Darstellen der CLP-Konfiguration. iDRAC6 verwendet dieses Profil für eigene Umsetzung von CLP.
17. Profilregistrierung Bestimmt CIM-Klassen zur Ankündigung von Profil-Implementierungen. iDRAC 6 verwendet dieses Profil, um eigene implementierte Profile, wie in dieser Tabelle dargestellt, anzukündigen.
18. Basismetrik Bestimmt CIM-Klassen zum Darstellen der Metrik. iDRAC 6 verwendet dieses Profil zum Darstellen der Metrik des Hostservers, um den Stromverbrauch, wie z. B. Wasserzeichen eines hohen und niedrigen Stromverbrauchs, zu beschreiben.
19. Einfache Identitätsverwaltung Bestimmt CIM-Klassen zum Darstellen der Identitäten. iDRAC 6 verwendet dieses Profil zum Konfigurieren von iDRAC 6-Konten.
20. USB-Umleitung Bestimmt CIM-Klassen zum Darstellen der Remote-Umleitung von lokalen USB-Anschlüssen. iDRAC 6 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 Bestimmt CIM- und Dell-Erweiterungsklassen zum Konfigurieren des iDRAC 6-Active Directory-Clients und der lokalen Berechtigungen für Active Directory-Gruppen.
2. Dells virtueller Datenträger Bestimmt CIM- und Dell-Erweiterungsklassen zum Konfigurieren des virtuellen iDRAC 6-Datenträgers. Erweitert USB-Umleitungsprofile.
3. Dells Ethernet-Anschluss Bestimmt CIM- und Dell-Erweiterungsklassen zum Konfigurieren der NIC-Seitenband-Schnittstelle für den iDRAC 6-NIC. Erweitert Ethernet-Anschlussprofile.
4. Dells Stromeinsatzverwaltung Bestimmt CIM- und Dell-Erweiterungsklassen zum Darstellen, Konfigurieren und Überwachen des Strombudgets des Hostservers.

Weitere Informationen finden Sie unter **www.dmtf.org/standards/profiles/**. Aktualisierungen in der Profilliste oder Informationen hierzu finden Sie in den Versionshinweisen oder in der Infodatei von WS-MAN.

Die WS-MAN-Implementierung stimmt mit der DMTF-WS-MAN-Spezifikation Version 1.0.0 überein. Bekannte, kompatible Hilfsprogramme, die das WS-MAN-Protokoll unterstützen, umfassen (sind aber nicht beschränkt auf) Microsoft Windows® Remote-Verwaltung (WinRM)-, open wsman- und wsmancli-Hilfsprogramme.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC 6-SM-CLP-Befehlszeilenschnittstelle verwenden

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Dieser Abschnitt enthält Informationen zum im iDRAC 6 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-Angaben vertraut sind. Weitere Informationen zu diesen Angaben finden Sie auf der Website zur Distributed Management Task Force (DMTF) unter **www.dmtf.org**.

Das iDRAC 6-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 auf mehreren Plattformen. Die SM-CLP-Spezifikation beschreibt die standardisierten Verben und Ziele zum Ausführen verschiedener Verwaltungsaufgaben in Verbindung mit den Spezifikationen zur verwalteten Elementadressierung und zahlreichen Profilen zur SM-CLP-Zuordnungsspezifikation.

Support für iDRAC 6-SM-CLP

Das SM-CLP wird von der iDRAC 6-Controller-Firmware aus gehostet und unterstützt Telnet, SSH und seriell basierte Schnittstellen. Die iDRAC 6-SM-CLP-Schnittstelle basiert auf der SM-CLP-Spezifikation Version 1.0, bereitgestellt von der DMTF-Organisation. iDRAC 6-SM-CLP unterstützt alle Profile, die unter Tabelle 11-1 "Unterstützte CIM-Profile" beschrieben sind.

Die folgenden Abschnitte enthalten eine Übersicht der SM-CLP-Funktion, die vom iDRAC 6 gehostet wird.

SM-CLP-Funktionen

Das SM-CLP fördert das Konzept von Verben und Zielen und stellt Systemverwaltungsfähigkeiten durch die CLI bereit. Das Verb zeigt 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	Wechselt mittels der Shell durch den MAP.
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	Bewegt ein Binärbild von einer URL zu einer bestimmten Zieladresse.

SM-CLP verwenden

SSH (oder Telnet) am iDRAC 6 mit den richtigen Anmeldeinformationen.

Die SMCLP-Eingabeaufforderung (/admin1->) wird angezeigt.

SM-CLP-Ziele

Tabelle 12-2 enthält eine Liste von durch das SM-CLP gebotenen Zielen, um die in Tabelle 12-1 beschriebenen Vorgänge zu unterstützen.

Tabelle 12-2. SM-CLP-Ziele

Ziel	Definitionen
admin1	admin domain
admin1/profiles1	Im iDRAC 6 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-Erfassung der verwalteten Systemfunktionen
admin1/system1/capabilities1/pwrcap1	Funktionen zur Energieausnutzung des verwalteten Systems
admin1/system1/capabilities1/elecap1	Zielfähigkeiten 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-Erfassung der verwalteten Systemeinstellungen
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 Serviceprozessorfähigkeiten
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	Energieausnutzung-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	Erfassung der Serviceprozessorprotokolle
admin1/system1/sp1/logs1/log1	Systemdatensatzprotokoll
admin1/system1/sp1/logs1/log1/record*	Systemprotokolleintrag
admin1/system1/sp1/settings1	Erfassung der Serviceprozessoreinstellungen
admin1/system1/sp1/settings1/clpsetting1	CLP-Dienst-Einstellungsdaten
admin1/system1/sp1/settings1/ipsettings1	IP-Schnittstellenzuweisung-Einstellungsdaten (statisch)
admin1/system1/sp1/settings1/ipsettings1/staticipsettings1	Statische IP-Schnittstellenzuweisung-Einstellungsdaten
admin1/system1/sp1/settings1/ipsettings1/dnssettings1	DNS-Client-Einstellungsdaten
admin1/system1/sp1/settings1/ipsettings2	IP-Schnittstellenzuweisung-Einstellungsdaten (DHCP)
admin1/system1/sp1/settings1/ipsettings2/dhcpsettings1	DHCP-Client-Einstellungsdaten
admin1/system1/sp1/clpsvc1	CLP-Dienst-Protokolldienst
admin1/system1/sp1/clpsvc1/clpendpt*	CLP-Dienst-Protokollendpunkt
admin1/system1/sp1/clpsvc1/tcpendpt*	CLP-Dienst-Protokoll-TCP-Endpunkt
admin1/system1/sp1/jobq1	Aufgabenwarteschlange 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-Authentifizierungs-(MFA)-Konto
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 Authentifizierungs-(RBA)-Dienst
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 (SOL)-Rolle
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	Verwaltungsdienst zur Energieausnutzung
admin1/system1/sp1/pwrutilmgtsvc1/pwrcurr1	Einstellundsdaten der aktuellen Stromzuweisund für den Energieausnutzungs-Verwaltundsdienst
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

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Das Dienstprogramm Befehlszeilenoberfläche des virtuellen Datenträgers (VMCLI) ist eine Befehlszeilenoberfläche, die 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 einsetzen.

Dieser Abschnitt bietet Informationen zum Einbinden des VMCLI-Dienstprogramms in Ihr Betriebsnetz.

Bevor Sie beginnen

Stellen Sie vor Verwendung des VMCLI-Dienstprogramms sicher, dass die gewünschten Remote-Systeme und das Betriebsnetz 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
- Startabbilddatei(en) des Betriebssystems

  Die Image-Datei muss das ISO-Image einer Betriebssystem-CD oder einer CD/DVD mit einem dem Industriestandard entsprechenden startfähigen Format sein.

Startfähige Abbilddatei erstellen

Bevor Sie die Abbilddatei für die Remote-Systeme bereitstellen, ist sicherzustellen, dass ein unterstütztes System von der Datei starten kann. Um die Image-Datei zu prüfen, übertragen Sie sie mithilfe der iDRAC6-Web-Benutzeroberfläche auf ein Testsystem und führen Sie dann einen Neustart des Systems durch.

Die folgenden Abschnitte enthalten spezifische Informationen über das Erstellen von Abbilddateien für Linux- und Microsoft® Windows®-Systeme.

Abbilddatei für Linux-Systeme erstellen

Verwenden Sie das Datenvervielfältigungs-Dienstprogramm (dd), um eine startfähige Image-Datei für das Linux-System zu erstellen.

Um das Dienstprogramm auszuführen, öffnen Sie eine Eingabeaufforderung und geben Sie Folgendes ein:

```
dd if=<Eingabekomponente> der=<Ausgabedatei>
```

Zum Beispiel:

```
dd if=/dev/sdc0 of=mycd.img
```

Abbilddatei für Windows-Systeme erstellen

Achten Sie bei der Auswahl eines Daten-Replikator-Dienstprogramms für Windows-Abbilddateien darauf, dass es sich um ein Dienstprogramm handelt, welches die Abbilddatei 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 Bereitstellungs- Abbilddatei zur Bereitstellung des Betriebssystems an die Remote-Systeme verfügen, können Sie diesen Schritt überspringen.

   Wenn Sie über keine startfähige, vorkonfigurierte Bereitstellungs-Abbilddatei 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 Abbilddatei Programme enthalten, die den von Microsoft Systems Management Server (SMS) verwendeten Bereitstellungsmethoden ähnlich sind.

   Wenn Sie die Abbilddatei erstellen, führen Sie folgendes aus:

   - Die netzwerkbasierten Standardinstallationsverfahren befolgen.
   - Markieren Sie das Bereitstellungs-Abbild als *schreibgeschützt*", um sicherzustellen, dass jedes Zielsystem startet und dasselbe Bereitstellungsverfahren ausführt.

4. Eines der folgenden Verfahren ausführen:

   - Intiegrieren Sie **IPMItool** und die Befehlszeilenoberfläche des virtuellen Datenträgers (VMCLI) in Ihre 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.

Sehen Sie sich, bevor Sie beginnen, das Beispielskript **vm6deploy** an, das im VMCLI-Dienstprogramm enthalten ist. Das Skript zeigt die detaillierten Schritte auf, die zur Bereitstellung des Betriebssystems an Remote-Systemen in Ihrem Netzwerk erforderlich sind.

Das folgende Verfahren enthält eine hochstufige Übersicht zur Bereitstellung des Betriebssystems auf Remote-Zielsystemen.

1. Geben Sie die iDRAC6-IPv4-Adressen der Remote-Systeme an, die in der Textdatei **ip.txt** bereitgestellt werden (eine IPv4-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 an der Befehlszeile ein:

```
vm6deploy -r ip.txt -u <idrac-Benutzer> -p <idrac-Kennwt> -c {<iso9660-img> | <Pfad>}-f {<floppy-img>|<Pfad>}
```

wobei

- *<idrac-Benutzer>* der iDRAC6-Benutzername, z. B. **root, ist**
- *<idrac-Kennwt>* das Kennwort für den iDRAC6-Benutzer, z. B. **calvin, ist**
- *<iso9660-img>* ist der Pfad zu einem ISO9660-Image der Betriebssystem-Installations-CD-ROM oder -DVD
- *<Pfad>* ist der Pfad zu dem Gerät, das die Betriebssystem-Installations-CD, DVD oder Floppy enthält
- *<floppy-img>* ist der Pfad zu einem gültigen Floppy-Abbild

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-Adressen aus der festgelegten Datei und führt das Dienstprogramm **VMCLI** einmal pro Zeile aus. Wenn das Argument der Option **-r** kein Dateiname ist, sollte 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, die die Funktionen des virtuellen Datenträgers von der Management Station zum iDRAC6 bereitstellt.

Das VMCLI-Dienstprogramm bietet folgende Funktionen:

ANMERKUNG: Beim Virtualisieren von schreibgeschützten Abbilddateien können sich mehrere Sitzungen dieselben Abbilddatenträger teilen. Beim Virtualisieren von physischen Laufwerken kann zu einem bestimmten Zeitpunkt jeweils nur eine Sitzung auf ein gegebenes physisches Laufwerk zugreifen.

- Wechselmedienkomponenten oder Abbilddateien, die mit den Plug-ins des virtuellen Datenträgers übereinstimmen
- Automatische Terminierung, wenn die Einmal-Startoption 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.

Wenn das Betriebssystem Administratorrechte oder eine betriebssystemspezifische Berechtigung oder Gruppenmitgliedschaft unterstützt, sind auch Administratorrechte 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 Administratorrechte 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 Administratorrechte 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 Systemverwaltungs-Softwareprodukte einschließlich Diagnose, Speicherverwaltung, Remote-Zugriffs-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 zum Bereitstellen von Software an mehrere Remote-Systeme verwendet werden.

ANMERKUNG: Das **vm6deploy**-Skript hängt bei seiner Installation von den anderen, in seinem Verzeichnis vorhandenen, Dateien ab. Wenn Sie das Skript von einem anderen Verzeichnis aus verwenden möchten, müssen Sie auch alle Dateien kopieren. 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 folgendermaßen 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 weiterhin ausgeführt, bis eine der folgenden Situationen zutrifft:

- Die VMCLI-Verbindung wird aus einem beliebigen Grund abgebrochen.
- Das Verfahren wird mit einer Betriebssystemsteuerung manuell abgebrochen. Beispiel: In Windows können Sie den Task-Manager verwenden, um das Verfahren abzubrechen.

VMCLI:Parameter

iDRAC6-IP-Adresse

`-r <iDRAC-IP-Adresse>[:<iDRAC-SSL-Port>]`

Dieser Parameter gibt die iDRAC6-IPv4-Adresse und die SSL-Anschluss an, die das Dienstprogramm zum Herstellen einer Verbindung des virtuellen Datenträgers zum Ziel-iDRAC6 benötigt. Wenn Sie eine ungültige IPv4-Adresse oder einen ungültigen DDNS-Namen eingeben, wird eine Fehlermeldung angezeigt, und der Befehl wird abgebrochen.

<iDRAC-IP-Adresse> ist eine gültige, eindeutige IPv4-Adresse oder der iDRAC6-DDNS-Name (dynamisches Domainnamenssystem) ist, falls unterstützt. Wenn *<iDRAC-SSL-Anschluss>* ausgelassen wird, wird der Anschluss 443 (Standard-Anschluss) verwendet. Solange der iDRAC6-Standard-SSL-Anschluss nicht geändert wird, ist der optionale SSL-Anschluss nicht erforderlich.

iDRAC6-Benutzername

`-u <iDRAC-Benutzername>`

Dieser Parameter gibt den iDRAC6-Benutzernamen an, der den virtuellen Datenträger ausführen wird.

Der <*iDRAC-Benutzername*> muss die folgenden Attribute aufweisen:

- Gültiger Benutzername
- iDRAC6-Benutzerberechtigung für den virtuellen Datenträger

Wenn die iDRAC6-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.

iDRAC6-Benutzerkennwort

`-p <iDRAC-Benutzerkennwort>`

Dieser Parameter gibt das Kennwort für den angegebenen iDRAC6-Benutzer an.

Wenn die iDRAC6-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.

Diskette/Festplatten-Komponente oder Abbilddatei

`-f {<Gerätename> | <Abbilddatei>}`

wobei <*Gerätename*> ein gültiger Laufwerkbuchstabe (bei Windows-Systemen) oder ein gültiger Gerätekomponentenname (bei Linux-Systemen) ist; <*Image-Datei*> ist der Dateiname und Pfad einer gültigen Image-Datei.

ANMERKUNG: Bereitstellungspunkte für das VMCLI-Dienstprogramm werden nicht unterstützt.

Dieser Parameter bestimmt die Komponente oder die Datei, die den virtuellen Disketten-/Festplatten-Datenträger liefern.

Beispiel: Eine Abbilddatei 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 der Abbilddatei schreiben. Konfigurieren Sie das Betriebssystem so, dass eine Disketten-Abbilddatei, die nicht überschrieben werden soll, mit einem Schreibschutz versehen wird.

Beispiel: Eine Komponente 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 derzeit keine Unterstützung für mehrere LUNs und wird dies auch in Zukunft nicht tun. Der Kernel unterstützt diese Funktionalität jedoch, nur müssen Sie Red Hat Enterprise Linux Version 4 aktivieren, um ein SCSI-Gerät mit mehreren LUNs anhand folgender Schritte zu erkennen:

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-Abbild zu erhalten, geben Sie in die Befehlszeile den folgenden Befehl ein:

   uname -r

3. Gehen Sie zum Verzeichnis **/boot** und löschen Sie die Kernel-Abbilddatei, deren Namen Sie in Schritt 2 erfahren 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 2 zu überprüfen:

   cat /sys/modules/scsi_mod/max_luns

Wenn die Komponente eine Schreibschutzfunktion anbietet, können Sie diese Funktion verwenden, um sicherzustellen, dass der virtuelle Datenträger dem Datenträger nicht schreibt.

Lassen Sie diesen Parameter aus der Befehlszeile aus, wenn Sie keine Diskettendatenträger virtualisieren. Wenn ein ungültiger Wert festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.

CD/DVD-Komponente oder -Abbilddatei

`-c {<Gerätename> | <Image-Datei>}`

wobei <*Gerätename*> ein gültiger CD/DVD-Laufwerkbuchstabe (bei Windows-Systemen) oder ein gültiger CD/DVD-Gerätedateiname (bei Linux-Systemen) ist, und wobei <*Image-Datei*> der Dateiname und Pfad einer gültigen ISO-9660-Image-Datei ist.

Dieser Parameter bestimmt die Komponente oder Datei, welche die virtuellen CD/DVD-ROM-Datenträger liefert:

Beispiel: Eine Abbilddatei wird wie folgt angegeben:

`-c c:\temp\mydvd.img` (Windows-Systeme)

`-c /tmp/mydvd.img` (Linux-Systeme)

Beispiel: Eine Komponente 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 festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.

Geben Sie mit dem Befehl mindestens einen Datenträgertyp (Diskette oder CD/DVD-Laufwerk) an, es sei denn, es werden nur Switch-Optionen vorgegeben. Andernfalls wird eine Fehlermeldung angezeigt und der Befehl mit einem Fehler abgebrochen.

Versionsanzeige

`-v`

Dieser Parameter wird zur Anzeige der VMCLI-Dienstprogrammversion verwendet. Wenn keine anderen Nicht-Switch-Optionen geboten werden, wird der Befehl ohne Fehlermeldung abgebrochen.

Hilfeanzeige

`-h`

Dieser Parameter zeigt eine Zusammenfassung der VMCLI-Dienstprogrammparameter an. Wenn keine anderen Nicht-Switch-Optionen geboten werden, wird der Befehl ohne Fehler 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 iDRAC-Konfigurationsschnittstellen, wie z.B. der RACADM- oder Webschnittstelle nicht auf *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 Befehlsshell-Funktionen des Betriebssystems, um zu veranlassen, dass das Dienstprogramm im Hintergrund ausgeführt wird. Unter einem Linux-Betriebssystem wird z. B. durch das auf den Befehl folgende Et-Zeichen (&) veranlasst, dass das Programm als neues Hintergrundverfahren erzeugt 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 Verfahren 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

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

---

IPMI konfigurieren

Dieser Abschnitt enthält Informationen zum Konfigurieren und Verwenden der iDRAC 6-IPMI-Schnittstelle. Die Schnittstelle enthält Folgendes:

- IPMI über LAN
- IPMI über seriell
- Seriell über LAN

Der iDRAC 6 ist vollständig IPMI 2.0-konform. Die iDRAC 6-IPMI kann mit folgenden Hilfsmitteln konfiguriert werden:

- iDRAC 6-GUI Ihres Browsers.
- Open Source-Dienstprogramm, wie z. B. *IPMItool.*
- Dell™ OpenManage™-IPMI-Shell **ipmish**
- RACADM

Weitere Informationen zum Verwenden von IPMI-Shell und ipmish finden Sie im *Dell OpenManage Baseboard-Verwaltungs-Controller-Dienstprogramme-Benutzerhandbuch* unter **support.dell.com\manuals**.

Weitere Informationen über die Verwendung von RACADM finden Sie unter "RACADM im Remote-Zugriff verwenden."

IPMI mittels der Internet-basierten Schnittstelle konfigurieren

Weitere Informationen hierzu 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 auf 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 auf die Eingabetaste.

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <Klasse>
      ```

      wobei <*Klasse*> eines von Folgendem darstellt:

      - 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 auf die Eingabetaste.

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <Schlüssel>
```

wobei <*Schlüssel*> ein aus 20 Zeichen bestehender Verschlüsselungsschlüssel in einem gültigen Hexadezimal-Format ist.

3. IPMI Seriell über LAN (SOL) konfigurieren.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie auf die Eingabetaste.

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a. Aktualisieren Sie die IPMI-SOL-Mindestzugriffsstufe.

ANMERKUNG: Die IPMI-SOL-Mindestzugriffsstufe bestimmt die Mindestberechtigung, die zum Aktivieren von IPMI SOL erforderlich ist. Weitere Informationen enthält die IPMI 2.0-Spezifikation.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie auf die Eingabetaste.

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <Klasse>
```

wobei <*Klasse*> eines von Folgendem darstellt:

- 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 identisch mit der Baudrate des Managed Systems ist.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie auf die Eingabetaste.

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <Baudrate>
```

wobei <*Baudrate*> 9600, 19200, 57600 oder 115200 Bits pro Sekunde ist.

Zum Beispiel:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. SOL für einen einzelnen Benutzer aktivieren.

ANMERKUNG: SOL kann für jeden einzelnen Benutzer aktiviert oder deaktiviert werden.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie auf die Eingabetaste.

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <ID> 2
```

wobei <*ID*> die eindeutige Benutzer-ID ist.

4. Konfigurieren Sie IPMI-Seriell.

a. Ändern Sie den Modus der IPMI-Seriell-Verbindung zur entsprechenden Einstellung.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie auf die Eingabetaste.

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

b. Stellen Sie die IPMI-Seriell-Baudrate ein.

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein, und drücken Sie auf die Eingabetaste.

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <Baudrate>
```

wobei <*Baudrate*> 9600, 19200, 57600 oder 115200 Bits pro Sekunde ist.

Zum Beispiel:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600
```

c. Aktivieren Sie die IPMI-Seriell-Hardwareablaufsteuerung.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie auf die Eingabetaste.

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

d. Stellen Sie die IPMI-Seriell-Mindest-Kanalzugriffsstufe ein.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie auf die Eingabetaste.

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <Klasse>
```

wobei <*Klasse*> eines von Folgendem darstellt:

- 2 (Benutzer)
- 3 (Operator)
- 4 (Administrator)

Beispiel: Um die seriellen IPMI-Kanalberechtigungen 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 ordnungsgemäß im BIOS- Setup-Programm eingestellt ist.

- Starten Sie das System neu.
- Drücken Sie während des POST auf <F2>, um das BIOS-Setup-Programm einzugeben.
- Wechseln Sie zu **Serial Communication**.
- Stellen Sie im Menü **Serial Connection** sicher, dass **External Serial Connector** auf **Remote Access Device** gesetzt ist.
- Speichern und beenden Sie das BIOS-Setup-Programm.
- Starten Sie das System neu.

Die IPMI- Konfiguration ist abgeschlossen.

Wenn sich IPMI-Seriell 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 den Programmzugriff, wie z. B. die IPMI-Shell (IPMISH), die zusammen mit dem Baseboard-Verwaltungsdienstprogramm (BMU) enthalten ist.

So konfigurieren Sie den IPMI-Modus mittels RACADM:

1. Deaktivieren Sie die serielle RAC-Schnittstelle.

   Geben Sie in der Befehlszeile Folgendes 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 "iDRAC 6-Definitionen für Eigenschafts-Datenbankgruppen und Objekte".

Seriell über LAN mittels webbasierter Schnittstelle konfigurieren.

Weitere Informationen hierzu finden Sie unter "IPMI konfigurieren".

ANMERKUNG: Seriell über LAN kann mit den folgenen Dell OpenManage-Hilfsprogrammen verwendet werden: SOLProxy und IPMItool. Weitere Informationen hierzu finden Sie im *Dell OpenManage Baseboard-Verwaltungs-Controller-Dienstprogramme-Benutzerhandbuch* unter

support.dell.com \ manuals.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC-Konfigurations-Dienstprogramm verwenden

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

---

Übersicht

Das iDRAC-Konfigurationsprogramm 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
- Virtuellen Datenträger konfigurieren
- die Smart Card konfigurieren
- den administrativen Benutzernamen bzw. das administrative Kennwort ändern
- die iDRAC-Konfiguration auf die Werkseinstellungen zurücksetzen
- SEL-Meldungen (Systemereignisprotokoll) anzeigen oder Meldungen aus dem Protokoll löschen
- die LCD konfigurieren
- Systemdienste konfigurieren

Die Tasks, die Sie mit dem iDRAC-Konfigurationsdienstprogramm ausführen können, lassen sich auch mit anderen Dienstprogrammen ausführen, die durch den iDRAC oder die Dell™ OpenManage™-Software zur Verfügung gestellt werden. Diese Dienstprogramme schließen die Webschnittstelle, die SM-CLP-Befehlszeilenoberfläche und die Befehlszeilenoberfläche des lokalen RACADM ein.

---

iDRAC-Konfigurationsdienstprogramm starten

1. Schalten Sie den Server ein oder starten Sie ihn neu, indem Sie an seiner Vorderseite auf den Netzschalter drücken.
2. Wenn Sie die Meldung **Drücken Sie für das Remote-Zugriffs-Setup innerhalb von 5 Sek. auf <Strg-E>.....** sehen, drücken Sie sofort auf <Strg><E>.

ANMERKUNG: Wenn das Betriebssystem zu laden beginnt, bevor Sie auf <Strg><E> gedrückt haben, lassen Sie das System den Startvorgang beenden, starten Sie dann den Server neu und wiederholen Sie den Vorgang.

Das iDRAC-Konfigurationshilfsprogramm wird angezeigt. Die ersten beiden Zeilen enthalten Informationen zur iDRAC6-Firmware und zu den Firmware-Revisionen der primären Rückwandplatine. Die Revisionsstufen können nützlich sein, wenn Sie bestimmen möchten, ob ein Firmware-Upgrade erforderlich ist.

Die iDRAC6-Firmware ist der Teil der Firmware, der für externe Schnittstellen zuständig ist, wie z. B. die webbasierte Schnittstelle, SM-CLP und Webschnittstellen. Die Firmware der primären Rückwandplatine ist der Teil der Firmware, der mit der Serverhardware-Umgebung gekoppelt wird und diese überwacht.

---

iDRAC-Konfigurationshilfsprogramm verwenden

Unterhalb der Firmware-Revisionsmeldungen besteht der Rest des iDRAC-Konfigurationshilfsprogramms aus einem Menü von Elementen, auf die Sie über die Tasten <Nach oben> und <Nach unten> zugreifen können.

- Wenn ein Menüelement zu einem Untermenü oder einem bearbeitbaren Textfeld führt, drücken Sie auf <Eingabe>, um auf das Element zuzugreifen und auf <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 auf <Nach links>, <Nach rechts> oder auf die <Leertaste>, um einen Wert auszuwählen.
- Kann ein Element nicht bearbeitet werden, wird es blau angezeigt. Einige Elemente werden abhängig von anderen getroffenen Auswahlen bearbeitbar.
- In der unteren Zeile des Bildschirms werden Anleitungen zum aktuellen Element angezeigt. Sie können auf <F1> drücken, um bzgl. des aktuellen Elements Hilfe aufzurufen.
- Wenn Sie mit der Verwendung des iDRAC-Konfigurationshilfsprogramms fertig sind, drücken Sie auf <Esc>, um das Beenden-Menü anzuzeigen. Wählen Sie dort, ob Sie Ihre Änderungen speichern oder verwerfen möchten oder ob Sie zum Hilfsprogramm zurückkehren möchten.

In den folgenden Abschnitten werden die Menüelemente des iDRAC-Konfigurationshilfsprogramms beschrieben.

iDRAC6 LAN

Verwenden Sie die Tasten <Nach links> und <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 zuzulassen, wie z. B. webbasierte Schnittstelle, Telnet/SSH-Zugriff und RAC seriellen Zugriff auf die SM-CLP-Befehlszeilenschnittstelle, Konsolenumleitung und virtuelle Datenträger.

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

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

(iDRAC6-bandexterne Schnittstelle wird deaktiviert, wenn der LAN-Kanal AUS ist.)

Press any key to clear the message and continue.

(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 iDRAC-HTTP-, HTTPS-, Telnet- oder SSH-Schnittstellen zugreifen, der bandexterne Verwaltungsnetzwerkdatenverkehr (wie 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 die Tasten <Nach links> und <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:

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

(iDRAC IPMI über LAN bandexterne Schnittstelle wird deaktiviert, wenn der LAN-Kanal 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 auf <Eingabe>, um das Untermenü der LAN-Parameter anzuzeigen. Wenn Sie die Konfiguration der LAN-Parameter abgeschlossen haben, drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln.

Tabelle 15-1. LAN-Parameter

Element	Beschreibung
Allgemeine Einstellungen	
NIC-Auswahl	Verwenden Sie die Tasten <Nach links> und <Nach rechts> sowie die Leertaste, um zwischen den Betriebsarten auszuwählen. Die verfügbaren Betriebsarten sind: **Dediziert (Dedicated), Freigegeben (Shared)**, **Freigegeben mit Failover LOM2** und **Freigegeben mit Failover Alle LOMs**. Mit diesen Betriebsarten kann der iDRAC6 die entsprechende Schnittstelle zur Kommunikation mit der Außenwelt verwenden.
MAC-Adresse	Dies ist die nicht bearbeitbare MAC-Adresse der iDRAC6-Netzwerkschnittstelle.
VLAN aktivieren	Wählen Sie **Ein** aus, um die virtuelle LAN-Filterung für den iDRAC6 zu aktivieren.
VLAN-ID	Ist **VLAN aktivieren** auf **Ein** gestellt, geben Sie einen beliebigen VLAN ID-Wert von 1 bis 4094 ein.
VLAN	Ist **VLAN aktivieren** auf **Ein** eingestellt, wählen Sie die Priorität des VLAN von 0 bis 7.
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 finden.
iDRAC6-Name	Wenn **iDRAC-Name registrieren** auf **Ein** eingestellt ist, drücken Sie auf <Eingabe>, um das Textfeld **Aktueller DNS-iDRAC-Name** zu bearbeiten. Drücken Sie auf <Eingabe>, 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** aus, wenn Sie den Domänennamen von einem DHCP-Dienst auf dem Netzwerk abrufen möchten. Wählen Sie **Aus**, wenn Sie den Domänennamen festlegen möchten.
Domänenname	Wenn **Domainname von DHCP Aus** ist, drücken Sie auf <Eingabe>, um das Textfeld **Aktueller Domainname** zu bearbeiten. Drücken Sie auf <Eingabe>, 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, wie z. B. `meinefirma.com`.
Zeichenkette des Host-Namens	Drücken Sie zur Bearbeitung auf <Eingabe>. Geben Sie den Namen des Hosts für PET-Warnungen (Platform Event Trap) ein.
LAN-Warnung aktiviert	Wählen Sie **Ein** aus, um die PET-LAN-Warnung zu aktivieren.
Warnungsregel, Eintrag 1	Wählen Sie **Aktivieren** oder **Deaktivieren** aus, um das erste Warnungsziel zu aktivieren.
Warnungsziel 1	Geben Sie, wenn **LAN-Warnung aktiviert** auf **Ein** eingestellt ist, die IP-Adresse ein, an die PET-LAN-Warnungen weitergeleitet werden sollen.

IPv4-Einstellungen	Aktivieren oder deaktivieren Sie die Unterstützung der IPv4-Verbindung.
IPv4	Wahlen Sie für IPv4-Protokollunterstützung **Aktiviert** oder **Deaktiviert.**
Verschlüsselungsschlüssel RMCP+	Drücken Sie auf <Eingabe>, um den Wert zu bearbeiten, und auf <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 der IPMI Authentifizierung und Verschlüsselung 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 werden konnte, werden die Felder auf Null eingestellt. Wenn **Statisch** ausgewählt ist, werden die Elemente **Ethernet-IP-Adresse**, **Subnetzmaske** und **Standard-Gateway** bearbeitbar**.**
Ethernet-IP-Adresse	Wenn die **IP-Adressenquelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse ein, die dem iDRAC6 zugewiesen werden soll. Die Standardadresse ist **192.168.0.120**.
Subnetzmaske	Wenn die **IP-Adressenquelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene Subnetzmaskenadresse an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die Subnetzmaske für den iDRAC6 ein. Die Standardeinstellung ist **255.255.255.0.**
Standard-Gateway	Wenn die **IP-Adressenquelle** auf **DHCP** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse des Standard-Gateways an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse des Standard-Gateways ein. Die Standardeinstellung ist **192.168.0.1.**
DNS-Server von DHCP	Wählen Sie **Ein** aus, um DNS-Server-Adressen von einem DHCP-Dienst auf dem Netzwerk abzurufen. Wählen Sie **Aus** aus, um die unten stehenden DNS-Server-Adressen zu bestimmen.
DNS-Server 1	Wenn **DNS-Server von DHCP Aus** ist, geben Sie die IP-Adresse des ersten DNS-Servers ein.
DNS-Server 2	Wenn **DNS-Server von DHCP Aus** ist, geben Sie die IP-Adresse des zweiten DNS-Servers ein.
IPv6-Einstellungen	Aktivieren oder deaktivieren Sie die Unterstützung für die IPv6-Verbindung.
IP-Adressen-Quelle	Wählen Sie zwischen **AutoConfig** und **Statisch** aus. Wenn AutoConfig ausgewählt ist, werden die Felder **IPv6-Adresse 1**, **Präfixlänge** und **Standard-Gateway** vom DHCP abgerufen. Wenn **Statisch** ausgewählt ist, werden **IPv6-Adresse 1**, **Präfixlänge** und **Standard-Gateway** bearbeitbar.
IPv6-Adresse 1	Wenn die **IP-Adressenquelle** auf **AutoConfig** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse ein, die dem iDRAC6 zugewiesen werden soll.
Präfixlänge	Konfiguriert die Präfixlänge der IPv6-Adresse. Dieser Wert kann 1 bis einschließlich 128 lauten.
Standard-Gateway	Wenn die **IP-Adressenquelle** auf **AutoConfig** eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse des Standard-Gateways an. Wenn die **IP-Adressenquelle** auf **Statisch** eingestellt ist, geben Sie die IP-Adresse des Standard-Gateways ein.
IPv6 Link-Lokaladresse	Dies ist die nicht bearbeitbare **IPv6 Link-Lokaladresse** der iDRAC-Netzwerkschnittstelle.
IPv6-Adresse 2	Dies ist die nicht bearbeitbare **IPv6-Adresse 2** der iDRAC-Netzwerkschnittstelle.
DNS-Server von DHCP	Wählen Sie **Ein** aus, um DNS-Server-Adressen von einem DHCP-Dienst auf dem Netzwerk abzurufen. Wählen Sie **Aus** aus, um die unten stehenden DNS-Server-Adressen zu bestimmen.
DNS-Server 1	Wenn **DNS-Server von DHCP Aus** ist, geben Sie die IP-Adresse des ersten DNS-Servers ein.
DNS-Server 2	Wenn **DNS-Server von DHCP Aus** ist, geben Sie die IP-Adresse des ersten DNS-Servers ein.
Erweiterte LAN-Konfigurationen	
Automatische Verhandlung	Wenn **NIC Auswahl** auf **Dediziert** eingestellt ist, wählen Sie zwischen **Aktiviert** und **Deaktiviert**. Wird **Aktiviert** gewählt, werden die **Einstellungen** für **LAN-Geschwindigkeit** und **LAN-Duplex** automatisch konfiguriert.
LAN-Taktrateneinstellung	Ist **Auto-Negotiate** auf **Deaktiviert** eingestellt, wählen Sie zwischen 10 Mbps und 100 Mbps.
LAN-Duplexeinstellung	Ist **Auto-Negotiate** auf **Deaktiviert** eingestellt, wählen Sie zwischen **Halb-Duplex und 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 **Konsolenumleitungs**-Sitzungen verfügbar gemacht.

Wenn Sie **Abgetrennt** auswählen, können Benutzer während **Konsolenumleitungs**-Sitzungen nicht auf virtuelle Datenträgergeräte zugreifen.

ANMERKUNG: Um ein USB-Flashlaufwerk mit der Funktion **Virtueller Datenträger** zu verwenden, muss der **Emulationstyp des USB-Flashlaufwerks** im BIOS-Setup-Dienstprogramm auf **Festplatte** eingestellt sein. Sie können auf das BIOS-Setup-Dienstprogramm zugreifen, indem Sie während des Serverstarts auf <F2> drücken. Wenn der **Emulationstyp des USB-Flashlaufwerks** auf **Automatisch** eingestellt ist, erscheint das Flashlaufwerk dem System als Diskettenlaufwerk.

Virtual Flash

Drücken Sie die <Eingabetaste>, um **Deaktiviert** oder **Aktiviert** auszuwählen.

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

Deaktivieren veranlasst, dass der virtuelle Flash entfernt wird und nicht mehr zur Verfügung steht.

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

Smart Card-Anmeldung

Drücken Sie die <Eingabetaste>, um **Aktiviert** oder **Deaktiviert** auszuwählen. Diese Option konfiguriert die Smart Card Anmeldefunktion. Die verfügbaren Einstellungen sind **Aktiviert**, **Deaktiviert**. und **Mit RACADM aktiviert**.

ANMERKUNG: Wird **Aktiviert** gewählt, wird **IPMI über LAN** abgeschaltet und es ist keine Bearbeitung möglich.

Konfiguration der Systemdienste

System Services

Drücken Sie die <Eingabetaste>, um **Aktiviert** oder **Deaktiviert** auszuwählen. Weitere Informationen finden Sie im *Unified Server Configurator-Benutzerhandbuch*, das auf der Dell-Support-Website unter **support.dell.com\manuals** zur Verfügung steht.

ANMERKUNG: Durch Änderung dieser Option wird der Server zur Übernahme der neuen Einstellungen neu gestartet, wenn Sie auf **Speichern** und **Beenden** klicken.

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.

LCD-Konfiguration

Drücken Sie die <Eingabetaste>, um das Untermenü der **LCD-Konfiguration** anzuzeigen. Wenn Sie die Konfiguration der LCD-Parameter abgeschlossen haben, drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln.

Tabelle 15-2. LCD-Benutzerkonfiguration

LCD-Zeile 1	Verwenden Sie die Tasten <Nach links> und <Nach rechts> sowie die Leertaste, um zwischen den Optionen auszuwählen. Diese Funktion stellt die Anzeige **Startseite** auf der LCD auf eine der folgenden Optionen ein: **Umgebungstemp**, **Systemkennnr.**, **Host-Name**, **iDRAC6-IPv4-Adresse**, **iDRAC6-IPv6-Adresse**, **iDRAC6-MAC-Adresse**, **Modellnr.**, **Keine**, **Service-Tag-Nr.**, **Systemleistung**, **benutzerdefinierte Zeichenfolge.**.
Benutzerdefinierte LCD-Zeichenfolge	Ist die **LCD-Zeile 1** auf **Benutzerdefinierte Zeichenfolge** eingestellt, können Sie die auf der LCD anzuzeigende Zeichenfolge einsehen oder eingeben. Die Zeichenfolge darf aus maximal 62 Zeichen bestehen.
LCD-Systemnetzteileinheiten	Ist **LCD-Zeile 1** auf **Systemleistung** eingestellt, wählen Sie **Watt** oder **BTU/h** um die auf der LCD angezeigte Maßeinheit anzugeben.
LCD-Umgebungstemperatureinheiten	Ist **LCD-Zeile 1** auf **Umgebungstemp.** eingestellt, wählen Sie zwischen **Celsius** oder **Fahrenheit,** um die auf der LCD anzuzeigende Maßeinheit anzugeben.
LCD-Fehleranzeige	Wählen Sie **Einfach** oder **SEL** (System Event Log). Mit dieser Funktion können Fehlermeldungen in einem oder zwei Formaten auf der LCD angezeigt werden: Das Einfach-Format liefert eine englische Beschreibung des Ereignisses. Im SEL-Format werden Text-Zeichenfolgen des Systemereignisses angezeigt.
LCD-Remote-KVM-Indikation	Wählen Sie **Aktiviert**, um den Text *KVM* anzuzeigen, wann immer eine virtuelle KVM auf der Einheit aktiv ist.
LCD-Frontblendenzugriff	Verwenden Sie die Tasten <Nach rechts> und <Nach links> sowie die Leertaste, um zwischen **Deaktiviert**, **Einsehen/Ändern** und **Nur einsehen** auszuwählen.

	Diese Einstellung bestimmt die Benutzerberechtigungsklasse für die LCD.

LAN-Benutzerkonfiguration

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

Tabelle 15-3. LAN-Benutzerkonfiguration

Element	Beschreibung
Kontozugriff	Wählen Sie **Aktiviert** aus, um das Administratorkonto zu aktivieren. Wählen Sie **Deaktiviert** aus, um das Administratorkonto zu deaktivieren.
Kontoberechtigung	Wählen Sie zwischen **Admin**, **Benutzer**, **Operator** und **Kein Zugriff** aus.
Kontobenutzername	Drücken Sie auf <Eingabe>, um den Benutzernamen zu bearbeiten, und dann auf <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 das Kennwort des administrativen Benutzers vergessen haben oder den iDRAC6 von den Standardeinstellungen aus neu konfigurieren möchten.

Drücken Sie auf <Eingabe>, um das Element auszuwählen. Die folgende Warnungsmeldung wird eingeblendet:

```
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 auf <Eingabe>, um den iDRAC auf die Standardeinstellungen zurückzusetzen.

Menü des Systemereignisprotokolls

Das Menü **Systemereignisprotokoll** ermöglicht Ihnen, Meldungen des Systemereignisprotokolls (SEL) anzuzeigen und die Protokollmeldungen zu löschen. Drücken Sie auf <Eingabe>, um das **Menü des Systemereignisprotokolls** anzuzeigen. Das System zählt die Protokolleinträge und zeigt dann die Gesamtanzahl von Einträgen sowie die aktuellste Meldung an. Das SEL speichert maximal 512 Meldungen.

Um SEL-Meldungen anzuzeigen, wählen Sie **Systemereignisprotokoll anzeigen** aus und drücken Sie auf <Eingabe>. Verwenden Sie die Taste <Nach links>, um die vorhergehende (ältere) Meldung zu verschieben, und die Taste <Nach rechts>, um die nächste (neuere) Meldung zu verschieben. Geben Sie eine Eintragsnummer an, um zu diesem Eintrag zu wechseln. Drücken Sie auf <Esc>, wenn Sie mit dem Anzeigen von SEL-Meldungen fertig sind.

Wählen Sie zum Löschen des SEL **Systemereignisprotokoll löschen** aus und drücken Sie auf <Eingabe>.

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

iDRAC-Konfigurationshilfsprogramm beenden

Wenn Sie mit den Änderungen der iDRAC-Konfiguration fertig sind, drücken Sie auf die Taste <Esc>, um das Menü Beenden anzuzeigen.

Wählen Sie **Änderungen speichern und beenden** aus und drücken Sie dann auf <Eingabe>, um Ihre Änderungen beizubehalten.

Wählen Sie **Änderungen ablehnen und beenden** aus und drücken Sie auf <Eingabe>, um alle vorgenommenen Änderungen zu ignorieren.

Wählen Sie **Zu Setup zurückwechseln** aus und drücken Sie auf <Eingabe>, um zum iDRAC-Konfigurationshilfsprogramm zurückzuwechseln.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Überwachungs- und Warnungsverwaltung.

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Dieser Abschnitt erklärt, wie der iDRAC 6 überwacht wird, und enthält Verfahren zum Konfigurieren des Systems und des iDRAC 6, um Warnungen zum empfangen.

Das verwaltete System konfigurieren, um den Bildschirm Letzter Absturz zu erfassen

Bevor der iDRAC 6 den Bildschirm Letzter Absturz erfassen kann, müssen Sie das verwaltete System mit den folgenden Voraussetzungen konfigurieren.

1. Installieren Sie die Managed System-Software. Weitere Informationen über das Installieren der Managed System-Software erhalten Sie im *Server Administrator-Benutzerhandbuch*.

2. Führen Sie ein unterstütztes Microsoft® Windows®-Betriebssystem aus, wobei die Windows-Funktion "automatischer Neustart" 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 Autom. Wiederherstellung, und setzen Sie die Maßnahme **Autom. Wiederherstellung** auf **Reset**, **Herunterfahren** oder **Aus- und Einschaltzyklus**. Zum Konfigurieren des Zeitgebers für **Autom. Wiederherstellung** müssen Sie Server Administrator oder IT- Assistant verwenden.

   Informationen zur Konfiguration des Zeitgebers für **Autom. Wiederherstellung** finden Sie im *Server Administrator-Benutzerhandbuch*. Um sicherzustellen, dass der Bildschirm Letzter Absturz erfasst werden kann, muss der Zeitgeber für **Autom. 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 **Autom. Wiederherstellung** auf **Herunterfahren** oder **Aus- und Einschalten** gesetzt ist.

Die Windows-Option Automatischer Neustart deaktivieren

Um sicherzustellen, dass die Funktion Bildschirm Letzter Absturz der webbasierten iDRAC 6-Schnittstelle richtig funktioniert, deaktivieren Sie die Option **Automatischer Neustart** auf verwalteten Systemen, auf denen die Betriebssysteme Microsoft Windows Server® 2008 und Windows Server 2003 ausgeführt werden.

Die Option Automatischer Neustart in Windows Server 2008 deaktivieren

1. Öffnen Sie die Windows-**Systemsteuerung**, und doppelklicken Sie auf das **System**-Symbol.

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

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

4. Klicken Sie unter **Autostart und Wiederherstellung** auf **Einstellungen**.

5. Wählen Sie das Kontrollkästchen **Automatischer Neustart** ab.

6. Klicken Sie zweimal auf **OK**.

Die Option Automatischer Neustart in Windows Server 2003 deaktivieren

1. Öffnen Sie die Windows-**Systemsteuerung**, und doppelklicken Sie auf das **System**-Symbol.

2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Klicken Sie unter **Autostart und Wiederherstellung** auf **Einstellungen**.
4. Wählen Sie das Kontrollkästchen **Automatischer Neustart** ab.
5. Klicken Sie zweimal auf **OK**.

Plattformereignisse konfigurieren

Plattformereigniskonfiguration bietet einen Mechanismus, um das Remote-Zugriffsgerät dahingehend zu konfigurieren, dass ausgewählte Maßnahmen auf bestimmte Ereignismeldungen hin ausgeführt werden. Diese Maßnahmen umfassen Neustart, Aus-/Einschalten, Herunterfahren und das Auslösen einer Warnung (Plattformereignis-Trap [PET] und/oder E-Mail).

Die filterbaren Plattformereignisse umfassen die folgenden:

- Assertionsfilter Lüfter kritisch
- Assertionsfilter Batteriewarnung
- Assertionsfilter Batterie kritisch
- Assertionsfilter diskrete Spannung kritisch
- Assertionsfilter Temperaturwarnung
- Assertionsfilter Temperatur kritisch
- Assertionsfilter Intrusion kritisch
- Filter Redundanz herabgesetzt
- Filter Redundanz verloren
- Assertionsfilter Prozessorwarnung
- Assertionsfilter Prozessor kritisch
- Filter Prozessor nicht vorhanden
- Assertionsfilter Prozessorversorgungswarnung
- Assertionsfilter Prozessorversorgung kritisch
- Assertionsfilter Prozessorversorgung nicht vorhanden
- Assertionsfilter Ereignisprotokoll kritisch
- Assertionsfilter Watchdog kritisch
- Assertionfilter Systemstromwarnung
- Assertionfilter Systemstrom kritisch

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 Plattformereignisfilterliste der Internet-basierten 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 (wie eines Systemneustarts) konfiguriert ist, wird die Maßnahme ausgeführt.

Plattformereignisfilter (PEF) konfigurieren

Konfigurieren Sie Ihre Plattformereignisfilter, bevor Sie die Plattformereignis-Traps oder E-Mail-Warnungseinstellungen konfigurieren.

PEF mittels webbasierter Schnittstelle konfigurieren

Weitere Informationen hierzu 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 auf 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 ein Wert von 1 bis 19 sein. 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 auf die Eingabetaste.

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 <Maßnahme>
   ```

   wobei die *<Maßnahme>*-Wertbits folgendermaßen lauten:

   - 0 = Keine Warnungsmaßnahme
   - 1 = Server ausschalten
   - 2 = Server neustarten
   - 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 und 2 die PEF-Maßnahme für den Neustart ist.

PET konfigurieren

PEF mittels der Internet-Benutzeroberfläche konfigurieren

Weitere Informationen hierzu 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 auf 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) eingestellt 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 Ihre PET-Regel.

   Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie auf 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-Namenzeichenkette.

   Geben Sie in der Befehlszeile Folgendes ein:

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

E-Mail-Warnungen konfigurieren

E-Mail-Warnungen mittels der Internet-Benutzeroberfläche konfigurieren

Weitere Informationen hierzu 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 auf 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 auf 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) eingestellt 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 auf die Eingabetaste.

   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <*E-Mail-Adresse*>

   wobei 1 der E-Mail-Zielindex und <*E-Mail-Adresse*> die Ziel-E-Mail-Adresse ist, die die Plattformereigniswarnungen empfängt.

   Zum Konfigurieren einer kundenspezifischen Meldung geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie auf die Eingabetaste.

   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <*Kundenspezifische_Meldung*>

   wobei 1 der E-Mail-Zielindex und <*Kundenspezifische_Meldung*> die Meldung ist, 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 Managed 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-Zuhörerkonfigurationen, Traps für Systemereignisse zu empfangen, die auf dem Managed 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 unter den Unterbefehl-Beschreibungen "**testtrap**" und "**sslkeyupload**".

Häufig gestellte Fragen

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 ist der Get-**Community-Name = public** und der Set-**Community-Name = private**. Standardmäßig ist der Community-Name für den iDRAC 6-Agenten **public**. Wenn IT Assistant eine Set-Aufforderung sendet, erstellt der iDRAC 6-Agent den SNMP-Authentifizierungsfehler, weil er nur Aufforderungen von **Community = public** akzeptieren kann.

ANMERKUNG: Das ist der für die Ermittlung verwendete Community-Name des SNMP-Agenten.

Sie können den iDRAC 6-Community-Namen mittels RACADM ändern.

Um den iDRAC 6-Community-Namen anzuzeigen, geben Sie den folgenden Befehl ein:

```
racadm getconfig -g cfgOobSnmp
```

Um den iDRAC 6-Community-Namen einzustellen, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <Community-Name>
```

Um auf den Community-Namen des iDRAC 6-SNMP-Agenten mithilfe der webbasierten Schnittstelle zuzugreifen oder ihn zu konfigurieren, wechseln Sie zu **Remote-Zugriff**→ **Konfiguration**→ **Dienste** und klicken Sie auf **SNMP-Agent**.

Um zu verhindern, dass SNMP-Authentifizierungs-Fehler erstellt werden, müssen Sie Community-Namen eingeben, die vom Agenten akzeptiert werden. Da der iDRAC 6 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 des Managed System

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Dieser Abschnitt erklärt, wie man Aufgaben bezüglich der Wiederherstellung und Behebung von Störungen bei einem abgestürzten System mit Hilfe der webbasierten iDRAC6-Oberfläche ausführt.

- "Erste Schritte, um Störungen an einem Remote-System zu beheben"
- "Netzstrom auf einem Remote-System verwalten"
- "IPv6-Information"
- "Bildschirm Letzter Systemabsturz 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, hat sich der Strom unerwartet ausgeschaltet?

Überprüfen Sie für abgestürzte Systeme den Bildschirm des letzten Absturzes (siehe "Bildschirm Letzter Systemabsturz anzeigen"), und verwenden Sie die Konsolenumleitung und die Remote-Energieverwaltung (siehe "Netzstrom auf einem Remote-System verwalten"), um das System neu zu starten und das Neustartverfahren zu beobachten.

Netzstrom auf einem Remote-System verwalten

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 iDRAC6 webbasierten Schnittstelle auswählen

Um Leistungsverwaltungsmaßnahmen über die Webschnittstelle auszuführen, siehe "Durchführen von Stromsteuerungsmaßnahmen am Server."

Stromsteuerungsmaßnahmen von der iDRAC6-CLI auswählen

Wenden Sie den Befehl `racadm serveraction` an, 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** - Leitet einen Ein-/Ausschaltvorgang auf dem verwalteten System ein. 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 aus.

Systeminformationen anzeigen

Die Seite **Systemzusammenfassung** enthält Informationen über die folgenden Systemkomponenten:

- Hauptsystemgehäuse
- Integrierter Dell Remote-Zugriff-Controller 6 - Enterprise

Um auf die Systeminformationen zuzugreifen, erweitern Sie die **System**struktur, und klicken Sie auf **Eigenschaften**.

Hauptsystemgehäuse

Tabelle 17-1 und Tabelle 17-2 beschreiben die Eigenschaften des Hauptsystemgehäuses.

ANMERKUNG: Um Informationen zu **Hostname** und **BS-Name** erhalten zu können, müssen auf dem Managed System iDRAC6-Dienste installiert sein.

Tabelle 17-1. Systeminformationsfelder

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 17-2. Felder zur Autom. 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.

Integrierter Dell Remote-Zugriff-Controller 6 - Enterprise

Tabelle 17-3 beschreibt die Merkmale von iDRAC6 Enterprise.

Tabelle 17-3. Felder mit iDRAC6-Informationen

Feld	Beschreibung
Uhrzeit/Datum	Aktuelle Zeit im Format: Tag Monat TT HH:MM:SS:JJJJ
Firmware-Version	iDRAC-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 (RAC)-Service
MAC-Adresse	Zeigt die Medienzugriffssteuerungs-Adresse (MAC) an, die die einzelnen Knoten in einem Netzwerk eindeutig identifiziert

IPv4-Information

Tabelle 17-4 beschreibt die IPv4-Eigenschaften.

Tabelle 17-4. IPv4-Informationsfelder

Feld	Beschreibung
Aktiviert	Ja oder Nein
IP-Adresse	Die 32-Bit-Adresse, die die Netzwerkschnittstelle zu einem 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 eines Schalters. Der Wert wird im Punkttrennungs-Format angezeigt, z. B. 143.166.154.1.
DHCP aktiviert	Ja oder Nein. Weist darauf hin, dass das dynamische Host-Konfigurationsprotokoll (DHCP) aktiviert ist.

IPv6-Information

Tabelle 17-5 beschreibt die IPv6-Eigenschaften.

Tabelle 17-5. IPv6-Informationsfelder

Feld	Beschreibung
Aktiviert	Weist darauf hin, dass Ipv6-Stapel nicht aktiviert ist.
IP-Adresse 1	Gibt die IPv6-Adresse für den iDRAC-NIC an.
Präfixlänge	Eine ganze Zahl, die die Präfixlänge der IPv6-Adresse angibt. Dieser kann ein Wert zwischen 1 und einschließlich 128 sein.
IP-Gateway	Gibt den Gateway für die iDRAC-NIC an.
Link-Local-Adresse	Gibt die IPv6-Adresse für den iDRAC-NIC an.
IP-Adresse 2	Gibt die zusätzliche IPv6-Adresse für den iDRAC-NIC an, wenn dieser verfügbar ist.
Automatische Konfiguration	AutoConfig gestattet dem Server Administrator das Einholen der IPv6-Adresse für die iDRAC NIC vom Server des dynamischen Host-Konfigurationsprotokolls (DHCPv6). Deaktiviert und löscht die Statische IP-Adresse, Präfixlänge und die Werte für das statische Gateway.

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 Ereignisschweregrad sowie weitere Informationen angezeigt; siehe Tabelle 17-6.
3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Systemereignisprotokoll**, um fortzufahren (siehe Tabelle 17-6).

Tabelle 17-6. Statusanzeigesymbole

Symbol/Kategorie	Beschreibung
	Eine grüne Markierung zeigt eine gesunde (normale) Status-Bedingung an.
	Ein gelbes Dreieck, das ein Ausrufezeichen enthält, zeigt eine (nichtkritische) Warnungsstatus-Bedingung an.
	Ein rotes X zeigt eine kritische (Ausfall) Status-Bedingung an.
	Ein Fragezeichen-Symbol zeigt an, dass der Status unbekannt ist.
Uhrzeit/Datum	Datum und Uhrzeit des Ereigniseintritts. Wenn das Datumfeld leer ist, trat das Ereignis während des Systemstarts auf. Das Format lautet dd/mm/yyyy hh:mm:ss, basierend auf dem 24-Stunden-Zeitsystem.
Beschreibung	Eine kurze Beschreibung des Ereignisses

Tabelle 17-7. Schaltflächen der SEL-Seite

Schaltfläche	Abhilfe
Drucken	Druckt **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** erscheint nur, wenn Sie die Berechtigung **Protokolle löschen** besitzen.
Speichern unter	Öffnet ein Pop-Up-Fenster, das Ihnen ermöglicht, das **SEL** zu 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 herunter, die auf der Support-Website von Microsoft unter support.microsoft.com verfügbar ist.

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
```

Die Protokolle des POST Betriebssystemstarts verwenden

ANMERKUNG: Alle Protokolle werden bei einem Neustart des iDRAC6 gelöscht.

Diese Funktion des iDRAC6 ermöglicht Ihnen, ein Stop-Motion-Video der letzten drei Instanzen des BIOS-POST und des Betriebssystemstarts abzuspielen.

So zeigen Sie die Start-Capture-Protokolle des POST und des Betriebssystems 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 die Protokollnummer des POST-Protokolls oder des Start- Capture-Protokolls des Betriebssystems aus und klicken Sie auf **Wiedergabe**.

   Das Video der Protokolle wird auf einem neuen Bildschirm abgespielt.

   ANMERKUNG: Sie müssen ein offenes POST Start-Capture-Protokollvideo schließen, um ein anderes einsehen zu können. Sie können keine zwei Protokolle gleichzeitig ansehen.
4. Klicken Sie auf **Playback**→ **Wiedergabe**, um das Start-Capture-Protokollvideo zu starten.
5. Klicken Sie auf **STOPP**, um das Video zu stoppen.

Bildschirm Letzter Systemabsturz anzeigen

ANMERKUNG: Die Funktion Bildschirm Letzter Absturz setzt voraus, dass das verwaltete System mit der Funktion **Autom. Wiederherstellung**, in Server Administrator konfiguriert, ausgestattet ist. Stellen Sie außerdem sicher, dass die Funktion **Automatisierte Systemwiederherstellung** mittels DRAC aktiviert wird. Wechseln Sie zur Seite **Dienste** im Abschnitt **Remote-Zugriff** unter dem Register **Konfiguration**, um diese Funktion zu aktivieren.

Auf der Seite **Bildschirm Letzter Absturz** wird der letzte Absturzbildschirm mit Informationen über die Ereignisse vor dem Systemabsturz angezeigt. Die letzten Systemabsturz-Informationen werden im iDRAC6-Speicher gespeichert und sind im Remote-Zugriff zugänglich.

So zeigen Sie die Seite **Bildschirm Letzter Absturz** an:

1. Klicken Sie in der **System**struktur auf **System**.
2. Klicken Sie auf die Registerkarte **Protokolle** und dann auf die **Anzeige Letzter Absturz**.

Die Seite **Bildschirm Letzter Absturz** enthält die folgenden Schaltflächen (siehe Tabelle 17-8) in der rechten oberen Ecke des Bildschirms:

Tabelle 17-8. Schaltflächen der Seite Bildschirm Letzter Absturz

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

ANMERKUNG: Aufgrund von Schwankungen im Zeitgeber für Autom. 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 der **Bildschirm Letzter Absturz** ordnungsgemäß

arbeitet. Weitere Informationen finden Sie unter "Das verwaltete System konfigurieren, um den Bildschirm Letzter Absturz zu erfassen".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Den iDRAC 6 wiederherstellen und Fehler beheben

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

In diesem Abschnitt wird das Ausführen von Tasks beschrieben, die mit der Wiederherstellung und Fehlerbehebung eines abgestürzten iDRAC 6 in Verbindung stehen.

Die Fehlerbehebung des iDRAC 6 kann unter Verwendung eines der folgenden Hilfsprogramme durchgeführt werden:

- RAC-Protokoll
- Diagnosekonsole
- Ablaufverfolgungsprotokoll
- racdump
- coredump

RAC-Protokoll verwenden

Das **RAC-Protokoll** ist ein beständiges Protokoll, das in der iDRAC 6-Firmware geführt wird. Das Protokoll enthält eine Liste von Benutzermaßnahmen (wie z. B. An- und Abmelden, Änderungen der Sicherheitsregeln) und Warnungen, die vom iDRAC 6 ausgegeben werden. Die ältesten Einträge werden überschrieben, wenn das Protokoll voll wird.

So greifen Sie über die iDRAC 6-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 **RAC-Protokoll**.

Das **RAC-Protokoll** stellt die in Tabelle 18-1 aufgeführten Informationen zur Verfügung.

Tabelle 18-1. Informationen der RAC-Protokollseite

Feld	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit (z. B. 19. Dez. 16:55:47). Wenn der iDRAC 6 beim erstmaligen Start nicht in der Lage ist, mit dem verwalteten System zu kommunizieren, wird die entsprechende Uhrzeit als Systemstartzeit angezeigt.
Source	Die Schnittstelle, die das Ereignis verursacht hat.
Beschreibung	Eine kurze Beschreibung des Ereignisses und der Name des Benutzers, der sich am iDRAC 6 angemeldet hat.

Schaltflächen der RAC-Protokollseite verwenden

Die Seite **RAC-Protokoll** enthält die unter Tabelle 18-2 aufgeführten Schaltflächen.

Tabelle 18-2. Schaltflächen des RAC-Protokolls

Schaltfläche	Abhilfe
Drucken	Druckt die Seite **RAC-Protokoll** aus.
Protokoll löschen	Löscht die **RAC-Protokoll**-Einträge. **ANMERKUNG:** Die Schaltfläche **Protokoll löschen** wird nur angezeigt, wenn Sie über die Berechtigung **Protokolle löschen** verfügen.
Speichern unter	Öffnet ein Popup-Fenster, das Ihnen ermöglicht, das **RAC-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 herunter, die auf der Support-Website von Microsoft unter support.microsoft.com verfügbar ist.
Aktualisieren	Lädt die Seite **RAC-Protokoll** neu.

Befehlszeile verwenden

Zeigen Sie die RAC-Protokolleinträge mittels des Befehls `getraclog` an.

```
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 sämtliche Einträge aus dem RAC -Protokoll löschen.

```
racadm clrraclog
```

Diagnosekonsole verwenden

Der iDRAC 6 bietet einen Standardsatz von Netzwerkdiagnose-Hilfsprogrammen (siehe Tabelle 18-3), die den mit Microsoft® Windows®- oder Linux-basierten Systemen gelieferten Hilfsprogrammen ähnlich sind. Mit der webbasierten iDRAC 6-Schnittstelle können Sie auf die Hilfsprogramme zum Debuggen des Netzwerks zugreifen.

So greifen Sie auf die Seite **Diagnosekonsole** zu:

1. Klicken Sie in der **System**-Struktur auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Diagnose**.

Tabelle 18-3 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 18-3. 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 Netzschnittstellentabelle an.
netstat	Druckt den Inhalt der Routingtabelle aus. Wenn die optionale Schnittstellenzahl im Textfeld rechts von der Option **netstat** angegeben wird, druckt netstat zusätzliche Informationen bezüglich des Verkehrs durch die Schnittstelle, des Puffergebrauchs und anderer Informationen zur Netzwerkschnittstelle aus.
ping *<IP-Adresse>*	Überprüft, ob die Ziel-IP-Adresse unter Verwendung des Inhalts der aktuellen Routing-Tabelle vom iDRAC 6 aus erreichbar ist. In das Feld rechts von dieser Option muss eine Ziel-IP-Adresse eingegeben werden. Ein ICMP-Echo-Paket (Internetsteuerungsmeldungsprotokoll) 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".

Ablaufverfolgungsprotokoll verwenden

Das interne iDRAC 6-Ablaufverfolgungsprotokoll wird von Administratoren verwendet, um Warnmeldungen und Netzwerkbetriebprobleme des iDRAC 6 zu debuggen.

So greifen Sie über die webbasierte iDRAC 6-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 Befehlszeilenschnittstelle 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 iDRAC 6-Firmware enthalten, die sich auf die interne iDRAC 6-Firmware beziehen und nicht auf das Betriebssystem des verwalteten Systems.

ANMERKUNG: Der iDRAC 6 gibt kein Echo eines ICMP (Ping) mit einer Paketgröße über 1500 Byte zurück.

---

racdump verwenden

Der Befehl **racadm racdump** bietet einen Einzelbefehl zum Abrufen von Informationen zum Speicherauszug, zum Status sowie zur allgemeinen iDRAC 6-Platine.

ANMERKUNG: Dieser Befehl steht nur auf Telnet- und SSH-Schnittstellen zur Verfügung. Weitere Informationen stehen unter dem Befehl "racdump" zur Verfügung.

---

coredump verwenden

Mit dem Befehl **racadm coredump** werden detaillierte Informationen angezeigt, die mit kritischen Problemen in Verbindung stehen, die vor kurzem beim RAC aufgetreten sind. Die coredump-Informationen können zur Diagnose dieser kritischen Probleme eingesetzt werden.

Wenn verfügbar, sind die coredump-Informationen beständig über Betriebszyklen des RAC und werden verfügbar bleiben, bis eine der folgenden Bedingungen eintritt:

- Die coredump-Informationen werden mit dem Unterbefehl **coredumpdelete** gelöscht.
- Auf dem RAC tritt eine weitere kritische Bedingung 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 in den Unterbefehlen "coredump" und "coredumpdelete".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Sensoren

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Hardwaresensoren oder -sonden können Ihnen dabei behilflich sein, die Systeme auf dem Netzwerk auf effizientere Weise zu überwachen, indem Ihnen ermöglicht wird, entsprechende Maßnahmen zum Verhindern von Notfallsituationen, wie eine Instabilität oder Beschädigung des Systems, zu ergreifen.

Sie können den iDRAC6 zum Überwachen von Hardwaresensoren für Batterien, Lüftersonden, Gehäuseeingriff, Netzteilen, verbrauchtem Strom, Temperatur und Spannung einsetzen.

Batteriesonden

Die Batteriesonden bieten Informationen zu Systemplatinen-CMOS und Speicher-ROMB-Batterien (RAM auf Hauptplatine).

ANMERKUNG: Die Einstellungen für Speicher-ROMB-Batterien sind nur verfügbar, wenn sich auf dem System ein ROMB befindet.

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 voreingestellter 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 ausfallen sollte.

ANMERKUNG: Sollte sich im System nur ein Netzteil befinden, wird der Abschnitt zur Netzteilredundanz **nicht angezeigt**.

Stromüberwachungssonden

Die Stromüberwachung bietet Informationen zum Stromverbrauch in *Echtzeit*, in Watt und Ampere.

Sie haben auch die Möglichkeit, eine grafische Darstellung des Stromverbrauchs 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 Warnungsschwellenwert-Bereichs und kritischen Schwellenwert-Bereichs befindet.

Spannungssonden

Bei den folgenden Sonden handelt es sich um typische Spannungssonden. Es ist möglich, dass sich diese Sonden und/oder andere Sonden auf Ihrem System befinden.

- CPU [n] VCORE
- Systemplatine 0,9 V PG
- Systemplatine 1,5 V ESB2 PG
- Systemplatine 1,5 V PG
- Systemplatine 1,8 V PG
- Systemplatine 3,3 V PG
- Systemplatine 5 V PG
- Systemplatine Backplane PG
- Systemplatine CPU VTT
- Systemplatine Linear PG

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Zum Einstieg mit iDRAC 6

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Der iDRAC 6 ermöglicht Ihnen, ein Dell-System im Remote-Zugriff zu überwachen und zu reparieren und auf das System Fehlerbehebungsmaßnahmen anzuwenden, selbst wenn es ausgeschaltet ist. Der iDRAC 6 bietet eine umfangreiche Auswahl an Funktionen wie Konsolenumleitung, virtueller Datenträger, virtuelle KVM, Smart Card-Authentifizierung und mehr.

Die *Management Station* ist das System, von dem aus ein Administrator ein Dell-System mit iDRAC 6 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 iDRAC 6 kann den Bildschirm des letzten Absturzes nicht erfassen.

Um den iDRAC6einzustellen, 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*, das auf der Dell Support-Website unter **support.dell.com\manuals** zur Verfügung steht.

1. Konfigurieren Sie die Eigenschaften, Netzwerkeinstellungen und Benutzer des iDRAC 6 - Der iDRAC 6 kann sowohl unter Verwendung des iDRAC 6-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 iDRAC 6 zugreifen zu können, wodurch Ihnen ermöglicht wird, iDRAC 6- Benutzerberechtigungen den vorhandenen Bentzern in der Active Directory-Software hinzuzufügen und zu steuern.

3. Konfigurieren Sie die Smart Card-Authentifizierung - Smart Card bietet für Ihr Unternehmen eine zusätzliche Sicherheitsstufe.

4. Konfigurieren Sie Remote-Zugriffs-Punkte wie Konsolenumleitung und virtueller Datenträger.

5. Konfigurieren Sie die Sicherheitseinstellungen.

6. Konfigurieren Sie Warnmeldungen zum Zweck effizienter Systemverwaltungkapazität.

7. Konfigurieren Sie zum Verwenden der auf Standards beruhenden IPMI- Hilfsprogramme die iDRAC 6-IPMI-Einstellungen (Intelligente Plattform-Verwaltungsschnittstelle), um die Systeme auf dem Netzwerk zu verwalten.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Energieüberwachung und Energieverwaltung

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Dell™ PowerEdge™-Systeme enthalten viele neu und erweiterte Energieverwaltungsfunktionen. Die gesamte Plattform, von der Hardware zur Firmware bis hin zur Systemverwaltungssoftware, wurde mit Fokus auf Energieeffizienz, Energieüberwachung und Energieverwaltung entwickelt.

Das Design der Basis-Hardware wurde in Bezug auf den Leistungsaspekt optimiert:

- Das Design schließt nun hoch leistungsfähige Netzteile und Spannungsregler ein.
- Wo immer möglich, wurden die Leistungskomponenten mit den niedrigsten Leistungsanforderungen verwendet.
- Das Chassis-Design hat den Luftstrom durch das System optimiert, um die Leistungsaufnahme des Lüfters zu minimieren.

PowerEdge-Systeme bieten viele Funktionen zur Energieüberwachung und -verwaltung:

- **Strominventar und -budgetierung:** Ein Systeminventar leitet beim Start die Kalkulation eines Systemstrombudgets für die aktuelle Konfiguration ein.
- **Strombegrenzung:** Die Systeme können auf einen bestimmten Stromgrenzwert beschränkt werden.
- **Energieüberwachung:** Der iDRAC6 fragt die Netzteile ab, um Leistungsaufnahmewerte zu erfassen. Der iDRAC6 dokumentiert eine Historie von Energiemesswerten und berechnet Durchschnitts- und Spitzenwerte. Mithilfe der webbasierten iDRAC6-Schnittstelle können Sie die Informationen auf der Seite **Energieüberwachung** einsehen.

