Controller-Firmware Version 1.4 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.**

Februar 2009 Rev. A00

Zurück zum Inhaltsverzeichnis

Übersicht der RACADM-Unterbefehle

Controller-Firmware Version 1.4 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 "benannten" 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	Typ	Konsolen
root	192.168.0.10	Telnet	Virtuelle KVM

- `racadm getssninfo -A`

  `"root" 192.168.174.19 "Telnet" "NONE"`

- `racadm getssninfo -A -u *`

  `"root" "192.168.174.19" "Telnet" "NONE"`

- `"bob" "192.168.174.19" "GUI" "NONE"`

---

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`

  `"Systeminformationen:" "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "EIN"`

- `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

Don Dez 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.

ANMERKUNG: 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.

ANMERKUNG: 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 192.168.157.103
```

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:   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

---

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 192.168.157.103: 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 <Typ> [-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

Controller-Firmware Version 1.4 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 Lesen)

Zulässige Werte

Zeichenkette mit bis zu 63 ASCII-Zeichen.

Standardeinstellung

Integrierter Dell Remote Access Controller

Beschreibung

Eine Textzeichenkette, die das Produkt identifiziert.

idRacDescriptionInfo (Nur Lesen)

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 Lesen)

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 muss.

cfgDNSDomainName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette von 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 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

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:

```
Warning: Session no longer valid, may have timed out (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:

```
Warning: Session no longer valid, may have timed out (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 dieAnschlussnummer 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

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.

---

cfgActiveDirectory

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

cfgADRacDomain (Lesen/Schreiben)

Zulässige Werte

Eine beliebige druckbare Textzeichenkette ohne Leerraum. 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 Leerraum. 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-Authentifizierungsauffoerdungen 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

Controller-Firmware Version 1.4 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_grouppprivilege (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
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

/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 dieAnschlussnummer 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

Controller-Firmware Version 1.4 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 Servernummer.
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

Controller-Firmware Version 1.4 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
- Einfache Anmeldung über die CMC-Webschnittstelle - Sobald die Anmeldeinformationen vom CMC akzeptiert worden sind, können Benutzer auf beliebige iDRACs zugreifen, ohne sich noch einmal anmelden zu müssen

  ANMERKUNG: Wenn während des Vorgangs der einfachen Anmeldung eine Warnmeldung eingeblendet wird, muss diese innerhalb von 20 Sekunden deaktiviert werden, da die einfache Anmeldung sonst fehlschlägt.

- One-to-Many-Firmware-Aktualisierung - Ermöglicht die vom Benutzer konfigurierbare Aktualisierung von mehr als einem iDRAC unter Verwendung der CMC-GUI und der Befehlszeile
- 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 für höhere Sicherheit verwendet
- Beschränkung der Anmeldefehlschläge pro IP-Adresse, mit Anmeldeblockierung der IP-Adresse bei Überschreitung der Grenze
- Eingeschränkter IP-Adressenbereich für Clients, die eine Verbindung zum iDRAC herstellen

---

Verbesserungen der iDRAC-Firmware

Die folgenden Verbesserungen wurden an der iDRAC-Firmware vorgenommen:

- Bedeutende Verbesserungen der Leistung beim Einsehen des Active Directory
- Verbesserte Reaktionsfähigkeit des TCP-IP-Netzwerkbetriebs-Stacks
- Verbesserte Funktionszustandsschnittstelle zwischen iDRAC und CMC
- Sicherheitsverbesserungen unter Verwendung von Analyse-Tools von Fremdherstellern

---

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*, welches 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 10 (Gold) (x86_64)
VMware	ESX(i) 3.5 U2 oder höher

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-Zugriffsverbindungen

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
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 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 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 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 / an der Dokumentation wieder oder enthalten fortgeschrittenes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC konfigurieren

Controller-Firmware Version 1.4 Benutzerhandbuch

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

Bevor Sie beginnen

Legen Sie vor der Konfiguration des iDRAC folgende Artikel zurecht:

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

Schnittstellen zur Konfiguration des iDRAC

Sie können das 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 cfgRacTuneLocalConfigDisable (Lesen/Schreiben)) oder von der GUI (siehe Lokalen Konfigurationszugriff aktivieren oder deaktivieren) deaktiviert werden.

ANMERKUNG: 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 Managed Server zu starten, anzuhalten oder zurückzusetzen.
Gehäuse-LCD-Bedienfeld	Das LCD-Bedienfeld des Gehäuses, welches das 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 Managed 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 das im iDRAC integrierte Serververwaltungs-Befehlszeilenprotokoll (Server Management-Command Line Protocol, SM-CLP) der verteilten Management Task Force (Distributed Management Task Force, DMTF). 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 das iDRAC, um mit anderen integrierten Systemen und Verwaltungsanwendungen zu kommunizieren. Sie können die iDRAC-Webschnittstellen-, SM-CLP- oder RACADM-Befehle zur Konfiguration von IPMI-Plattformereignisfiltern (PEFs) und Plattformereignis-Traps (PETs) verwenden. PEFs bewirken, dass das iDRAC auswählbare Maßnahmen ausführt (z. B. den Neustart des verwalteten Servers), wenn er einen entsprechenden Zustand feststellt. PETs weisen das iDRAC an, E-Mail- oder IPMI-Warnungen zu senden, wenn es 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 es 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 cfgRacTuneLocalConfigDisable (Lesen/Schreiben)) 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 das 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 das lokale iDRAC einrichten. Das 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

ANMERKUNG: Wenn iDRAC in einer Active Directory-Umgebung verwendet wird, müssen Sie sicherstellen, dass Ihre Benutzernamen mit der in Ihrer Umgebung vorherrschenden Active Directory-Benennungsregel übereinstimmen.

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 das 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 - siehe 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.

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 Managed 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.

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

Die Konfiguration der Funktion FlexAddress wird mithilfe der CMC-Webschnittstelle ausgeführt. Weitere Informationen zur Funktion FlexAddress und deren Konfiguration finden Sie im *Benutzerhandbuch 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.

Aktualiseren der iDRAC-Firmware

Durch das Aktualisieren der iDRAC-Firmware wird ein neues Firmware-Image im Flash-Speicher des iDRAC installiert. iDRAC 1.4 unterstützt One-to-Many-Firmware-Aktualisierungen über den CMC im Normalmodus (nicht nur bei Fehlern). 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 (diese Methode muss verwendet werden, wenn die iDRAC-Firmware beschädigt ist, oder um One-to-Many-Aktualisierungen mit CMC 2.0 oder höherer Firmware vorzunehmen; weitere Informationen befinden sich im *Benutzerhandbuch zur CMC -Firmware*.)

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 muss zum Aktualisieren der Firmware verwendet werden, wenn der CMC ermittelt, 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.

Die CMC-Webschnittstelle (CMC 2.0 oder höher) bietet auch eine iDRAC-Firmware-Aktualisierungskapazität für One-to-Many/Out-of-Band, die jederzeit eingesetzt werden kann.

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.

VORSICHT: Wenn Sie für den 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. Verwenden Sie diese Option nur dann, wenn Sie von einem Kundendienstberater des Dell Support ausdrücklich dazu aufgefordert wurden, da hierdurch sämtliche Ihrer 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.

   a. Geben Sie den folgenden Befehl ein:

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

   b. 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 (Primärer Schlüsselfingerabdruck): 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
      ```

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

   c. 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?

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


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

      Ihre Entscheidung?)
      ```

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

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

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

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

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

   Der öffentliche Schlüssel muss nur einmal importiert und bestätigt werden.

4. Laden Sie sich das erforderliche Paket (z.B. das Linux-DUP oder 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-Sicherheit-öffentlicher Schlüssel.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: unchanged: 1

   (gpg: Schlüssel 23B66A9D: "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>" not changed (nicht verändert)
   gpg: Gesamtzahl verarbeitet: 1
   gpg: unverändert: 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 den folgenden Befehl ein:

      ```
      fpr
      trust
      ```

   c. Geben Sie 5 <Eingabe> ein, um `I trust ultimately` (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>"

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

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

   ```
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg: There is no indication that the signature belongs to the owner.
   Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D

   (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 zum Entfernen/Löschen aller *alter* Webseiten, die eventuell im System gespeichert sind, gelöscht werden.

Internet Explorer

1. Starten Sie 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).

---

iDRAC zur Verwendung mit IT Assistant konfigurieren

Dell™ OpenManage™ IT Assistant wird in vorkonfiguriertem Zustand zur Ermittlung verwalteter Geräte geliefert, die die Anforderungen für SNMP-Version 1 und -Version 2c (Einfaches Netzwerkverwaltungsprotokoll) und IPMI-Version 2.0 (Intelligente Platform-Managementschnittstelle) erfüllen.

iDRAC erfüllt die Anforderungen für IPMI-Version 2.0. In diesem Abschnitt werden die Schritte zum Konfigurieren eines iDRACs zur Ermittlung und Überwachung durch IT Assistant beschrieben. Sie können dies auf zwei verschiedene Arten ausführen: durch das iDRAC-Konfigurationsdienstprogramm und durch die grafische Webschnittstelle des iDRAC.

iDRAC-Konfigurationsdienstprogramm zum Aktivieren von Ermittlung und Überwachung verwenden

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

Wenn der Bildschirm **iDRAC-Konfigurationsdienstprogramm** eingeblendet wird, scrollen Sie mit den Pfeiltasten nach unten.

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

ANMERKUNG: Wenden Sie sich an den leitenden Netzwerkadministrator oder CIO, um das Einführen dieser Option zu besprechen, da sie wertvollen zusätzlichen Sicherheitsschutz bietet und standortweit eingesetzt werden muss, um ordnungsgemäß funktionieren zu können.

3. Drücken Sie bei **LAN-Parameter** die Eingabetaste, um den Unterbildschirm aufzurufen. Verwenden Sie zum Navigieren die Nach- oben- und Nach-unten-Tasten.
4. Schalten Sie **LAN-Warnung aktiviert** mit der Leertaste auf **Ein**.
5. Geben Sie die IP-Adresse der Verwaltungsstation unter **Warnungsziel 1** ein.
6. Geben Sie unter Verwendung einer Benennungsregel, die in Ihrem gesamten Datencenter einheitlich befolgt wird, eine Namenszeichenkette unter **iDRAC-Name** ein. Die Standardeinstellung lautet iDRAC- {*Service-Tag-Nummer*}.

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

iDRAC-Webschnittstelle zum Aktivieren von Ermittlung und Überwachung verwenden

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

1. Geben Sie die IP-Adresse des iDRACs in Ihren Browser ein.
2. Melden Sie sich unter Verwendung eines Benutzernamens und Kennworts mit Administratorrechten an.
3. Wählen Sie **iDRAC**→ **Netzwerk/Sicherheit**→ **Netzwerk** aus.
4. Scrollen Sie zu **IPMI-LAN-Einstellungen** herunter.
5. Stellen Sie sicher, dass **IPMI-über-LAN aktivieren** ausgewählt ist.
6. Stellen Sie **Berechtigungen auf Kanalebene** auf **Administrator** ein.
7. Geben Sie, falls verwendet, den **Verschlüsselungsschlüssel** für RMCP+ Ihrer Site ein.
8. Klicken Sie, falls erforderlich, auf **Anwenden**.
9. Navigieren Sie zu **System**→ **Warnungsverwaltung**→ **Plattformereignisse**.
10. Aktivieren Sie **Warnungen** für die **Plattformereignis**-Kategorien, für die Sie Traps einrichten möchten.
11. Klicken Sie auf **Anwenden**, falls Sie Änderungen vorgenommen haben.
12. Klicken Sie auf **Trap-Einstellungen**.
13. Geben Sie die IP-Adresse der Verwaltungsstation im ersten verfügbaren Textfeld für die **Ziel-IP-Adresse** ein.
14. Stellen Sie sicher, dass das **Aktiviert**-Kästchen ausgewählt ist.
15. Klicken Sie auf **Anwenden**, falls Sie Änderungen vorgenommen haben.

Sie können jetzt einen Test-Trap senden, indem Sie auf den **Senden**-Link klicken.

Dell empfiehlt dringend, dass Sie zu Sicherheitszwecken für IPMI-Befehle ein separates Benutzerkonto mit eigenem Benutzernamen, IPMI-über-LAN-Berechtigungen und Kennwort einrichten.

1. Navigieren Sie zu **iDRAC**→ **Netzwerk/Sicherheit**→ **Benutzer**
2. Klicken Sie auf die Nummer eines undefinierten **Benutzers**.
3. Aktivieren Sie im Unterbildschirm den **Benutzer**, und geben Sie einen **Namen** und ein **Kennwort** ein.
4. Stellen Sie sicher, dass **Maximale LAN-Benutzerberechtigung gewährt** auf **Administrator** eingestellt ist.
5. Klicken Sie auf **Apply** (Übernehmen), um die Änderungen zu speichern.

Dell IT Assistant zum Anzeigen von iDRAC-Status und -Ereignissen verwenden

Nachdem die Ermittlung abgeschlossen ist, werden die iDRACs in der **Server**-Kategorie des Bildschirms **Details zu ITA-Geräten** eingeblendet, und die iDRAC-Informationen können durch Klicken auf den iDRAC-Namen angezeigt werden. Dies ist anders als bei DRAC5-Systemen, bei denen die Verwaltungskarte in der RAC-Gruppe angezeigt wird. Der Grund hierfür ist, dass iDRAC statt SNMP die IPMI-Ermittlung verwendet.

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

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfiguration der Verwaltungsstation

Controller-Firmware Version 1.4 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 Seriell über LAN konfigurieren und 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 auftreten, wenn Konnektivitätprobleme vorliegen, oder wenn die Firewll aktiviert ist. Hierbei handelt es sich um bekannte Probleme bei Internet Explorer 6. Da diese Probleme bei Internet Explorer 7 nicht auftreten, empfiehlt Dell ein Upgrade auf diese Version.

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

   Das Fenster **Internetoptionen** wird angezeigt.
3. Wählen Sie **Extras**→**Internetoptionen**→ **Sicherheit**→ **Lokales Netzwerk (**Internet Explorer 7) -oder- **Lokales Intranet** (Internet Explorer 6) aus.
4. Klicken Sie auf die **Benutzerdefinierte Stufe**.
5. Wählen Sie aus dem Drop-Down-Menü **Mittel-Niedrig** aus, und klicken Sie auf **Reset.** Klicken Sie zum Bestätigen auf **OK**. Sie werden den Dialog **Benutzerdefinierte Stufe** erneut eingeben müssen, indem Sie auf die entsprechende Schaltfläche klicken.
6. Scrollen Sie zum Abschnitt mit der Bezeichnung **ActiveX-Steuerelemente und -Plug-ins** herunter, und markieren Sie alle Einstellungen, da verschiedene Versionen von Internet Explorer unterschiedliche Einstellungen im Zustand **Mittel-Niedrig** haben:
   - Automatische Eingabeaufforderung für ActiveX-Steuerelemente: **Aktivieren**
   - Binäre und Script-Verhaltensweisen: **Aktivieren**
   - Download von signierten ActiveX-Steuerelementen: **Eingabeaufforderung**
   - Initialisieren- und Script-ActiveX-Steuerelemente nicht als sicher gekennzeichnet: **Eingabeaufforderung**
   - ActiveX-Steuerelemente und Plug-ins ausführen**: Aktivieren**
   - Script-ActiveX-Steuerelemente, die für das Scripting als sicher gekennzeichnet wurden**: Aktivieren**

   Im Abschnitt zu **Downloads**:
   - Automatische Eingabeaufforderung für Datei-Downloads: **Aktivieren**
   - Datei-Download: **Aktivieren**
   - Schriftart-Download: **Aktivieren**

   Im Abschnitt **Verschiedenes**:
   - META-AKTUALISIERUNG zulassen: **Aktivieren**
   - Scripting von Web-Browser-Steuerung für Internet Explorer zulassen**: Aktivieren**
   - Durch Scripts eingeleitete Fenster ohne Größen- oder Positionsbeschränkungen zulassen**: Aktivieren**
   - Keine Eingabeaufforderungen für die Client-Zertifikatsauswahl anzeigen, wenn keine Zertifikate vorliegen, oder wenn nur ein einziges Zertfikat vorhanden ist: **Aktivieren**
   - Programme und Dateien in einem IFRAME starten: **Aktivieren**
   - Dateien nach Inhalt, nicht nach Dateierweiterung öffnen**: Aktivieren**
   - Softwarekanal-Berechtigungen: **Niedrige Sicherheitsstufe**
   - Daten nicht verschlüsselter Formulare senden**: Aktivieren**
   - Pop-up-Blocker verwenden: **Deaktivieren**

   Im Abschnitt **Scripting**:
   - Aktives Scripting: **Aktivieren**
   - Einfügen-Vorgänge über Script zulassen**: Aktivieren**
   - Scripting von Java-Applets: **Aktivieren**
7. Wählen Sie **Extras**→ **Internetoptionen**→ **Erweitert** aus.
8. Stellen Sie sicher, dass die folgenden Elemente markiert oder unmarkiert sind:

   Im Abschnitt **Browsen**:
   - URLs immer als UTF-8 senden: markiert
   - Script-Debuggen deaktivieren (Internet Explorer): markiert
   - Script-Debuggen deaktivieren (Andere): markiert
   - Zu jedem Script-Fehler eine Benachrichtigung anzeigen: unmarkiert
   - Aktivieren von Installation nach Bedarf (Andere): markiert
   - Seitenübergänge aktivieren**:** markiert
   - Browser-Erweiterungen von Fremdherstellern aktivieren: markiert

- Windows zum Starten von Verknüpfungen erneut verwenden: unmarkiert

Im Abschnitt **HTTP 1.1-Einstellungen**:

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

Im Abschnitt **Java (Sun)**:

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

Im Abschnitt **Multimedia**:

- Automatische Größenänderung des Bildes aktivieren: markiert
- Auf Webseiten Animationen abspielen: markiert
- Auf Webseiten Videos abspielen: markiert
- Bilder zeigen: markiert

Im Abschnitt **Sicherheit**:

- Auf Zertifikatwiderruf des Herausgebers überprüfen: unmarkiert
- Bei heruntergeladenen Programmen auf Signaturen überprüfen: markiert
- SSL 2.0 verwenden: unmarkiert
- SSL 3.0 verwenden: markiert
- TLS 1.0 verwenden: markiert
- Zu ungültigen Standortzertifikaten Warnungen ausgeben: markiert
- Warnung ausgeben, wenn zwischen sicherem und nicht sicherem Modus gewechselt wird: markiert
- Warnung ausgeben, wenn Einreichung des Formulars umgeleitet wird: markiert

ANMERKUNG: Wenn Sie sich entscheiden, eine oder mehrere der oben aufgeführten Einstellungen zu ändern, ist es wichtig, dass Sie zuerst verstehen, welche Konsequenzen dies nach sich ziehen würde. Wenn Sie z. B. wählen, Popups zu blockieren, werden gewisse Bereiche der iDRAC-Webbenutzeroberfläche nicht funktionieren.