Strominventar, Strombudgetierung und - begrenzung

Aus der Verbrauchsperspektive kann es auf Rack-Level zu begrenzter Kühlung kommen. Mit einer benutzerdefinierten Strombegrenzung können Sie Strom je nach Bedarf zur Erfüllung Ihrer Leistungsanforderungen zuordnen.

Der iDRAC6 überwacht die Leistungsaufnahme und beschränkt die Prozessoren dynamisch, um die von Ihnen definierte Strombegrenzung zu optimieren, wodurch Ihre Leistung optimiert, Ihre Leistungsanforderungen aber dennoch erfüllt werden.

Stromüberwachung

Der iDRAC6 überwacht kontinuierlich den Stromverbrauch in PowerEdge-Servern. Der iDRAC6 errechnet folgende Stromwerte und zeigt die Informationen tauf seiner webbasierten Schnittstelle oder der RACADM-Befehlszeilenschnittstelle (CLI) an:

- Kumulative Stromenergie
- Durchschnittliche, minimale und maximale Stromenergie
- Strom-Headroom-Werte
- Stromverbrauch (wird grafisch auch auf der Webschnittstelle angezeigt)

Konfiguration und Verwaltung der Energieeinstellungen

Sie können die webbasierte iDRAC6-Schnittstelle und die RACADM-Befehlszeilenschnittstelle (CLI - command line interface) zur Verwaltung und Konfiguration der Stromsteuerungen im PowerEdge-System verwenden. Genauer gesagt können Sie:

- den Netzstromstatus des Servers anzeigen
- Stromsteuerungsmaßnahmen auf dem Server (z. B. Strom EIN, Strom AUS, System-Reset, Aus- und Einschalten) ausführen
- Budgetinformationen für den Server und die installierten Netzteile, z.B. die niedrigste und die höchste Leistungsaufnahme anzeigen
- den Schwellenwert für das Strombudget des Servers anzeigen

Den Funktionszustand der Netzteileinheiten anzeigen

Die Seite **Netzteile** zeigt den Status und die Zulassungen der Netzteile an, die im Server installiert sind.

Die webbasierte Schnittstelle verwenden

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 enthält folgende Informationen:
   - **Redundanz-Status 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 eines von ihnen ist defekt. Keine Redundanz
     - **Deaktiviert**: Nur eines der zwei 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 Warnungsmeldungen ausgegeben wurden, und dass innerhalb des vom Administrator festgelegten Zeitraums Korrekturmaßnahmen vorgenommen werden müssen. Wenn innerhalb des vom Administrator festgelegten Zeitraums keine Korrekturmaßnahmen vorgenommen werden, kann dies zu kritischen oder schwerwiegenden Stromausfällen führen, die sich wiederum auf die Integrität des Servers auswirken können.
       - **Schwerwiegend:** Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Der Fehlerstatus zeigt einen Stromausfall des Servers an und es müssen umgehend Korrekturmaßnahmen getroffen werden.
     - **Position** Zeigt den Namen der Netzteileinheit an: PS-n, wobei n die Nummer der Netzteileinheit ist.
     - **Typ:** zeigt den Netzteiltyp an, z.B. AC oder DC (AC-in-DC oder DC-an-DC-Spannungswandlung).
     - **Eingangsleistung** zeigt die Eingangsleistung des Netzteils in Watt an, d. h. die höchste Wechselstromlast, die das System einem 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 des Netzteils an; vorhanden und OK, Eingang ausgefallen, fehlt oder absehbares Versagen.
     - **FW-Version**: Zeigt die Firmware-Version des Netzteils an.

ANMERKUNG: Aufgrund der Netzteileffizienz ist die Höchstleistung in Watt nicht unbedingt dasselbe wie die Eingangsleistung. Beispiel: Beträgt die Effizienz des Netzteils 89 % und die Höchstleistung beträgt 717 W, dann beträgt die Eingangsleistung in etwa 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 Übersichten zum Status des Strombudgets für das Strom-Subsystem auf der Seite **Informationen zum Strombudget**.

Webschnittstelle verwenden

ANMERKUNG: Um Energieverwaltungsmaßnahmen auszuführen, brauchen Sie **Administrator**rechte.

1. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
2. Klicken Sie auf die Registerkarte **Energieverwaltung**.
3. Wählen Sie die Option **Strombudget** aus.
4. Die Seite **Informationen zum Strombudget** wird angezeigt.

Die erste Tabelle enthält die Minimal- und Maximalgrenzen der vom Benutzer spezifizierten Stromschwellenwerte für die aktuelle Systemkonfiguration. Diese stellen den Bereich der Wechselstrom-Leistungsaufnahme dar, den Sie als Begrenzung für das System einrichten können. Wird die Begrenzung ausgewählt, entspricht sie dem Höchstwert der Wechselstromlast, 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

Strombudget-Schwellenwert bestimmt, wenn aktiviert, die Strombegrenzung für das System. Die Systemleistung wird dynamisch angepasst, um den Stromverbrauch an den festgelegten Schwellenwert anzunähern. Der tatsächliche Stromverbrauch kann bei niedriger Auslastung geringer sein und den Schwellenwert für einen Augenblick überschreiten, bis Leistungsanpassungen abgeschlossen sind.

Wenn Sie **Aktiviert** für den Strombudgetgrenzwert markieren, wendet das System den benutzerspezifischen Grenzwert an. Bleibt der Strombudgetgrenzwert **unmarkiert**, begrenzt das System den Strom nicht. Beispiel: Eine beliebige Systemkonfiguration sieht für den höchsten potenziellen Stromverbrauch 700 W und für den geringsten potenziellen Stromverbrauch 500 W vor. Sie können einen Strombudgetgrenzwert spezifizieren und die Strombudgetbegrenzungsfunktion aktivieren, um die Leistungsaufnahme von derzeit 650 W auf 525 W zu senken. Ab diesem Punkt wird die Leistung des Systems dynamisch angepasst, um die Leistungsaufnahme unter dem benutzerspezifizierten Grenzwert von 525 W zu halten.

Auf die webbasierte Schnittstelle zugreifen

1. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
2. Klicken Sie auf die Registerkarte **Power Management** (Energieverwaltung).
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 aus der **Strombudgetgrenzwert-Tabelle** ein. Der von Ihnen spezifizierte Wert in Watt oder BTU/h stellt dann den Grenzwert für das Strombudget dar. Wenn Sie einen Prozentwert angeben, ist dies ein Prozentsatz der Maximum-bis-Minimum-Spanne der potenziellen Leistungsaufnahme. Beispiel: 100% Grenzwert bedeutet maximale potenzielle Leistungsaufnahme, während 0% minimale potenzielle Leistungsaufnahme bedeutet.

   ANMERKUNG: Der Strombudgetgrenzwert kann nicht über der maximalen potenziellen Leistungsaufnahme oder unter der minimalen potenziellen Leistungsaufnahme liegen.

5. Markieren Sie **Aktiviert**, um den Grenzwert zu aktivieren oder lassen Sie ihn unmarkiert. Wenn Sie **Aktiviert** markieren, wendet das System den benutzerspezifischen Grenzwert an. Bei **unmarkierter** Funktion, begrenzt das System die Leistung nicht.
6. Klicken Sie auf **Änderungen übernehmen**.

RACADM verwenden

```
racadm config -g cfgServerPower -o cfgServerPowerCapWatts <Strombegrenzung in Watt>

racadm config -g cfgServerPower -o cfgServerPowerCapBTUhr <Strombegrenzung in BTU/h>

racadm config -g cfgServerPower -o cfgServerPowerCapPercent <Stromkapazitätswert in %>
```

ANMERKUNG: Bei einem Strombudgetgrenzwert in BTU/h wird bei der Umrechung in Watt auf die nächste ganze Zahl gerundet. Bei der Rückumwandlung von Watt in BTU/h erfolgt dieselbe Abrundung. Folglich kann sich der geschriebene Wert nominal vom abgelesenen Wert unterscheiden. Beispiel: Ein auf 600 BTU/h eingestellter Grenzwert wird als 601 BTU/h abgelesen.

Energieüberwachung anzeigen

Webschnittstelle verwenden

Um die Energieüberwachungsdaten anzuzeigen:

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

Die Informationen auf der Seite **Energieüberwachung** wird nachstehend beschrieben:

Stromüberwachung

- **Status**: **OK** weist darauf hin, dass Netzteile vorhanden sind und mit dem Server kommunizieren; **Warnung** verweist darauf, dass eine Warnmeldung versandt wurde, und **Schwerwiegend** verweist darauf, dass eine Fehlermeldung versandt 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

- **Position:** Zeigt den Namen der Netzteileinheit an: PS-n, wobei n die Nummer der Netzteileinheit ist.
- **Messwert**: Der aktuelle Stromverbrauch in Ampere

Stromüberwachungsstatistik

ANMERKUNG: In der Liste der aktuellen Zeit und der Spitzenzeit ist ein unbehobener Defekt enthalten. Der unter der aktuellen Zeit angegebene Wert ist in Wirklichkeit die Spitzenzeit und umgekehrt.

- **Kumulativ**: Zeigt die aktuelle gesamte Netzstromaufnahme für den Server an, gemessen von der Eingangsseite der Netzteile. Der Wert wird in kWh angegeben und ist ein kumulativer Wert, der die gesamte vom System verwendete Energie angibt. Dieser Wert kann mit der Schaltfläche **Kumulativ zurücksetzen** zurückgesetzt werden.
- **Max. Spitzenstromstärke** - Gibt die Spitzenstromstärke innerhalb des Intervalls zwischen Startzeit und aktueller Zeit an. Dieser Wert kann mit der Schaltfläche **Max. Spitzenstromstärke zurücksetzen** zurückgesetzt werden.
- **Max. Spitzenstromstärke in Watt** - Gibt die Spitzenstromstärke innerhalb des Intervalls zwischen Startzeit und aktueller Zeit an. Dieser Wert kann mit der Schaltfläche **Max. Spitzenwerte zurücksetzen** zurückgesetzt werden.
- **Startzeit** - Zeigt das Aufzeichnungsdatum und die Zeit an, zu der der Wert für die Stromaufnahme des Systems zuletzt gelöscht wurde und der neue Messzyklus begann. Für **Kumulativ** können Sie diesen Wert mit der Schaltfläche **Kumulativ zurücksetzen** zurücksetzen, aber er bleibt bei einer Systemrückstellung oder einem System-Failover erhalten. Für **Max. Spitzenstromstärke** und Max. Spitzenstromstärke in Watt können Sie diesen Wert mit der Schaltfläche **Max. Spitzenwerte zurücksetzen** zurücksetzen, aber er bleibt bei einer Systemrückstellung oder einem System-Failover erhalten.
- **Endzeit** für die Anzeige des **Kumulativwertes** zeigt das aktuelle Datum und die Zeit an, zu der die Kalkulation der anzuzeigenden Leistungsaufnahme des Systems erfolgte. Bei **Spitzenstromstärke** und **Spitzenstromstärke in Watt** zeigen die Felder **Endzeiten** die Zeiten des Auftretens dieser Spitzenwerte an.

ANMERKUNG: Stromüberwachungsstatistiken werden während System Resets kontinuierlich erstellt und zeigen sämtliche Aktivitäten von der Start- bis zur Endzeit der Messung an. Die Schaltfläche **Max. Spitzenwerte rücksetzen** setzt das jeweilige Feld auf Null zurück. In der nächsten Tabelle werden die Daten zur Leistungsaufnahme nicht aufgezeichnet und werden bei einer Zurücksetzung des Systems auf Null zurückgesetzt. Die angezeigten Stromwerte sind kumulative Durchschnittswerte im jeweiligen Zeitintervall (vorangehende Minute, Stunde, Tag und Woche). Da die Intervalle der Start- zur Beendigungszeiten hier von den Stromüberwachungsstatistiken abweichen können, ist es möglich, dass Stromwerte (maximale Spitzenwattwerte gegenüber maximalem Stromverbrauch) voneinander abweichen.

Leistungsaufnahme

- Zeigt die durchschnittliche, maximale und minimale Leistungsaufnahme in dem 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.
- Maximale und minimale Stromaufnahme: Die maximale und minimale Stromaufnahme, die im gegebenen Zeitintervall gemessen wurde.
- Zeit der maximalen und minimalen Leistungsaufnahme: Die Zeiten, zu denen die maximale und minimale Stromaufnahmen auftraten.

Headroom

Momentaner Spielraum des Systems (System Instantaneous Headroom) zeigt den Unterschied zwischen der in den Netzteilen verfügbaren Leistung und der aktuellen Leistungsaufnahme des Systems an.

Spitzen-Spielraum des Systems zeigt den Unterschied zwischen der in den Netzteilen verfügbaren Leistung und der Spitzen-Leistungsaufnahme des Systems an.

Diagramm anzeigen

Durch Klicken auf diese Schaltfläche werden Diagramme aufgerufen, die die iDRAC6-Leistung und die aktuelle Leistungsaufnahme während der letzten Stunde jeweils in Watt und Ampere anzeigen. Der Benutzer kann die Statistiken bis zu einer Woche im Rückblick einsehen, indem er in dem Drop-down-Menü über den Diagrammen entsprechend auswählt.

ANMERKUNG: Die Dateieinträge im Diagramm zeigen jeweils Durchschnittsmesswerte über einen Zeitraum von 5 Minuten. Aus diesem Grund geben die Diagramme kurze Abweichungen oder den aktuellen Verbrauch eventuell nicht wieder.

Durchführen von Stromsteuerungsmaßnahmen am Server

ANMERKUNG: Um Energieverwaltungsmaßnahmen durchführen zu können, benötigen Sie **Administratorrechte für die Gehäusesteuerung**.

Mit dem iDRAC6 können im Remote-Zugriff mehrere Stromverwaltungsmaßnahmen durchgeführt werden, so z. B. das ordnungsgemäße Herunterfahren.

Webschnittstelle verwenden

1. Melden Sie sich bei der iDRAC6-Webschnittstelle an.
2. Klicken Sie auf die Registerkarte **Energieverwaltung**. Die Seite **Energiesteuerung** wird angezeigt.
3. Wählen Sie eine der folgenden **Stromsteuerungsvorgänge** aus, indem Sie auf die Optionsschaltfläche klicken:
   - **System einschalten** - Schaltet den Server EIN (entspricht dem Drücken des Netzschalters, wenn der Systemstrom AUSgeschaltet ist). Diese Option ist deaktiviert, wenn der Server bereits EINgeschaltet ist.
   - **System ausschalten** - Schaltet den Strom zum System 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.
   - **Warm-Neustart** - Startet das System neu, ohne den Strom abzuschalten. Diese Option ist deaktiviert, wenn das System bereits AUSgeschaltet ist.
   - **System aus- und einschalten (Hardware-Neustart)** - Schaltet den Server aus und startet ihn daraufhin neu. Diese Option ist deaktiviert, wenn das System bereits AUSgeschaltet ist.
4. Klicken Sie auf **Anwenden**. Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
5. Klicken Sie auf **OK**, um die gewählte Energieverwaltungsmaßnahme 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, Abschalten, Aus-/Einschalten, Hardwareneustart oder Energiestatus ist.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Sicherheitsfunktionen konfigurieren

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Der iDRAC 6 enthält die folgenden Sicherheitsfunktionen:

- Erweiterte Sicherheitsoptionen für den iDRAC 6-Aministrator:
  - Mittels der Deaktivierungsoption für die Konsolenumleitung können Benutzer des *lokalen* Systems die Konsolenumleitung anhand der DRAC 6-Konsolenumleitungsfunktion deaktivieren.
  - Die Deaktivierungsfunktionen für die lokale Konfiguration ermöglichen dem *Remote*-DRAC-Administrator, die Fähigkeit zum Konfigurieren des DRAC 6 über folgende Möglichkeiten selektiv zu deaktivieren:
    - BIOS-POST, Options-ROM
    - Betriebssystem unter Verwendung des lokalen RACADM und der Dell™ OpenManage™ Server Administrator-Dienstprogramme
- Vorgang für RACADM-CLI und Internet-basierte Schnittstelle, der SSL-128-Bit-Verschlüsselung und SSL-40-Bit-Verschlüsselung (für Länder, in denen 128 Bit nicht annehmbar ist) unterstützt

  ANMERKUNG: Telnet unterstützt SSL-Verschlüsselung nicht.

- Sitzungszeitlimit-Konfiguration (in Sekunden) über die Internet-basierte Schnittstelle oder RACADM-CLI
- Konfigurierbare IP-Schnittstellen (wo anwendbar)
- Secure Shell (SSH), die eine verschlüsselte Transportschicht für höhere Sicherheit verwendet.
- Anmeldungsfehlversuch-Beschränkung pro IP-Adresse, mit Anmeldungsblockierung der IP-Adresse, wenn die Grenze überschritten wird.
- Eingeschränkter IP-Adressenbereich für Clients, die eine Verbindung zum iDRAC 6 herstellen

---

Erweiterte Optionen für den iDRAC 6-Aministrator

Lokale iDRAC 6-Konfiguration deaktivieren

Administratoren können die lokale Konfiguration über die DRAC 6-GUI (Grafische Benutzeroberfläche) deaktivieren, indem sie **Remote-Zugriff**→ **Konfiguration**→ **Dienste** auswählen. Wenn das Kontrollkästchen **Lokale DRAC-Konfiguration mittels Options-ROM deaktivieren** ausgewählt ist, wird das iDRAC 6-Konfigurationsdienstprogramm (auf das Sie durch Drücken auf <Strg+E> während des Systemstarts zugreifen können) im schreibgeschützten Modus betrieben, wodurch lokale Benutzer daran gehindert werden, die Komponente zu konfigurieren. Wenn der Administrator das Kontrollkästchen **Lokale DRAC-Konfiguration mittels RACADM deaktivieren** auswählt, können lokale Benutzer den iDRAC 6 nicht über das RACADM-Dienstprogramm oder mittels des Dell OpenManage Server Administrator konfigurieren, obwohl die Konfigurationseinstellungen noch immer abgelesen werden können.

Administratoren können eine oder beide dieser Optionen gleichzeitig aktivieren. Zusätzlich zum Aktivieren über die GUI können Administratoren 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 deaktiviert, den iDRAC 6 während des Systemneustarts zu konfigurieren.

```
racadm config -g cfgRacTuning -o

cfgRacTuneCtrlEConfigDisable 1
```

ANMERKUNG: Diese Option wird nur im iDRAC 6-Konfigurationsdienstprogramm unterstützt. Um ein Upgrade 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 deaktiviert, den iDRAC 6 unter Verwendung des lokalen RACADM oder mithilfe der Dell OpenManage Server Administrator-Dienstprogramme zu konfigurieren.

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

VORSICHT: Durch diese Funktionen wird die Fähigkeit des lokalen Benutzers, den iDRAC 6 über das lokale System zu konfigurieren sowie einen Reset auf die Standardeinstellung der Konfiguration vorzunehmen, stark eingeschränkt. Dell empfiehlt, die Verwendung dieser Funktionen gut abzuwägen und nur eine Schnittstelle auf einmal zu deaktivieren, um einem vollständigen Verlust der Anmeldungsberechtigungen vorzubeugen.

ANMERKUNG: Weitere Informationen stehen im Weißbuch zum Thema *Lokale Konfiguration und virtuelle Remote-KVM im DRAC deaktivieren* auf der Support-Site von Dell unter **support.dell.com** zur Verfügung.

Obwohl Administratoren die lokalen Konfigurationsoptionen mithilfe von lokalen RACADM-Befehlen einstellen können, ist es aus Sicherheitsgründen nur möglich, die Optionen über eine bandexterne webbasierte iDRAC 6-Schnittstelle oder Befehlszeilenschnittstelle zurückzusetzen. Die Option `cfgRacTuneLocalConfigDisable` gilt, sobald der Einschalt-Selbsttest des Systems abgeschlossen ist und das System in eine Betriebssystemumgebung gestartet wurde. Das Betriebssystem kann vom Typ Microsoft® Windows Server® oder Enterprise Linux sein - ein Betriebssystem, das Befehle des lokalen RACADM ausführen kann - oder ein beschränkt einsetzbares Betriebssystem wie die Microsoft Windows®-Vorinstallationsumgebung oder vmlinux, die zum Ausführen der Befehle des lokalen RACADM im Dell OpenManage Deployment Toolkit verwendet werden.

Es gibt verschiedene Situationen, in denen ein Administrator eine lokale Konfiguration deaktivieren muss. Beispiel: In einem Datenzentrum mit verschiedenen Administratoren für Server und Remote-Zugriffs-Komponenten benötigen diejenigen, die für die Wartung von Serversoftware-Stacks zuständig sind, eventuell keine Administratorrechte zum Zugriff auf Remote-Zugriffs-Komponenten. 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 ihnen dabei jedoch nicht möglich sein, Remote-Zugriffs-Komponenten zu konfigurieren. Administratoren von Remote-Zugriffs-Komponenten sollten in Anbetracht der Möglichkeit solcher Situationen erwägen, die lokale Konfiguration zu deaktivieren.

Administratoren sollten in Betracht ziehen, dass das Deaktivieren lokaler Konfigurationen die Berechtigung zum Ausführen lokaler Konfigurationen stark einschränkt, was auch das Zurücksetzen des iDRAC 6 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 Anmeldungsberechtigung vorzubeugen. Wenn Administratoren z. B. alle lokalen iDRAC 6-Benutzer deaktiviert haben und nur Benutzern des Microsoft Active Directory®-Verzeichnisdienstes gestatten, sich am iDRAC 6 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 iDRAC 6 mit statischer IP-Adresse einem Netzwerk hinzufügen, das bereits einen DHCP-Server (Dynamisches Host-Konfigurationsprotokoll) enthält und der DHCP-Server die iDRAC 6-IP-Adresse daraufhin einer anderen Komponente auf dem Netzwerk zuweist. Durch den sich ergebenden Konflikt kann die bandexterne Konnektivität des DRAC deaktiviert werden, woraufhin Administratoren die Firmware über eine serielle Verbindung auf ihre standardmäßigen Einstellungen zurücksetzen müssen.

Virtuelle iDRAC 6-Remote-KVM deaktivieren

Administratoren können die iDRAC 6-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, muss er von Administratoren umgekehrt werden, damit die Remote-vKVM neu aktiviert werden kann. Die Umkehrung kann durch die Verwendung des Arguments 0 vorgenommen werden:

```
racadm LocalConRedirDisable 0
```

In verschiedenen Situationen ist die Deaktivierung von iDRAC 6-Remote-vKVM erforderlich. Es ist z. B. möglich, dass Administratoren vermeiden möchten, dass ein Remote-iDRAC 6-Benutzer die auf einem System konfigurierten BIOS-Einstellungen anzeigen kann. In diesem Falle können Administratoren die Remote-vKVM während des System-POST deaktivieren, indem Sie den Befehl `LocalConRedirDisable` anwenden. Es empfiehlt sich vielleicht auch, 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 Benutzeranmeldungs-Scripts auszuführen.

ANMERKUNG: Weitere Informationen stehen im Weißbuch zum Thema *Lokale Konfiguration und virtuelle Remote-KVM im DRAC deaktivieren* auf der Support-Site von Dell unter **support.dell.com** zur Verfügung.

Weitere Informationen zu Anmeldungs-Scripts sind unter **technet2,microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx** enthalten.

---

iDRAC 6-Datenübertragung mit SSL und digitalen Zertifikaten sichern

Dieser Unterabschnitt enthält Informationen über die folgenden Datensicherheitsfunktionen, die in Ihrem iDRAC 6 integriert sind:

Secure Sockets Layer (SSL)

Der iDRAC 6 beinhaltet einen Web Server, der zur Verwendung des SSL-Sicherheitsprotokolls nach industriellem Standard konfiguriert wurde, um verschlüsselte Daten über das Internet zu übertragen. SSL ist aufgebaut auf öffentlicher und privater Verschlüsselungstechnologie und eine allgemein akzeptierte Technik, um authentifizierte und verschlüsselte Kommunikationen zwischen Clients und Servern zu bieten, und unbefugtes Lauschen auf dem Netzwerk zu verhindern.

Merkmale eines SSL-aktivierten Systems:

- Sich an einem SSL-aktivierten Client authentifizieren

- Dem Client erlauben, sich am Server zu authentifizieren
- Beiden Systemen gestatten, eine verschlüsselte Verbindung herzustellen

Dieses Verschlüsselungsverfahren gewährt eine hohe Datenschutzstufe. Der iDRAC 6 verwendet den 128-Bit-SSL-Verschlüsselungsstandard, die sicherste Form der Verschlüsselung, die für Webbrowser in Nordamerika allgemein verfügbar ist.

Der iDRAC 6-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 Aufforderung an den iDRAC 6 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 zum Schutz der Identität eines Remote-Systems und damit sichergestellt werden kann, dass mit dem Remote-System ausgetauschte Informationen von anderen weder gesehen noch geändert werden können. Um die Sicherheit für den DRAC 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 von CAs schließen Thawte und VeriSign ein. 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 iDRAC 6-Firmware hochgeladen werden. Die auf der iDRAC 6-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 **Konfiguration** und dann auf **SSL**.

Verwenden Sie das **SSL-Hauptmenü** (siehe Tabelle 21-1), um eine CSR zu erstellen, laden Sie ein bestehendes Serverzertifikat hoch oder zeigen Sie ein bestehendes Serverzertifikat an. Die CSR-Informationen werden in der iDRAC 6-Firmware gespeichert. Tabelle 21-2 beschreibt die auf der **SSL-Seite** verfügbaren Schaltflächen.

Tabelle 21-1. SSL-Hauptmenü

Feld	Beschreibung
Zertifikatsignierungsanforderung (CSR) erstellen	Klicken Sie auf **Weiter**, um die Seite zu öffnen, die Ihnen ermöglicht, eine CSR zu erstellen, die an eine Zertifizierungsstelle gesendet werden kann, um ein sicheres Internet-Zertifikat anzufordern.
Serverzertifikat hochladen	Klicken Sie auf **Weiter**, um ein vorhandenes Zertifikat hochzuladen, das Ihrer Firma gehört und für die Zugriffsteuerung auf den iDRAC 6 verwendet wird. **ANMERKUNG:** Der iDRAC 6 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 iDRAC 6 erhalten haben.
Serverzertifikat anzeigen	Klicken Sie auf **Weiter**, um ein vorhandenes Serverzertifikat anzuzeigen.

Tabelle 21-2. SSL-Hauptmenüschaltflächen

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 iDRAC Ihre CR annimmt, muss die signierte 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 21-3 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 21-4 beschreibt die auf der Seite **Zertifikatsignierungsanforderung (CSR) erstellen** verfügbaren Schaltflächen.

Tabelle 21-3. 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, Unterstreichungszeichen und Punkte sind gültig. Leerstellen sind nicht gültig.
Name der Organisation	Der mit dieser Organisation assoziierte Name (zum Beispiel, XYZ Unternehmen). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Organisationseinheit	Der mit einer organisatorischen Einheit assoziierte Name, wie z. B. eine Abteilung (zum Beispiel, Unternehmensgruppe). 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, wo sich das Unternehmen, das sich um Zertifikat bewirbt, befindet. Verwenden Sie das Drop-Down-Menü, um das Land auszuwählen.
E-Mail	Die mit der CSR verbundene E-Mail-Adresse. Sie können die E-Mail-Adresse Ihrer Firma eingeben oder eine E-Mail-Adresse, die mit der CSR in Verbindung stehen soll. Dieses Feld ist optional.

Tabelle 21-4. 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. Wählen Sie auf der Seite **SSL-Hauptmenü** die Option **Serverzertifikat anzeigen,** und klicken Sie auf **Weiter**.

   Tabelle 21-5 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 21-5. Zertifikatinformationen

Feld	Beschreibung
Seriennummer	Seriennummer des Zertifikats
Bewerberinformationen	Vom Bewerber eingegebene Zertifikatsattribute
Ausstellerinformationen	Vom Aussteller zurückgegebene Zertifikatsattribute
Gültig von	Ausgabedatum des Zertifikats
Gültig bis	Ablaufdatum des Zertifikats

Verwenden der Secure Shell (SSH)

Weitere Informationen über die Verwendung von SSH finden Sie unter "Verwenden der Secure Shell (SSH)".

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 **Konfiguration** und dann auf **Dienste**.
3. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Lokale Konfiguration (Tabelle 21-6)
   - Web Server (Tabelle 21-7)
   - SSH (Tabelle 21-8)
   - Telnet (Tabelle 21-9)
   - Remote-RACADM (Tabelle 21-10)
   - SNMP-Agent (Tabelle 21-11)
   - Automatisierter Systemwiederherstellungs-Agent (Tabelle 21-12)

   Verwenden Sie den **Automatisierten Systemwiederherstellungs-Agent**, um die Funktion **Bildschirm Letzter Absturz** des iDRAC 6 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 iDRAC 6 funktionieren kann.
4. Klicken Sie auf **Änderungen übernehmen**.
5. Klicken Sie auf der Seite **Dienste** auf die entsprechende Schaltfläche, um fortzufahren. Siehe Tabelle 21-13.

Tabelle 21-6. 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> einzugeben.
Lokale iDRAC-Konfiguration mittels RACADM deaktivieren	Deaktiviert die lokale Konfiguration des iDRAC mithilfe von RACADM.

Tabelle 21-7. 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 ungenutzt bleiben kann. Die Sitzung wird abgebrochen, wenn das Zeitlimit 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	Die vom iDRAC verwendete Schnittstelle, die auf eine Serververbindung hört. Die Standardeinstellung ist **80**.
HTTPS-Anschlussnummer	Die vom iDRAC verwendete Schnittstelle, die auf eine Serververbindung hört. Die Standardeinstellung ist **443**.

Tabelle 21-8. 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 Zeitlimit-Funktion zu deaktivieren. Die Standardeinstellung ist **300.**
Anschlussnummer	Der Anschluss, an dem der iDRAC 6 abhört, ob eine Browser-Verbindung besteht. Die Standardeinstellung ist **22.**

Tabelle 21-9. Telnet-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert Telnet. Wenn markiert, ist Telnet aktiviert.
Zeitüberschreitung	Die Telnet-Zeitüberschreitung wegen Leerlauf, in Sekunden. Der Zeitüberschreitungsbereich beträgt 60 bis 1920 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitlimit-Funktion zu deaktivieren. Die Standardeinstellung ist **300.**
Anschlussnummer	Der Anschluss, an dem der iDRAC 6 abhört, ob eine Browser-Verbindung besteht. Die Standardeinstellung ist **23.**

Tabelle 21-10. 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 21-11. SNMP-Agent-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert den SNMP-Agenten. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Community-Name	Der Name der Community, die 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 21-12. Einstellung des automatisierten Systemwiederherstellungs-Agenten

Einstellung	Beschreibung
Aktiviert	Aktiviert den automatisierten Systemwiederherstellungs-Agenten.

Tabelle 21-13. Schaltflächen der Dienste-Seite

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Dienste**.
Aktualisieren	Aktualisiert die Seite **Dienste**.
Änderungen übernehmen	Wendet die Einstellungen für die Seite **Dienste** an.

Zusätzliche iDRAC 6-Sicherheitsoptionen aktivieren

Um einen unberechtigten Zugriff auf das Remote-System zu verhindern, enthält der iDRAC 6 die folgenden Funktionen:

- IP-Adressenfilter (IPRange) - Definiert einen spezifischen Bereich von IP-Adressen, die auf den iDRAC 6 zugreifen können.
- Blockierung von IP-Adressen - Beschränkt die Anzahl von fehlgeschlagenen Anmeldungsversuchen von einer spezifischen IP-Adresse

Diese Funktionen sind in der iDRAC 6-Standardkonfiguration deaktiviert. Verwenden Sie den folgenden Unterbefehl oder die Internet-basierte Schnittstelle, um diese Funktionen zu aktivieren.

```
racadm config -g cfgRacTuning -o <Objektname> <Wert>
```

Verwenden Sie darüber hinaus diese Funktionen 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 iDRAC 6-Zugriff nur von Clients oder Verwaltungsstationen aus, deren IP-Adressen innerhalb eines benutzerspezifischen Bereichs liegen. Alle anderen Anmeldungsversuche 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 iDRAC 6 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 steht unter "iDRAC 6-Definitionen für Eigenschafts-Datenbankgruppen und Objekte" zur Verfügung.

Tabelle 21-14. Eigenschaften der IP-Adressenfilterung (IpRange)

Eigenschaft	Beschreibung
cfgRacTuneIpRangeEnable	Aktiviert die IP-Bereichs-Überprüfungsfunktion.
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 iDRAC 6-Sitzung herzustellen. Anmeldeversuche von IP-Adressen, die sich außerhalb dieses Bereichs befinden, werden fehlschlagen. Die Standardwerte in jeder Eigenschaft erlauben einem Adressenbereich von 192.168.1.0 bis 192.168.1.255, eine iDRAC 6-Sitzung herzustellen.
cfgRacTuneIpRangeMask	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Subnetzmaske sollte in der Form einer Netzmaske sein, wobei die bedeutenderen Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu Nullen (0) in den niederwertigeren Bits.

IP-Filter aktivieren

Es folgt ein Beispiel-Befehl 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 Bit 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 höchstwertigen 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 sollte Nullen in allen niederwertigen Bits haben, wo Nullen in der Maske sind.

IP-Blockierung

Durch IP-Blockierung wird dynamisch festgestellt, wenn von einer bestimmten IP-Adresse aus übermäßige Anmeldefehlschläge auftreten und die Adresse blockiert bzw. daran gehindert wird, eine bestimmte Zeit lang eine Anmeldung am iDRAC 6 durchzuführen.

Der IP-Blockierungsparameter wendet **cfgRacTuning**-Gruppenfunktionen an, die Folgendes umfassen:

- Die Anzahl von zulässigen Anmeldungsfehlversuchen
- 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

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

ANMERKUNG: Wenn Anmeldungsversuche von der Client-IP-Adresse abgelehnt werden, können einige SSH-Clients die folgende Meldung anzeigen: ssh exchange identification: Verbindung vom Remote-Host geschlossen.

Eine vollständige Liste von **cfgRacTune**-Eigenschaften steht unter "iDRAC 6-Definitionen für Eigenschafts-Datenbankgruppen und Objekte" zur Verfügung.

Tabelle 21-15 führt die vom Benutzer definierten Parameter auf.

Tabelle 21-15. Anmeldungswiederholungs-Beschränkungseigenschaften

Eigenschaft	Definition
cfgRacTuneIpBlkEnable	Aktiviert die IP-Blockierungsfunktion. Wenn aufeinander folgende Fehlversuche (**cfgRacTuneIpBlkFailCount**) von einer einzelnen IP-Adresse innerhalb eines spezifischen Zeitraums festgestellt werden (**cfgRacTuneIpBlkFailWindow**), werden alle weiteren Versuche, von dieser Adresse eine Sitzung zu beginnen, während einer bestimmten Zeitspanne zurückgewiesen (**cfgRacTuneIpBlkPenaltyTime**).
cfgRacTuneIpBlkFailCount	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche zurückgewiesen werden.
cfgRacTuneIpBlkFailWindow	Die Zeitspanne in Sekunden, während der die Fehlversuche gezählt werden. Wenn die Fehlversuche diese Grenze überschreiten, werden sie aus dem Zähler gelöscht.
cfgRacTuneIpBlkPenaltyTime	Legt die Zeitspanne in Sekunden fest, während der alle Anmeldungsversuche 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 zu beginnen, wenn dieser Client innerhalb einer Minute fünf fehlerhafte Anmeldungsversuche 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 eine Stunde lang zusätzliche Anmeldungsversuche.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

Konfiguration der Netzwerksicherheitseinstellungen mit der iDRAC 6-GUI

ANMERKUNG: Zum Ausführen der nachfolgenden Schritte müssen Sie über die Berechtigung **iDRAC 6 konfigurieren** verfügen.