9. Klicken Sie auf **Anwenden**.
10. Klicken Sie auf **OK**.
11. Wählen Sie die Registerkarte **Verbindungen** aus.
12. Klicken Sie unter **LAN-Einstellungen (Lokales Netzwerk)** auf **LAN- Einstellungen**.
13. Wenn das Kästchen **Proxyserver verwenden** markiert ist, wählen Sie das Kästchen **Proxyserver für lokale Adressen deaktivieren** aus.
14. Klicken Sie zweimal auf **OK**.
15. Schließen Sie den Browser, und starten Sie ihn anschließend neu, um sicherzustellen, dass alle Änderungen wirksam werden.

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 und 7.0 (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_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 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:

   ```
   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.

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 **Einstellungname 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.

Installation einer Java-Laufzeitumgebung (JRE)

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:

   ```
   Backspace will be sent as delete. (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

---

Installation des Dell OpenManage IT Assistant

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

- DVD *Dell Systems Management Tools and Documentation* - Enthält alle neuesten Konsolenprodukte der Dell-Systemverwaltung, darunter Dell OpenManage IT Assistant; bietet die Tools, die Sie zum Konfigurieren des Systems benötigen und liefert Firmware, Diagnose und Dell-optimierte Treiber für das System und verhilft Ihnen, stets Zugriff auf die neuesten Dokumentationen zum System, zu Systemverwaltungs-Softwareprodukten, Peripheriegeräten und RAID-Controllern zu haben.
- 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 DVD *Dell Systems Management Tools and Documentation* 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

Controller-Firmware Version 1.4 Benutzerhandbuch

In diesem Abschnitt werden die Tasks zum Einrichten des verwalteten Servers zur Erweiterung der Remote-Verwaltungsfähigkeiten beschrieben. Diese Tasks schließen die Installation der Software Dell Open Manage Server Administrator und die Konfiguration des Managed Servers, um den letzten Absturz des Bildschirms zu erfassen.

Softwareinstallation auf dem Managed Server

Die Verwaltungssoftware von Dell schließt die folgenden Funktionen ein:

- Lokale RACADM-CLI - ermöglicht, den iDRAC vom verwalteten System aus zu konfigurieren und zu 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, welche 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 zum Installieren von Server Administrator die DVD *Dell Systems Management Tools and Documentation*.Anleitungen zum Installieren dieser Software sind im *Schnellinstallationshandbuch* enthalten.

Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz

Das 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. Dell OpenManage Server Administrator (OMSA) muss installiert werden. 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 das 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

Controller-Firmware Version 1.4 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 einen unterstützten Webbrowser.

   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 z. B. ein Benutzer in einem Register mit Hauptbenutzerrechten anmeldet und dann in einem anderen als Administrator, erhalten beide geöffneten Register Administratorrechte. Durch das Schließen eines beliebigen Registers laufen alle Register der iDRAC-Webschnittstelle ab.

Das Verhalten der Register in Firefox 2 ist identisch mit dem Registerverhalten in Internet Explorer 7; neue Register leiten neue Sitzungen ein. Das Window-Verhalten in Firefox ist jedoch unterschiedlich. Firefox-Fenster werden mit denselben Berechtigungen betrieben wie das Fenster, das als letztes geöffnet wurde. Wenn z. B. ein Firefox-Fenster mit einem angemeldeten Hauptbenutzer und ein anderes Fenster mit Administratorrechten geöffnet ist, haben nun **beide** Benutzer Administratorrechte.

Tabelle 5-1. Benutzerrechte-Verhalten in unterstützten Browsern

Browser	Registerverhalten	Fensterverhalten
Microsoft Internet Explorer 6	-	Neue Sitzung
Microsoft Internet Explorer 7	Von letzter geöffneter Sitzung	Neue Sitzung
Firefox 2	Von letzter geöffneter Sitzung	Von letzter geöffneter Sitzung

---

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 5-2 und Tabelle 5-3 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 5-4.

Tabelle 5-2. Netzwerkeinstellungen

Einstellung	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 5-3. IPMI LAN-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 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 5-4. 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 5-5 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 5-6.

Tabelle 5-5. 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 5-6. 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 5-7 aufgeführt.

Tabelle 5-7. Filterbare 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) konfigurieren beschriebenen 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) konfigurieren beschriebenen 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 5-8 beschreibt die **allgemeinen** Einstellungen zur Konfiguration eines Benutzernamens und -kennworts für iDRAC.

   Tabelle 5-9 beschreibt die **IPMI-LAN-Berechtigungen** zum Konfigurieren der LAN-Berechtigungen des Benutzers.

   Tabelle 5-10 beschreibt die **Benutzergruppen**-Berechtigungen für die Einstellungen der **IPMI-LAN-Berechtigungen** und der **iDRAC-Benutzerberechtigungen**.

   Tabelle 5-11 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 5-12.

Tabelle 5-8. 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 5-9. 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 5-10. 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 5-11.
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 5-11. 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 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

Tabelle 5-12. 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 5-13 beschreibt die Optionen, die zum Erstellen einer CSR verfügbar sind.

Tabelle 5-14 beschreibt die auf der Seite **SSL-Hauptmenü** verfügbaren Schaltflächen.

Tabelle 5-13. 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 5-14. 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 5-15 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 5-16.

Tabelle 5-15. 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 5-16. 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 abgeschlossenen Dateinamen und die Dateierweiterung enthält.

3. Klicken Sie auf **Anwenden**.

4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-17.

Tabelle 5-17. Seitenschaltflächen Zertifikat hochladen

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 5-18 erläutert die Felder und zugehörigen Beschreibungen, die im **Zertifikat**-Fenster aufgeführt werden.

2. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-19.

Tabelle 5-18. 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 5-19. 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 5-20 führt die Optionen der Seite **Active Directory-Hauptmenü** auf.
3. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-20.

Tabelle 5-20. 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 5-21. 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 5-22 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 5-23.

5. Klicken Sie zum Konfigurieren der Rollengruppen für das Active Directory-Standardschema auf die individuelle Rollengruppe (1 - 5). Siehe Tabelle 5-24 und Tabelle 5-25.

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

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

Einstellung	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 5-23. 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 5-24. Rollengruppenberechtigungen

Einstellung	Beschreibung
Zugriffsstufe der Rollengruppe	Legt die maximale iDRAC-Benutzerberechtigung als eine der Folgenden fest: **Administrator**, **Hauptbenutzer**, **Gastbenutzer**, **Keine** oder **Benutzerdefiniert**. Siehe Tabelle 5-25 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 5-25. 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 5-26.

Tabelle 5-26. 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 5-27 erläutert die Felder und zugehörigen Beschreibungen, die im **Zertifikat**-Fenster aufgeführt werden.

2. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-28.

Tabelle 5-27. 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 5-28. 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.

---

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 5-29 für Web Server-Einstellungen
   - SSH - siehe Tabelle 5-30 für Informationen zu SSH-Einstellungen

- Telnet - siehe Tabelle 5-31 für Informationen zu Telnet-Einstellungen
- Automatisierter Systemwiederherstellungsagent - siehe Tabelle 5-32 für die Einstellungen des automatisierten Systemwiederherstellungsagenten

4. Klicken Sie auf **Anwenden**.
5. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-33.

Tabelle 5-29. 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. Zeitüberschreitungsbereich ist 60 bis 10.800 Sekunden. Die Standardeinstellung ist **1.800** 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 5-30. 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 sind. 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. Zeitüberschreitungsbereich ist 60 bis 10.800 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitlimit-Funktion zu deaktivieren. Die Standardeinstellung ist **1.800**.
Anschlussnummer	Der Anschluss, an dem der iDRAC abhört, ob eine SSH-Verbindung besteht. Die Standardeinstellung ist **22.**

Tabelle 5-31. 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. Zeitüberschreitungsbereich ist 60 bis 10.800 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitlimit-Funktion zu deaktivieren. Die Standardeinstellung ist **1.800**.
Anschlussnummer	Der Anschluss, an dem der iDRAC abhört, ob eine Telnet-Verbindung besteht. Die Standardeinstellung ist **23.**

Tabelle 5-32. Einstellung des automatisierten Systemwiederherstellungs-Agenten

Einstellung	Beschreibung
Aktiviert	Aktiviert den automatisierten Systemwiederherstellungs-Agenten.