1. Klicken Sie in der **System**-Struktur auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** und klicken Sie 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 21-16 beschreibt die Einstellungen der Seite **Netzwerksicherheit**.
5. Klicken Sie auf die Schaltfläche der entsprechenden **Netzwerksicherheits**- Seite, um fortzufahren. Unter Tabelle 21-17 steht eine Beschreibung der Schaltflächen der Seite **Netzwerksicherheit** zur Verfügung.

Tabelle 21-16. Einstellungen der Seite Netzwerksicherheit

Einstellungen	Beschreibung
IP-Bereich aktiviert	Aktiviert die Funktion zum Prüfen des IP-Bereichs, mit der ein bestimmter Bereich an IP-Adressen definiert wird, die auf den iDRAC 6 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 iDRAC 6-Sitzung herzustellen. Anmeldeversuche von IP-Adressen, die sich außerhalb dieses Bereichs befinden, werden fehlschlagen. Die Standardwerte in jeder Eigenschaft erlauben einem Adressenbereich von 192.168.1.0 bis 192.168.1.255, eine iDRAC 6-Sitzung herzustellen.
IP-Bereichs-Subnetzmaske	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Subnetzmaske sollte in Form einer Netzmaske sein, wobei die bedeutenderen Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu nur Nullen (0) in den niederwertigeren Bits. Zum Beispiel: **255.255.255.0**

IP-Blockierung aktiviert	Aktiviert die IP-Adressen-Blockierungsfunktion, mit der während einer festgelegten Zeitspanne die Anzahl von Anmeldungsfehlversuchen einer spezifischen IP-Adresse eingeschränkt wird.
IP-Blockierung, Zählung von Fehlversuchen	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche von dieser Adresse zurückgewiesen werden.
IP-Blockierung, Fenster der Fehlversuche	Bestimmt die Zeitspanne in Sekunden, während der die gezählten IP-Blockierungs-Fehlversuche auftreten müssen, um die IP-Blockierungs-Penalty-Zeit auszulösen.
IP-Blockierungs-Penalty-Zeit	Die Zeitspanne in Sekunden, während der Anmeldungsversuche von einer IP-Adresse aufgrund übermäßiger Fehlversuche zurückgewiesen werden.

Tabelle 21-17. 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 **Netzwerkkonfiguration** zurück.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Grundlegende Installation des iDRAC6

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Dieser Abschnitt enthält Informationen über Installation und Setup 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 im optionalen Einbausatz)
- iDRAC6-Installationsverfahren (in diesem Kapitel enthalten)
- DVD *Dell Systems Management Tools and Documentation*

Die iDRAC6 Express/Enterprise-Hardware installieren

ANMERKUNG: Die iDRAC6-Verbindung emuliert eine USB-Tastaturverbindung. Infolgedessen wird Sie das System beim Neustart nicht benachrichtigen, wenn keine Tastatur angeschlossen ist.

Der iDRAC6 kann auf Ihrem System vorinstalliert oder getrennt in einem Einbausatz erhältlich sein. Informationen zum Einstieg mit dem auf dem System installierten iDRAC6 stehen unter Übersicht zu Softwareinstallation und -konfiguration zur Verfügung.

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

System zur Verwendung eines iDRAC6 konfigurieren

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

Das iDRAC6-Konfigurationsdienstprogramm wie folgt ausführen:

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 die 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 Tasten <Nach links> und <Nach rechts> eine der folgenden NIC-Optionen aus:

      - **Dediziert** - Wählen Sie diese Option aus, um das Remote-Zugriffsgerät zur Verwendung der dedizierten Netzschnittschnelle auf dem iDRAC Enterprise zu aktivieren. Diese Schnittstelle wird nicht an das Host-Betriebssystem freigegeben und leitet den Verwaltungsverkehr zu einem separaten physischen Netzwerk, wodurch es vom Anwendungsverkehr getrennt wird. Diese Option steht nur dann zur Verfügung, wenn auf dem System ein iDRAC6-Enterprise vorhanden ist.

      - **Freigegeben** - Diese Option auswählen, um die Netzschnittstelle an das Host-Betriebssystem freizugeben. Die Remote-Zugriffs-Gerätenetzschnittstelle ist vollständig funktionsfähig, wenn das Host-Betriebssystem für das 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, ist der Zugriff auf das Remote-Zugriffsgerät nicht möglich.

      - **Freigegeben mit Failover-LOM 2** - Wählen Sie diese Option aus, um die Netzschnittstelle an das Host-Betriebssystem freizugeben. Die Remote-Zugriffs-Gerätenetzschnittstelle ist vollständig funktionsfähig, wenn das Host-Betriebssystem für das 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 zu NIC 2. Das Remote-Zugriffsgerät verwendet NIC 2 weiterhin für die Datenübertragung. Wenn der NIC 2 fehlerhaft ist, schaltet das Remote-Zugriffsgerät für alle Datenübertragungen zum NIC1 1 zurück. Dies geschieht jedoch nur, wenn der ursprüngliche NIC 1-Fehler korrigiert wurde.

      - **Freigegeben mit Failover All LOMs**- Wählen Sie diese Option aus, um die Netzschnittstelle an das Host-Betriebssystem freizugeben. Die Remote-Zugriffs-Gerätenetzschnittstelle ist vollständig funktionsfähig, wenn das Host-Betriebssystem für das NIC-Teaming konfiguriert ist. Das Remote-Zugriffsgerät empfängt Daten über NIC 1, NIC 2, NIC3 und NIC 4; es sendet Daten jedoch nur über NIC 1. Wenn NIC 1 ausfällt, schaltet das Remote-Zugriffsgerät für alle Datenübertragungen zu NIC 2 zurück. Wenn NIC 2 ausfällt, schaltet das Remote-Zugriffsgerät für alle Datenübertragungen zu NIC 3 zurück. Wenn NIC 3 ausfällt, schaltet das Remote-Zugriffsgerät für alle Datenübertragungen zu NIC 4 zurück. Wenn 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.

4. Konfigurieren Sie die LAN-Parameter des Netzwerk-Controllers zur Verwendung von DHCP oder einer statischen IP-Adressenquelle.
    a. Wählen Sie mit der Nach-unten-Taste **LAN-Parameter** aus, und drücken Sie auf die <Eingabetaste>.
    b. Wählen Sie die **IP-Adressenquelle** mit der Nach-oben- und Nach- unten-Taste aus.
    c. Wählen Sie mit den Tasten <Nach links> und <Nach rechts> **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 auf <Esc>.
5. Drücken Sie auf <Esc>.
6. Wählen Sie **Änderungen speichern und beenden** aus.

Übersicht zu Softwareinstallation und - konfiguration

Dieser Abschnitt bietet eine Übersicht auf höchster Ebene des 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 dem verwalteten System installieren".

Konfiguration des iDRAC6

So konfigurieren Sie den iDRAC6:

1. Wählen Sie eines der folgenden Konfigurationshilfsprogramme aus:
    - Webbasierte Oberfläche - Siehe "iDRAC 6 mittels der Webschnittstelle konfigurieren"
    - RACADM-CLI - Siehe "iDRAC 6-SM-CLP-Befehlszeilenschnittstelle verwenden"
    - Telnet-Konsole - siehe "Telnetkonsole 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 "iDRAC 6- Netzwerkeinstellungen konfigurieren".
3. iDRAC6-Benutzer hinzufügen und konfigurieren Siehe "iDRAC6- Benutzer hinzufügen und konfigurieren".
4. Konfigurieren Sie den Internet-Browser, um auf die Internet-basierte Schnittstelle zuzugreifen. Siehe "Einen unterstützten Web-Browser konfigurieren".
5. Deaktivieren Sie die Microsoft® Windows® -Option Automatischer Neustart. Siehe "Die Windows-Option Automatischer Neustart deaktivieren".
6. Die iDRAC6-Firmware aktualisieren Siehe "Die iDRAC6-Firmware aktualisieren".

Software auf dem verwalteten System installieren

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

Installieren Sie die Managed-System-Software, indem Sie die Software unter Verwendung der DVD *Dell Systems Management Tools and Documentation* auf dem verwalteten System installieren. Die vollständige Installationsanleitung für die Software finden Sie in der *Schnellinstallationsanleitung*, die auf der Dell Support-Website unter **support.dell.com / manuals** erhältlich ist.

Die Managed-System-Software installiert Ihre Auswahlen aus 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 Letzter Absturz des Systems anzeigen noch die Funktion **Autom. Wiederherstellung** verwenden.

Weitere Informationen zum Bildschirm des letzten Absturzes finden Sie unter "Bildschirm Letzter Systemabsturz anzeigen".

Software auf der Management Station installieren

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

· DVD root - Enthält das Dell Systems Build and Update-Hilfsprogramm, das Informationen zur Server-Einrichtung und Systeminstallation bereitstellt

SYSMGMT - Enthält die Systemmanagement-Softwareprodukte einschließlich Dell OpenManage Server Administrator

· Docs: Dieses Verzeichnis enthält Dokumentation für System- Management Software-Produkte, Peripheriegeräte und RAID-Controller.

· SERVICE - Enthält die Instrumente zur Systemkonfiguration und liefert die neuesten Diagnosen und Dell-optimierte Treiber für Ihr System

Informationen über Server Administrator, IT Assistant und Unified Server Configurator finden Sie im *Server Administrator Benutzerhandbuch*, dem *IT Assistant Benutzerhandbuch* und dem *Unified Server 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, laden Sie die DVD *Dell Systems Management Tools and Documentation* unter Verwendung des folgenden Befehls oder eines ähnlichen Befehls:

   ```
   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 zum Installieren der RAC-Software verwendet wurde.

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

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

Die 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 "Die iDRAC6-Firmware über RACADM aktualisieren"
- Dell Aktualisierungspakete Siehe "iDRAC6-Firmware mittels Dell Aktualisierungspaketen für unterstützte Windows- und Linux-Betriebssysteme aktualisieren"

Bevor Sie beginnen

Bevor Sie die iDRAC6-Firmware anhand von lokalem RACADM oder Dell Aktualisierungspaketen 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 entladen Sie ihn.

   ANMERKUNG: Wird die iDRAC6-Firmware-Aktualisierung aus irgendeinem Grund unterbrochen, kann es bis zu 30 Minuten dauern, bis eine erneute Aktualisierung zugelassen wird.

5. Stellen Sie sicher, dass der USB aktiviert ist.

Die 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 in Ihrem lokalen System.

Die folgenden Software-Komponenten sind in Ihrem iDRAC6-Firmware-Paket enthalten:

- Kompilierte iDRAC6-Firmware-Codes und -Daten
- Webbasierte Benutzerschnittstelle, JPEG und andere Benutzeroberflächen-Datendateien
- Standardeinstellungskonfigurationsdateien

iDRAC6-Firmware mittels der webbasierten Benutzerschnittstelle aktualisieren

Weitere Informationen finden Sie unter "iDRAC 6 Firmware/Systemdienste-Wiederherstellungs-Image aktualisieren".

Die 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-Image von Dells Support-Website unter **support.dell.com** auf das verwaltete System herunter.

   Zum Beispiel:

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

2. Führen Sie den folgenden RACADM-Befehl aus:

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

   Sie können die Firmware auch unter Verwendung von remote RACADM aktualisieren.

   Zum Beispiel:

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

   wobei *path* die Position auf dem TFTP-Server ist, wo **firmimg.d6** gespeichert ist.

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

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

ANMERKUNG: Wird die iDRAC6-Firmware mit dem Dienstprogramm des Dell Aktualisierungspakets in Linux aktualisiert, werden womöglich 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
```

Dabei handelt es sich um 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 dem Firmware-Upgrade löschen Sie den Cache des Internet-Browsers.

Die Online-Hilfe Ihres Internet-Browsers enthält weitere Informationen.

Einen unterstützten Web-Browser konfigurieren

Die folgenden Abschnitte enthalten Anleitungen zum Konfigurieren von unterstützten Internet-Browsern.

Konfigurieren des Internet-Browsers, um eine Verbindung zur Internet-basierten Schnittstelle des iDRAC6 herzustellen

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

So konfigurieren Sie den Internet Explorer-Browser, 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 **Proxy-Server verwenden** ausgewählt ist, wählen Sie das Kästchen **Proxy-Server für lokale Adressen umgehen** aus.
6. Klicken Sie zweimal auf **OK**.

Liste vertrauenswürdiger Domänen

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

32-Bit- und 64-Bit-Internet-Browser

Die webbasierte iDRAC6-Schnittstelle wird auf 64-Bit-Internet-Browsern 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 Internet-Browser 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 sich am iDRAC6 an.

Lokalisierte Versionen der webbasierten Schnittstelle anzeigen

Windows

Die webbasierte iDRAC6-Schnittstelle wird bei 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 auf <Strg>.
5. Wählen Sie Ihre bevorzugte Sprache aus, und klicken Sie auf **Nach oben**, um die Sprache an die Spitze der Liste zu bewegen.
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 im Red Hat Enterprise Linux-Betriebssystem (Version 4) für vereinfachtes Chinesisch 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 Befehls-Terminal.
2. Geben Sie "locale" ein, und drücken Sie auf die <Eingabetaste>. Die folgende Ausgabe wird eingeblendet.

```
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. iDRAC6 neu starten

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

Informationen zu erweiterten iDRAC6-Konfigurationen finden Sie unter "Erweiterte Konfiguration des iDRAC 6".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC 6 mittels der Webschnittstelle konfigurieren

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Der iDRAC 6 beinhaltet eine Webschnittstelle, über die Sie die iDRAC 6-Eigenschaften und Benutzer konfigurieren, Remote-Verwaltungs-Tasks ausführen sowie Fehler und Probleme auf einem (verwalteten) Remote-System feststellen und beheben können. Verwenden Sie die iDRAC 6-Webschnittstelle für die tägliche Systemverwaltung. Dieses Kapitel gibt darüber Auskunft, wie allgemeine Systemverwaltungs-Tasks über die iDRAC 6-Webschnittstelle ausgeführt werden, und enthält Links zu dazugehörigen Informationen.

Die meisten Webschnittstellen-Konfigurationsaufgaben 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 "iDRAC 6-SM-CLP-Befehlszeilenschnittstelle verwenden", und über RACADM-Befehle unter "Übersicht der RACADM-Unterbefehle" und "iDRAC 6-Definitionen für Eigenschafts-Datenbankgruppen und Objekte".

Zugriff auf die Webschnittstelle

Führen Sie zum Zugriff auf die iDRAC 6-Webschnittstelle folgende Schritte aus:

1. Öffnen Sie einen unterstützten Webbrowser.

   Weitere Informationen finden Sie unter "Unterstützte 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-address>

   Drücken Sie dann <Eingabe>.

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-address>]

   Drücken Sie dann <Eingabe>.

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

   https://<iDRAC-IP-address>:<port-number>

   wobei *iDRAC-IP-address* die IP-Adresse des iDRAC 6 und *port-number* die HTTPS-Anschlussnummer ist.

5. Geben Sie in das Feld **Adresse** https://<iDRAC-IP-address> ein und drücken Sie auf <Eingabe>.

   Wenn die Standard-HTTPS-Portnummer (Port 443) geändert wurde, geben Sie folgendes ein:

   https://*<iDRAC-IP-address>:<port-number>*

   wobei *iDRAC-IP-address* die IP-Adresse des iDRAC 6 und *port-number* die HTTPS-Anschlussnummer ist.

Das iDRAC6-**Anmelde**-Fenster wird eingeblendet.

Anmeldung

Sie können sich als iDRAC 6-Benutzer oder als Microsoft® Active Directory®-Benutzer anmelden. Standardmäßig sind der Benutzername und das Kennwort für einen iDRAC 6-Benutzer jeweils **root** und **calvin**.

Damit Sie sich am iDRAC 6 anmelden können, muss Ihnen der Administrator zuerst die Berechtigung zur **Anmeldung bei iDRAC** gewähren.

Um sich anzumelden, führen Sie die folgenden Schritte aus.

1. Geben Sie eine der folgenden Eingaben in das Feld **Benutzername** ein:
   - Ihr iDRAC 6-Benutzername.

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

     Active Directory-Namen können in einem der folgenden Formate eingegeben werden: <*Benutzername*>, <*Domäne*>\<*Benutzername*>, <*Domäne*>/<*Benutzername*> oder <*Benutzer*>@<*Domäne*>. Es wird bei ihnen 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 iDRAC 6-Benutzerkennwort oder Ihr Active Directory-Benutzerkennwort ein. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden.
3. Wählen Sie im Drop-Down-Feld **Domäne** *Diesen iDRAC* aus, um sich als iDRAC 6-Benutzer anzumelden, oder wählen Sie eine der verfügbaren Domänen aus, um sich als Active Directory-Benutzer anzumelden.

   ANMERKUNG: Als Active Directory-Benutzer wählen Sie *Diesen iDRAC* im Drop-Down-Menü aus, wenn Sie den Domänennamen als Teil des Benutzernamens angegeben haben.
4. Klicken Sie auf **OK**, oder drücken Sie auf 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 erreicht wurde.

ANMERKUNG: Wenn Sie die iDRAC 6-Webschnittstelle im Microsoft Internet Explorer mit der Schließen-Schaltfläche ("x") in der oberen rechten Ecke des Fensters schließen, kann dies zu einem Anwendungsfehler führen. Um dieses Problem zu lösen, laden Sie von der Microsoft Support-Website unter **support.microsoft.com** die neueste kumulative Sicherheitsaktualisierung für Internet Explorer herunter.

---

iDRAC 6-NIC konfigurieren

Für diesen Abschnitt wird angenommen, dass der iDRAC 6 bereits konfiguriert wurde und über das Netzwerk auf ihn zugegriffen werden kann. Hilfe bei der ersten iDRAC 6-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. iDRAC 6 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) beim Ausführen aktiviert ist, stellen Sie sicher, dass auch PortFast oder eine ähnliche Technologie wie folgt eingeschaltet ist:

- An den Anschlüssen für den mit dem iDRAC 6 verbundenen Schalter.
- An den Anschlüssen, die an die Management Station angeschlossen sind, auf der eine iDRAC 6-KVM-Sitzung ausgeführt wird.

  ANMERKUNG: Eventuell wird die folgende Meldung eingeblendet, wenn das System beim POST anhält: Drücken Sie zum Fortfahren die Taste F1 und zum Ausführen des System-Setup-Programms die Taste F2Eine mögliche Ursache für diesen Fehler könnte eine Netzwerküberlastung sein, die dazu führt, dass die Verbindung zum iDRAC 6 unterbrochen wird. Starten Sie das System neu, wenn die Netzwerküberlastung nachgelassen hat.

  1. Klicken Sie auf **Remote-Zugriff**→ **Konfiguration**→ **Netzwerk.**
  2. Auf der Seite **Netzwerk** können Sie Einstellungen für die Netzwerkschnittstellenkarte, allgemeine iDRAC-Einstellungen, IPv4-Einstellungen, IPv6-Einstellungen, IPMI-Einstellungen und VLAN- Einstellungen vornehmen. Siehe Tabelle 4-1, Tabelle 4-2, Tabelle 4-3, Tabelle 4-4, Tabelle 4-5 und Tabelle 4-6 für Beschreibungen dieser Einstellungen.

3. Wenn Sie die erforderlichen Einstellungen vorgenommen haben, klicken Sie auf **Änderungen übernehmen.**

4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-7.

Tabelle 4-1. Netzwerkschnittstellenkarte - Einstellungen

Einstellung	Beschreibung
NIC-Auswahl	Konfiguriert den aktuellen Modus aus den vier möglichen Modi: · Dediziert (iDRAC-NIC) **ANMERKUNG:** Diese Option steht nur auf iDRAC 6 Enterprise zur Verfügung. · Freigegeben (LOM1) · Freigegeben mit Failover: LOM2 · Freigegeben mit Failover: Alle LOMs
MAC-Adresse	Zeigt die Medienzugriffssteuerungs-Adresse (MAC) an, die die einzelnen Knoten in einem Netzwerk eindeutig identifiziert.
NIC aktivieren	Wenn markiert, weist dies darauf hin, dass die NIC aktiviert ist und die verbleibenden Steuerungen dieser Gruppe aktiviert werden. Wenn eine NIC deaktiviert ist, wird jegliche Datenübertragung zum und vom iDRAC 6 über das Netzwerk blockiert. Die Standardeinstellung ist **Ein**.
Automatische Übertragung	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 Duplex-Modus manuell (Aus) einstellen. Falls **NIC-Auswahl** *nicht* auf **Dediziert** eingestellt ist, wird die Einstellung "Automatische Verhandlung" immer aktiviert sein **(Ein)**.
Netzwerkgeschwindigkeit	Ermöglicht Ihnen, die Netzwerkgeschwindigkeit auf 100 Mb oder 10 Mb, entsprechend der Netzwerkumgebung, einzustellen. Diese Option steht nicht zur Verfügung, wenn Automatische Verhandlung auf **Ein** eingestellt ist.
Duplexmodus	Ermöglicht Ihnen, den Duplex-Modus auf Voll- oder Halbduplex, entsprechend der Netzwerkumgebung, einzustellen. Diese Option ist nicht verfügbar, wenn **Automatische Verhandlung** auf **Ein** eingestellt ist.

Tabelle 4-2. Allgemeine iDRAC-Einstellungen

Einstellung	Beschreibung
iDRAC auf DNS registrieren	Registriert den iDRAC 6-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.
DHCP für den DNS-Domänennamen verwenden	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**. **ANMERKUNG:** Wenn das Kontrollkästchen **DHCP für den DNS-Domänennamen verwenden** ausgewählt werden soll, müssen Sie auch das Kontrollkästchen **DHCP verwenden (für NIC-IP-Adresse)** auswählen.
DNS-Domänenname	Der Standard-**DNS-Domänenname** ist leer. Wenn das Kontrollkästchen **DHCP für den DNS-Domänennamen verwenden** ausgewählt ist, ist diese Option grau unterlegt und das Feld kann nicht geändert werden.

Tabelle 4-3. IPv4-Einstellungen

Einstellung	Beschreibung
Aktiviert	Wenn der NIC aktiviert ist, wird die IPv4-Protokoll-Unterstützung ausgewählt und die anderen Felder in diesem Abschnitt werden aktiviert.
Verwenden Sie DHCP (für die NIC-IP-Adresse)	Fordert den iDRAC 6 auf, eine IP-Adresse für den NIC vom Server für das dynamische Host-Konfigurationsprotokoll (DHCP) abzurufen. Die Standardeinstellung ist **Aus**.
IP-Adresse	Gibt die IP-Adresse für den iDRAC-NIC an.
Subnetzmaske	Ermöglicht Ihnen, eine statische IP-Adresse für den iDRAC 6-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 DHCP zum Abrufen von DNS-Server-Adressen, indem Sie das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** auswählen. Wenn Sie DHCP nicht zum Abrufen der DNS-Server-Adressen verwenden, geben Sie die IP-Adressen in die Felder **Bevorzugter DNS-Server** und **Alternativer DNS-Server** ein. Die Standardeinstellung ist **aus**. **ANMERKUNG:** Wenn das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** markiert ist, können IP-Adressen nicht in die Felder **Bevorzugter DNS-Server** und **Alternativer DNS-Server** eingetragen werden.
Bevorzugter DNS-Server	IP-Adresse des DNS Servers.
Ersatz DNS-Server	Alternative IP-Adresse.

Tabelle 4-4. IPv6-Einstellungen

Einstellung	Beschreibung
Aktiviert	Wenn das Kontrollkästchen markiert ist, ist IPv6 aktiviert. Wenn das Kontrollkästchen nicht markiert ist, ist IPv6 deaktiviert. Die Standardeinstellung ist deaktiviert.
Automatische Konfiguration	Durch Markieren dieses Kontrollkästchens kann der iDRAC 6 die IPv6-Adresse für den iDRAC 6-NIC vom Server des dynamischen Host-Konfigurationsprotokolls (DHCPv6) abrufen. Wenn **Automatische Konfiguration** aktiviert wird, werden auch die statischen Werte für IP-Adresse 1, Präfixlänge und IP-Gateway deaktiviert und gelöscht.
IP-Adresse 1	Konfiguriert die IPv6-Adresse für den iDRAC-NIC. Zum Ändern dieser Einstellung, müssen Sie erst **Automatische Konfiguration** deaktivieren, indem Sie das entsprechende Kontrollkästchen abwählen.
Präfixlänge	Konfiguriert die Präfixlänge der IPv6-Adresse. Dieser kann ein Wert zwischen 1 und einschließlich 128 sein. Zum Ändern dieser Einstellung, müssen Sie zuerst **Automatische Konfiguration** deaktivieren, indem Sie das entsprechende Kontrollkästchen abwählen.
IP-Gateway	Konfiguriert den statischen Gateway für den iDRAC-NIC. Zum Ändern dieser Einstellung, müssen Sie erst **Automatische Konfiguration** deaktivieren, indem Sie das entsprechende Kontrollkästchen abwählen.
Link-Local-Adresse	Gibt die IPv6-Adresse für den iDRAC-NIC an.
IP-Adresse 2	Gibt die zusätzliche IPv6-Adresse für den iDRAC-NIC an, wenn dieser verfügbar ist.
DHCP zum Abrufen von DNS-Serveradressen verwenden	Aktivieren Sie DHCP zum Abrufen von DNS-Server-Adressen, indem Sie das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** auswählen. Wenn Sie nicht DHCP zum Abrufen der DNS-Server-Adressen verwenden, geben Sie die IP-Adressen in die Felder **Bevorzugter DNS-Server** und **Alternativer DNS-Server** ein. Die Standardeinstellung ist Aus. Überprüfen Sie das Rezensionsexemplar. 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.
Ersatz 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 4-5. 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 Channel-Berechtigungsebene	Konfiguriert die niedrigste Berechtigungsebene für den Benutzer, der 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 4-6. VLAN-Einstellungen

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

Tabelle 4-7. Schaltflächen der Seite Netzwerkkonfiguration

Schaltfläche	Beschreibung
Drucken	Druckt die Werte der **Netzwerkkonfiguration** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Netzwerkkonfiguration** erneut.
Erweiterte Einstellungen	Öffnet die Seite **Netzwerksicherheit**, auf der Benutzer den IP-Bereich sowie IP-Blockierungsattribute eingeben können.
Änderungen übernehmen	Speichert alle neuen Einstellungen, die Sie auf der Seite Netzwerkkonfiguration vorgenommen haben. **ANMERKUNG:** Wenn Sie Änderungen an den Einstellungen der NIC-IP-Adresse vornehmen, werden alle Benutzersitzungen geschlossen und Benutzer müssen unter Verwendung der aktualisierten IP-Adresseneinstellungen eine neue Verbindung zur iDRAC 6-Webschnittstelle herstellen. Alle anderen Änderungen erfordern, dass die NIC zurückgesetzt wird, was einen kurzzeitigen Verlust der Konnektivität 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**→ **Konfiguration** und dann auf die Registerkarte **Netzwerk**, um die Seite **Netzwerk** zu öffnen.
2. Klicken Sie auf **Erweiterte Einstellungen**, um die Netzwerksicherheitseinstellungen zu konfigurieren.

   Tabelle 4-8 beschreibt die Einstellungen der **Seite Netzwerksicherheit**. Wenn Sie mit den Einstellungen fertig sind, klicken Sie auf **Anwenden**.
3. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-9.

Tabelle 4-8. Einstellungen der Seite Netzwerksicherheit

Einstellungen	Beschreibung
IP-Bereich aktiviert	Aktiviert die Funktion zum Prüfen des IP-Bereichs, mit der eine Reihe von IP-Adressen definiert wird, die auf den 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 erlaubten IP-Adresse zu bestimmen. Jeder IP-Adresse, die dieses Bitmuster in ihrem oberen Bitbereich enthält, wird erlaubt, eine iDRAC 6-Sitzung herzustellen. Anmeldeversuche von IP-Adressen, die sich außerhalb dieses Bereichs befinden, werden fehlschlagen. Die Standardwerte in jeder Eigenschaft erlauben einem Adressenbereich von 192.168.1.0 bis 192.168.1.255, eine iDRAC 6-Sitzung herzustellen.
IP-Bereichs-Subnetzmaske	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Subnetzmaske sollte in Form einer Netzmaske sein, wobei die bedeutenderen Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu nur Nullen (0) in den niederwertigeren Bits. Der Standardwert ist **255.255.255.0**.
IP-Blockierung aktiviert	Aktiviert die IP-Adressen-Blockierungsfunktion, mit der während einer festgelegten Zeitspanne die Anzahl von Anmeldungsfehlversuchen einer spezifischen IP-Adresse eingeschränkt wird. Die Standardeinstellung ist **aus**.
IP-Blockierung, Zählung von Fehlversuchen	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche von dieser Adresse zurückgewiesen werden. Die Standardeinstellung ist **10.**
IP-Blockierung, Fenster der Fehlversuche	Bestimmt die Zeitspanne in Sekunden, während der die gezählten IP-Blockierungs-Fehlversuche auftreten müssen, um die IP-Blockierungs-Penalty-Zeit auszulösen. Die Standardeinstellung ist **3600.**
IP-Blockierungs-Penalty-Zeit	Der Zeitraum in Sekunden, während dem Anmeldeversuche von einer IP-Adresse auf Grund übermäßiger Fehler abgewiesen werden. Die Standardeinstellung ist **3600.**

Tabelle 4-9. 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.
Änderungen übernehmen	Speichert alle neuen Einstellungen, die Sie auf der Seite **Netzwerksicherheit** vorgenommen haben.
Zur Seite Netzwerkkonfiguration zurückkehren.	Kehrt zur Seite **Netzwerkkonfiguration** zurück.

Plattformereignisse konfigurieren

Die Plattformereigniskonfiguration bietet einen Mechanismus zur Konfiguration des iDRAC 6, damit auf bestimmte Ereignismeldungen hin ausgewählte Maßnahmen getroffen werden können. Die Maßnahmen schließen ein: Keine Maßnahme, System neu starten, System aus- und einschalten, System ausschalten und Warnung erstellen (Plattformereignis-Trap [PET] und/oder E-Mail).

Die filterbaren Plattformereignisse sind unter Tabelle 4-10 aufgeführt.

Table 4-10. Platform Event Filters

Index	Plattformereignis
1	Assertion Lüfter kritisch
2	Assertion Batteriewarnung
3	Assertion Batterie kritisch
4	Diskrete Spannung, Assertion Kritisch
5	Assertion Temperaturwarnung
6	Assertion Temperatur kritisch
7	Assertion Eingriff kritisch
8	Lüfterredundanz herabgesetzt
9	Lüfterredundanz 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

.

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 (wie eines Systemneustarts) konfiguriert ist, wird die Maßnahme ausgeführt.

Plattformereignisfilter (PEF) konfigurieren

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

1. Melden Sie sich über einen unterstützten Internet-Browser 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** und dann auf **Änderungen übernehmen**.

   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**.
6. Wählen Sie **Warnung erstellen** aus oder ab, um diese Maßnahme zu aktivieren oder zu deaktivieren.

   ANMERKUNG: Warnung erstellen muss aktiviert sein, damit eine Warnung an ein gültiges konfiguriertes Ziel gesendet werden kann (PET oder E-Mail).
7. Klicken Sie auf **Änderungen übernehmen**.

   Sie sind zur Seite **Plattformereignisse** zurückgekehrt, 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 hinzufügen oder aktivieren/deaktivieren zu können. Die folgenden Optionen stehen nur dann zur Verfügung, wenn Sie die Berechtigung **iDRAC konfigurieren** besitzen.

1. Melden Sie sich über einen unterstützten Internet-Browser am Remote- System an. Siehe "Zugriff auf die Webschnittstelle".
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 **Änderungen übernehmen**.
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 Plattformereigniszie**l.

   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 **Änderungen übernehmen**.

   ANMERKUNG: Die Ziel-Community-Zeichenkette muss mit der iDRAC 6-Community-Zeichenkette übereinstimmen.
9. Wiederholen Sie die Schritte 4 bis 7, um zusätzliche IPv4- oder IPv6- Zielnummern zu konfigurieren.

Konfiguration von E-Mail-Warnungen

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

1. Melden Sie sich über einen unterstützten Internet-Browser 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**, deren Zieladresse Sie konfigurieren möchten.
5. Wählen Sie auf der Seite **E-Mail-Warnung einstellen** entweder **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 **Änderungen übernehmen.**
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 im 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 sein. Der SMTP-Server verwendet die Einstellung IP-Adresse zum Kommunizieren mit dem iDRAC 6, um E-Mail-Warnungen zu senden, wenn ein Plattformereignis auftritt.
11. Klicken Sie auf **Änderungen übernehmen.**
12. Wiederholen Sie die Schritte 4 bis 9, um zusätzliche E-Mail- Warnungsziele zu konfigurieren.

IPMI konfigurieren

1. Melden Sie sich über einen unterstützten Internet-Browser 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 **Konfiguration** und dann auf **Netzwerk**.

   c. Wählen Sie auf der Seite **Netzwerkkonfiguration** unter **IPMI-LAN- Einstellungen** die Option **IPMI über LAN aktivieren** aus, und klicken Sie auf **Änderungen übernehmen**.

   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-LAN-Einstellungen** auf das Drop-Down-Menü **Beschränkung der Kanalzugriffsstufe**, wählen Sie **Administrator**, **Operator** oder **Benutzer** aus, und klicken Sie auf **Änderungen übernehmen**.

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

   ANMERKUNG: iDRAC 6-IPMI unterstützt das RMCP+-Protokoll.

   Geben Sie unter **IPMI-LAN-Einstellungen** im Feld **Verschlüsselungsschlüssel** den Verschlüsselungsschlüssel ein, und klicken Sie auf **Änderungen anwenden**.

   ANMERKUNG: Der Verschlüsselungsschlüssel muss aus einer geraden Anzahl hexadezimaler Zeichen mit maximal 40 Zeichen bestehen.

3. IPMI Seriell über LAN (SOL) konfigurieren.

   a. Klicken Sie in der **System**-Struktur auf **Remote-Zugriff**.

   b. Klicken Sie im Register **Konfiguration** auf **Seriell über LAN**.

   c. Auf der Seite **Seriell über LAN-Konfiguration** wählen Sie **Seriell über LAN aktivieren**.

   d. Aktualisieren Sie die IPMI-SOL-Baudrate.

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

   e. Klicken Sie auf das **Baudraten**-Drop-Down-Menü, wählen Sie die entsprechende Baudrate aus, und klicken Sie auf **Änderungen übernehmen**.

   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 Drop-Down-Menü **Beschränkung der Kanalzugriffsstufe**, und wählen Sie **Benutzer**, **Operator** oder **Administrator**.

   g. Klicken Sie auf **Änderungen übernehmen**.

4. Konfigurieren Sie IPMI-Seriell.

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

   b. Im Menü **Serielle Konfiguration** ändern Sie den IPMI-Seriell- Verbindungsmodus zu der entsprechenden Einstellung.

   Unter **IPMI-Seriell** klicken Sie auf das Drop-Down-Menü **Verbindungsmoduseinstellung**, und wählen Sie den entsprechenden Modus aus.

   c. Stellen Sie die IPMI-Seriell-Baudrate ein.

   Klicken Sie auf das **Baudraten**-Drop-Down-Menü, wählen Sie die entsprechende Baudrate aus, und klicken Sie auf **Änderungen übernehmen**.

   d. Stellen Sie die Beschränkung der Kanalzugriffsstufe ein.

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

   e. Klicken Sie auf **Änderungen übernehmen**.

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

      - Starten Sie das System neu.
      - Drücken Sie während des POST auf <F2>, um das BIOS-Setup-Programm einzugeben.
      - Wechseln Sie zu **Serial Communication**.
      - Stellen Sie im Menü **Serial Connection** sicher, dass **External Serial Connector** auf **Remote Access Device** 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 *Dell OpenManage Baseboard Management Controller Utilities-Benutzerhandbuch* unter **support.dell.com\manuals**\.

---

iDRAC6-Benutzer konfigurieren

Genauere Informationen finden Sie unter "iDRAC6-Benutzer hinzufügen und konfigurieren".

---

iDRAC 6-Datenübertragung mit SSL und digitalen Zertifikaten sichern

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

- Secure Sockets Layer (SSL)
- Zertifikatsignierungsanforderung (CSR)
- Auf SSL über die webbasierte Schnittstelle zugreifen
- CSR erstellen
- Ein Server-Zertifikat hochladen
- Ein Server-Zertifikat ansehen

Secure Sockets Layer (SSL)

Der iDRAC 6 beinhaltet einen Webserver, der zur Verwendung des SSL-Sicherheitsprotokolls der Industrienorm konfiguriert wurde, um verschlüsselte Daten über ein Netzwerk zu übertragen. SSL ist aufgebaut auf öffentlicher und privater Verschlüsselungstechnologie und eine allgemein akzeptierte Technologie, die authentifizierte und verschlüsselte Kommunikationen zwischen Clients und Servern bietet, um unbefugtes Abhören auf dem Netzwerk zu verhindern.

Ein SSL-aktiviertes System kann die folgenden Tasks ausführen:

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

Das Verschlüsselungsverfahren bietet eine hohe Datensicherungsstufe. Der iDRAC 6 verwendet den 128-Bit-SSL-Verschlüsselungsstandard, die sicherste Form der Verschlüsselung, die für Webbrowser in Nordamerika allgemein verfügbar ist.

Der iDRAC 6-Web Server enthält standardmäßig ein selbstsigniertes Dell-SSL-Digitalzertifikat (Server-ID). Um für Internetübertragungen eine hohe Sicherheitsstufe zu gewährleisten, ersetzen Sie das Web Server-SSL-Zertifikat durch ein Zertifikat, das von einer bekannten Zertifizierungsstelle signiert wurde. Um das Verfahren zum Erhalt eines signierten Zertifikats einzuleiten, können Sie die iDRAC 6-Webschnittstelle zum Erstellen einer Zertifikatsignierungsanforderung (CSR) mit den Informationen zu Ihrem Unternehmen verwenden. Sie können die erstellte CSR dann an eine Zertifizierungsstelle (CA) wie VeriSign oder Thawte senden.

Zertifikatsignierungsanforderung (CSR)

Eine CSR ist eine digitale Bewerbung an eine CA um ein sicheres Server-Zertifikat. 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 Geschäftsunternehmen, das in der IT-Industrie dafür anerkannt ist, hohe Ansprüche bezüglich der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger Sicherheitskriterien zu erfüllen. Beispiele von CAs schließen Thawte und VeriSign ein. 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 iDRAC 6-Firmware hochgeladen werden. Die auf der iDRAC 6-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→ Konfiguration.**

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 iDRAC 6-Firmware gespeichert.
- Ein Serverzertifikat hochladen.
- Ein Serverzertifikat anzeigen.

Tabelle 4-11 beschreibt die o.g. Optionen auf der Seite **SSL**.

Tabelle 4-11.

Feld	Beschreibung
Zertifikatsignierungsanforderung (CSR) erstellen	Mit dieser Option können Sie eine CSR zum Senden an eine CA erstellen, um ein sicheres Webzertifikat anzufordern. **ANMERKUNG:** Jede neue CSR überschreibt die vorherige CSR 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 Ihrer Firma gehört und für die Zugriffsteuerung auf den iDRAC 6 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 iDRAC 6 erhalten haben.
Serverzertifikat anzeigen	Mit dieser Option können Sie ein vorhandenes Serverzertifikat anzeigen.

Optionen auf der Seite SSL

Zertifikatsignierungsanforderung erstellen

ANMERKUNG: Jede neue Zertifikatsignierungsanforderung überschreibt alle vorangegangenen in der Firmware gespeicherten Daten. Damit iDRAC Ihre CSR annimmt, muss die signierte CSR in der Firmware mit dem von der Zertifizierungsstelle zurückgesendeten Zertifikat übereinstimmen.

1. Wählen Sie auf der Seite **SSL 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 4-12 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 4-13.

Tabelle 4-12. Zertifikatsignierungsanforderung-Attribute erstellen

Feld	Beschreibung
Allgemeiner Name	Der genaue Name, der zertifiziert werden soll (normalerweise der Domänenname des iDRAC, z. B. **www.xyzcompany.com**). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen und Punkte sind gültig. Leerstellen sind nicht gültig.
Name der Organisation	Der mit dieser Organisation assoziierte Name (zum Beispiel, XYZ Unternehmen). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Organisationseinheit	Der einer Organisationseinheit, wie z. B. einer Abteilung (z. B. Informationstechnik) zugehörige 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, wo sich das Unternehmen, das sich um Zertifikat bewirbt, befindet.
E-Mail	Die mit der CSR verbundene E-Mail-Adresse. Geben Sie die E-Mail-Adresse der Firma oder eine beliebige mit der CSR in Zusammenhang stehende E-Mail-Adresse ein. Dieses Feld ist optional.

Tabelle 4-13. Schaltflächen der Seite Zertifikatsignierungsanforderung (CSR) erstellen

Schaltfläche	Beschreibung
Drucken	Druckt die Werte **Zertifikatsignierungsanforderung erstellen** aus, die auf dem Bildschirm angezeigt werden.
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.

Ein Serverzertifikat hochladen

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

   Die Seite **Serverzertifikat anzeigen** wird angezeigt.

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

ANMERKUNG: Der Wert **Dateipfad** zeigt den relativen Dateipfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad eingeben, der den vollen 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 4-14.

Tabelle 4-14. Seitenschaltflächen 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 iDRAC 6-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 4-15 erläutert die Felder und zugehörigen Beschreibungen, die in der Tabelle **Zertifikat** aufgeführt werden.

2. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-16.

Tabelle 4-15. Zertifikatinformationen

Feld	Beschreibung
Seriennummer	Seriennummer des Zertifikats
Bewerberinformationen	Vom Bewerber eingegebene Zertifikatsattribute
Ausstellerinformationen	Vom Aussteller zurückgegebene Zertifikatsattribute
Gültig von	Ausgabedatum des Zertifikats
Gültig bis	Ablaufdatum des Zertifikats

Tabelle 4-16. 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-Zertifikate 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 verwenden oder konfigurieren zu können.

ANMERKUNG: Bevor Sie die Active Directory-Funktion konfigurieren oder verwenden, muss sichergestellt sein, dass der Active Directory-Server für die Kommunikation mit dem iDRAC 6 konfiguriert ist.

ANMERKUNG: Weitere Informationen zur Active Directory-Konfiguration und zur Konfiguration von Active Directory mit erweitertem Schema oder Standardschema finden Sie unter "iDRAC6 mit Microsoft Active Directory verwenden".

Zum Zugriff auf die Seite **Active Directory-Konfiguration und -Verwaltung**:

1. Klicken Sie auf **Remote-Zugriff→ Konfiguration.**
2. Klicken Sie auf **Active Directory**, um die Seite **Active Directory- Konfiguration und Verwaltung** zu öffnen.

   Tabelle 4-17 führt die Optionen der Seite **Active Directory-Konfiguration und -Verwaltung** auf.
3. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-18.

Tabelle 4-17. Optionen der Seite Active Directory-Konfiguration und -Verwaltung

Attribut	Beschreibung
Allgemeine Einstellungen	
Active Directory aktiviert	Gibt an, ob Active Directory aktiviert oder deaktiviert ist.
Schemaauswahl	Gibt an, ob Standardschema oder erweitertes Schema gerade mit Active Directory verwendet wird.
Benutzerdomänenname	Dieser Wert enthält bis zu 40 Benutzerdomäneneinträge. Wenn er konfiguriert ist, wird die Liste der Benutzerdomänennamen auf der Anmeldeseite als Pulldown-Menü zur Auswahl für den anmeldenden Benutzer angezeigt. Wenn er nicht konfiguriert ist, können sich Active Directory-Benutzer noch 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 in Sekunden an, bis die Active Directory-Abfragen beendet sind. Der Standardwert beträgt 120 Sekunden.
Domänen-Controller-Serveradresse 1-3 (FQDN oder IP)	Gibt den FQDN (vollständig qualifizierter Domänenname) des Domänen-Controllers oder der IP-Adresse an. Mindestens eine der 3 Adressen muss konfiguriert werden. iDRAC versucht, mit jeder der konfigurierten Adressen nacheinander zu verbinden, bis eine Verbindung erfolgreich hergestellt wurde. Wenn das erweiterte Schema ausgewählt ist, sind dies die Adressen der Domänen-Controller, auf denen sich das iDRAC-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	iDRAC verwendet beim Herstellen einer Verbindung zu Active Directory immer LDAP (Lightweight-Verzeichniszugriffsprotokoll) über SSL (Secure Socket Layer). Standardmäßig verwendet der iDRAC die in den iDRAC geladene zertifizierte Zertifizierungsstelle, um das SSL-Serverzertifikat des Domänen-Controllers beim SSL-Handshake zu überprüfen, und gewährleistet hohe Sicherheit. Die Zertifikatsvalidierung kann für Testzwecke deaktiviert werden, oder der Systemadministrator wählt, 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 lautet standardmäßig NULL. **iDRAC-Domänenname**: Der DNS-Name (Zeichenkette) der Domäne, in der sich das Active Directory-iDRAC-Objekt befindet. Dieser Wert lautet standardmäßig NULL.
Einstellungen zum Standardschema	**Globaler Katalogserver-Adresse 1-3 (FQDN oder IP)**: Gibt en FQDN (vollständig qualifizierter Domänenname) der IP-Adresse des/der globalen Katalogserver/s an. Mindestens eine der 3 Adressen muss konfiguriert werden. iDRAC versucht, mit jeder der konfigurierten Adressen nacheinander zu verbinden, bis eine Verbindung erfolgreich hergestellt wurde. Der globale Katalogserver ist nur für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen auf verschiedenen Domänen befinden. **Rollengruppen**: Gibt die Liste der dem iDRAC 6 zugeordneten Rollengruppen an.

	Gruppenname: Gibt den Namen an, der die Rollengruppe im Active Directory identifiziert, die dem iDRAC 6 zugeordnet ist. **Gruppendomäne**: Gibt die Domäne der Gruppe an. **Gruppenberechtigung**: Gibt die Berechtigungsebene für die Gruppe an.

Tabelle 4-18. 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 Ihnen, Active Directory zu konfigurieren. Genauere Informationen zur Konfiguration finden Sie unter "iDRAC6 mit Microsoft Active Directory verwenden".
Einstellungen testen	Ermöglicht Ihnen, die Konfiguration von Active Directory mithilfe der von Ihnen festgelegten Einstellungen zu testen. Einzelheiten zum Verwenden der Option **Einstellungen testen** finden Sie unter "iDRAC6 mit Microsoft Active Directory verwenden".

---

iDRAC 6-Dienste konfigurieren

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

1. Klicken Sie auf **Remote-Zugriff→ Konfiguration.** Klicken Sie dann auf die Registerkarte **Dienste**, um die Seite **Dienste**-Konfiguration anzuzeigen.

2. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Informationen zur lokalen Konfiguration - siehe Tabelle 4-19
   - Web Server - siehe Tabelle 4-20 für Informationen zu Web Server-Einstellungen
   - SSH - siehe Tabelle 4-21 für Informationen zu SSH-Einstellungen
   - Telnet - siehe Tabelle 4-22 für Informationen zu Telnet-Einstellungen
   - Remote-RACADM - siehe Tabelle 4-23 für Informationen zu Remote-RACADM-Einstellungen
   - SNMP-Agent - siehe Tabelle 4-24 für Informationen zu SNMP-Einstellungen
   - Automatisierter Systemwiederherstellungs (ASR)-Agent - siehe Tabelle 4-25 für Informationen zu ASR-Agent-Einstellungen

3. Klicken Sie auf **Anwenden**.

4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 4-26.

Tabelle 4-19. 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 Schnittstellen-Engine, die BMC- und iDRAC-Konfiguration gestattet. Das Options-ROM fordert Sie auf, das Setup-Modul durch Drücken von <Strg+E> einzugeben.
Lokale iDRAC-Konfiguration mittels RACADM deaktivieren	Deaktiviert die lokale Konfiguration des iDRAC mithilfe von RACADM.

Tabelle 4-20. Web Server-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert den iDRAC 6-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 Sitzungen, die für dieses System zulässig sind. Dieses Feld kann nicht bearbeitet werden. Die maximale Anzahl gleichzeitiger Sitzungen beträgt fünf.
Aktive Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich dem Wert der **Max. Sitzungen**. Dieses Feld kann nicht bearbeitet werden.
Zeitüberschreitung	Die Zeit in Sekunden, für die eine Verbindung ungenutzt bleiben kann. Die Sitzung wird abgebrochen, wenn das Zeitlimit 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, an dem der iDRAC 6 abhört, ob eine Browser-Verbindung besteht. Die Standardeinstellung ist **80.**
HTTPS-Anschlussnummer	Der Anschluss, an dem der iDRAC 6 abhört, ob eine Browser-Verbindung besteht. Die Standardeinstellung ist **443.**

Tabelle 4-21. 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 Zeitlimit-Funktion zu deaktivieren. Die Standardeinstellung ist **300.**
Anschlussnummer	Der Anschluss, an dem der iDRAC 6 abhört, ob eine SSH-Verbindung besteht. Die Standardeinstellung ist **22.**

Tabelle 4-22. Telnet-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert Telnet. Wenn markiert, ist Telnet aktiviert.
Zeitüberschreitung	Die Telnet-Zeitüberschreitung wegen Leerlauf, in Sekunden. Der Zeitüberschreitungsbereich beträgt 60 bis 1920 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitlimit-Funktion zu deaktivieren. Die Standardeinstellung ist **300.**
Anschlussnummer	Der Anschluss, an dem der iDRAC 6 abhört, ob eine Browser-Verbindung besteht. Die Standardeinstellung ist **23.**

Tabelle 4-23. 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.

Tabelle 4-24. 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, die die IP-Adresse für das SNMP-Warnungsziel enthält. Der Community-Name kann aus bis zu 31 Zeichen bestehen, die nicht leer sein dürfen. Die Standardeinstellung ist **öffentlich**.

Tabelle 4-25. Einstellung des automatisierten Systemwiederherstellungs-Agenten

Einstellung	Beschreibung
Aktiviert	Aktiviert/deaktiviert den automatisierten Systemwiederherstellungs-Agenten. Wenn markiert, ist der automatisierte Systemwiederherstellungs-Agent aktiviert.

Tabelle 4-26. Schaltflächen der Dienste-Seite

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Dienste**.
Aktualisieren	Aktualisiert die Seite **Dienste**.
Änderungen übernehmen	Wendet die Einstellungen für die Seite **Dienste** an.

---

iDRAC 6 Firmware/Systemdienste- Wiederherstellungs-Image aktualisieren

ANMERKUNG: Wenn die iDRAC 6-Firmware beschädigt wird, was eintreten könnte, wenn der iDRAC 6-Firmware-Aktualisierungsvorgang vor seinem Abschluss abgebrochen wird, können Sie den iDRAC 6 mithilfe der iDRAC 6-Webschnittstelle wiederherstellen.

ANMERKUNG: Die Firmware-Aktualisierung behält standardmäßig die aktuellen iDRAC 6-Einstellungen bei. Während des Aktualisierungsvorgangs haben Sie die Möglichkeit, die iDRAC 6-Konfiguration auf die Werkseinstellungen zurückzusetzen. Wenn Sie die Konfiguration auf die Werkseinstellungen einstellen, müssen Sie das Netzwerk unter Verwendung des iDRAC6-Konfigurationshilfsprogramms konfigurieren.

1. Öffnen Sie die webbasierte iDRAC 6-Schnittstelle und melden Sie sich am Remote-System an.

2. Klicken Sie auf **Remote-Zugriff** und dann auf die Registerkarte **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** oder vom Systemdienst-Wiederherstellungs-Image heruntergeladen haben.

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

   Zum Beispiel:

   `C:\Updates\V1.0\<Image-Name>`.

   ODER

   `\\192.168.1.10\Aktualisierungen\V1.0\<Image_name>`

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

4. Klicken Sie auf **Hochladen**.

   Die Datei wird auf den iDRAC 6 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 Validierung einsehen, die auf der hochgeladenen Image-Datei durchgeführt wurde.

   - Wenn die Image-Datei erfolgreich hochgeladen wurde und alle Überprüfungsvorgänge durchlaufen sind, wird der Name der Image-Datei 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 iDRAC 6 erneut zu aktualisieren, oder auf **Abbrechen** klicken, um den iDRAC 6 in den normalen Betriebsmodus zurückzusetzen.

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

   ANMERKUNG: Wenn Sie die Markierung im Kontrollkästchen **Konfiguration beibehalten** entfernen, wird der iDRAC 6 auf seine Standardeinstellungen zurückgesetzt. Das LAN ist in den Standardeinstellungen aktiviert. Sie werden u. U. nicht in der Lage sein, sich an der iDRAC 6-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 Firmwareaktualisierung erfolgreich abgeschlossen ist, wird der iDRAC 6 automatisch zurückgesetzt. Sie müssen das aktuelle Browserfenster schließen und eine neue iDRAC 6-Verbindung in einem neuen Browserfenster herstellen. Wenn ein Fehler auftritt, wird eine entsprechende Fehlermeldung eingeblendet.

   Wenn die Systemdienst-Wiederherstellungsaktualisierung erfolgreich abgeschlossen ist/fehlschlägt, wird eine entsprechende Fehlermeldung angezeigt.

Zurücksetzen der iDRAC 6-Firmware

iDRAC 6 verfügt über die Möglichkeit, zwei Firmware-Images gleichzeitig beizubehalten. Sie können wählen, von dem Firmware-Image Ihrer Wahl aus zu starten (oder darauf zurückzusetzen).

1. Öffnen Sie die webbasierte iDRAC 6-Schnittstelle und melden Sie sich am Remote-System an.

   Klicken Sie auf **System→ Remote-Zugriff** und dann auf die Registerkarte **Aktualisierung**.

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

   Konfiguration beibehalten bietet Ihnen die Möglichkeit, die bestehende iDRAC 6-Konfiguration beizubehalten oder zu löschen. Diese

Option ist standardmäßig ausgewählt.

ANMERKUNG: Wenn Sie die Markierung im Kontrollkästchen **Konfiguration beibehalten** entfernen, wird der iDRAC 6 auf seine Standardeinstellungen zurückgesetzt. Das LAN ist in den Standardeinstellungen aktiviert. Sie werden u. U. nicht in der Lage sein, sich an der iDRAC 6-Webschnittstelle anzumelden. Sie müssen die LAN-Einstellungen mithilfe des iDRAC 6-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 Zurücksetzenvorgangs 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 Firmwareaktualisierung erfolgreich abgeschlossen ist, wird der iDRAC 6 automatisch zurückgesetzt. Sie müssen das aktuelle Browserfenster schließen und eine neue iDRAC 6-Verbindung in einem neuen Browserfenster herstellen. Wenn ein Fehler auftritt, wird eine entsprechende Fehlermeldung eingeblendet.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Erweiterte Konfiguration des iDRAC 6

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Dieser Abschnitt bietet Informationen zur erweiterten iDRAC 6-Konfiguration und wird Benutzern mit fortgeschrittenen Kenntnissen im Bereich Systemverwaltung empfohlen, die die iDRAC 6-Umgebung ihren speziellen Bedürfnissen anpassen möchten.

Bevor Sie beginnen

Die grundlegende Installation bzw. das grundlegende Setup der iDRAC 6-Hardware und -Software sollte zu diesem Zeitpunkt bereits abgeschlossen sein. Weitere Informationen finden Sie unter "Grundlegende Installation des iDRAC6".

---

iDRAC 6 zur Anzeige der seriellen Ausgabe im Remote-Zugriff über SSH/Telnet konfigurieren

Sie können den iDRAC 6 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** aus.
4. Stellen Sie die Optionen der Seite **Serial Communication** folgendermaßen ein:

   serial communication....On with serial redirection via com2

   ANMERKUNG: Solange das serielle Gerät2 im Feld serielle Schnittstellenadresse auch auf COM1 eingestellt ist, kann die serielle Datenübertragung auf **On with serial redirection via com1** eingestellt sein.

   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

   Wählen Sie danach **Save Changes** aus.

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

iDRAC 6-Einstellungen zum Aktivieren von SSH/Telnet konfigurieren

Als nächstes konfigurieren Sie die iDRAC 6-Einstellungen zum Aktivieren von SSH/Telnet, die entweder durch RACADM oder die iDRAC 6-Webschnittstelle erfolgen können.

Führen Sie zum Konfigurieren der iDRAC 6-Einstellungen für die Aktivierung von SSH/Telnet mittels RACADM die folgenden Befehle aus:

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

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

Wie sie die RACADM-Befehle im Remote-Zugriff ausführen, finden Sie unter "RACADM im Remote-Zugriff verwenden".

Führen Sie zum Konfigurieren der iDRAC 6-Einstellungen für die Aktivierung von SSH/Telnet mittels der iDRAC 6-Webschnittstelle die folgenden Schritte aus:

1. Erweitern Sie die **System**-Struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** 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 iDRAC 6 über Telnet oder SSH hergestellt.

Eine Textkonsole über Telnet oder SSH starten

Nachdem Sie sich über die Management Station-Terminal-Software mittels Telnet oder SSH am iDRAC 6 angemeldet haben, können Sie die Textkonsole des verwalteten Systems umleiten, indem Sie den Telnet-/SSH-Befehl **console com2** verwenden. Es wird nur jeweils ein einzelner **console com2**-Client unterstützt.

Öffnen Sie zum Herstellen einer Verbindung zur Textkonsole des verwalteten Systems eine iDRAC 6-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 Tastatureingaben oder neue Zeichen von der seriellen Schnittstelle 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>
```

Wie Sie Linux für die Konsolenumleitung während des Startvorgangs konfigurieren, finden Sie unter "Linux während des Starts für die Umleitung der seriellen Konsole konfigurieren".

Telnetkonsole verwenden

Telnet mittels Microsoft® Windows® XP oder Windows 2003 ausführen

Wenn Ihre Management Station Windows XP oder Windows 2003 ausführt, kann ein Problem mit den Zeichen in einer iDRAC 6-Telnet-Sitzung auftreten. Dieses Problem kann sich als eingefrorene Anmeldung äußern, bei der die Eingabetaste nicht reagiert und keine Kennwort-Eingabeaufforderung eingeblendet wird.

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

Telnet mittels Windows 2000 ausführen

Wenn Ihre Management Station Windows 2000 ausführt, können Sie nicht mittels 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 - ein 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-Emulation eingestellt ist. Wenn dieses Problem auftritt, können Sie die Anzeige aktualisieren, indem Sie die BIOS-Konsolenumleitung zum ANSI-Modus ändern. Um dieses Verfahren im BIOS-Setup-Menü auszuführen, wählen Sie **Konsolenumleitung**→ **Remote-Terminaltyp** → **ANSI** aus.

1. Aktivieren Sie **Telnet** in den **Windows-Komponentendiensten**.
2. Stellen Sie eine Verbindung zum iDRAC 6 in der Management Station her.

   Öffnen Sie eine Eingabeaufforderung, geben Sie Folgendes ein, und drücken Sie auf die Eingabetaste:

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

wobei *IP-Adresse* die IP-Adresse für den iDRAC 6 und *Anschlussnummer* die Telnet-Anschlussnummer ist (wenn 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 Eingabeaufforderungs-Fenster (falls erforderlich).
2. Wenn noch keine Telnet-Sitzung ausgeführt wird, geben Sie Folgendes ein:

   `telnet`

   Wenn Sie eine Telnet-Sitzung ausführen, drücken Sie auf die Taste <Strg><]>.
3. Geben Sie in der Befehlszeile Folgendes ein:

   `set bsasdel`

   Die folgende Meldung wird eingeblendet:

   `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 Befehlszeile Folgendes ein:

   `telnet`

Verwenden der Secure Shell (SSH)

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

Secure Shell (SSH) ist eine Befehlszeilensitzung, die dieselben Fähigkeiten wie eine Sitzung von Telnet umfasst, jedoch mit verbesserter Sicherheit. Der iDRAC 6 unterstützt SSH-Version 2 mit Kennwortauthentifizierung. SSH wird auf dem iDRAC 6 aktiviert, wenn Sie die iDRAC 6-Firmware installieren oder aktualisieren.

Sie können entweder PuTTY oder OpenSSH auf der Management Station verwenden, um eine Verbindung zum iDRAC 6 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 iDRAC 6 gesteuert.

ANMERKUNG: OpenSSH sollte von einem VT100 oder ANSI-Terminalemulator auf Windows ausgeführt werden. Das Ausführen von OpenSSH an der Windows-Eingabeaufforderung ergibt keine volle Funktionalität (d. h. einige Tasten reagieren nicht, und es werden keine Grafiken angezeigt).

Zu beliebigen Zeitpunkten werden nur vier SSH-Sitzungen unterstützt. Die Sitzungszeitüberschreitung wird durch die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert, wie unter "iDRAC 6-Definitionen für Eigenschafts-Datenbankgruppen und Objekte" beschrieben.

Geben Sie zum Aktivieren der SSH auf dem iDRAC 6 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` and `cfgRacTuneSshPort` finden Sie unter "iDRAC 6-Definitionen für Eigenschafts-Datenbankgruppen und Objekte".

Die iDRAC 6-SSH-Umsetzung unterstützt mehrfache Verschlüsselungs-Schemata, wie in Tabelle 5-1 dargestellt.

Tabelle 5-1. Verschlüsselungs-Schemata

Schema-Typ	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 wären bei der Verwendung eines anderen Bootloaders erforderlich.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster oder die Anwendung, die die umgeleitete Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine ordnungsgemäße Textanzeige sicherzustellen, Andernfalls könnten einige Textbildschirmanzeigen entstellt 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 beiden Zeilen hinzu:

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

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

   ```
   kernel ..... console=ttyS1,57600
   ```

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 (erstellt durch)
#
# Note that you do not have to rerun grub after making changes
# to this file
# (Beachten Sie, dass grub nach dem Vornehmen von Änderungen nicht erneut ausgeführt
# werden muss. zu dieser Datei)
# NOTICE: You do not have a /boot partition. This means that
#          all kernel and initrd paths are relative to /, e.g.
# (HINWEIS: Sie haben keine /Startpartition.  Dies bedeutet, dass
#          alle Kernel und initrd-Pfade relativ zu / sind, z. B.)
#          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=ttyS1,57600
   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 GRUB-Grafikschnittstelle, und verwenden Sie die textbasierte Schnittstelle; andernfalls wird der GRUB-Bildschirm nicht in der RAC-Konsolenumleitung angezeigt. Zum Deaktivieren der Grafikschnittstelle kommentieren Sie die Zeile aus, die mit `splashimage` beginnt.

2. Zum Aktivieren mehrerer GRUB-Optionen um Konsolensitzungen über die serielle RAC-Verbindung zu starten, fügen Sie allen Optionen die folgende Zeile hinzu:

   ```
   console=ttyS1,57600
   ```

   Tabelle 5-2 zeigt `console=ttyS1,57600` nur der 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 der seriellen COM2-Schnittstelle zu konfigurieren:

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

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

Tabelle 5-3. Beispieldatei: /etc/innitab

```
#
# inittab  This file describes how the INIT process should set up
#          the system in a certain run-level.
#          (Diese Datei beschreibt das Setup des INIT-Verfahrens
#          das System auf einer bestimmten Ausführungsstufe.)
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
# (Autor:  Miquel van Smoorenburg
#          Geändert für RHS Linux von Marc Ewing und Donnie Barnes)
#
# Default runlevel. The runlevels used by RHS are:
# (Standard-Ausführungsstufe. Die von RHS verwendeten Ausführungsstufen lauten:)
#   0 - halt (Do NOT set initdefault to this)(halt (NICHT initdefault einstellen))
#   1 - Single user mode (Einzelbenutzermodus)
#   2 - Multiuser, without NFS (The same as 3, if you do not have
#       networking)
#       (Multibenutzer, ohne NFS (Gleich wie 3, wenn Sie keinen
#       Netzwerkbetrieb haben))
#   3 - Full multiuser mode (Voller Multibenutzer-Modus)
#   4 - unused (ungebraucht)
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#       (neustarten (NICHT initdefault einstellen))
#
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.
# (Wenn USV Stromausfall angibt, annehmen, dass einige vorhanden
# Minuten Strom übrig. Planen Sie ein Herunterfahren in 2 Minuten.
# Es wird hierbei natürlich angenommen, dass Strom anliegt, und dass das
# USV angeschlossen ist und korrekt funktioniert.)
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
# (Wenn Strom wiederhergestellt wurde, bevor das Herunterfahren eingeleitet wurde,
# brechen Sie ab.)
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
# Run gettys in standard runlevels
# (gettys in Standard-Ausführungsstufen ausführen)
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
```

```
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
# (xdm in Ausführungsstufe 5 ausführen
# xdm ist jetzt separater Dienst)
x:5:respawn:/etc/X11/prefdm -nodaemon
```

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

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

```
ttyS1
```

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

Tabelle 5-4. Beispieldatei: /etc/securetty

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

---

iDRAC 6 für serielle Datenübertragung konfigurieren

Zum Herstellen einer Verbindung zum iDRAC 6 über die serielle Datenübertragung kann jede der folgenden Schnittstellen verwendet werden:

- iDRAC 6-CLI
- Direktverbindung - grundlegender Modus
- Direktverbindung - Terminalmodus

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

Konfigurieren Sie das **BIOS**, um die serielle Datenübertragung 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** aus.
4. Stellen Sie den Bildschirm **Serial Communication** folgendermaßen ein:

   external serial connector....remote access device

   Wählen Sie danach **Save Changes** aus.

5. Drücken Sie auf <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 Null-Modem-Kabel für die serielle Konsole verbinden".

Vergewissern Sie sich dann, ob die Verwaltungssoftware der Terminal-Emulation für die serielle Datenübertragung konfiguriert ist. Siehe "Terminalemulations-Software der Management Station konfigurieren".

Schließlich konfigurieren Sie die iDRAC 6-Einstellungen zum Aktivieren der seriellen Datenübertragungen, die entweder durch RACADM oder die iDRAC 6-

Webschnittstelle erfolgen können.

Führen Sie zum Konfigurieren der iDRAC 6-Einstellungen für die Aktivierung der seriellen Datenübertragungen mittels RACADM die folgenden Befehle aus:

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

Führen Sie zum Konfigurieren der iDRAC 6-Einstellungen für die Aktivierung der seriellen Datenübertragungen mittels der iDRAC 6-Webschnittstelle die folgenden Schritte aus:

1. Erweitern Sie die **System**-Struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** 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 eine Eingabeaufforderung zum Anmelden eingeblendet werden. Geben Sie den Benutzernamen und das Kennwort des iDRAC 6 ein (die Standardwerte sind jeweils `root` und `calvin`).

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

```
racadm getsel
```

iDRAC 6 für Direktverbindung - grundlegender Modus und Direktverbindung - Terminalmodus konfigurieren

Führen Sie mithilfe von RACADM den folgenden Befehl aus, um die iDRAC 6-Befehlszeilenschnittstelle zu deaktivieren:

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

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

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

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

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

Dieselben Maßnahmen können auch mithilfe der iDRAC 6-Webschnittstelle ausgeführt werden.

1. Erweitern Sie die **System**-Struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** und dann auf **Seriell**.
3. Wählen Sie **Aktiviert** im Abschnitt **Serieller RAC** ab.

   Für Direktverbindung - grundlegender Modus:

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

   Für Direktverbindung - Terminalmodus:

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

4. Klicken Sie auf **Änderungen übernehmen**. Weitere Informationen über Direktverbindung - grundlegender Modus und Direktverbindung - Terminalmodus finden Sie unter "Seriellen Modus und Terminal-Modus konfigurieren".

Direktverbindung - grundlegender Modus ermöglicht Ihnen, Hilfsprogramme wie ipmish direkt über die serielle Datenübertragung 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 - Terminalmodus ermöglicht Ihnen, ASCII-Befehle an den iDRAC 6 auszugeben. Beispiel: Zum Ein-/Ausschalten des Servers über den Direktverbindung - Terminalmodus:

1. Stellen Sie eine Verbindung zum iDRAC 6 über die Terminal- Emulationssoftware 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 auf erfolgreiche 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 Direktverbindung - Terminalmodus und serieller Konsolenumleitung umschalten

Der iDRAC 6 unterstützt Sequenzen der Taste Escape, die eine Umschaltung zwischen Direktverbindung - Terminalmodus und serieller Konsolenumleitung zulassen.

Um Ihr System zum Zulassen dieser Funktionsweise einzustellen, befolgen Sie die folgenden Schritte:

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

   serial communication -- On with serial redirection via com2

   ANMERKUNG: Solange das **serial device2** im Feld **serial port address** auch auf COM1 eingestellt ist, kann das Feld **serial communication** auf **On with serial redirection via com1** eingestellt sein.

   serial port address -- Serial device1 = com1, serial device2 = com2

   external serial connector -- Serial device 2

   failsafe baud rate....115200

   remote terminal type ...vt100/vt220

   redirection after boot ... Enabled

   Wählen Sie danach **Save Changes** aus.

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

Verwenden Sie die folgende Escape-Tastensequenz, um zum seriellen Konsolenumleitungsmodus umzuschalten, wenn Sie sich im Terminalmodus der Direktverbindung befinden:

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

Verwenden Sie die folgende Escape-Tastensequenz, um zum Terminalmodus der Direktverbindung umzuschalten, wenn Sie sich im seriellen Konsolenumleitungsmodus befinden:

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

DB-9- oder Null-Modem-Kabel für die serielle Konsole verbinden

Um mit einer seriellen Textkonsole auf das Managed System zuzugreifen, schließen Sie ein DB-9-Null-Modemkabel an den COM-Anschluss auf dem Managed System an. Damit die Datenübertragung auch über das Nullmodemkabel funktioniert, sollten die entsprechenden Einstellungen zur seriellen Datenübertragung im CMOS-Setup vorgenommen werden. Nicht alle DB-9-Kabel führen das Pinout/die Signale, die für diese Verbindung benötigt werden. 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. Erforderliches Pinout für das DB-9-Null-Modemkabel

Signalname	DB-9-Pin (Server-Pin)	DB-9-Pin (Workstation-Pin)
FG (Gehäusemasse)	-	-
TD (Daten senden)	3	2
RD (Daten empfangen)	2	3
RTS (Aufforderung zu senden)	7	8
CTS (Frei zum Senden)	8	7
SG (Betriebserde)	5	5
DSR (Datensatz bereit)	6	4
CD (Trägerermittlung)	1	4
DTR (Datenterminal bereit)	4	1 und 6

Terminalemulations-Software der Management Station konfigurieren

Ihr iDRAC 6 unterstützt eine serielle oder Telnet-Textkonsole von einer Management Station aus, auf der einer der folgenden Typen der Terminal-Emulationssoftware ausgeführt wird:

- Linux Minicom in einem Xterm
- Hilgraeves 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 der seriellen Schnittstelle für Linux. Die folgenden Schritte beziehen sich auf die Konfiguration der Minicom-Version 2.0. Andere Minicom-Versionen können ein bisschen unterschiedlich sein, aber dieselben grundlegenden Einstellungen benötigen. 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, empfiehlt Dell, dass Sie ein Xterm-Fenster zur Anzeige der Telnet-Konsole 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 Maus-Pfeil in die untere rechte Ecke des Fensters, und ändern Sie die Größe des Fensters zu 80 x 25.
3. Wenn Sie keine Minicom-Konfigurationsdatei haben, fahren Sie mit dem folgenden Schritt fort.