Tabelle 5-33. 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

ANMERKUNG: 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. Die CMC- Webschnittstelle (CMC 2.0 oder höher) bietet auch eine iDRAC-Firmware- Aktualisierungskapazität für One-to-Many/Out-of-Band, die jederzeit eingesetzt werden kann.

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.

6. 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

Controller-Firmware Version 1.4 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

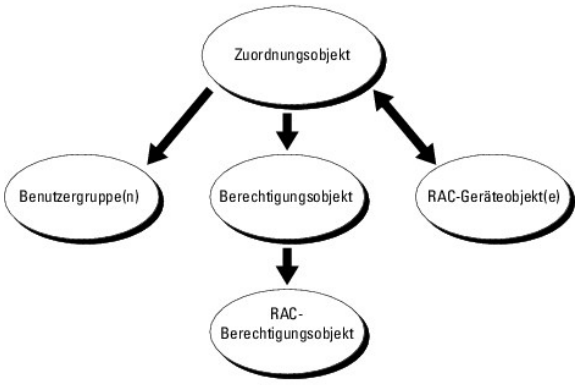
Für jedes der physischen RACs auf dem Netzwerk, das Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein RAC-Geräteobjekt erstellen. Sie können verschiedene Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt mit 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.

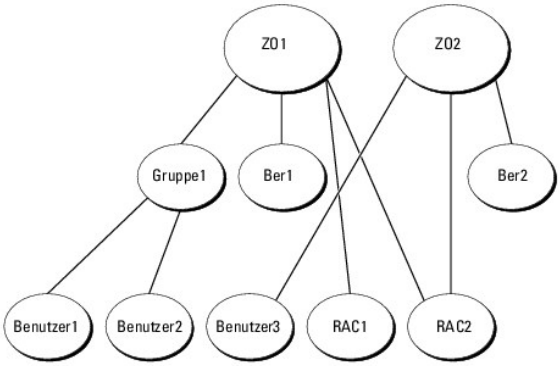
Sie können je nach Bedarf eine beliebige Anzahl von Zuordnungsobjekten erstellen. Es ist jedoch erforderlich, dass Sie mindestens ein Zuordnungsobjekt erstellen, und Sie müssen ein RAC-Geräteobjekt für jeden RAC (iDRAC) auf dem Netzwerk besitzen, das zum Zweck der Authentifizierung und Autorisierung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



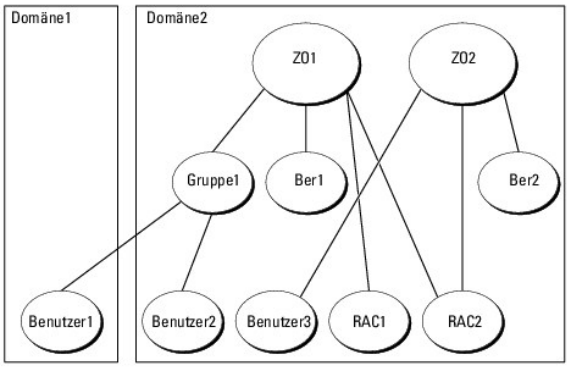
Um die Objekte für das Einzeldomänen-Szenario zu konfigurieren, führen Sie die folgenden Tasks aus:

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 Anmeldeberechtigung 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 für beide iDRACs und Benutzer3 mit Anmeldeberechtigungen für RAC2.

Abbildung 6-3. Einrichten der Active Directory-Objekte in mehreren Domänen



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 Anmeldeberechtigung 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 Schema Extender befinden sich auf der DVD *Dell Systems Management Tools and Documentation* in den folgenden jeweiligen Verzeichnissen:

- *DVD-Laufwerk*:**\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files**
- *DVD-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 Verwenden des Dell Schema Extender.

Sie können den Schema Extender bzw. die LDIF-Dateien von einem beliebigen Standort kopieren und ausführen.

Verwenden des Dell Schema Extender

ANMERKUNG: 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 **Fertigstellen**.

   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 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
delIsLogClearAdmin TRUE, wenn der Benutzer Protokolllöschungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
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 dellAssociationObjectMember, 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 mit der DVD *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In erweitern, 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.

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

Erstellen des RAC-Geräteobjekt

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 einen unterstützten Webbrowser.
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. Im Abschnitt Allgemeine Einstellungen:
   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 zur Auswahl des Active Directory-Schemas auf **Erweitertes Schema verwenden**.
8. Im Abschnitt Erweiterte Schemaeinstellungen:
   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 Erstellen des RAC-Geräteobjekt").
   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 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.
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 5-11 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

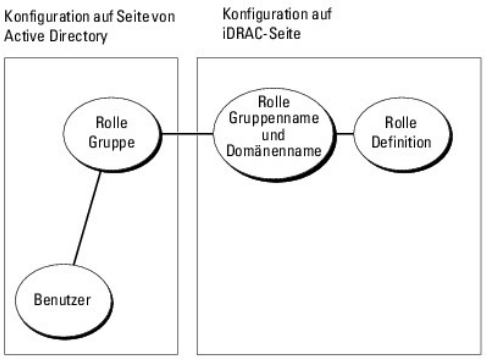


Tabelle 6-9. Standardeinstellungsberechtigungen der Rollengruppe

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 einen unterstützten Webbrowser.
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. Im Abschnitt Allgemeine Einstellungen:
   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 5-11 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 einen unterstützten Webbrowser.
    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

Controller-Firmware Version 1.4 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 die folgenden Informationen über die E/A-Mezzanine-Karten, die auf dem verwalteten Server installiert sind:

- Verbindung - Führt die auf dem verwalteten Server installierte(n) E/A-Mezzaninkarte(n) auf.
- Kartentyp - Der physische Typ der installierten Mezzanine-Karte/-Verbindung.
- Modellname - Modellnummer, Typ oder Beschreibung der installierten Mezzanine-Karte(n).

Integrierte Speicherkarte

Dieser Abschnitt der iDRAC-Webschnittstelle bietet Informationen über die integrierte Speicher-Controller-Karte, die auf dem verwalteten Server installiert ist:

- Kartentyp - zeigt den Modellnamen der installierten Speicherkarte.

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 15-3. 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

Seriell über LAN konfigurieren und verwenden

Controller-Firmware Version 1.4 Benutzerhandbuch

Seriell über LAN (SOL) ist eine IPMI-Funktion, die ermöglicht, dass die textbasierten Konsolendaten eines verwalteten Servers, die herkömmlicherweise über die serielle E/A-Schnittstelle gesendet würden, über das dedizierte Außenband-Ethernet-Verwaltungsnetzwerk des iDRACs umgeleitet werden. Die SOL-Außenbandkonsole ermöglicht Systemadministratoren, die textbasierte Konsole des Blade-Servers von einem beliebigen Standort mit Netzwerkzugriff aus im Remote-Zugriff zu verwalten. Mit SOL können Sie:

- Im Remote-Verfahren und ohne Zeitüberschreitung auf Betriebssysteme zugreifen.
- Hostsysteme auf Emergency Management Services (EMS) oder Special Administrator Console (SAC) für Windows oder in einer Linux-Shell diagnostizieren.
- Den Fortschritt eines Blade-Servers während POST anzeigen und das BIOS-Setup-Programm neu konfigurieren (während der Umleitung auf eine serielle Schnittstelle).

Seriell über LAN im BIOS aktivieren

Um einen Server ordnungsgemäß für Seriell über LAN zu konfigurieren, sind die folgenden Konfigurationsschritte erforderlich, die im Detail beschrieben werden:

1. Seriell über LAN im BIOS konfigurieren (standardmäßig deaktiviert)
2. iDRAC für Seriell über LAN konfigurieren
3. Eine Methode zum Initialisieren von Seriell über LAN auswählen (SSH, Telnet, SOL Proxy oder IPMI-Hilfsprogramm)
4. Betriebssystem für SOL konfigurieren

Die serielle Kommunikation ist im BIOS standardmäßig **aus**geschaltet. Um die Daten der Hosttextkonsole zu Seriell über LAN umzuleiten, müssen Sie die Konsolenumleitung über COM1 aktivieren. Um die BIOS-Einstellung zu ändern, führen Sie die folgenden Schritte aus:

1. Starten Sie den verwalteten Server.
2. Drücken Sie <F2>, um das BIOS-Setup-Dienstprogramm während des POST aufzurufen.
3. Scrollen Sie zu Serielle Kommunikation herunter, und drücken Sie die Eingabetaste.

   Im Popup-Fenster wird die Liste der seriellen Kommunikation mit den folgenden Optionen angezeigt:

   - Aus
   - Ein ohne Konsolenumleitung
   - Ein mit Konsolenumleitung über COM1

   Verwenden Sie die Pfeiltasten, um zwischen Optionen hin- und her zu navigieren.
4. Stellen Sie sicher, dass **Ein mit Konsolenumleitung über COM1** aktiviert ist.
5. Stellen Sie sicher, dass die **Failsafe-Baudrate** mit der SOL-Baudrate identisch ist, die auf iDRAC konfiguriert ist. Der Standardwert sowohl für die Einstellung der Failsafe-Baudrate als auch der SOL-Baudrate des iDRACs lautet 115,2 kbps.
6. **Umleitung nach Start** aktivieren (der Standardwert lautet DEAKTIVIERT). Durch diese Option wird die BIOS-SOL-Umleitung über nachfolgende Neustarts aktiviert.
7. Speichern Sie die Änderungen und beenden Sie.

   Der verwaltete Server startet neu.

Seriell über LAN in der iDRAC-Web-GUI konfigurieren

1. Öffnen Sie die Seite **Seriell über LAN-Konfiguration**, indem Sie **System**→ **Remote-Zugriff**→ **iDRAC**→ **Netzwerk/Sicherheit**→ **Seriell über LAN** auswählen.

2. Stellen Sie sicher, dass die Option **Seriell über LAN aktivieren** ausgewählt (aktiviert) ist. Standardmäßig ist sie aktiviert.

3. Aktualisieren Sie die IPMI-SOL-Baudrate, indem Sie aus dem **Baudraten**- Drop-Down-Menü eine Datengeschwindigkeit auswählen. Die Optionen lauten 19,2 kbps, 57,6 kbps und 115,2 kbps. Der Standardwert lautet 115,2 kbps.

   ANMERKUNG: Stellen Sie sicher, dass die SOL-Baudrate mit der Failsafe-Baudrate, die im BIOS eingestellt wurde, identisch ist.

4. Klicken Sie auf **Anwenden,** falls Sie Änderungen vorgenommen haben.

Tabelle 8-1. Einstellungen der Seite Seriell über LAN-Konfiguration

Einstellung	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 8-2. 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.

5. Ändern Sie ggf. die Konfiguration auf der Seite **Erweiterte Einstellungen**. Dell empfiehlt die Verwendung der Standardwerte. **Erweiterte Einstellungen** ermöglicht Ihnen, die SOL-Leistung einzustellen, indem Sie die Werte für das **?Intervall der Zeichenakkumulation** und den **Schwellenwert der gesendeten Zeichen** ändern. Verwenden Sie zum Erzielen einer optimalen Leistung die Standardeinstellungen von 10 Millisekunden bzw. 250 Zeichen.

Tabelle 8-3. Einstellungen der Seite Seriell über LAN-Konfiguration - Erweiterte Einstellungen

Einstellung	Beschreibung
?Intervall der Zeichenakkumulation	Der typische Zeitumfang, während dessen iDRAC abwartet, bevor er ein teilweises SOL-Datenpaket sendet. Dieser Parameter wird in Millisekunden und in Inkrementen von 10 Millisekunden angegeben.
Schwellenwert der gesendeten Zeichen	Gibt die Anzahl von Zeichen pro SOL-Datenpaket an. Sobald die Anzahl der vom iDRAC akzeptierten Zeichen gleich oder größer dem Schwellenwert der gesendeten Zeichen ist, beginnt der iDRAC, SOL-Datenpakete zu übertragen, die Anzahlen von Zeichen enthalten, die gleich oder kleiner dem Schwellenwert der gesendeten Zeichen sind. Wenn ein Paket weniger Zeichen enthält als dieser Wert, wird es als teilweises SOL-Datenpaket definiert.

ANMERKUNG: Wenn Sie diese Werte auf niedrigere Werten herabsetzen, ergibt sich für die SOL-Konsolenumleitungsfunktion eventuell eine Leistungsherabsetzung. Des Weiteren muss die SOL-Sitzung den Empfang einer Bestätigung für jedes Paket abwarten, bevor das nächste Paket gesendet werden kann. Es ergibt sich daraus eine bedeutend herabgesetzte Leistung.

Tabelle 8-4. 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.

6. Konfigurieren Sie SSH/Telnet für SOL unter **System**→ **Remote-Zugriff**→ **iDRAC**→ **Netzwerk/Sicherheit**→ **Dienste**.

   ANMERKUNG: Jeder Blade-Server unterstützt lediglich eine aktive SOL-Sitzung über SSH oder das Telnet-Protokoll.

   ANMERKUNG: Das SSH-Protokoll ist standardmäßig aktiviert. Das Telnet-Protokoll ist standardmäßig deaktiviert.

7. Klicken Sie auf **Dienste**, um die Seite **SSH- und Telnet-Konfiguration** zu öffnen.

   ANMERKUNG: Sowohl SSH- als auch Telnet-Programme bieten Zugriff auf ein Remote-System.

8. Klicken Sie je nach Bedarf auf **Aktivieren** - entweder auf **SSH** oder auf **Telnet**. **SSH** ist standardmäßig eingeschaltet.

9. Klicken Sie auf **Anwenden**.

   ANMERKUNG: Aufgrund besserer Sicherheits- und Verschlüsselungsmechanismen wird SSH empfohlen.

   ANMERKUNG: Die SSH/Telnet-Sitzungsdauer kann unendlich sein, solange der Zeitüberschreitungswert auf 0 eingestellt wird. Der Standard-Zeitüberschreitungswert beträgt **1800 Sekunden**.

10. Aktivieren Sie die iDRAC-Außenbandschnittstelle (IPMI-über-LAN), indem Sie **System→ Remote-Zugriff→ iDRAC→ Netzwerk/Sicherheit→ Netzwerk** auswählen.

11. Aktivieren Sie die Option **IPMI-über-LAN** unter **IPMI-LAN- Einstellungen**. Die **IPMI-über-LAN**-Funktionalität ist standardmäßig deaktiviert.

12. Klicken Sie auf **Anwenden**.

Seriell über LAN (SOL) verwenden

Dieser Abschnitt bietet mehrere Methoden zum Initialisieren einer Seriell über LAN-Sitzung einschließlich eines Telnet-Programms, eines SSH-Clients, IPMItool und SOL Proxy. Der Zweck der Seriell über LAN-Funktion besteht darin, die serielle Schnittstelle des verwalteten Servers über iDRAC in die Konsole Ihrer Management Station umzuleiten.

Modell zum Umleiten von SOL über Telnet oder SSH

Telnet (Schnittstelle 23)/ SSH (Schnittstelle 22) Client↔WAN-Anschluss↔iDRAC-Server

Die IPMI-basierte SOL-über-SSH/Telnet-Implementierung macht ein zusätzliches Dienstprogramm überflüssig, da die Seriell-zu-Netzwerk-Übersetzung innerhalb des iDRAC stattfindet. Die verwendete SSH- oder Telnet-Konsole sollte in der Lage sein, die Daten zu interpretieren, die von der seriellen Schnittstelle 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. Die serielle Konsole wird automatisch auf Ihre SSH- oder Telnet-Konsole umgeleitet. Die SOL-Umleitung kann dann vom Ziel **/system/sol1** aus gestartet werden.

Informationen zur Verwendung von Telnet und SSH-Clients bei iDRAC finden Sie unter Telnet- oder SSH-Clients installieren.

Modell für den SOL Proxy

Telnet Client (Schnittstelle 623)↔WAN-Anschluss↔SOL Proxy↔iDRAC-Server

Wenn der SOL Proxy mit dem Telnet-Client auf einer Management Station kommuniziert, verwendet er das TCP/IP-Protokoll. Der SOL Proxy kommuniziert jedoch mit dem iDRAC des verwalteten Systems über das RMCP/IPMI/SOL-Protokoll, das ein UDP-basiertes Protokoll ist. Wenn Sie daher mit dem iDRAC des verwalteten Systems vom SOL Proxy aus über einen WAN-Anschluss kommunizieren, treten eventuell Probleme mit der Netzwerkleistung auf. Das empfohlene Modell der Verwendung besteht darin, dass sich der SOL Proxy und der iDRAC-Server auf demselben LAN befinden. Die Management Station mit dem Telnet-Client kann dann über einen WAN-Anschluss eine Verbindung zum SOL Proxy herstellen. In diesem Verwendungsmodell wird der SOL Proxy wie gewünscht funktionieren.

Modell zum Umleiten von SOL über IMPItool

IPMItool↔WAN-Anschluss↔iDRAC-Server

Das IPMI-basierte SOL-Dienstprogramm, IPMItool, verwendet das Protokoll RMCP+, das unter Verwendung von UDP-Datengrammen an Schnittstelle 623 geliefert wird. iDRAC erfordert, dass diese RMCP+-Verbindung verschlüsselt ist. Der Verschlüsselungsschlüssel (KG-Schlüssel) muss Nullzeichen oder NULL enthalten, die in der iDRAC-Web-GUI oder im iDRAC-Konfigurationsdienstprogramm konfiguriert werden können. Sie haben auch die Möglichkeit, den Verschlüsselungsschlüssel zu löschen, indem Sie die Rücktaste drücken, sodass der iDRAC als Verschlüsselungsschlüssel standardmäßig NULL-Zeichen ausgeben wird. Der Vorteil der Verwendung von RMCP+ besteht darin, dass Authentifizierung, Datenintegritätsprüfungen und Verschlüsselung sowie die Fähigkeit, verschiedene Arten von Nutzlasten zu tragen, verbessert werden. Weitere Informationen stehen Ihnen unter SOL über IPMItool verwenden oder auf der IPMItool-Hauptseite zur Verfügung: **http://ipmitool.sourceforge.net/manpage.html**.