   Wenn Sie eine Minicom-Konfigurationsdatei haben, geben Sie `minicom <Minicom-config-Dateiname>` ein, und fahren Sie mit Schritt 17 fort.
4. Geben Sie an der Xterm-Eingabeaufforderung `minicom -s` ein.
5. Wählen Sie die Option **Serial Port Setup** (Seriellen Anschluss einrichten) aus, und drücken Sie die <Eingabetaste>.
6. Drücken Sie auf <a>, und wählen Sie das entsprechende serielle Gerät (z. B. **/dev/ttyS0**) aus.
7. Drücken Sie auf <e>, und stellen Sie die Option **Bps/Par/Bits** auf **57600 8N1** ein.
8. Drücken Sie auf <f>, und stellen Sie die **Hardware-Datenflusssteuerung** auf **Ja** und die **Software-Datenflusssteuerung** auf **Nein** ein.
9. Um das Menü **Setup der seriellen Schnittstelle** zu beenden, drücken Sie auf die Eingabetaste.
10. Wählen Sie **Modem und Wählen** aus, und drücken Sie auf die Eingabetaste.

11. Drücken Sie im Menü **Modem-Wählen und Parameter-Setup** auf <Rücktaste>, um die Einstellungen **init**, **reset**, **connect** und **hangup** zu löschen, sodass Sie leer sind.

12. Drücken Sie auf die Eingabetaste, um jeden leeren Wert zu speichern.

13. Wenn alle angegebenen Felder gelöscht sind, drücken Sie auf die Eingabetaste, um das Menü **Modem-Wählen und Parameter-Setup** zu beenden.

14. Wählen Sie **Setup als config_name speichern** aus, und drücken Sie auf die Eingabetaste.

15. Wählen Sie **Minicom beenden** aus, und drücken Sie auf die Eingabetaste.

16. Geben Sie an der Befehls-Shell-Eingabeaufforderung `minicom <Minicom-config-Dateiname>` ein.

17. Um das Minicom-Fenster auf 80 x 25 zu erweitern, wenden Sie die Zieh- Funktion an der Ecke des Fensters an.

18. Drücken Sie auf <Strg+a>, <z>, <x>, um Minicom zu beenden.

ANMERKUNG: Wenn Sie Minicom für die serielle Textkonsolenumleitung verwenden, um das Managed System-BIOS zu konfigurieren, wird empfohlen, in Minicom die Farbeinstellung zu wählen. Geben Sie zum Einschalten von 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 Managed System 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

Einstellung der Beschreibung	Erforderliche Einstellung
Bit/s/Par/Bit	57600 8N1
Hardware-Datenflusssteuerung	Ja
Software-Datenflusssteuerung	Nein
Terminalemulation	ANSI
Modemwählen 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 für die serielle Schnittstelle von Microsoft Windows. Um die Größe Ihres Konsolenbildschirms entsprechend einzustellen, verwenden Sie Hilgraeves HyperTerminal Private Edition, Version 6.3.

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:** die COM-Schnittstelle auf der Management Station (z. B. COM2) aus, mit der Sie das DB-9-Null-Modemkabel verbunden 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 der COM-Schnittstelle der Management Station

Einstellung der Beschreibung	Erforderliche Einstellung
Bits pro Sekunde	57600
Datenbits	8
Parität	Keine
Stopbits	1
Datenflusssteuerung	Hardware

Seriellen Modus und Terminal-Modus konfigurieren

IPMI und seriellen iDRAC 6 konfigurieren

1. Erweitern Sie die **System**-Struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** 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 iDRAC 6-Einstellungen.

   Eine Beschreibung zu den seriellen iDRAC 6-Einstellungen ist unter Tabelle 5-9 verfügbar.
5. Klicken Sie auf **Änderungen übernehmen**.
6. Klicken Sie auf der Seite **Serielle Konfiguration** auf die entsprechende Schaltfläche, um fortzufahren. Eine Beschreibung der seriellen Konfigurationsseiten-Einstellungen ist unter Tabelle 5-10 verfügbar.

Tabelle 5-8. Serielle IPMI-Einstellungen

Einstellung	Beschreibung
Verbindungsmoduseinstellung	• 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.
Ablaufsteuerung	• Keine - Hardware-Datenflusssteuerung aus • RTS/CTS - Hardware-Datenflusssteuerung ein
Beschränkung der Channel-Berechtigungsebene	• Administrator • Operator • Benutzer

Tabelle 5-9. Serielle iDRAC 6-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert die serielle iDRAC 6-Konsole. Markiert=Aktiviert; Unmarkiert=Deaktiviert
Zeitüberschreitung	Die maximale Sekundenzahl der Leitungsleerlaufzeit, 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 der externen seriellen Schnittstelle. Die Werte betragen **9600 Bit/s**, **28,8 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 zur Konsole geschriebenen Zeichen enthält. Maximum und Standard = 8192 Zeichen.
Anmeldungsbefehl	Die auf die gültige Anmeldung hin auszuführende iDRAC 6-Befehlszeile.

Tabelle 5-10. Einstellungen der Seite Serielle Konfiguration

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Serielle Konfiguration** aus.
Aktualisieren	Aktualisieren Sie die Seite **Serielle Konfiguration**.
Änderungen anwenden	Übernehmen Sie die IPMI- und seriellen iDRAC 6-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 **Konfiguration** und dann auf **Seriell**.
3. Klicken Sie auf der Seite **Serielle Konfiguration** auf **Terminalmodus- Einstellungen**.
4. Konfigurieren Sie die Terminalmodus-Einstellungen.

   Beschreibung der Terminalmodus-Einstellungen unter Tabelle 5-11 verfügbar.
5. Klicken Sie auf **Änderungen übernehmen**.
6. Klicken Sie auf der Seite **Terminalmodus-Einstellungen** auf die entsprechende Schaltfläche, um fortzufahren. Beschreibung der Schaltflächen der Seite Terminalmodus-Einstellungen unter Tabelle 5-12 verfügbar.

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 **Keine**, **<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	Aktualisieren Sie die Seite **Terminalmodus-Einstellungen**.
Zurück zur Konfiguration der seriellen Schnittstelle	Zur Seite **Konfiguration der seriellen Schnittstelle** zurückkehren.
Änderungen anwenden	Übernehmen Sie die Änderungen der Terminalmodus-Einstellungen.

---

iDRAC 6-Netzwerkeinstellungen konfigurieren

VORSICHT: Durch Ändern der iDRAC 6-Netzwerkeinstellungen wird möglicherweise die aktuelle Netzwerkverbindung getrennt.

Konfigurieren Sie die iDRAC 6-Netzwerkeinstellungen mithilfe eines der folgenden Hilfsprogramme:

- Internet-basierte Schnittstelle - Siehe "iDRAC 6-NIC konfigurieren"
- RACADM-CLI - Siehe "cfgLanNetworking"
- iDRAC 6-Konfigurationsdienstprogramm - Siehe "System zur Verwendung eines iDRAC6 konfigurieren"

ANMERKUNG: Wird der iDRAC 6 in einer Linux-Umgebung eingesetzt, finden Sie entsprechende Informationen unter "RACADM installieren".

Über ein Netzwerk auf den iDRAC 6 zugreifen

Nachdem Sie den iDRAC 6 konfiguriert haben, können Sie im Remote-Zugriff mittels einer der folgenden Schnittstellen auf das verwaltete System zugreifen:

- Web-basierte Schnittstelle
- RACADM
- Telnet-Konsole
- SSH
- IPMI

Tabelle 5-13 beschreibt jede iDRAC 6-Schnittstelle.

Tabelle 5-13. iDRAC 6-Schnittstellen

Schnittstelle	Beschreibung
Web-basierte Schnittstelle	Ermöglicht Remote-Zugriff auf den iDRAC 6 über eine grafische Benutzeroberfläche. Die webbasierte Schnittstelle ist in die iDRAC 6-Firmware integriert und der Zugriff auf die Schnittstelle erfolgt über die NIC-Schnittstelle von einem unterstützten Internet-Browser auf der Management Station aus. Eine Liste unterstützter Internet-Browser steht unter "Unterstützte Webbrowser" zur Verfügung.

RACADM	Ermöglicht Remote-Zugriff auf den iDRAC 6 mittels einer Befehlszeilenschnittstelle. RACADM verwendet die iDRAC 6-IP-Adresse, um RACADM-Befehle auszuführen.
	
	ANMERKUNG: Die Option racadm-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 verwenden, die sich auf Dateivorgänge beziehen, wie z. B.:
	
	`racadm getconfig -f <Dateiname>`
	
	oder:
	
	`racadm sslcertupload -t 1 -f c:\cert\cert.txt Unterbefehle`

Telnet-Konsole	Bietet Zugriff auf den iDRAC 6 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 - in Klartext übersendet. Verwenden Sie beim Übersenden vertraulicher Informationen die SSH-Schnittstelle.
SSH-Schnittstelle	Bietet dieselben Fähigkeiten wie die Telnet-Konsole, die eine verschlüsselte Transportschicht zum Zweck höherer Sicherheit verwendet.
IPMI-Schnittstelle	Bietet über den iDRAC 6 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 *Dell OpenManage Baseboard-Verwaltungs-Controller-Dienstprogramme-Benutzerhandbuch* unter **support.dell.com\manuals**.

ANMERKUNG: Der Standard-Benutzername des iDRAC 6 lautet root und das Standardkennwort calvin.

Sie können mithilfe eines unterstützten Internet-Browsers sowohl über den iDRAC 6-NIC als auch über den Server Administrator oder IT Assistant auf die webbasierte iDRAC 6-Schnittstelle zugreifen.

Eine Liste unterstützter Internet-Browser erhalten Sie unter "Unterstützte Webbrowser".

Starten Sie zum Zugriff auf die iDRAC 6-Remote-Zugriffs-Schnittstelle mittels Server Administrator den Server Administrator. Von der Systemstruktur im linken Fensterbereich der Server Administrator-Einstiegsseite 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 iDRAC 6, bevor Sie die RACADM-Remote-Fähigkeit verwenden. Weitere Informationen zum Setup des iDRAC 6 sowie eine Liste von in Beziehung stehenden Dokumenten 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 iDRAC 6-IP-Adresse erforderlich.

ANMERKUNG: Wenn das System, von dem aus Sie auf das Remote-System zugreifen, kein iDRAC 6-Zertifikat in seinem standardmäßigen Zertifikatspeicher enthält, wird beim Eingeben eines RACADM-Befehls eine Meldung eingeblendet. Weitere Informationen über iDRAC 6-Zertifikate finden Sie unter "iDRAC 6-Datenübertragung mit SSL und digitalen Zertifikaten sichern".

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

(Sicherheitswarnung: Zertifikat ist ungültig – Name auf Zertifikat ist ungültig oder stimmt nicht mit Standortnamen überein)

Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors.

(Ausführung wird fortgesetzt. Verwenden Sie die Option -S für racadm, um die Ausführung bei zertifikatbezogenen Fehlern anzuhalten.)
```

RACADM setzt die Ausführung des Befehls fort. Wenn Sie jedoch die Option –S verwenden, hält RACADM die Ausführung des Befehls an und blendet die folgende Meldung ein:

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

(Sicherheitswarnung: Zertifikat ist ungültig – Name auf Zertifikat ist ungültig oder stimmt nicht mit Standortnamen überein)

Racadm not continuing execution of the command.

(Racadm setzt die Ausführung des Befehls nicht fort.)
```

FEHLER: Verbindung zum iDRAC 6 konnte unter angegebener IP-Adresse nicht hergestellt werden.

ANMERKUNG: Die RACADM-Remote-Fähigkeit wird nur auf Management Stations unterstützt. Weitere Informationen befinden sich in der *Dell Systems Software-Supportmatrix* unter **Dell OpenManage Software** auf der Dell Support-Website unter **support.dell.com\manuals**.

ANMERKUNG: Wenn Sie die RACADM-Remote-Fähigkeit verwenden, müssen Sie über Schreibberechtigungen auf den Ordnern verfügen, in denen Sie die RACADM-Unterbefehle verwenden, die sich auf Dateivorgänge beziehen, wie z. B.:

```
racadm getconfig -f <Dateiname>

oder

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

RACADM Übersicht

```
racadm -r <iDRAC 6-IP-Adresse> -u <Benutzername> -p <Kennwort> <Unterbefehl> <Unterbefehl-Optionen>

racadm -i -r <iDRAC 6-IP-Adresse> <Unterbefehl> <Unterbefehl-Optionen>
```

Zum Beispiel:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo

racadm -i -r 192.168.0.120 getsysinfo
```

Wenn die HTTPS-Schnittstellennummer des iDRAC 6 zu einer von der Standardschnittstelle (443) abweichenden benutzerdefinierten Schnittstelle geändert wurde, muss die folgende Syntax verwendet werden:

```
racadm -r <iDRAC 6-IP-Adresse>:<Anschluss> -u <Benutzername> -p <Kennwort> <Unterbefehl> <Unterbefehl-Optionen>

racadm -i -r <iDRAC 6-IP-Adresse>:<Anschluss> <Unterbefehl> <Unterbefehl-Optionen>
```

RACADM-Optionen

Tabelle 5-14 führt die Optionen für den RACADM-Befehl auf.

Tabelle 5-14. racadm-Befehlsoptionen

Option	Beschreibung
-r <RAC-IP-Adr> **-r <RAC-IP-Adr>:<Anschlussnummer>**	Bestimmt die Remote-IP-Adresse des Controllers. Verwenden Sie <*Schnittstellennummer*>, wenn die iDRAC 6-Schnittstellennummer nicht der Standardschnittstelle (443) entspricht
-i	Weist RACADM an, den Benutzer interaktiv nach dem Benutzernamen und dem Kennwort zu fragen.
-u <Benutzername>	Gibt den Benutzernamen an, der verwendet wird, um die Befehlstransaktion zu bestätigen. Wenn die Option **-u** verwendet wird, muss auch die Option **-p** verwendet werden, wobei die Option **-i** (interaktiv) nicht verwendet werden darf.
-p <Kennwort>	Gibt das Kennwort an, das zur Bestätigung der Befehlstransaktion verwendet wird. Wenn die Option **-p** verwendet wird, ist die Option **-i** nicht erlaubt.
-S	Legt fest, dass RACADM auf ungültige Zertifikatfehler 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 iDRAC 6-Unterbefehle auf.
help *<Unterbefehl>*	Listet die Verwendungsaussage 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 (Bildschirm letzter Absturz, letzter blauer Bildschirm).
clrraclog	Löscht das iDRAC 6-Protokoll. Es wird ein einzelner Eintrag vorgenommen, um anzuzeigen, von welchem Benutzer und zu welcher Uhrzeit das Protokoll gelöscht wurde.
config	Konfiguriert den iDRAC 6.
getconfig	Zeigt die aktuellen iDRAC 6-Konfigurationseigenschaften an.
coredump	Zeigt den letzten Coredump des iDRAC 6 an.
coredumpdelete	Löscht den im iDRAC 6 gespeicherten Coredump.
fwupdate	Führt iDRAC 6-Firmware-Aktualisierungen durch oder zeigt deren Status an.
getssninfo	Zeigt Informationen über aktive Sitzungen an
getsysinfo	Zeigt allgemeine Informationen zum iDRAC 6 und zum System an.
getractime	Zeigt die iDRAC6-Uhrzeit an.
ifconfig	Zeigt die aktuelle iDRAC 6-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 Routing-Tabelle vom iDRAC 6 aus erreichbar ist.
setniccfg	Stellt die IP-Konfiguration für den Controller ein.
getniccfg	Zeigt die derzeitige IP-Konfiguration für den Controller an.
getsvctag	Zeigt Service-Tag-Nummern an.
racdump	Liest den iDRAC 6-Status sowie Zustandsinformationen zum Debuggen aus.
racreset	Setzt den iDRAC 6 zurück.
racresetcfg	Setzt den iDRAC 6 auf die Standardkonfiguration zurück.
serveraction	Führt Stromverwaltungsvorgänge auf dem Managed 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 oder Serverzertifikat auf den iDRAC 6 hoch.
sslcertdownload	Lädt ein CA-Zertifikat herunter.
sslcertview	Zeigt ein Zertifizierungsstellenzertifikat oder Serverzertifikat im iDRAC 6 an.
sslkeyupload	Zwingt den iDRAC 6, eine Test-E-Mail über den iDRAC 6-NIC zu senden, um die E-Mail-Konfiguration zu überprüfen.
testtrap	Zwingt den iDRAC 6, einen Test-SNMP-Trap über den iDRAC 6-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 iDRAC 6-Resets (mithilfe des Befehls racadm racreset) gebe ich einen Befehl aus, wodurch die folgende Meldung angezeigt wird:

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

Was bedeutet diese Meldung?

Sie müssen warten, bis der iDRAC 6-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 iDRAC 6-IP-Adresse von meinem System aus pinge und meine iDRAC 6-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.

Mehrfache iDRAC 6-Controller konfigurieren

Mit RACADM können Sie einen oder mehrere iDRAC 6s mit identischen Eigenschaften konfigurieren. Wenn Sie eine spezifische iDRAC 6-Karte mit deren Gruppen-ID und Objekt-ID abfragen, erstellt RACADM die **racadm.cfg**-Konfigurationsdatei aus den abgerufenen Informationen. Wenn Sie die Datei in eine oder mehreren iDRAC 6-Karten exportieren, können Sie in kürzester Zeit Ihre Controller mit identischen Eigenschaften konfigurieren.

ANMERKUNG: Einige Konfigurationsdateien enthalten eindeutige iDRAC 6-Informationen (wie die statische IP-Adresse), die vor dem Exportieren der Datei in andere iDRAC 6-Karten geändert werden müssen.

Führen Sie zum Konfigurieren von mehrfachen iDRAC 6-Controllern die folgenden Anweisungen aus:

1. Verwenden Sie RACADM, um den Ziel-iDRAC 6 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 iDRAC 6-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-iDRAC 6 zu ändern.

   Geben Sie an der Eingabeaufforderung Folgendes ein:

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

4. Setzen Sie den konfigurierten Ziel-iDRAC 6 zurück.

   Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   racadm racreset
   ```

Der Unterbefehl **getconfig -f racadm.cfg** fordert die iDRAC 6-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 andere iDRAC 6-Karten. 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. Formatierung verwirrt den Parser, wodurch die RACADM-Datenbank beschädigt werden kann.

iDRAC6-Konfigurationsdatei erstellen

Die iDRAC 6-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 iDRAC 6 von dieser Datei aus konfigurieren. Sie können einen beliebigen Dateinamen verwenden, und die Dateierweiterung **.cfg** ist nicht notwendig (obwohl in diesem Teilabschnitt mit dieser Erweiterung auf die Datei Bezug genommen wird).

Die Datei **.cfg** 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 ermittelt wurde, und eine einfache Meldung beschreibt das Problem. Die vollständige Datei wird geparst und alle Fehler angezeigt. Schreibbefehle werden nicht zum iDRAC 6 übertragen, wenn ein Fehler in der **.cfg**-Datei festgestellt wird. Der Benutzer muss *alle* Fehler beheben, bevor eine Konfiguration vorgenommen werden kann. Die Option **-c** kann für den Unterbefehl **config** verwendet werden, wodurch nur die Syntax überprüft wird, jedoch *keine* Schreibvorgänge zum iDRAC 6 vorgenommen werden.

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 aus dem iDRAC 6 für diese Gruppe. Alle Objekte innerhalb dieser Gruppe sind einfache Modifizierungen, wenn der iDRAC 6 konfiguriert wird. Wenn ein modifiziertes Objekt einen neuen Index darstellt, wird der Index während der Konfiguration auf dem iDRAC 6 erstellt.

- In einer **.cfg**-Datei können Sie keinen Index Ihrer Wahl bestimmen.

  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 geändert. Wenn kein Index vorhanden ist, wird der erste verfügbare Index verwendet. Diese Methode sorgt für Flexibilität, wenn indizierte Einträge hinzugefügt werden, wobei der Benutzer keine genauen Index-Übereinstimmungen zwischen allen verwalteten RACs vorzunehmen braucht. Neue Benutzer werden dem ersten verfügbaren Index hinzugefügt. Dadurch kann eine **.cfg**-Datei, die auf einem iDRAC 6 richtig 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 alle iDRAC 6-Karten mit identischen Eigenschaften zu konfigurieren.

  Verwenden Sie den Unterbefehl **racresetcfg**, um den iDRAC 6 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.

Parsen-Regeln

- Alle Zeilen, die mit '#' beginnen, werden als Anmerkungen betrachtet.

  Eine Anmerkungszeile *muss* in Spalte 1 beginnen. Das Zeichen '#' in anderen Spalten 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 iDRAC 6 ausführen, ohne dass Sie Escape-Zeichen hinzufügen müssen.

  Beispiel:

  ```
  #

  # Dies ist eine Anmerkung

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<Modem init # ist keine Anmerkung>
  ```

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

  Das **"["**-Startzeichen, das einen Gruppennamen angibt, *muss* in Spalte eins 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 "iDRAC 6-Definitionen für Eigenschafts-Datenbankgruppen und Objekte" 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 in "Objekt=Wert"-Paaren ohne Leerzeichen zwischen 'Objekt', '=' oder 'Wert' angegeben.

  Leerstellen nach dem Wert werden ignoriert. Eine Leerstelle innerhalb einer Wertezeichenkette bleibt unverändert. Jedes Zeichen rechts von '=' wird als solches betrachtet (zum Beispiel, ein zweites '=' oder ein '#', '[', ']' und so weiter). Bei diesen Zeichen handelt es sich um gültige Modemchat-Scriptzeichen.

  Siehe Beispiel unter vorhergehendem Punkt.

- Der **.cfg**-Parser ignoriert einen Index-Objekteintrag.

  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 eine Anmerkung vor die Index-Objekte, durch die dem Benutzer die enthaltenen Anmerkungen 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 NULL-Zeichenkette (durch die beiden Zeichen "" gekennzeichnet) weist den iDRAC 6 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 iDRAC 6-Konfiguration. Diese Konfigurationsdatei kann als Beispiel und als Ausgangspunkt für Ihre eindeutige **.cfg**-Datei verwendet werden.

iDRAC 6-IP-Adresse ändern

Wenn Sie die iDRAC 6-IP-Adresse in der Konfigurationsdatei ändern, entfernen Sie alle unnötigen **<***Variable***>**=**Wert**-Einträge. Es verbleibt lediglich die tatsächliche Bezeichnung der variablen Gruppe mit "[" und "]" zusammen mit den beiden **<***Variable***>**=**Wert**-Einträgen, die sich auf die IP-Adressenänderung beziehen.

Zum Beispiel:

```
#

# Objektgruppe "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Die Datei wird wie folgt aktualisiert:

```
#

# Objektgruppe "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# Anmerkung, 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. Derselbe, im vorhergehenden Beispiel verwendete Befehl **getconfig** kann außerdem zur Bestätigung der Aktualisierung verwendet werden.

Diese Datei kann für das Herunterladen unternehmensweiter Änderungen oder zum Konfigurieren neuer Systeme über das Netzwerk verwendet werden.

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

iDRAC 6-Netzwerkeigenschaften konfigurieren

Geben Sie Folgendes ein, um eine Liste verfügbarer Netzwerkeigenschaften zu erstellen:

```
racadm getconfig -g cfgLanNetworking
```

Wenn DHCP zum Erhalt einer IP-Adresse verwendet werden soll, kann der folgende Befehl zum Schreiben des Objekts **cfgNicUseDhcp** und zum Aktivieren dieser Funktion verwendet werden:

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

Die Befehle bieten dieselbe Konfigurationsfunktionalität wie das iDRAC 6-Konfigurationsdienstprogramm beim Systemstart, wenn Sie die Aufforderung erhalten, <Strg><E> zu drücken. Weitere Informationen zum Konfigurieren von Netzwerkeigenschaften mit dem iDRAC 6-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 iDRAC 6-LAN selbst dann deaktiviert, wenn DHCP aktiviert ist.

iDRAC 6-Modi

Der iDRAC 6 kann anhand eines von vier Modi konfiguriert werden:

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

Tabelle 5-16 bietet eine Beschreibung der einzelnen Modi.

Tabelle 5-16. iDRAC 6-NIC-Konfigurationen

Modus	Beschreibung
Dediziert	Der iDRAC 6 verwendet seinen eigenen NIC (RJ-45-Anschluss) und die iDRAC 6-MAC-Adresse für den Netzwerkverkehr.
Freigegeben	Der iDRAC 6 verwendet LOM1 auf dem Planar.
Freigegeben mit Failover: LOM2	Der iDRAC 6 verwendet LOM1 und LOM2 als Team für das Failover. Das Team verwendet die iDRAC 6-MAC-Adresse.
Freigegeben mit Failover: Alle LOMs	Der iDRAC 6 verwendet LOM1, LOM2, LOM3 und LOM4 als Team für das Failover. Das Team verwendet die iDRAC-MAC-Adresse.

Häufig gestellte Fragen

Wenn ich auf die webbasierte iDRAC 6-Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die aussagt, dass der Hostname des SSL-Zertifikats nicht mit dem Hostnamen des iDRAC 6 übereinstimmt.

Der iDRAC 6 enthält ein Standard-iDRAC 6-Serverzertifikat, um Netzwerksicherheit für die webbasierte Schnittstelle und die Remote-RACADM-Funktionen zu gewährleisen. Wenn dieses Zertifikat verwendet wird, zeigt der Internet-Browser eine Sicherheitswarnung an, weil das Standardzertifikat als **iDRAC 6-Standardzertifikat** ausgegeben wird, das nicht mit dem Hostnamen des iDRAC 6 (z. B. IP-Adresse) übereinstimmt.

Um dieses Sicherheitsbedenken zu beseitigen, laden Sie ein iDRAC 6-Serverzertifikat herunter, das auf die IP-Adresse oder den iDRAC-Namen des iDRAC 6 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 (f**alls Zertifikat auf IP ausgestellt**) des iDRAC 6 (z. B. 192.168.0.120) oder dem registrierten DNS-iDRAC 6-Namen (**falls Zertifikat auf den registrierten iDRAC-Namen ausgestellt**) übereinstimmt.

So stellen Sie sicher, dass die CSR dem eingetragenen DNS-iDRAC 6-Namen entspricht:

1. Klicken Sie in der **System**-Struktur auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** und klicken Sie auf **Netzwerk**.
3. In der Tabelle **Allgemeine Einstellungen**:
   a. Wählen Sie das Kontrollkästchen **iDRAC auf DNS registrieren** aus.
   b. Geben Sie den iDRAC 6-Namen in das Feld **DNS-iDRAC-Name** ein.
4. Klicken Sie auf **Änderungen übernehmen**.

Weitere Informationen über die Erstellung von Zertifikatsignierungsanforderungen und zur Ausgabe von Zertifikaten finden Sie unter "iDRAC 6-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 iDRAC 6-Web Servers verfügbar sind.

Der iDRAC 6-Web Server führt nach den folgenden Ereignissen einen Reset durch:

- Wenn die Netzwerkkonfiguration oder Netzwerk-Sicherheitseigenschaften mittels der iDRAC 6-Internet-Benutzeroberfläche geändert werden
- Wenn die Eigenschaft **cfgRacTuneHttpsPort** geändert wird (einschließlich der Änderung durch eine config -f-<*Konfigurationsdatei*>)
- Wenn **racresetcfg** verwendet wird
- Wenn der iDRAC 6 zurückgesetzt wird
- Wenn ein neues SSL Server-Zertifikat hochgeladen wird

Warum registriert mein DNS-Server meinen iDRAC 6 nicht?

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

Wenn ich auf die webbasierte iDRAC 6 Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die aussagt, dass das SSL-Zertifikat von einer nicht vertrauenswürdigen Zertifizierungsstelle (CA) ausgegeben wurde.

Der iDRAC 6 enthält ein Standard-iDRAC 6-Serverzertifikat, um Netzwerksicherheit für die webbasierte Schnittstelle und die Remote-RACADM-Funktionen zu gewährleisen. Dieses Zertifikat wurde von einer nicht vertrauenswürdigen CA ausgegeben. Um diese Sicherheitsbedenken zu beseitigen, laden Sie ein von einer vertrauenswürdigen CA (z. B. Microsoft-CA, Thawte oder Verisign) ausgegebenes iDRAC 6-Serverzertifikat hoch. Weitere Informationen zur Ausgabe von Zertifikaten finden Sie unter "iDRAC 6-Datenübertragung mit SSL und digitalen Zertifikaten sichern".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6-Benutzer hinzufügen und konfigurieren

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

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

Die iDRAC6-Internetschnittstelle verwenden, um

iDRAC6-Benutzer hinzufügen und konfigurieren

Um das System mit dem iDRAC 6 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**→ **Konfiguration**→ **Benutzer**.

   Die Seite Benutzer zeigt die folgenden Informationen für iDRAC-Benutzer an: **Benutzer-ID, Zustand (Aktiviert/Deaktiviert), Benutzername,** RAC-Berechtigung, IPMI-LAN-Berechtigung, Serielle IPMI-LAN-Berechtigung und IPMI Serielle Berechtigung und Seriell über LAN-Zustand (Aktiviert/Deaktiviert). Tabelle 6-1 beschreibt die Benutzerzustände und Berechtigungen zur Konfiguration von iDRAC-Benutzern.

   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 **Benutzerhauptmenü** können Sie einen Benutzer konfigurieren, ein Benutzerzertifikat anzeigen, ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (CA) hochladen oder ein Zertifikat einer vertrauenswürdigen CA anzeigen.

   Wenn Sie **Benutzer konfigurieren** auswählen und auf **Weiter** klicken, wird die Seite **Benutzerkonfiguration** angezeigt. Fahren Sie mit Schritt 4 fort.

   Wie Sie eine Option unter **Smart Card-Konfiguration** auswählen, finden Sie unter Tabelle 6-2.

3. Konfigurieren Sie auf der Seite **B**enutzerkonfiguration 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.
Status	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 für den iDRAC 6 dürfen nicht die Zeichen **/** (Schrägstrich) oder **.** (Punkt) enthalten. **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, zu der der Benutzer zugewiesen ist (Administrator, Operator, schreibgeschützt oder keine).
IPMI-LAN-Berechtigung	Zeigt die IPMI-LAN-Berechtigungsebene an, zu der der Benutzer zugewiesen ist (Administrator, Operator, schreibgeschützt oder keine).
Serielle IPMI-Berechtigung	Zeigt die serielle Schnittstelle der IPMI-Berechtigungsebene an, zu der der Benutzer zugewiesen ist (Administrator, Operator, schreibgeschützt oder keine).
Seriell über LAN.	Ermöglicht dem Benutzer, IPMI Seriell über LAN zu verwenden oder gestattet es ihm nicht.

Tabelle 6-2. Smart Card-Konfigurationsoptionen

Option	Beschreibung
Benutzerzertifikat anzeigen	Zeigt die Seite des Benutzerzertifikats an, die auf den iDRAC hochgeladen wurde.
Zertifikat der vertrauenswürdigen CA hochladen	Ermöglicht Ihnen, das Zertifikat der vertrauenswürdigen CA auf den iDRAC hochzuladen und es in das Benutzerprofil zu importieren.
Zertifikat der vertrauenswürdigen CA anzeigen	Zeigt das Zertifikat der vertrauenswürdigen CA an, das auf den iDRAC hochgeladen wurde. Das Zertifikat der vertrauenswürdigen CA wird von der CA 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 iDRAC 6 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.

Table 6-4. IPMI-Benutzerberechtigungen

Eigenschaft	Beschreibung
Maximale LAN-Benutzerberechtigung gewährt	Legt die maximale Berechtigung des Benutzers auf dem IPMI-LAN-Kanal auf eine der folgenden Benutzergruppen fest: **Administrator**, **Operator**, **Benutzer** oder **Keine**.
Maximale Benutzerberechtigung der seriellen Schnittstellen 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.
Bei 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 virtuelle Datenträger	Ermöglicht dem Benutzer, virtuelle Datenträger auszuführen und zu verwenden.
Testwarnungen	Ermöglicht dem Benutzer, einem bestimmten Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Tabelle 6-6. iDRAC-Gruppenberechtigungen

Benutzergruppe	Gewährte Berechtigungen
Administrator	**Anmeldung bei iDRAC**, **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: **Anmeldung bei iDRAC**, **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Server-Maßnahmenbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf virtuellen Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Schreibgeschützt.	**Bei iDRAC anmelden**
Keine	Keine zugewiesenen Berechtigungen

Tabelle 6-7. Schaltflächen der Seite Benutzerkonfiguration

Schaltfläche	Abhilfe
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 anwenden	Speichert alle neuen Einstellungen, die an der Benutzerkonfiguration vorgenommen wurden.

Das RACADM-Dienstprogramm zum Konfigurieren von iDRAC6-Benutzern verwenden

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

Die Internet-basierte iDRAC6-Schnittstelle bietet die schnellste Möglichkeit, einen iDRAC6-Benutzer zu konfigurieren. Wenn Sie Befehlszeilen- oder Skript-Konfigurationen bevorzugen oder mehrere iDRAC6-Karten konfigurieren müssen, verwenden Sie RACADM, das mit den iDRAC6-Agents auf dem Managed System installiert ist.

Um mehrere iDRAC6-Karten 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-Eigenschaftendatenbank 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 umfasst.

Mehrere Parameter und Objekt-IDs werden mit ihren aktuellen Werten angezeigt. Zwei Objekte von Interesse 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 außerdem der Befehl **racadm config** -**f racadm.cfg** zur Angabe einer beliebigen Anzahl von zu schreibenden Gruppen/Objekten verwendet wird, kann der Index nicht angegeben werden. Ein neuer Benutzer wird dem ersten verfügbaren Index hinzugefügt. Diese Verfahrensweise bietet eine größere Flexibilität bei der Konfiguration mehrerer iDRAC6-Benutzer mit den selben Einstellungen.

iDRAC6-Benutzer hinzufügen

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

1. Legen Sie den Benutzernamen fest.
2. Legen Sie das Kennwort fest.
3. Legen Sie folgende Benutzerberechtigungen fest:
   - iDRAC-Berechtigung
   - IPMI-LAN-Berechtigung
   - Serielle IPMI-Berechtigung
   - 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 der Berechtigung zur ANMELDUNG 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 RAC-Benutzers verwendet werden kann:

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

Eine Null-Kette doppelter 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 Administratorrechten (rollenbasierte Autorität) zu aktivieren, ist als Erstes ein verfügbarer Benutzerindex ausfindig zu machen, indem Sie die unter "Bevor Sie beginnen" beschriebenen Schritte ausführen. Geben Sie im Anschluss daran die folgenden Befehlszeilen mit dem neuen Benutzernamen und neuen 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 mit Microsoft Active Directory verwenden

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Ein Verzeichnisdienst wird verwendet, um eine allgemeine Datenbank aller Informationen aufrechtzuerhalten, die erforderlich sind, um Benutzer, Computer, Drucker etc. auf einem Netzwerk zu steuern. Wenn Ihre Firma die Microsoft® Active Directory® Service-Software verwendet, kann die Software so konfiguriert werden, dass sie Zugriff auf den iDRAC6 bietet. Sie können dann bestehenden Benutzern in der Active Directory-Software iDRAC6-Benutzerberechtigungen zuteilen und diese steuern.

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 neun 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 zu erlauben, auf das System zuzugreifen.
Protokolle löschen	Ermöglicht dem Benutzer, die iDRAC6-Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer, RACADM-Befehle auszuführen.
Auf die 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-Authenifizierung des iDRAC6

Um die Active Directory-Authentifizierungsfunktion auf dem iDRAC6 verwenden zu können, 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 herzustellen. Sie benötigen daher auch eine integrierte PKI für die Active Directory-Infrastruktur. Weitere Informationen zum PKI-Setup finden Sie auf der Microsoft-Website.

Um eine korrekte Authentifizierung zu allen Domänen-Controllern vornehmen zu können, müssen Sie auch die SSL-Verschlüsselung auf sämtlichen Domänen-Controllern aktivieren, zu denen iDRAC6 eine Verbindung herstellt. Unter "SSL auf einem Domänen-Controller aktivieren" finden Sie detailliertere Informationen.

Unterstützte Active Directory- Authentifizierungsmechanismen

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

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

Die Vorteile bei der Verwendung des erweiterten Schemas sind:

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

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

Übersicht des Active Directory mit erweitertem Schema

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

Erweiterung des Active Directory-Schemas

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

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

Der Schema Extender und das MMC Snap-in für Active Directory Benutzer und Computer sind auf der DVD *Dell Systems Management Tools and Documentation* verfügbar. Nähere Informationen erhalten Sie unter "Erweiterung des Active Directory Schemas" und "Installation der Dell Extension auf dem Active Directory Benutzer und Computer-Snap-In." Einzelheiten zur Erweiterung des Schemas für das iDRAC6 die Installation des Active Directory 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 bzw. darin aufgenommen werden können. Die Benutzerklasse ist ein Beispiel einer Klasse, die in der Datenbank gespeichert wird. Einige Beispiel-Attribute der Benutzerklasse sind Vorname, Nachname, Telefonnummer usw. des Benutzers. Firmen können die Active Directory-Datenbank erweitern, indem sie ihre eigenen eindeutigen Attribute und Klassen hinzufügen, um sich an umgebungsspezifische Bedürfnisse zu richten. Dell hat das Schema erweitert, um die erforderlichen Änderungen zur Unterstützung der Remote-Verwaltung-Authentifizierung und Autorisierung einzuschließen.

Jedes Attribut bzw. jede Klasse, die 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 überlagern sich nicht. Um das Schema im Active Directory von Microsoft zu erweitern, hat Dell eindeutige OIDs (Namenserweiterungen) und eindeutig verlinkte Attribut-IDs für die Attribute und Klassen erhalten, die dem Verzeichnisdienst hinzugefügt werden.

Die Dell Dateierweiterung ist: dell

Die Dell Basis-OID lautet: 1.2.840.113556.1.8000.1280

Der RAC-LinkID-Bereich ist: 12070 bis 12079

Übersicht der iDRAC-Schema-Erweiterungen

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

Active Directory - Objekt-Übersicht

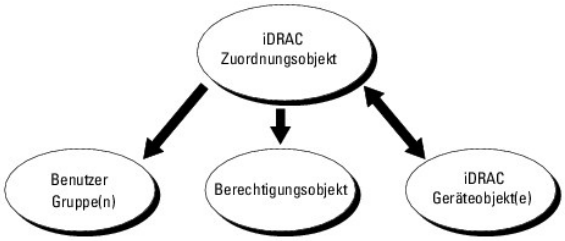
Für jedes physische iDRAC auf dem Netzwerk, das Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein iDRAC-Geräteobjekt erstellen. Sie können verschiedene Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt mit beliebig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

Jedes Zuordnungsobjekt darf jedoch nur mit einem Berechtigungsobjekt verbunden werden bzw. darf jedes Zuordnungsobjekt 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 außerdem auch mindestens einem Zuordnungsobjekt den iDRAC 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 jedes 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 sowie 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 der selben Domäne mit dem Verbindungsobjekt verbunden werden. Mit der Dell-Erweiterung können keine Gruppen oder iDRAC-Objekte aus anderen Domänen als Product-Member des Verbindungsobjektes hinzugefügt werden.

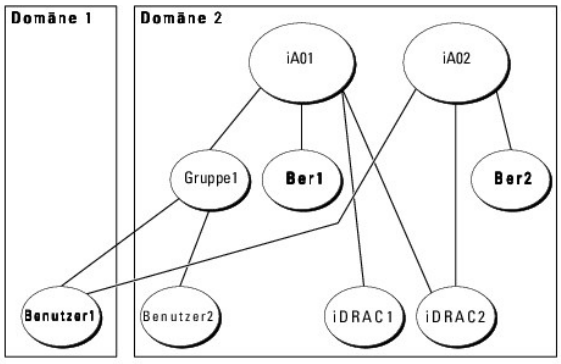
Benutzer, Benutzergruppen oder verschachtelte Benutzergruppen jeglicher Domäne können dem Verbindungsobjekt hinzugefügt werden. Lösungen des Erweiterten Schemas unterstützen jede Art von Benutzergruppe und alle über mehrere, von Microsoft Active Directory zugelassenen Domänen verschachtelten Benutzergruppen.

Unter Verwendung des erweiterten Schemas Berechtigungen ansammeln

Die Methode der Authentifizierung des erweiterten Schemas unterstützt das Ansammeln von Berechtigungen über unterschiedliche Berechtigungsobjekte, die mit demselben Benutzer durch verschiedene Zuordnungsobjekte in Verbindung stehen. Mit anderen Worten sammelt die Authentifizierung des erweiterten Schemas Berechtigungen an, um dem Benutzer den Super-Satz aller zugewiesener Berechtigungen zur Verfügung stellen zu können, die den verschiedenen, mit demselben Benutzer in Verbindung stehenden, Berechtigungsobjekten entsprechen.

Abbildung 7-2 bietet ein Beispiel des Ansammelns von Berechtigungen unter Verwendung des erweiterten Schemas.

Abbildung 7-2. Ansammeln von Berechtigungen für einen Benutzer



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

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

Die Authentifizierung des erweiterten Schemas sammelt Berechtigungen an, um dem Benutzer den maximalen Satz aller möglichen Berechtigungen zur Verfügung stellen zu können und berücksichtigt dabei die zugewiesenen Berechtigungen der verschiedenen Berechtigungsobjekte für diesen Benutzer.

In dieser Konfiguration verfügt Benutzer1 über die Berechtigungen von Priv1 und Priv2 auf dem iDRAC2. Benutzer1 besitzt ausschließlich Priv1 Berechtigungen auf dem iDRAC1. Benutzer2 hat die Berechtigung 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 iDRAC konfigurieren

Konfigurieren Sie vor der Verwendung von Active Directory zum Zugriff auf iDRAC6 die Active Directory-Software und den iDRAC6, indem Sie die folgenden Schritte in der vorgegebenen Reihenfolge ausführen:

1. Erweitern Sie das Active Directory-Schema (s. "Erweiterung des Active Directory-Schemas").

2. Erweitern Sie das Snap-In von Active Directory-Benutzer und -Computer (s. "Dell Erweiterung zum Active Directory-Benutzer und -Computer-Snap-In

installieren").

3. Fügen Sie iDRAC6-Benutzer und ihre Berechtigungen ins Active Directory (s. "iDRAC-Benutzer und -Berechtigungen zum 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 Active Directory mit erweitertem Schema mit der iDRAC6 -Webschnittstelle" oder "Konfiguration des Active Directory mit erweitertem Schema mit 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, ist sicherzustellen, dass Sie Schema-Admin-Rechte 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-Skript-Datei verwenden.

Die LDIF-Dateien und Dell Schema Extender befinden sich auf der DVD *Dell Systems Management Tools and Documentation* in den folgenden jeweiligen Verzeichnissen:

- *DVD Laufwerk*:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- <**DVD** *Laufwerk*>:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender**

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Dateien**. Informationen zur Verwendung von Dell Schema Extender zum Erweitern des Active Directory-Schemas befinden sich unter "Dell Schema Extender verwenden".

Sie können den Schema Extender bzw. die LDIF-Dateien von 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 auf **Weiter**.

3. Wählen Sie **Aktuelle Anmeldeinformationen verwenden** aus, oder geben Sie einen Benutzernamen und ein Kennwort mit Schema-Administratorrechten ein.

4. Klicken Sie auf **Weiter**, um den Dell Schema Extender auszuführen.

5. Klicken Sie auf **Fertig stellen**.

   Das Schema wird erweitert. Um die Schema-Erweiterung zu überprüfen, verwenden Sie die Microsoft Verwaltungskonsole (MMC) und das Active Directory Schema-Snap-In, um zu überprüfen, ob folgende Elemente vorhanden sind:

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

Näheres zur Benutzung der Verwaltungskonsole und des Active Directory Schema Snap-in finden Sie in Ihrem Microsoft Handbuch.

Tabelle 7-2. Klassendefinitionen für zum Active Directory-Schema hinzugefügte Klassen

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)
delliDRACGerät	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACZuordnung	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	Stellt das Dell iDRAC-Gerät dar. Das iDRAC-Gerät muss als delliDRACDevice im Active Directory konfiguriert werden. 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. delliDRACZuordnungsobjekt Klasse

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	1.2.840.113556.1.8000.1280.1.1.2.1	FALSE

Die Liste von dellPrivilege-Objekten, die zu diesem Attribut gehören.	Definierter Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellProductMembers Liste der dellRac-Geräte und delliDRAC-Geräteobjekte, die der Zuordnung angehören. Dieses Attribut ist die Vorwärtsverbindung zur dellAssociationMembers-Rückwärtsverbindung. Link-ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Definierter 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-Befehls-Admin-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion Die Aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren.	1.2.840.113556.1.8000.1280.1.1.2.12 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Dieses Attribut ist der Aktuelle Rac-Typ für das dellRacDevice-Objekt und der Rückwärtslink zum dellAssociationObjectMembers-Vorwärtslink.	1.2.840.113556.1.8000.1280.1.1.2.13 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Liste der dellAssociationObjectMembers in diesem Produkt. Dieses Attribut ist das Rückwärtslink zum verknüpften Attribut dellProductMembers. Link-ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Definierter Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch die Active Directory-Benutzer und das Computer-Snap-In erweitern, 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 Dell-Erweiterung zum **Snap-In von Active Directory-Benutzern und -Computern** auswählen. Das *Schnellinstallationshandbuch zu Dell OpenManage-Software* enthält zusätzliche Anleitungen zur Installation von Systemverwaltungssoftware. Für x64-Bit-Windows-Betriebssysteme befindet sich das Snap-In-Installationsprogramm unter **<DVD Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64**.

Weitere Informationen über Active Directory-Benutzer- und Computer-Snap-In erhalten Sie in Ihrem Microsoft Handbuch.

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 "Snap-In von Active Directory-Benutzer und -Computer öffnen" finden Sie weitere Informationen.

Snap-In von Active Directory-Benutzer und -Computer öffnen

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

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

   Wenn Sie nicht auf dem Domänen-Controller angemeldet sind, muss das entsprechende Microsoft-Administratorpaket auf dem lokalen System installiert sein. Um dieses Administrator Pack zu installieren, klicken Sie auf **Start→ Ausführen**, geben Sie `MMC` ein und drücken Sie **Eingabe**.

   Die Microsoft Verwaltungskonsole erscheint.

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 dann auf **OK**.

iDRAC-Benutzer und -Berechtigungen zum 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. Führen Sie zum Hinzufügen der einzelnen Objektarten folgende Verfahren aus:

- Erstellen eines iDRAC-Geräteobjekts
- Berechtigungsobjekt erstellen
- Zuordnungsobjekt erstellen
- Konfigurieren eines Zuordnungsobjekts

Erstellen eines iDRAC-Geräteobjekts

1. Klicken Sie im Fenster MMC-**Console Root** mit der rechten Maustaste auf einen Container.

2. Wählen Sie **Neu→ Dell Remote Management Object Advanced**.

   Das Fenster **Neues Objekt** wird geöffnet.

3. Tippen Sie einen Namen für das neue Objekt ein. Der Name muss mit dem iDRAC-Namen übereinstimmen, den Sie in Schritt A von "Konfiguration des Active Directory mit erweitertem Schema mit der iDRAC6 -Webschnittstelle" eingeben.

4. Wählen Sie iD**RAC-Geräteobjekt**.

5. Klicken Sie auf **OK**.

Berechtigungsobjekt erstellen

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

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.

2. Wählen Sie **Neu→ Dell Remote Management Object Advanced**.

   Das Fenster **Neues Objekt** wird geöffnet.

3. Tippen Sie einen Namen für das neue Objekt ein.

4. Wählen Sie **Berechtigungsobjekt** aus.

5. Klicken Sie auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf das Berechtigungsobjekt, das Sie erstellt haben, und wählen Sie **Eigenschaften** aus.
7. Klicken Sie auf die Registerkarte **Remote Management-Berechtigungen** und wählen Sie die Berechtigungen aus, die der Benutzer haben soll.

Zuordnungsobjekt erstellen

ANMERKUNG: Das iDRAC-Verbindungsobjekt bezieht sich auf eine Gruppe und hat einen Wirkungsbereich in einer lokalen Domäne.

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

   Hierdurch wird das Fenster **Neues Objekt** geöffnet.
3. Tippen Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Zuordnungsobjekt**.
5. Wählen Sie die Reichweite für das **Zuordnungsobjekt**.
6. Klicken Sie auf **OK**.

Konfigurieren eines Zuordnungsobjekts

Durch die Verwendung 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 **Zuordnungsobjekt** und wählen Sie **Eigenschaften**.
2. Wählen Sie die Registerkarte **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 die Registerkarte **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, die 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 die Registerkarte **Berechtigungsobjekt** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Berechtigungsobjektnamen ein und klicken Sie auf **OK**.

Wählen Sie die Registerkarte **Produkte** und fügen Sie ein iDRAC-Gerät hinzu, dass mit dem Netzwerk verbunden ist, an das die gewählten Benutzer oder Benutzergruppen angeschlossen sind. Mehrere iDRAC-Geräte können einem Zuordnungsobjekt hinzugefügt werden.

Hinzufügen von iDRAC-Geräten

So fügen Sie iDRAC-Geräte hinzu:

1. Wählen Sie das Register **Produkte** aus 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 Active Directory mit erweitertem Schema mit der iDRAC6 - Webschnittstelle

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 **Konfiguration** und wählen Sie **Active Directory** aus.
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** erscheint.
6. Markieren Sie unter **Zertifikat Einstellungen** die Option **Überprüfung des Zertifikats aktivieren**, falls Sie das SSL-Zertifikat Ihrer 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 vollen Pfad und den abgeschlossenen Dateinamen und die Dateierweiterung enthält.

8. Klicken Sie auf **Hochladen.**

   Die Zertifikatsinformationen für das Active Directory CA-Zertifikat, das Sie hochgeladen haben, erscheint.
9. Klicken Sie auf **Weiter,** um zu **Schritt 2 von 4 Active Directory Konfiguration und Verwaltung** zu gehen.
10. Klicken Sie auf **Active Directory aktivieren.**
11. Klicken Sie auf **Hinzufügen**, um den Benutzer-Domänennamen einzugeben.
12. Geben Sie den Namen der Benutzerdomäne in die Kommandozeile ein und klicken Sie **OK**. Dieser Schritt ist optional. Wenn Sie eine Liste der Benutzerdomänen erstellen, ist diese Liste Bei der Anmeldung an der Webschnittstelle zugänglich. Sie können eine Auswahl treffen, sodass Sie anschließend nur noch den Benutzernamen eingeben müssen.
13. Geben Sie die **Zeitüberschreitungszeit** in Sekunden ein, um anzugeben, wie lange der iDRAC6 auf Antworten des Active Directory wartet. Der Standardwert beträgt 120 Sekunden.
14. Geben Sie die Server Adresse des Domänen-Controllers ein. Sie können bis zu drei Active Directory Server zur Anmeldung eingeben, aber Sie müssen mindestens einen Server konfigurieren, indem Sie die IP-Adresse oder den vollqualifizierten Namen der Domäne (FQDN) eingeben. iDRAC6 versucht, eine Verbindung mit jedem konfigurierten Server aufzubauen, bis diese Verbindung hergestellt ist.

    ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie in diesem Feld angeben, sollte mit dem Feld Server oder Server Alternativer Name im Zertifikat Ihres Domänen-Controllers übereinstimmen, wenn Sie die Überprüfung des Zertifikats aktiviert haben.
15. Klicken Sie auf **Weiter,** um zu **Schritt 3 von 4 Active Directory Konfiguration und Verwaltung** zu gehen.
16. Wählen Sie unter **Schema Auswahl** die Option **Erweitertes Schema**.
17. Klicken Sie auf **Weiter,** um zu **Schritt 4 von 4 Active Directory Konfiguration und Verwaltung** zu gehen.
18. Geben Sie unter **Erweitertes Schema Einstellungen** den iDRAC-Namen und den Domänennamen ein, um das iDRAC-Geräteobjekt zu konfigurieren. Der iDRAC-Domänenname befindet sich in der Domäne, in der das iDRAC-Objekt erstellt wird.
19. Klicken Sie auf **Fertig stellen**, um die Active Directory Erweitertes Schema-Einstellungen zu speichern.

    Der iDRAC6-Web Server kehrt automatisch auf die Seite **Active Directory-Konfiguration und -Verwaltung** zurück.
20. Klicken Sie auf **Einstellungen überprüfen**, um die Active Directory Erweitertes Schema-Einstellungen zu prüfen.
21. Geben Sie Ihren Active Directory-Benutzernamen und das Kennwort ein.

    Die Testergebnisse und das Testprotokoll werden angezeigt. Weitere Informationen finden Sie unter "Einstellungen testen".

ANMERKUNG: Um die Anmeldung beim Active Directory zu unterstützen, müssen Sie einen DNS-Server korrekt im iDRAC-Programm konfiguriert haben. Gehen Sie zum Fenster **Remote Access→ Konfiguration→ Netzwerk** um einen oder mehrere DNS-Server manuell zu konfigurieren oder verwenden Sie DHCP um einen oder mehrere Server zu erhalten.

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

Konfiguration des Active Directory mit erweitertem Schema mit RACADM

Verwenden Sie die folgenden Befehle, um die iDRAC-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 <RAC common name>

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

   racadm config -g cfgActiveDirectory -o cfgDomainController1 <fvollqualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>

   racadm config -g cfgActiveDirectory -o cfgDomainController2 <fvollqualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>

   racadm config -g cfgActiveDirectory -o cfgDomainController3 <fvollqualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ANMERKUNG: Mindestens eine der drei Adressen muss konfiguriert werden. iDRAC versucht, mit jeder der konfigurierten Adressen nacheinander zu verbinden, bis eine Verbindung erfolgreich hergestellt wurde. Wenn die erweiterte Schemaoption ausgewählt ist, sind dies die FQDN- oder IP-Adressen des Domänen-Controllers auf dem sich das iDRAC-Gerät befindet. Global Catalog Server werden im Modus Erweitertes Schema nicht verwendet.

   ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie in diesem Feld angeben, sollte mit dem Feld Server oder Server Alternativer Name im Zertifikat 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 müssen Sie kein CA-Zertifikat laden.

   Wenn Sie für den SSL-Handshake die Überprüfung des Zertifikats erzwingen möchten, geben Sie den folgenden RACADM-Befehl ein:

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

   In diesem Fall müssen Sie über den folgendenRACADM-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 Ihre DNS-IP- Adresse manuell eingeben möchten, 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, arbeiten Sie mit dem folgenden Befehl:

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

   Sie können bis zu 40 Benutzerdomänen mit Indexzahlen zwischen 1 and 40 erstellen.

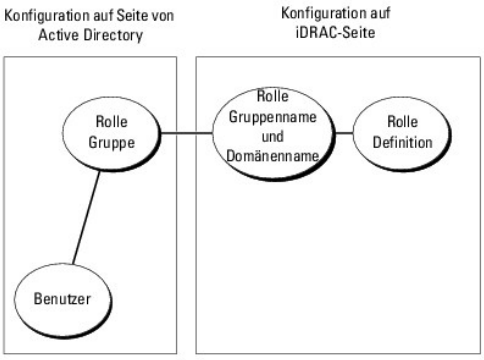
   Mehr Informationen über Benutzerdomänen unter "Active Directory zur Anmeldung beim iDRAC6 verwenden".

5. Drücken Sie **Enter** um die Konfiguration des Active Directory mit erweitertem Schema abzuschließen.

Übersicht des Standardschema-Active Directory

Wie in Abbildung 7-3dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration unter Active Directory als auch unter iDRAC6.

Abbildung 7-3. Konfiguration des iDRAC mit Microsoft Active Directory und Standardschema



Auf der Seite des Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der Zugang zum iDRAC6 hat, wird ein Mitglied der Rollengruppe sein. Um diesem Benutzer Zugriff auf einen bestimmten iDRAC6 zu gewähren, muss der Rollengruppenname und dessen Domänenname auf dem bestimmten iDRAC6 konfiguriert werden. Im Gegensatz zur Schemaerweiterungslösung 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 die Berechtigungen einer Standard-Rollengruppe.

Tabelle 7-9. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppen	Standard-Zugriffsstufe	Gewährte Berechtigungen	Bit-Maske
Rollengruppe 1	Administrator	**Anmeldung bei iDRAC**, **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf virtuellen Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**	0x000001ff
Rollengruppe 2	Operator	**Bei iDRAC anmelden**, **iDRAC konfigurieren, Serversteuerungsbefehle ausführen**, **auf Konsolenumleitung zugreifen**, **auf virtuellen Datenträger zugreifen**, **Warnungen testen, 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.

Einfache Domänen (Single Domains) und Mehrfache Domänen (Multiple Domains)

Wenn sich alle Login-Benutzer und Rollengruppen sowie die verschachtelten Benutzergruppen in der selben Domäne befinden, müssen lediglich die Adressen der Domänen-Controller auf dem iDRAC6 konfiguriert werden. In diesem Muster einer einfachen Domäne wird jede Art von Gruppe unterstützt.

Wenn alle Login-Benutzer und Rollengruppen sowie eine der verschachtelten Benutzergruppen mehrfachen Domänen angehören, müssen Global Catalog Server-Adressen auf dem iDRAC6 eingerichtet werden. In diesem Muster einer mehrfachen Domäne müssen alle Rollengruppen und, wenn vorhanden, alle verschachtelten Benutzergruppen einer Universal Group angehören.

Standardschema von Active Directory zum Zugriff auf iDRAC konfigurieren

Active Directory muss mit den folgenden Schritten konfiguriert werden, um Active Directory-Benutzern den Zugang zum 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 oder RACADM (siehe "Konfiguration des Active Directory mit Standardschema mit der iDRAC6 -Webschnittstelle" oder "Konfiguration des Active Directory mit Standardschema mit RACADM").

3. Fügen Sie den Active Directory-Benutzer als Mitglied der Active Directory-Gruppe hinzu, um auf den iDRAC zuzugreifen.

Konfiguration des Active Directory mit Standardschema mit der iDRAC6 -Webschnittstelle

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 **Konfiguration** und wählen Sie **Active Directory** aus.
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** erscheint.
6. Markieren Sie unter **Zertifikat Einstellungen** die Option **Überprüfung des Zertifikats aktivieren**, falls Sie das SSL-Zertifikat Ihrer 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 vollen Pfad und den abgeschlossenen Dateinamen und die Dateierweiterung enthält.
8. Klicken Sie auf **Hochladen.**

   Die Zertifikatsinformationen für das Active Directory CA-Zertifikat, das Sie hochgeladen haben, erscheint.
9. Klicken Sie auf **Weiter,** um zu **Schritt 2 von 4 Active Directory Konfiguration und Verwaltung** zu gehen.
10. Klicken Sie auf **Active Directory aktivieren.**
11. Klicken Sie auf **Hinzufügen**, um den Benutzer-Domänennamen einzugeben.
12. Geben Sie den Namen der Benutzerdomäne in die Kommandozeile ein und klicken Sie **OK**.
13. Geben Sie die **Zeitüberschreitungszeit** in Sekunden ein, um anzugeben, wie lange der iDRAC6 auf Antworten des Active Directory wartet. Der Standardwert beträgt 120 Sekunden.
14. Geben Sie die Server Adresse des Domänen-Controllers ein. Sie können bis zu drei Active Directory Server zur Anmeldung eingeben, aber Sie müssen mindestens einen Server konfigurieren, indem Sie die IP-Adresse oder den FQDN eingeben. iDRAC6 versucht, eine Verbindung mit jedem konfigurierten Server aufzubauen, bis diese Verbindung hergestellt ist.

   ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie in diesem Feld angeben, sollte mit dem Feld Server oder Server Alternativer Name im Zertifikat Ihres Domänen-Controllers übereinstimmen, wenn Sie die Überprüfung des Zertifikats aktiviert haben.
15. Klicken Sie auf **Weiter,** um zu **Schritt 3 von 4 Active Directory Konfiguration und Verwaltung** zu gehen.
16. Wählen Sie unter **Schema Auswahl** die Option **Standardschema**.
17. Klicken Sie auf **Weiter,** um zur **Seite Schritt 4a von 4 Active Directory Konfiguration und Verwaltung** zu gehen.
18. Geben Sie unter **Standardschemaeinstellungen** die Adresse des Global Catalog-Servers in Active Directory ein. Sie müssen den Standort mindestens eines Global Catalog-Servers konfigurieren.

    ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie in diesem Feld angeben, sollte mit dem Feld Server oder Server Alternativer Name im Zertifikat Ihres Domänen-Controllers übereinstimmen, wenn Sie die Überprüfung des Zertifikats aktiviert haben.

    ANMERKUNG: Der Global Catalog-Server ist nur dann für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen in verschiedenen Domänen befinden. Bei einer mehrfachen Domäne wie dieser kann nur die Universal Group genutzt werden.
19. Klicken Sie unter **Rollengruppen** auf eine **Rollengruppe**.

    Die Seite **Schritt 4b von 4** wird angezeigt.

20. Geben Sie den **Rollengruppennamen** an.

    Der **Rollengruppenname** identifiziert die Rollengruppe im Active Directory, das dem iDRAC zugeordnet ist.

21. Geben Sie die **Rollengruppendomäne** an, die die Domäne der Rollengruppe ist.

22. Geben Sie die **Rollengruppenberechtigungen** an, indem Sie die **Rollengruppenberechtigungsebene** auswählen. Wenn Sie zum Beispiel **Administrator** auswählen, werden alle Berechtigungen für diese Berechtigungsebene ausgewählt.

23. Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern.

    Der iDRAC6-Web Server kehrt automatisch auf die Seite **Schritt 4a von 4 Active Directory-Konfiguration und -Verwaltung** zurück, **auf der Ihre Einstellungen angezeigt werden.**

24. Wiederholen Sie die Schritte 18 bis 22, um zusätzliche Rollengruppen zu konfigurieren, oder klicken Sie auf **Fertig stellen,** um auf die Seite **Active Directory-Konfiguration und -Verwaltung zurückzukehren, auf der alle** Standardschema-Konfigurationseinstellungen **angezeigt werden**.

25. Klicken Sie auf **Einstellungen überprüfen**, um die Active Directory Standardschema-Einstellungen zu prüfen.

26. 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. Gehen Sie zum Fenster **Remote Access→ Konfiguration→ Netzwerk** um einen oder mehrere DNS-Server manuell zu konfigurieren oder verwenden Sie DHCP um einen oder mehrere Server zu erhalten.

Die Konfiguration des Active Directory mit Standardschema ist nun abgeschlossen.

Konfiguration des Active Directory mit Standardschema mit RACADM

Verwenden Sie die folgenden Befehle zum Konfigurieren der Active Directory-Funktion von iDRAC mit Standardschema unter Verwendung der RACADM-CLI statt der Webschnittstelle.

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

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

   ```
   racadm config -g cfgActiveDirectory -o cfgADType 2
   ```

   ```
   racadm config -g cfgStandardSchema -i <Index> -o
   cfgSSADRoleGroupName <Name der Rollengruppe>
   ```

   ```
   racadm config -g cfgStandardSchema -i <Index> -o
   cfgSSADRoleGroupDomain <vollqualifizierter Domänenname>
   ```

   ```
   racadm config -g cfgStandardSchema -i <Index> -o
   cfgSSADRoleGroupPrivilege <Bitmasken-Zahlenwerte für
   spezielle Benutzerberechtigungen>
   ```

   ANMERKUNG: Siehe Tabelle B-2 für Bitmasken-Zahlenwerte.

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController1 <vollqualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController2 <vollqualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController3 <vollqualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie in diesem Feld angeben, sollte mit dem Feld Server oder Server Alternativer Name im Zertifikat 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 nacheinander, mit jeder der konfigurierten Adressen eine Verbindung aufzubauen, bis eine Verbindung hergestellt ist. Im Standardschema sind dies die Adressen des Domänen-Controllers, auf denen sich die Benutzerkonten und die Rollengruppen befinden.

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController1 <vollqualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController2 <vollqualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController3 <vollqualifizierter 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. Bei einer mehrfachen Domäne wie dieser kann nur die Universal Group genutzt werden.

   ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie in diesem Feld angeben, sollte mit dem Feld Server oder Server Alternativer Name im Zertifikat 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 müssen Sie kein CA-Zertifikat laden.

Wenn Sie für den SSL-Handshake die Überprüfung des Zertifikats erzwingen möchten, geben Sie den folgenden RACADM-Befehl ein:

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

In diesem Fall müssen Sie über den folgenden RACADM-Befehl auch das CA-Zertifikat laden:

```
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 folgende RACADM-Befehle ein:

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

3. Wenn DHCP auf dem iDRAC6 deaktiviert ist oder Sie Ihre DNS-IP- Adresse manuell eingeben möchten, geben Sie die folgenden RACADM- Befehle ein:

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

   racadm config -g cfgLanNetworking -o cfgDNSServer1 <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, arbeiten Sie mit dem folgenden Befehl:

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

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

   Mehr Informationen über Benutzerdomänen unter "Active Directory zur Anmeldung beim iDRAC6 verwenden".

Einstellungen testen

Wenn Sie überprüfen möchten, ob eine Konfiguration korrekt funktioniert oder ob eine Problemanalyse anhand der Fehlermeldung bei der Anmeldung zum Active Directory notwendig ist, können Sie Ihre Einstellungen von der iDRAC6-Webschnittstelle aus testen.

Nach Abschluss der Konfiguration der iDRAC6-Webschnittstelle klicken Sie auf **Einstellungen überprüfen** am unteren Rand der Seite. Sie müssen nun einen Test-Benutzernamen (zum Beispiel benutzername@domäne.com) und ein Kennwort eingeben, um die Überprüfung durchzuführen. Je nach den zu überprüfenden Einstellungen kann es einige Zeit in Anspruch nehmen, bis alle Schritte der Überprüfung durchgeführt sind und das Ergebnis für jeden einzelnen Schritt angezeigt werden kann. Am unteren Rand der Ergebnisseite wird ein ausführliches Protokoll der Überprüfung angezeigt.

Überprüfen Sie gegebenenfalls jede einzelne Fehlermeldung und mögliche Lösungen im Testprotokoll. Informationen zu den häufigsten Fehlermeldungen erhalten Sie unter "Häufig gestellte Fragen."

Wenn Sie Ihre Einstellungen ändern müssen, wählen Sie die Registerkarte **Active Directory** und ändern Sie die Konfiguration Schritt für Schritt.

SSL auf einem Domänen-Controller aktivieren

Wenn Benutzer durch das iDRAC gegen einen Active Directory-Domänen-Controller authentifiziert werden, wird eine SSL-Sitzung mit dem Domänen-Controller gestartet. Der Domänen-Controller sollte jetzt ein von der Zertifizierungsstelle (CA) signiertes Zertifikat erstellen - das Stammzertifikat, das auch in das iDRAC geladen wird. Damit, anders ausgedrückt, die DRAC-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→ Verwaltung→ Domänensicherheitsregeln**.
   b. Erweitern Sie den Ordner **Richtlinien öffentlicher Schlüssel** klicken Sie mit der rechten Maustaste auf **Automatische Zertifikatanforderungs-Einstellungen** und klicken Sie auf **Automatische Zertifikatanforderung**.
   c. Klicken Sie im **Setup-Assistent der automatischen Zertifikatanforderung** auf **Weiter** und wählen Sie **Domänen- Controller** aus.
   d. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Exportieren des CA-Stammzertifikats des Domänen-Controllers auf das iDRAC

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

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

1. Machen Sie den Domänen-Controller ausfindig, der den Microsoft Enterprise-CA -Dienst ausführt.
2. 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 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 Tasks** aus, und klicken Sie auf **Exportieren...**.
12. Klicken Sie im **Zertifikate exportieren-Assistenten** auf **Weiter** und wählen Sie **Privaten Schlüssel nicht exportieren** aus.
13. Klicken Sie auf **Weiter** und wählen Sie **Base-64-codiert 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 Active Directory mit erweitertem Schema mit der iDRAC6 -Webschnittstelle" oder "Konfiguration des Active Directory mit Standardschema mit RACADM".

    Um das Zertifikat über die Webschnittstelle herunterzuladen, siehe "Konfiguration des Active Directory mit erweitertem Schema mit der iDRAC6 -Webschnittstelle" oder "Konfiguration des Active Directory mit Standardschema mit der iDRAC6 -Webschnittstelle".

SSL-Zertifikat der iDRAC6-Firmware importieren

ANMERKUNG: Wenn der Active Directory-Server so eingestellt ist, dass der Nutzer in der Initialisierungsphase einer SSL-Sitzung authentifiziert wird, muss das iDRAC-Serverzertifikat auf den Active Directory Domänen-Controller geladen 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 iDRAC-SSL-Zertifikat ist identisch mit dem Zertifikat, das für den iDRAC-Web Server verwendet wird. Alle iDRAC-Controller werden mit einem selbstsignierten Standard-Zertifikat versandt.

Zum Herunterladen des iDRAC-SSL-Zertifikats 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 Tasks** und klicken Sie auf **Import**.
3. Klicken Sie auf **Weiter** und suchen Sie die SSL-Zertifikatdatei.

4. Installieren Sie das iDRAC-SSL-Zertifikat in der **vertrauenswürdigen Stammzertifizierungsstelle** jedes Domänen-Controllers.

   Wenn Sie Ihr eigenes Zertifikat installiert haben, stellen Sie sicher, dass die Zertifizierungsstelle, die das Zertifikat signiert hat, in der Liste **Vertrauenswürdige Stammzertifizierungsstellen** aufgeführt ist. Wenn die Zertifizierungsstelle nicht auf der Liste enthalten ist, muss sie auf allen Ihren Domänen-Controllern installiert werden.

5. Klicken Sie auf **Weiter** und wählen Sie aus, ob Windows automatisch einen Zertifikatspeicher aussuchen soll, der vom Zertifikattyp abhängt, oder ob Sie nach einem eigenen Speicher suchen wollen.

6. Klicken Sie auf **Fertig stellen** und dann auf **OK**.

Active Directory zur Anmeldung beim iDRAC6 verwenden

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

- Web-basierte 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 von 1 - 256 Byte ist.

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

ANMERKUNG: NetBIOS-Domänennamen, wie z.B. Americas können nicht festgelegt 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 Auswahl Menü wählen, sollten Sie nur einen Benutzernamen eingeben. Wenn Sie **dieses iDRAC** wählen, können Sie sich nach wie vor als Active Directory-Benutzer anmelden, wenn Sie die zuvor beschriebene Syntax "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 iDRAC 6 über die Smart Card".