SOL-Sitzung in SM-CLP abbrechen

Wenn Sie zum Zugriff auf Seriell über LAN-Funktionalität SSH- oder Telnet-Protokolle verwenden, werden Sie als erstes eine Verbindung zum SM-CLP-Dienst des iDRACs herstellen, von dem aus Sie die SOL-Sitzung mit einem SM-CLP-Befehl (`start /system1/sol1`) starten werden. Benutzer, die eine SOL-Sitzung abbrechen möchten, müssen daher zuerst die SOL-Sitzung über das SM-CLP beenden.

Befehle zum Abbrechen einer SOL-Sitzung sind dienstprogrammorientiert. Bitte lesen Sie diesen Abschnitt sorgfältig durch: Ein Dienstprogramm kann nur dann beendet werden, wenn eine SOL-Sitzung vollständig beendet worden ist.

Wenn Sie bereit sind, die SOL-Umleitung von SM-CLP 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 SOL-Sitzung wird geschlossen.

ANMERKUNG: Wenn eine SOL-Sitzung im Dienstprogramm nicht erfolgreich vollständig geschlossen wurde, stehen eventuell keine weiteren SOL-Sitzungen zur Verfügung. Sie können dieses Problem beheben, indem Sie die SMASH-Konsole in der Web-GUI unter System→ Remote-Zugriff→ iDRAC→ Netzwerk/Sicherheit→ Sitzungen löschen.

SOL über PuTTY verwenden

Um auf einer Windows-Management Station SOL von PuTTY aus zu starten, führen Sie folgende Schritte aus:

ANMERKUNG: Falls erforderlich, können Sie die standardmäßige SSH/Telnet- Zeitüberschreitung unter System→ Remote-Zugriff→ iDRAC→ Netzwerk/Sicherheit→ Dienste ändern.

1. Stellen Sie zum iDRAC eine Verbindung her, indem Sie an der Eingabeaufforderung den folgenden Befehl eingeben:

   ```
   putty.exe [-ssh | -telnet] <Anmeldename>@<iDRAC-IP-Adresse> <Schnittstellennummer>
   ```

2. Geben Sie an der SM-CLP-Eingabeaufforderung den folgenden Befehl ein, um SOL zu starten:

   ```
   start /system1/sol1
   ```

   ANMERKUNG: Hierdurch werden Sie mit der seriellen Schnittstelle des verwalteten Servers verbunden. Die SM-CLP-Befehle stehen Ihnen nicht mehr zur Verfügung. Sobald SOL gestartet ist, können Sie nicht zum SM-CLP zurückkehren. Sie müssen die SOL-Sitzung unter Verwendung der Befehlssequenz beenden, die unter SOL-Sitzung in SM-CLP abbrechen im Detail beschrieben ist, und eine neue Sitzung starten, um SM-CLP verwenden zu können.

SOL über Telnet mit Linux verwenden

Um auf einer Linux-Verwaltungsstation SOL von Telnet aus zu starten, führen Sie folgende Schritte aus:

ANMERKUNG: Falls erforderlich, können Sie die standardmäßige Telnet- Zeitüberschreitung unter System→ Remote-Zugriff→ iDRAC→ Netzwerk/Sicherheit→ Dienste ändern.

1. Starten Sie eine Shell.
2. Stellen Sie mit folgendem Befehl eine Verbindung zum iDRAC her:

   ```
   telnet <iDRAC-IP-Adresse>
   ```

   ANMERKUNG: Wenn Sie die Standardschnittstellennummer für den Telnet-Dienst, 23, geändert haben, fügen Sie die Schnittstellennummer am Ende des Telnet-Befehls hinzu.

3. Geben Sie den iDRAC-Benutzernamen und das iDRAC-Kennwort ein, um eine Verbindung zum iDRAC SM-CLP herzustellen.
4. Geben Sie an der SM-CLP-Eingabeaufforderung den folgenden Befehl ein:

   ```
   start /system1/sol1
   ```

5. Um eine SOL-Sitzung von Telnet auf Linux zu beenden, geben Sie <Strg><]> ein (drücken Sie die Strg-Taste, und geben Sie eine rechte eckige Klammer ein). Eine Telnet-Eingabeaufforderung wird angezeigt. Geben Sie `quit` ein, um Telnet zu beenden.

SOL über OpenSSH mit Linux verwenden

OpenSSH ist ein Open Source-Dienstprogramm zur Verwendung des SSH-Protokolls. Um auf einer Linux-Management Station SOL von OpenSSH aus zu starten, führen Sie folgende Schritte aus:

ANMERKUNG: Falls erforderlich, können Sie die standardmäßige SSH- Sitzungszeitüberschreitung unter System→ Remote-Zugriff→iDRAC→ Netzwerk/Sicherheit →Dienste ändern.

1. Starten Sie eine Shell.
2. Stellen Sie mit folgendem Befehl eine Verbindung zum iDRAC her:

   ```
   ssh <iDRAC-iP-Adresse> -l <Anmeldename>
   ```

3. Geben Sie an der SM-CLP-Eingabeaufforderung den folgenden Befehl ein um SOL zu starten:

   ```
   start /system1/sol1
   ```

   ANMERKUNG: Sie werden nun mit der seriellen Schnittstelle des verwalteten Servers verbunden. Die SM-CLP-Befehle stehen Ihnen nicht mehr zur Verfügung. Sobald SOL gestartet ist, können Sie nicht zum SM-CLP zurückkehren. Sie müssen die SOL-Sitzung beenden (beziehen Sie sich auf "Disconnecting SOL session in SM-CLP" [SOL-Sitzung in SM-CLP abbrechen] auf Seite 146, um eine aktive SOL-Sitzung zu schließen), und eine neue starten, um SM-CLP zu verwenden.

SOL über IPMItool verwenden

Auf der DVD *Dell Systems Management Tolls and Documentation* steht IPMItool zur Verfügung, das auf verschiedenen Betriebssystemen installiert werden kann. Sie können SOL mit IPMItool auf einer Management Station starten, indem Sie folgenden Schritte ausführen:

ANMERKUNG: Falls erforderlich, können Sie die standardmäßige SOL- Zeitüberschreitung unter System→ Remote-Zugriff→iDRAC→Netzwerk/Sicherheit→Dienste ändern.

1. Machen Sie die Datei IPMItool.exe unter dem richtigen Verzeichnis ausfindig.

   Der Standardpfad für Windows lautet **C:\Program Files\Dell\SysMgt\bmc**.

2. Stellen Sie sicher, dass der Verschlüsselungsschlüssel auf der folgenden Seite nur Nullen enthält: **System→Remote-Zugriff→iDRAC→Netzwerk/Sicherheit→Netzwerk→IPMI-LAN- Einstellungen**.

3. Geben Sie an der Windows-Eingabeaufforderung oder an der Linux-Shell- Eingabeaufforderung den folgenden Befehl ein, um SOL über iDRAC zu starten:

   ```
   ipmitool -H <iDRAC-iP-Adresse> -I lanplus -U <Anmeldename> -P <Anmeldekennwort> sol activate
   ```

   Sie werden nun mit der seriellen Schnittstelle des verwalteten Servers verbunden.

4. Sie können eine SOL-Sitzung von IPMItool aus beenden, indem Sie <~> und <.> drücken (drücken Sie die Taste mit der Tilde und die Taste mit dem Punkt nacheinander, der Reihenfolge nach). Die SOL-Sitzung wird geschlossen.

   ANMERKUNG: Wenn ein Benutzer die SOL-Sitzung nicht korrekt beendet, geben Sie den folgenden Befehl aus, um iDRAC neu zu starten. Warten Sie 1-2 Minuten ab, bis der Startvorgang des iDRACs abgeschlossen ist. Weitere Einzelheiten stehen unter RACADM-Unterbefehle zur Verfügung.

   ```
   racadm racreset
   ```

SOL mit SOL Proxy öffnen

Beim Seriell über LAN-Proxy (SOL Proxy) handelt es sich um einen Telnet-Dämon, der eine LAN-basierte Verwaltung von Remote-Systemen mit SOL-Protokollen (Seriell über LAN) und IPMI-Protokollen ermöglicht. Standardmäßige Telnet-Client-Anwendungen wie HyperTerminal unter Windows oder Telnet unter Linux können für den Zugriff auf Dämon-Funktionen verwendet werden. SOL kann entweder im Menümodus oder Befehlsmodus verwendet werden. Das SOL-Protokoll zusammen mit der BIOS-Konsolenumleitung des Remote-Systems ermöglicht Administratoren, die BIOS-Einstellungen eines Managed System im Remote-Zugriff über ein LAN anzuzeigen und zu ändern. Auf die serielle Konsole von Linux und Microsofts EMS/SAC-Schnittstellen kann ebenso über ein LAN mit SOL zugegriffen werden.

ANMERKUNG: Alle Versionen der Windows-Betriebssysteme enthalten die Terminalemulationssoftware HyperTerminal. Die integrierte Version bietet jedoch nicht alle Funktionen, die für Konsolenumleitung erforderlich sind. Sie können stattdessen eine beliebige Terminalemulationssoftware verwenden, die die Emulationsmodi VT100 oder ANSI unterstützt. Ein Beispiel für einen vollständigen VT100- oder ANSI-Terminalemulator, der Konsolenumleitung auf Ihrem System unterstützt, ist HyperTerminal Private Edition 6.1 oder höher.

ANMERKUNG: Weitere Informationen zur Konsolenumleitung, einschließlich Informationen zu erforderlicher Hardware und Software, sowie Anleitungen zum Konfigurieren von Host- und Client-Systemen zur Verwendung von Konsolenumleitung finden Sie im Benutzerhandbuch zum System.

ANMERKUNG: HyperTerminal- und Telnet-Einstellungen müssen mit den Einstellungen auf dem Managed System übereinstimmen. Die Baudraten und Terminalmodi sollten ebenso übereinstimmen.

ANMERKUNG: Der Windows-Telnet-Befehl, der von einer MS-DOS- Eingabeaufforderung ausgeführt wird, unterstützt die ANSI-Terminalemulation. Damit die ANSI-Emulation alle Bildschirme korrekt anzeigen kann, muss das BIOS eingestellt sein.

Vor der Verwendung des SOL Proxy

Bevor Sie den SOL Proxy verwenden, lesen Sie bitte im *Benutzerhandbuch zu den Dienstprogrammen des Baseboard-Verwaltungs-Controllers* nach, um zu erfahren, wie Sie Ihre Management Stationen konfigurieren müssen. Standardmäßig ist das BMC-Verwaltungsdienstprogramm auf Windows-Betriebssystemen im folgenden Verzeichnis installiert:

C:\Program Files\Dell\SysMgt\bmc

Das Installationsprogramm kopiert die Dateien an die folgenden Speicherorte auf Linux Enterprise-Betriebssystemen:

/etc/init.d/SOLPROXY.cfg

/etc/SOLPROXY.cfg

/usr/sbin/dsm_bmu_solproxy32d

/usr/sbin/solconfig

/usr/sbin/impish

SOL Proxy-Sitzung einleiten

Gehen Sie wie folgt vor, um eine Verbindung zu SOL Proxy herzustellen und diesen zu verwenden:

- Für Windows 2003:

Um den SOL Proxy-Dienst nach der Installation auf einem Windows-System zu starten, können Sie das System neu starten (nach einem Neustart wird SOL Proxy automatisch gestartet). Sie haben auch die Möglichkeit, den SOL Proxy-Dienst manuell zu starten, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz**, und klicken Sie dann auf **Verwalten**.

   Das Fenster **Computerverwaltung** wird angezeigt.

2. Klicken Sie auf **Dienste und Anwendungen** und dann auf **Dienste**.

   Verfügbare Dienste werden rechts angezeigt.

3. Machen Sie **DSM_BMU_SOLProxy** in der Liste von Diensten ausfindig, und klicken Sie mit der rechten Maustaste darauf, um den Dienst zu starten.

Abhängig von der Konsole, die Sie verwenden, müssen unterschiedliche Schritte ausgeführt werden, um auf den SOL Proxy zuzugreifen. Innerhalb dieses Abschnitts wird die Management Station, auf der SOL Proxy ausgeführt wird, als SOL Proxy-Server bezeichnet.

- Für Linux Enterprise-Betriebssysteme:

Der SOL Proxy wird automatisch während des Systemstarts gestartet. Alternativ dazu können Sie in das Verzeichnis **/etc/init.d** wechseln und folgende Befehle für die Verwaltung des SOL Proxy-Dienstes eingeben:

```
solproxy status

dsm_bmu_solproxy32d start

dsm_bmu_solproxy32d stop

solproxy restart
```

Telnet mit SOL Proxy verwenden

ANMERKUNG: Hierbei wird angenommen, dass der SOL Proxy-Dienst auf der Management Station bereits eingerichtet ist und ausgeführt wird.

Für Windows 2003:

1. Öffnen Sie auf der Management Station die Eingabeaufforderung.

2. Geben Sie den Befehl `telnet` in die Befehlszeile ein, und geben Sie `localhost` als IP-Adresse an, wenn der SOL Proxy-Server auf demselben System ausgeführt wird, sowie die Schnittstellennummer, die Sie in der SOL Proxy-Installation festgelegt haben (Standardwert ist 623). Zum Beispiel:

   ```
   telnet localhost 623
   ```

Für Linux Enterprise-Betriebssysteme:

1. Öffnen Sie eine Linux Shell auf der Management Station.

2. Geben Sie den Befehl `telnet` ein, und geben Sie `localhost` als IP- Adresse für den SOL Proxy-Server sowie die Schnittstellennummer an, die Sie während der Installation von SOL Proxy festgelegt haben (Standardwert ist 623). Zum Beispiel:

   ```
   telnet localhost 623
   ```

ANMERKUNG: Egal, ob das Hostbetriebssystem Windows oder Linux ist, geben Sie die IP-Adresse des SOL Proxy-Servers ein, statt localhost, wenn der SOL Proxy- Server auf einem anderen System als auf der Management Station ausgeführt wird.

```
telnet <IP-Adresse des SOL Proxy-Servers> 623
```

HyperTerminal mit SOL Proxy verwenden

1. Öffnen Sie die Datei **HyperTerminal.exe** von der Remote-Station aus.

2. Wählen Sie **TCPIP(Winsock)** aus.

3. Geben Sie die Hostadresse `localhost` ein und die Schnittstellennummer 623.

Eine Verbindung zum BMC des Remote Managed System herstellen

Sobald eine SOL Proxy-Sitzung erfolgreich eingerichtet ist, werden Ihnen die folgenden Optionen zur Auswahl geboten:

1. Connect to the Remote Server's BMC (Eine Verbindung zum BMC des Remote-Servers herstellen)
2. Configure the Serial-Over-LAN for the Remote Server (Seriell über LAN für den Remote-Server konfigurieren)
3. Activate Console Redirection (Konsolenumleitung aktivieren)
4. Reboot and Activate Console Redirection (Konsolenumleitung neu starten und aktivieren)
5. Help (Hilfe)
6. Exit (Beenden)

ANMERKUNG: Es können mehrere SOL-Sitzungen gleichzeitig aktiv sein, es darf jedoch nur eine Konsolenumleitungssitzung für ein Managed System aktiv sein.

ANMERKUNG: Drücken Sie zum Beenden einer aktiven SOL-Sitzung die Tasten <~><.>. Mit dieser Sequenz wird SOL beendet, und das Hauptmenü wird wieder angezeigt.

1. Wählen Sie Option 1 im Hauptmenü aus.
2. Geben Sie die **iDRAC-IP-Adresse** des Remote Managed System ein.
3. Geben Sie den iDRAC-**Benutzernamen** und das **Kennwort** für den iDRAC auf dem verwalteten System ein. iDRAC-Benutzername und -Kennwort müssen im nicht-flüchtigen Speicher des iDRAC zugewiesen und gespeichert werden.

   ANMERKUNG: Es ist nur eine SOL-Konsolenumleitungssitzung mit iDRAC auf einmal zulässig.

   ANMERKUNG: Falls erforderlich, können Sie die SOL-Sitzungsdauer auf unendlich erweitern, indem Sie den Telnet-Zeitüberschreitungswert auf der iDRAC-Web-GUI-Seite unter **System**→ **Remote-Zugriff**→ **iDRAC**→ **Netzwerk/Sicherheit**→ **Dienste** zu Null ändern.

4. Geben Sie den IPMI-Verschlüsselungsschlüssel an, wenn er im iDRAC konfiguriert wurde.

   ANMERKUNG: Sie können den IPMI-Verschlüsselungsschlüssel in der iDRAC-GUI unter **System**→ **Remote-Zugriff**→ **iDRAC**→ **Netzwerk/Sicherheit**→ **Netzwerk**→ **IPMI-LAN-Einstellungen**→ **Verschlüsselungsschlüssel** finden.

   ANMERKUNG: Der standardmäßige IPMI-Verschlüsselungsschlüssel besteht ausschließlich aus Nullen. Wenn Sie für die Verschlüsselungsoption die Eingabetaste drücken, wird iDRAC diesen standardmäßigen Verschlüsselungsschlüssel verwenden.