ANMERKUNG: Der Windows 2008 Active Directory-Server unterstützt nur eine Zeichenkette <Benutzername>@<Domänenname> mit eine maximalen Länge von 256 Zeichen.

Häufig gestellte Fragen

Die Active Directory-Anmeldung ist gescheitert. Wie kann ich das Problem beheben?

iDRAC6 bietet über die Webschnittstelle ein Diagnoseprogramm. Melden Sie sich auf der Webschnittstelle als lokaler Benutzer mit Administratorrechen an. Wechseln Sie zu **Remote-Zugriff**→ **Konfiguration**→ **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 Passwort ein und klicken Sie auf **Überprüfung starten**. iDRAC6 führt die Überprüfungen Schritt für Schritt aus und zeigt jedes einzelne Ergebnis an. Ein detaillierter Testbericht wird ebenfalls protokolliert, anhand dessen Sie die verschiedensten Probleme lösen können. Klicken Sie auf die Registerkarte **Active Directory**, um zur Seite **Active Directory-Konfiguration und Verwaltung** zurückzukehren. 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 Test-Benutzer die Autorisierung erhält.

Ich habe die Überprüfung des Zertifikats deaktiviert, konnte mich aber trotzdem nicht anmelden. Ich habe die Diagnosen vom GUI aus durchgeführt, und das Protokoll zeigt die folgende Nachricht an:

FEHLER: Keine Verbindung zum LDAP-Server möglich, Fehler:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: CA-Zertifikat auf iDRAC prüfen. Prüfen Sie bitte auch, ob die Gültigkeit des iDRAC die der Zertifikate nicht überschreitet und ob die Adresse des in iDRAC konfigurierten Domänen-Controllers mit dem Ziel des Zertifikats für den Directory Server übereinstimmt.

Wo könnte das Problem und wie kann ich es beheben?

Wenn die Funktion zur Überprüfung des Zertifikats aktiviert ist, nutzt iDRAC6 bei bestehender SSL-Verbindung mit dem Server das verfügbare CA-Zertifikat zur Überprüfung des Active Directory Server-Zertifikats. Die häufigsten Gründe für das Scheitern der Zertifizierung:

1. Das Gültigkeitsdatum für das iDRAC6 liegt über dem der Server- Zertifizierung oder des CA-Zertifikats. Überprüfen Sie aktuelle iDRAC6- Zeit und die Gültigkeitsdauer Ihres Zertifikats.

2. Die im iDRAC6 konfigurierten Adressen der Domänen-Controller stimmen nicht mit dem Servernamen oder dem alternativen Servernamen im Verzeichnis überein. Falls Sie eine IP-Adresse verwenden, lesen Sie bitte die folgende Frage und die Antwort. Wenn Sie einen FQDN verwenden, stellen Sie bitte sicher, dass Sie den FQDN des Domänen- Controllers verwenden 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 Domain-Controller-Zertifikats. Für gewöhnlich verwendet Active Directory den Hostnamen und nicht die IP-Adresse des Domänen-Controllers im Feld Servername oder alternativer Servername des Domänen-Controller-Zertifikats. Das Problem lässt sich auf verschiedene Weisen beheben.

1. Konfigurieren Sie den Hostnamen (FQDN) des Domänen Controllers als *Adresse(n) des Domänen Controllers* auf das iDRAC6, damit er mit dem Servernamen oder alternativen Servernamen des Server-Zertifikats übereinstimmt.

2. Erstellen Sie das Server-Zertifikat erneut um eine IP-Adresse im Feld Servername oder alternativer Servername eine IP-Adresse zu verwenden, die auf iDRAC6 konfiguriert ist.

3. Deaktivieren Sie die Überprüfung des Zertifikats, wenn Sie dem Domänen Controller beim SSL-Handshake ohne diese Überprüfung vertrauen.

Ich verwende ein erweitertes Schema in einer Umgebung mit mehreren Domänen. Wie muss ich die Domänen-Controller-Adresse konfigurieren?

Es sollte der Hostname (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 Standardschema verwenden und Benutzer und Rollengruppen verschiedenen Domänen angehören, sind Global Catalog-Adressen erforderlich. In diesem Fall kann nur Universal Group verwendet werden.

Wenn Sie Standardschema verwenden und alle Benutzer und alle Rollengruppen der selben Domäne angehören, sind keine Global Catalog-Adressen erforderlich.

Wie funktioniert die Abfrage im Standardschema?

iDRAC6 verbindet sich zuerst mit den Domänen-Controller-Adressen, wenn sich die Benutzer und die 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 erlangt werden, werden diese Berechtigungen aufgespeichert.

Verwendet iDRAC6 immer LDAP über SSL?

Ja. Der gesamte Transfer erfolgt über den geschützten Port 636 und/oder 3269.

Bei *Einstellungen überprüfen* führt iDRAC6 einen LDAP CONNECT aus, um das Problem zu isolieren, es führt jedoch keinen LDAP BIND auf einer unsicheren Verbindung aus.

Warum ist in der Standardkonfiguration des iDRAC6 die Überprüfung des Zertifikats aktiviert?

iDRAC6 arbeitet bei der Identifikation des Domänen Controllers mit dem iDRAC6 eine Verbindung herstellt mit einem hohen Sicherheitsstandard. 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?

In dieser Version nicht.

Was muss ich überprüfen, wenn ich mich nicht über Active Directory bei iDRAC6 anmelden kann?

Sie können das Problem diagnostizieren, indem Sie in der iDRAC6-Webschnittstelle am unteren Rand der Seite Active Directory-Konfiguration und -Verwaltung auf Einstellungen überprüfen klicken. Anschließend können Sie das Problem anhand 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 statt des NetBIOS-Namens verwenden.

2. Wenn Sie ein lokales iDRAC6-Benutzerkonto besitzen, melden Sie sich mit Ihren lokalen Anmeldeinformationen am iDRAC6 an.

   Wenn Sie angemeldet sind:

   a. Stellen Sie sicher, dass das Kästchen **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 richtig ist.

   c. Stellen Sie sicher, dass Sie das richtige Stamm-CA-Zertifikat des Active Directory auf das 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 den Namen in Ihrem Active Directory übereinstimmen.

      Wenn Sie mit dem erweiterten Schema arbeiten, prüfen Sie, ob der **Gruppenname** und **Gruppendomänenname** mit den Namen in Ihrem Active Directory übereinstimmen.

3. Überprüfen Sie, ob die iDRAC6-Gültigkeitsdauer die der SSL-Zertifikate der Domain Controller nicht überschreitet.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Smart Card-Authentifizierung konfigurieren

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Der iDRAC 6 unterstützt die Funktion der Zweifaktor-Authentifizierung (TFA), wenn die **Smart Card-Anmeldung** aktiviert ist.

Für herkömmliche Authentifizierungsschemata werden der Benutzername und das Kennwort zum Authentifizieren von Benutzern verwendet. Diese Option bietet nur eine minimale Stufe der Sicherheit.

Bei der TFA wird andererseits eine höhere Sicherheitsstufe geboten, indem Benutzer zwei Faktoren der Authentifizierung gewährleisten, und zwar mit dem, 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 z. B. ein Kennwort oder eine PIN.

Für die Zweifaktor-Authentifizierung ist es erforderlich, dass Benutzer ihre Identität durch die Angabe *beider* Faktoren bestätigen.

Smart Card-Anmeldung am iDRAC 6 konfigurieren

Wechseln Sie zum Aktivieren der iDRAC 6-Funktion Smart Card-Anmeldung über die webbasierte Schnittstelle zu **Remote-Zugriff**→ **Konfiguration**→ **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, wie z. B. Telnet, SSH, serielle, 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 iDRAC 6-Administratoren, die Einstellung **Mit Remote-Racadm aktivieren** nur zu verwenden, um auf die webbasierte iDRAC 6-Schnittstelle zum Ausführen von Scripts mittels der Remote-RACADM-Befehle zuzugreifen. Wenn es für einen Administrator nicht erforderlich ist, Remote-RACADM zu verwenden, empfiehlt Dell, die Einstellung **Aktiviert** für die Smart Card-Anmeldung zu wählen. Stellen Sie vor der Aktivierung der **Smart Card -Anmeldung** ebenfalls sicher, dass die Konfiguration des lokalen iDRAC 6-Benutzers und/oder die Konfiguration des Active Directory abgeschlossen wurden.

- Smart Card-Konfiguration **deaktivieren** (Standardeinstellung). Diese Auswahloption deaktiviert die TFA-Smart Card-Anmeldefunktion, und Sie werden bei der nächsten Anmeldung an der iDRAC 6-GUI aufgefordert, einen Microsoft® Active Directory®- oder lokalen Anmelde-Benutzernamen bzw. -Kennwort einzugeben, die als Standard-Anmeldeaufforderung von der Webschnittstelle angezeigt werden.
- **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 iDRAC 6-Benutzer für Smart Card- Anmeldung konfigurieren

Sie können die lokalen iDRAC 6-Benutzer zum Anmelden am iDRAC 6 mittels Smart Card konfigurieren. Wechseln Sie zu **Remote-Zugriff**→ **Konfiguration**→ **Benutzer**.

Bevor sich der Benutzer jedoch mittels der Smart Card am iDRAC 6 anmelden kann, muss das Smart Card-Zertifikat des Benutzers sowie das Zertifikat der vertrauenswürdigen Zertifizierungsstelle (CA) auf den iDRAC 6 hochgeladen werden.

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 iDRAC 6 hochgeladen werden. Die vertrauenswürdige Zertifizierungsstelle, die die Smart Card-Benutzerzertifikate ausstellt, sollte auch das CA-Zertifikat in eine Datei mit Base64-kodiertem Format exportieren. Laden Sie diese Datei als Datei der vertrauenswürdigen CA 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 iDRAC 6 darauf, dass der im iDRAC 6 konfigurierte Benutzername in Bezug auf Groß- bzw. Kleinschreibung von Buchstaben identisch mit dem Benutzerprinzipalnamen (UPN) im Smart Card-Zertifikat ist.

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 Active Directory-Benutzer so zu konfigurieren, dass sie sich mittels Smart Card am iDRAC 6 anmelden müssen, muss der iDRAC 6-Administrator den DNS-Server konfigurieren, das Active Directory-CA-Zertifikat auf den iDRAC 6 hochladen und die Active Directory-Anmeldung aktivieren. Weitere Informationen zum Setup von Active Directory-Benutzern finden Sie unter "iDRAC6 mit Microsoft Active Directory verwenden".

ANMERKUNG: Wenn der Smart Card-Benutzer im Active Directory vorhanden ist, werden sowohl ein Active Directory-Kennwort als auch eine SC-PIN benötigt. In zukünftigen Versionen ist das Active Directory-Kennwort eventuell nicht mehr erforderlich.

Active Directory kann über **Remote-Zugriff**→ **Konfiguration**→ **Active Directory** konfiguriert werden.

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 **Konfiguration** und dann auf **Smart Card**.
3. Konfigurieren Sie die Smart Card-Anmeldungseinstellungen.

   Tabelle 8-1 enthält Informationen über die Einstellungen der Seite **Smart Card**.
4. Klicken Sie auf **Änderungen übernehmen**.

Tabelle 8-1. Smart Card-Einstellungen

Einstellung	Beschreibung
Konfigurieren Sie die Smart Card-Anmeldung.	• Deaktiviert - Deaktiviert die Smart Card-Anmeldung. Bei nachfolgenden Anmeldungen über die grafische Benutzeroberfläche (GUI) wird die reguläre Anmeldungsseite angezeigt. Alle bandexternen Befehlszeilenschnittstellen 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. • Aktiviert mit Remote Racadm - 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 iDRAC 6-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 steht nur Benutzern der Active Directory-Anmeldung zur Verfügung. Wählen Sie diese Option aus, wenn der iDRAC 6 die Zertifikatsperrliste (CRL) auf Widerrufung des Smart Card-Zertifikats des Benutzers prüfen soll. Der Benutzer wird nicht in der Lage sein, sich anzumelden, wenn folgende Bedingungen erfüllt werden: • Das Benutzerzertifikat wird in der CRL-Datei als widerrufen aufgeführt. • Der iDRAC 6 ist nicht in der Lage, mit dem CRL-Verteilungsserver zu kommunizieren. • Der iDRAC 6 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 **Konfiguration**→ **Netzwerk** korrekt konfigurieren.

Anmeldung am iDRAC 6 über die Smart Card

Die iDRAC 6-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 iDRAC 6-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 auf die iDRAC 6-Website über https zu.

https://<*IP-Adresse*>

Wenn die Standard-HTTPS-Portnummer (Port 443) geändert wurde, geben Sie folgendes ein:

https://<*IP-Adresse*>:<*Portnummer*>

wobei <*IP-Adresse*> die IP-Adresse des iDRAC 6 und <*Portnummer*> die Nummer des HTTPS-Ports ist.

Die iDRAC 6-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 iDRAC 6 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 iDRAC 6 Sie zum Eingeben 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 iDRAC 6, 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 iDRAC 6 angemeldet.

Unter Verwendung der Active Directory-Smart Card-Authentifizierung am iDRAC 6 anmelden

1. Melden Sie sich am iDRAC 6 über https an.

   https://<*IP-Adresse*>

   Wenn die Standard-HTTPS-Portnummer (Port 443) geändert wurde, geben Sie folgendes ein:

   https://<*IP-Adresse*>:<*Portnummer*>

   wobei <*IP-Adresse*> die IP-Adresse des iDRAC 6 und <*Portnummer*> die Nummer des HTTPS-Ports ist.

   Die iDRAC 6-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 eingeblendet.

3. Geben Sie die PIN ein, und klicken Sie auf **OK**.

4. Geben Sie zum Authentifizieren der Smart Card das Active Directory- Benutzerkennwort ein und klicken Sie auf **OK**.

   Sie sind jetzt über Ihre im Active Directory festgelegten Anmeldeinformationen am iDRAC 6 angemeldet.

ANMERKUNG: Wenn der Smart Card-Benutzer im Active Directory vorhanden ist, werden sowohl ein Active Directory-Kennwort als auch eine SC-PIN benötigt. In zukünftigen Versionen ist das Active Directory-Kennwort eventuell nicht mehr erforderlich.

Fehler bei der Smart Card-Anmeldung am iDRAC 6 beheben

Wenden Sie die folgenden Tipps an, die beim Debuggen einer Smart Card behilflich sein können, auf die kein Zugriff besteht.

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 eine beschränkte Anzahl von Cryptographic Service Providers (CSP) für die Smart Card.

Tipp: Sie können generell überprüfen, ob die Smart Card-CSPs auf einem bestimmten Client vorhanden sind, indem Sie die Smart Card 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 nach, ob die Smart Card aufgrund übermäßiger Versuche mit einer falschen PIN gesperrt worden ist. In solchen Fällen kann Ihnen der Aussteller der Smart Card in der Organisation dabei behilflich sein, eine neue Smart Card zu erhalten.

Anmeldung am lokalen iDRAC 6 nicht möglich.

Wenn ein lokaler iDRAC 6-Benutzer nicht in der Lage ist, sich anzumelden, überprüfen Sie, ob der Benutzername und die auf den iDRAC 6 hochgeladenen Benutzerzertifikate abgelaufen sind. Die iDRAC 6-Ablaufverfolgungsprotokolle enthalten eventuell wichtige Protokollmeldungen, die sich auf die Fehler beziehen. Hierbei ist jedoch zu beachten, dass Fehlermeldungen aus Sicherheitsgründen manchmal absichtlich unklar formuliert werden.

Anmeldung am iDRAC 6 als Active Directory-Benutzer nicht möglich.

Wenn Sie sich als Active Directory-Benutzer nicht am iDRAC 6 anmelden können, versuchen Sie, sich am iDRAC 6 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 iDRAC 6-Ablaufverfolgungsprotokoll sollte im Falle eines CRL-Fehlers wichtige Meldungen enthalten.

Sie haben auch die Möglichkeit, die Smart Card-Anmeldung über den lokalen racadm zu deaktivieren, indem Sie den folgenden Befehl verwenden:

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

GUI-Konsolenumleitung verwenden

Integrierter Dell™ Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

Dieser Abschnitt enthält Informationen über die Anwendung 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 eine Konsolenumleitungssitzung bereits von der Management Station zum iDRAC6 geöffnet ist, führt der Versuch, eine neue Sitzung von der gleichen Management Station zum iDRAC6 zu öffnen, dazu, dass die vorhandene Sitzung aktiv wird. Es wird keine neue Sitzung generiert.

ANMERKUNG: Es können mehrere Konsolenumleitungssitzungen von einer einzelnen Management Station zu mehreren iDRAC6-Karten gleichzeitig geöffnet werden.

Die Seite **Konsolenumleitung** ermöglicht Ihnen, das Remote-System zu verwalten, indem Sie Tastatur, Video und Maus auf Ihrer lokalen Verwaltungsstation verwenden, um die entsprechenden Geräte auf einem verwalteten Remote-Server zu steuern. Diese Funktion kann in Verbindung mit der Virtuellen Datenträger-Funktion 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 Konsole des verwalteten Servers gleichzeitig an.
- Es kann nur eine Sitzung zu einem Remote-Server (iDRAC6) von der gleichen Client-Konsole (Management Station) geöffnet werden. Es sind jedoch mehrere Sitzungen zu mehreren Remote-Servern vom gleichen Client 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 iDRAC ist eine Sitzung mit Komplettzugriff. Wenn ein zweiter Benutzer eine Konsolenumleitung anfordert, wird der erste Benutzer benachrichtigt und erhält die Optionen ablehnen, **schreibgeschützt zulassen** oder **berechtigen**. Der zweite Benutzer wird benachrichtigt, dass ein anderer Benutzer die Steuerung übernommen hat. Wenn der erste Benutzer dann nicht innerhalb von 30 Sekunden antwortet, wird für den zweiten Benutzer automatisch der Zugriff abgelehnt.

Sämtliche **schreibgeschützten** Sitzungen enden automatisch, wenn die letzte Sitzung mit Komplettzugriff beendet wurde.

Management Station konfigurieren

Zur Verwendung der Konsolenumleitung auf der Management Station führen Sie die folgenden Verfahren aus:

1. Installieren und konfigurieren Sie einen unterstützten Internet-Browser. Weitere Informationen finden Sie in den folgenden Abschnitten:
   - "Unterstützte Webbrowser"
   - "Einen unterstützten Web-Browser konfigurieren"

   ANMERKUNG: Es muss die Java Run Time Environment auf der Management Station installiert sein, damit die Konsolenumleitung funktioniert.

2. Wenn Sie Internet Explorer verwenden, stellen Sie wie folgt sicher, dass beim Browser das Herunterladen von verschlüsselten Inhalten aktiviert ist:
   - GehenSie zu den Optionen oder Einstellungen von Internet Explorer Options, und wählen Sie **Extras**→ **Internetoptionen**→ **Erweitert**.
   - Gehen Sie zu **Sicherheit** und wählen Sie diese Option ab:

     Verschlüsselte Seiten nicht auf der Festplatte speichern

3. Es wird empfohlen, die Bildschirmauflösung auf 1280x1024 Pixel oder höher einzustellen.

ANMERKUNG: Wenn eine aktive Konsolenumleitungssitzung vorhanden ist und ein Monitor mit niedriger Auflösung an der iDRAC KVM angeschlossen wird, wird die Serverkonsolenauflösung eventuell zurückgesetzt, wenn der Server auf der lokalen Konsole ausgewählt wird. Wenn der Server ein Linux-Betriebssystem ausführt, kann eine X11-Konsole auf dem lokalen Monitor eventuell nicht angezeigt werden. Durch Drücken auf <Strg><Alt><F1> auf der iDRAC KVM wird Linux auf eine Textkonsole geschaltet.

ANMERKUNG: Gelegentlich stoßen Sie möglicherweise auf den folgenden Java Script-Kompilierungsfehler: "Expected: ;". Um dieses Problem zu beheben, ändern Sie die Netzwerkeinstellungen zur Verwendung der direkten Verbindung in JavaWebStart: "Edit->Preferences->General->Network Settings" (Bearbeiten->Einstellungen->Allgemein->Netzwerkeinstellungen), und wählen Sie "Direct Connection" (Direktverbindung) anstelle von "Use browser settings" (Browser-Einstellungen verwenden).

Konfiguration der Konsolenumleitung auf der iDRAC6-Webschnittstelle

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 9-1 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 9-2.

Tabelle 9-1. Konfigurationseigenschaften der Konsolenumleitung

Eigenschaft	Beschreibung
Aktiviert	Klicken Sie um die Konsolenumleitung zu aktivieren oder zu deaktivieren. **Markiert** zeigt an, dass die Konsolenumleitung aktiviert ist. **Nicht markiert** zeigt an, dass die Konsolenumleitung deaktiviert ist. Die Standardeinstellung ist **aktiviert**.
Max. Sitzungen	Zeigt die Anzahl der maximal möglichen Konsolenumleitungssitzungen an - 1 bis 4. Verwenden Sie das Drop-Down-Menü, um die maximal zulässigen Konsolenumleitungs-Sitzungen zu ändern. Die Standardeinstellung ist **2.**
Aktive Sitzungen	Zeigt die Anzahl der Sitzungen Aktiver Konsolen an. Dieses Feld ist schreibgeschützt.
Remote-Präsenz-Port	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.**
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.**
Lokales Servervideo aktiviert	Die Markierung weist darauf hin, dass die Ausgabe an den iDRAC KVM-Monitor während der Konsolenumleitung deaktiviert wird. Hierdurch wird sichergestellt, dass die unter Verwendung der **Konsolenumleitung** ausgeführten Tasks auf dem lokalen Monitor des verwalteten Servers nicht sichtbar sind.

ANMERKUNG: Für Informationen zur Verwendung des virtuellen Datenträgers mit Konsolenumleitung siehe Virtuellen Datenträger konfigurieren und verwenden.

Die Schaltflächen in Tabelle 9-2 sind auf der Seite **Konsole/Datenträgerkonfiguration** verfügbar.

Tabelle 9-2. Schaltflächen der Konfigurationsseite

Schaltfläche	Definition
Drucken	Druckt die Seite
Aktualisieren	Lädt die Seite **Konfiguration** neu.
Änderungen 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 Verwaltungsstation aus gesteuert werden.

Führen Sie folgende Schritte aus, um auf der Webschnittstelle eine Konsolenumleitungssitzung zu öffnen:

1. Klicken Sie auf **System**→ **Konsole/Datenträger**→ **Konfiguration**.

2. Verwenden Sie die Information in Tabelle 9-3, um sicherzustellen, dass eine Konsolenumleitungssitzung verfügbar ist.

   Sollten Sie einige der angezeigten Eigenschaftswerte neu konfigurieren wollen, finden Sie entsprechende Informationen unter Konfiguration der Konsolenumleitung auf der iDRAC6-Webschnittstelle.

Tabelle 9-3. Console Redirection

Eigenschaft	Beschreibung
Aktivierte Konsolenumleitung	Ja/Nein (ausgewählt\abgewählt)
Videoverschlüsselung aktiviert	Ja/Nein (ausgewählt\abgewählt)
Max. Sitzungen	Zeigt die maximale Anzahl unterstützter Konsolenumleitungssitzungen an
Aktive Sitzungen	Zeigt die aktuelle Anzahl aktiver Konsolenumleitungssitzungen an
Lokales Servervideo aktiviert	Nicht markiert, wenn die lokale Konsole nicht deaktiviert wurde. Wenn ausgewählt, ist kein Zugriff auf die Konsole möglich, wenn die lokale iDRAC KVM-Verbindung gerade im Remote-Zugriff verwendet wird.
Remote-Präsenz-Port	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: Für Informationen zur Verwendung des virtuellen Datenträgers mit Konsolenumleitung siehe Virtuellen Datenträger konfigurieren und verwenden.

Die Schaltflächen in Tabelle 9-4 sind auf der Seite **Konsolenumleitung und virtueller Datenträger** verfügbar.

Tabelle 9-4. Schaltflächen der Seite 'Konsolenumleitung und virtueller Datenträger'

Schaltfläche	Definition
Aktualisieren	Lädt die Seite **Konsolenumleitungskonfiguration** neu
Viewer starten	Öffnet eine Konsolenumleitungssitzung auf dem Remote-Ziel-System.
Drucken	Druckt die Seite **Konsolenumleitungskonfiguration**

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 innerhalb drei Minuten durch diese Dialogfelder wechseln. Ansonsten werden Sie aufgefordert, die Anwendung erneut zu starten.

   ANMERKUNG: Wenn in den folgenden Schritten ein Fenster oder mehrere Fenster zur **Sicherheitswarnung** eingeblendet werden, lesen Sie die Informationen im jeweiligen Fenster, und klicken Sie auf **Ja**, um fortzufahren.

   Die Verwaltungsstation wird mit dem iDRAC6 verbunden und der Desktop des Remote-Systems wird in der iDRAC KVM Viewer-Anwendung angezeigt.

4. Zwei Mauszeiger erscheinen im Viewer-Fenster: einer für das Remote- System und einer für das lokale System. Sie können zu einem einzelnen Mauszeiger wechseln, indem Sie im iDRAC KVM-Menü unter **Extras** die Option **Single Cursor** (Ein Cursor) auswählen.

Video Viewer verwenden

Der Video Viewer ist eine Benutzerschnittstelle zwischen der Verwaltungsstation und dem verwalteten Server, wodurch der Desktop des verwalteten Servers sichtbar wird und die Maus-und Tastaturfunktionen von der Verwaltungsstation aus gesteuert werden können. Wenn Sie eine Verbindung zum Remote-System herstellen, wird der Video Viewer in einem separaten Fenster gestartet.

ANMERKUNG: Wird der Remote-Server ausgeschaltet, wird die Nachricht **Kein Signal** angezeigt.

Der Video Viewer bietet die Möglichkeit verschiedener Steuerungseinsellungen wie Maussynchronisation, Snapshots, Tastaturmakros und Zugriff auf den virtuellen Datenträger. Um weitere Informationen zu diesen Funktionen zu erhalten, wählen Sie **System**→ **Konsole/Datenträger** und klicken Sie **auf der Seite Konsolenumleitung und virtueller Datenträger** auf **Hilfe**.

Wenn Sie eine Konsolenumleitungssitzung starten und der Video Viewer angezeigt wird, müssen Sie möglicherweise die Mauszeiger synchronisieren.

Lokales Servervideo deaktivieren oder aktivieren

Sie können den iDRAC6 so konfigurieren, dass iDRAC KVM-Verbindungen über die iDRAC6-Webschnittstelle unzulässig 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 iDRAC KVM angeschlossen sind, weiterhin aktiviert.

Wenden Sie zum Deaktivieren oder Aktivieren der lokalen Konsole das folgende Verfahren an:

1. Öffnen Sie auf Ihrer Verwaltungsstation einen unterstützten Webbrowser, und melden Sie sich am iDRAC6 an. Weitere Informationen finden Sie unter "Zugriff auf die Webschnittstelle".
2. Klicken Sie auf **System**→ **Konsole/Datenträger**→ **Konfiguration**.
3. Um das lokale Video auf dem Server zu deaktivieren (ausschalten), wählen Sie das Kontrollkästchen **Lokales Servervideo aktiviert** auf der Seite **Konfiguration** ab, und klicken Sie dann auf **Anwenden**. Der Standardwert lautet 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 (einschalten), wählen Sie das Kontrollkästchen **Lokales Servervideo aktiviert** auf der Seite **Konfiguration** aus, und klicken Sie dann auf **Anwenden**.

Häufig gestellte Fragen

Tabelle 9-5 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 9-5. Konsolenumleitung verwenden: Häufig gestellte Fragen

Frage	Antwort
Kann eine neue Remote-Konsolen-Videositzung gestartet werden, wenn das lokale Video auf dem Server ausgeschaltet ist?	Ja.
Warum dauert es 15 Sekunden, um das lokale Video auf dem Server auszuschalten, nachdem eine Aufforderung zum Ausschalten des lokalen Vidoes erteilt wurde?	Hierdurch wird einem lokalen Benutzer die Gelegenheit gegeben, Maßnahmen durchzuführen, bevor das Video ausgeschaltet wird.
Gibt es beim Einschalten des lokalen Videos eine Zeitverzögerung?	Nein. Sobald der iDRAC6 eine Aufforderung zum **EIN**schalten des lokalen Videos erhält, wird das Video sofort eingeschaltet.
Kann der lokale Benutzer das Video auch ausschalten?	Wenn die lokale Konsole deaktiviert ist, kann der lokale Benutzer das Video nicht einschalten.
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 unabhängig von der Remote-Konsolensitzung.
Welche Berechtigungen sind für einen iDRAC6-Benutzer erforderlich, um das lokale Server-Video 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 iDRAC-Webschnittstelle angezeigt. Der RACADM-CLI-Befehl **racadm getconfig -g cfgRacTuning** zeigt den Status im Objekt **cfgRacTuneLocalServerVideo** an.
Ich kann vom Konsolenumleitungsfenster aus 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 iDRAC KVM-Client zu verwenden.
Das Konsolenfenster ist entstellt.	Für den Konsolen-Viewer auf Linux ist ein UTF-8-Zeichensatz erforderlich. Überprüfen Sie Ihr Gebietsschema und setzen Sie den Zeichensatz ggf. zurück.
Warum synchronisiert die Maus nicht unter der Linux-Textkonsole?	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 Maussynchronisation.	Stellen Sie sicher, dass vor dem Beginn einer Konsolenumleitungssitzung die richtige Maus für das Betriebssystem ausgewählt ist. Sorgen Sie dafür, dass die Option **Ein Cursor** unter **Extras** im iDRAC KVM-Menü auf dem iDRAC KVM-Client ausgewählt ist.
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 auf 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?	Wenn über den iDRAC6 auf die Num-Taste zugegriffen wird, stimmt die Num-Taste auf der Management Station nicht unbedingt mit dem Zustand der Num-Taste auf dem Remote-Server überein. Der Zustand der Num-Taste hängt von der Einstellung auf dem Remote-Server ab, wenn die Remote-Sitzung verbunden wird, unabhängig vom Zustand der Num-Taste auf der Management Station.
Warum werden mehrere Session Viewer-Fenster eingeblendet, wenn ich vom lokalen Host aus eine 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 empfiehlt Dell eine 5 MB/s-Verbindung. Eine 1 MB/s-Verbindung ist zum Erzielen der Mindestleistung vorgeschrieben.
Was sind die Mindestsystemanforderungen für meine Management Station zum Ausführen der Konsolenumleitung?	Die Verwaltungsstation erfordert einen Intel® Pentium® III 500-MHz-Prozessor mit mindestens 256 MB RAM.
Warum wird die Meldung **Kein Signal** im iDRAC KVM Video Viewer angezeigt?	Sie sehen diese Meldung möglicherweise, da das iDRAC Virtual KVM-Plugin nicht das Remote-Server-Desktop-Video 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 ein Parameter, der für die Video-Erfassung erforderlich ist, sich außerhalb des Bereichs befindet, für den der iDRAC das Video erfassen kann. Wenn Parameter wie z. B. Auflösung oder Bildwiederholfrequenz zu hoch sind, kann dieser Zustand verursacht werden. Normalerweise wird der Maximalbereich der Parameter von physischen Begrenzungen, wie z. B. Videospeichergröße oder Bandbreite, bestimmt.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Integrierter Dell Remote Access Controller 6 (iDRAC 6) - Version 1.0 Benutzerhandbuch

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.

Irrtümer und technische Änderungen vorbehalten.
© 2009 Dell Inc. Alle Rechte vorbehalten.

Eine Vervielfältigung oder Wiedergabe dieser Materialien in jeglicher Weise ohne vorherige schriftliche Genehmigung von Dell Inc. ist strengstens untersagt.

In diesem Text verwendete Marken: *Dell*, das *DELL*-Logo, *Dell OpenManage* und *PowerEdge* sind Marken von Dell Inc.; *Microsoft*, *Windows*, *Windows Server*, Windows Vista und *Active Directory* sind entweder Marken oder eingetragene Marken von Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern; *Red Hat* und *Linux* sind eingetragene Marken von Red Hat, Inc. in den Vereinigten Staaten und anderen Ländern; *SUSE* ist eine eingetragene Marken von Novell Corporation. *Intel* und *Pentium* sind eingetragene Marken von Intel Corporation in den Vereinigten Staaten und anderen Ländern; *UNIX* ist eine eingetragene Marke von The Open Group in den Vereinigten Staaten und andern Ländern; VMware ist eine eingetragene Marke von VMware, Inc. in den Vereinigten Staaten und/oder anderen Gerichtsbarkeiten.

Copyright 1998-2006 The OpenLDAP Foundation. Alle Rechte vorbehalten. Der Weitervertrieb und die Nutzung in Quell- und Binärform ist mit oder ohne Änderungen gestattet, sofern durch die öffentliche Lizenz von OpenLDAP autorisiert. Eine Kopie dieser Lizenz ist in der Datei LICENSE im Verzeichnis der obersten Ebene der Verteilung erhältlich oder auch unter **www.OpenLDAP.org/license.html**. OpenLDAP ist eine eingetragene Marke der OpenLDAP Foundation. Individuelle Dateien und/oder beigetragene Pakete können durch andere Parteien urheberrechtlich geschützt sein und zusätzlichen Einschränkungen unterliegen. Diese Arbeit wird vom LDAP v3.3-Vertrieb der University of Michigan abgeleitet. Diese Arbeit enthält außerdem Materialien, die von öffentlichen Quellen stammen. Informationen zu OpenLDAP stehen unter **www.openldap.org/** zur Verfügung. Teil-Copyright 1998-2004 Kurt D. Zeilenga. Teil-Copyright 1998-2004 Net Boolean Incorporated. Teil-Copyright 2001-2004 IBM Corporation. Alle Rechte vorbehalten. Der Weitervertrieb und die Nutzung in Quell- und Binärform ist mit oder ohne Änderungen gestattet, sofern durch die öffentliche Lizenz von OpenLDAP autorisiert. Teil-Copyright 1999-2003 Howard Y.H. Chu. Teil-Copyright 1999-2003 Symas Corporation. Teil-Copyright 1998-2003 Hallvard B. Furuseth. Alle Rechte vorbehalten. Der Weitervertrieb und die Nutzung in Quell- und Binärform ist mit oder ohne Änderungen gestattet, sofern dieser Hinweis beibehalten wird. Die Namen der Inhaber des Urheberrechts dürfen nicht verwendet werden, um von dieser Software abgeleitete Produkte ohne vorherige schriftliche Genehmigung zu indossieren oder zu fördern. Diese Software wird ohne Mängelgewähr und ohne ausdrückliche oder stillschweigende Garantie zur Verfügung gestellt. Teil-Copyright (c) 1992-1996 Regents der University of Michigan. Alle Rechte vorbehalten. Der Weitervertrieb und die Nutzung in Quell- und Binärform ist gestattet, sofern dieser Hinweis beibehalten wird, und sofern anerkannt wird, dass die entsprechenden Materialien von der University of Michigan in Ann Arbor zur Verfügung gestellt wurden. Der Name der Universität darf ohne vorherige schriftliche Genehmigung nicht verwendet werden, um von dieser Software abgeleitete Produkte zu unterstützen oder zu fördern. Diese Software wird ohne Mängelgewähr und ohne ausdrückliche oder stillschweigende Garantie zur Verfügung gestellt. Alle anderen in dieser Dokumentation genannten Marken und Handelsbezeichnungen sind Eigentum der entsprechenden Hersteller und Firmen. Dell Inc. erhebt keinen Anspruch auf Markenzeichen und Handelsbezeichnungen mit Ausnahme der eigenen.

März 2009 Rev. A00

Zurück zum Inhaltsverzeichnis