5. Wählen Sie Option 2 im Hauptmenü aus.

   Das SOL-Konfigurationsmenü wird angezeigt. Abhängig vom aktuellen SOL-Status, variiert der Inhalt des SOL-Konfigurationsmenüs:

   - Wenn SOL bereits aktiviert ist, werden die aktuellen Einstellungen angezeigt, und es stehen Ihnen drei Optionen zur Auswahl:

     1. Disable Serial-Over-LAN (Seriell über LAN deaktivieren)
     2. Change Serial-Over-LAN setting (Seriell über LAN-Einstellungen ändern)
     3. Cancel (Abbrechen)

   - Wenn SOL aktiviert ist, ist sicherzustellen, dass die SOL-Baudrate mit der iDRAC-Baudrate übereinstimmt. Zum Aktivieren der Konsolenumleitung ist mindestens eine iDRAC-Benutzerberechtigungsebene von **Administrator** erforderlich.
   - Wenn SOL gegenwärtig deaktiviert ist, geben Sie Y ein, um SOL zu aktivieren, oder N, um SOL deaktiviert zu lassen.

- Wählen Sie Option 3 im Hauptmenü aus.

  Die Textkonsole des Remote Managed System wird auf die Management Station umgeleitet.

7. Wählen Sie Option 4 im Hauptmenü aus (optional).

   Der Energiezustand des Remote Managed System wird bestätigt. Wenn das System eingeschaltet ist, haben Sie die Wahl zwischen einem ordentlichen Herunterfahren und einem erzwungenen Herunterfahren.

   Der Stromzustand wird überwacht, bis der Status zu **eingeschaltet** wechselt. Die Konsolenumleitung wird gestartet und die Textkonsole des Remote Managed System wird an die Management Station umgeleitet.

   Während das Managed System neu gestartet wird, können Sie das BIOS-System-Setup-Programm aufrufen, um BIOS-Einstellungen anzuzeigen oder zu ändern.

8. Wählen Sie im Hauptmenü Option 5 aus, um eine detaillierte Beschreibung der einzelnen Optionen anzuzeigen.
9. Wählen Sie im Hauptmenü Option 6 aus, um Ihre Telnet-Sitzung zu beenden und die Verbindung zu SOL Proxy abzubrechen.

   ANMERKUNG: Wenn ein Benutzer die SOL-Sitzung nicht korrekt beendet, geben Sie den folgenden Befehl aus, um iDRAC neu zu starten. Warten Sie 1-2 Minuten ab, bis der Startvorgang des iDRACs abgeschlossen ist. Weitere Einzelheiten stehen unter RACADM-Unterbefehle zur Verfügung.

   ```
   racadm racreset
   ```

Konfiguration des Betriebssystems

Zum Konfigurieren generischer UNIX®-ähnlicher Betriebssysteme sind die nachstehenden Schritte auszuführen. Diese Konfiguration basiert auf Standardinstallationen von Red Hat Enterprise Linux 5.0, SUSE Linux Enterprise Server 10 SP1 und Windows 2003 Enterprise.

Linux Enterprise-Betriebssystem

1. Bearbeiten Sie die Datei **/etc/inittab**, um Hardware-Ablaufsteuerung zu aktivieren und Benutzern zu ermöglichen, sich über die SOL-Konsole anzumelden. Fügen Sie die nachstehende Zeile am Ende des Abschnitts `#Run gettys in standard runlevels` hinzu.

   ```
   7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220
   ```

Beispiel von originalem /etc/inittab:

```
_____________________________________________________________________

#

# inittab This file describes how the INIT process should set up

# the system in a certain run-level.

#


SKIP this part of file


# Run gettys in standard runlevels

1:2345:respawn:/sbin/migetty tty1

2:2345:respawn:/sbin/migetty tty1

3:2345:respawn:/sbin/migetty tty1

4:2345:respawn:/sbin/migetty tty1

5:2345:respawn:/sbin/migetty tty1

6:2345:respawn:/sbin/migetty tty1


# Run xdm in runlevel 5

x:5:respawn:/etc/X11/prefdm -nodaemon

_____________________________________________________________________
```

Beispiel von modifiziertem /etc/inittab:

```
_____________________________________________________________________

#

# inittab This file describes how the INIT process should set up

# the system in a certain run-level.

#


SKIP this part of file


# Run gettys in standard runlevels

1:2345:respawn:/sbin/migetty tty1

2:2345:respawn:/sbin/migetty tty1

3:2345:respawn:/sbin/migetty tty1

4:2345:respawn:/sbin/migetty tty1

5:2345:respawn:/sbin/migetty tty1
```

```
6:2345:respawn:/sbin/migetty tty1

7:2345:respawn:/sbin/agetty -h ttyS0 115200 vt220


# Run xdm in runlevel 5

x:5:respawn:/etc/X11/prefdm -nodaemon
```

_____

2. Bearbeiten Sie die Datei **/etc/securetty**, um Benutzern zu ermöglichen, sich über die SOL-Konsole als Root-Benutzer anzumelden. Fügen Sie die folgende Zeile im Anschluss an console hinzu:

   ```
   ttyS0
   ```

Beispiel von originalem /etc/securetty:

_____

```
console

vc/1

vc/2

vc/3

vc/4


SKIP the rest of file (Rest der Datei ÜBERSPRINGEN)
```

_____

Beispiel von modifiziertem /etc/securetty:

_____

```
console

ttyS0

vc/1

vc/2

vc/3

vc/4


SKIP the rest of file (Rest der Datei ÜBERSPRINGEN)
```

_____

3. Bearbeiten Sie die Datei **/boot/grub/grub.conf** oder **/boot/grub/menu.list**, um für SOL Startoptionen hinzuzufügen:
   a. Kommentieren Sie in den verschiedenen UNIX-ähnlichen Betriebssystemen die Zeilen der grafischen Anzeigen aus:
      - `splashimage=(had0,0)/grub/splash.xpm.gz` in RHEL 5
      - `gfxmenu (hda0,5)/boot/message` in SLES 10
   b. Fügen Sie die folgende Zeile vor der ersten Zeile mit der Bezeichnung `title= ...` hinzu:

   ```
   # Redirect OS boot via SOL
   ```

   c. Hängen Sie den folgenden Eintrag der ersten Zeile mit der Bezeichnung `title= ...` an:

   ```
   SOL redirection
   ```

   d. Hängen Sie den folgenden Text der Zeile `kernel/...` des ersten `title= ...` an:

   ```
   console=tty1 console=ttyS0,115200
   ```

ANMERKUNG: /boot/grub/grub.conf in Red Hat Enterprise Linux 5 ist eine symbolische Verknüpfung mit /boot/grub/menu.list. Sie können die Einstellungen in beiden ändern.

Beispiel von originalem /boot/grub/grub.conf in Red Hat Enterprise Linux 5:

_____

```
      # grub.conf generated by anaconda
      #
      # Note that you do not have to return grub after making changes to this
      # file
      # NOTICE: You have a /boot partition. This means that
      # all kernel and initrd paths are relative to /boot/, eg.
      # root (hd0,0)
      # kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00
      # initrd /initrd-version.img
      #boot=/dev/sda
      default=0
      timeout=5
      splashimage=(hd0,0)/grub/splash.xpm/gz
      hiddenmenu

      title Red Hat Enterprise Linux 5
            root (hd0,0)
            kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet
            initrd /initrd-2.6.18-8.el5.img
```

Beispiel von modifiziertem /boot/grub/grub.conf:

```
      # grub.conf generated by anaconda
      #
      # Note that you do not have to return grub after making changes to this
      # file
      # NOTICE: You have a /boot partition. This means that
      # all kernel and initrd paths are relative to /boot/, eg.
      # root (hd0,0)
      # kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00
      # initrd /initrd-version.img
      #boot=/dev/sda
      default=0
      timeout=5
      #splashimage=(hd0,0)/grub/splash.xpm/gz
      hiddenmenu

      # Redirect the OS boot via SOL
      title Red Hat Enterprise Linux 5 SOL redirection
            root (hd0,0)
            kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet console=tty1 console=ttyS0,115200
            initrd /initrd-2.6.18-8.el5.img
```

Beispiel von originalem /boot/grub/menu.list in SUSE Linux Enterprise Server 10:

```
_____________________________________________________________________

      #Modified by YaST2. Last modification on Sat Oct 11 21:52:09 UTC 2008

      Default 0

      Timeout 8

      gfxmenu (hd0.5)/boot/message


      ###Don't change this comment - YaST2 identifier: Original name: linux###

      title SUSE Linux Enterprise Server 10 SP1

            root (hd0,5)

            kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts

            initrd /boot/initrd-2.6.16.46-0.12-bigsmp

_____________________________________________________________________
```

Beispiel von originalem /boot/grub/menu.list in SLES 10:

```
_____________________________________________________________________

      #Modified by YaST2. Last modification on Sat Oct 11 21:52:09 UTC 2008

      Default 0

      Timeout 8

      #gfxmenu (hd0.5)/boot/message


      ###Don't change this comment - YaST2 identifier: Original name: linux###

      title SUSE Linux Enterprise Server 10 SP1 SOL redirection

            root (hd0,5)

            kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts
            console=tty1 console=ttyS0,115200

            initrd /boot/initrd-2.6.16.46-0.12-bigsmp

_____________________________________________________________________
```

Windows 2003 Enterprise

1. Bestimmen Sie die Starteintrags-ID, indem Sie an der Windows- Eingabeaufforderung bootcfg eingeben. Machen Sie die Starteintrags- ID für den Abschnitt **Windows Server 2003 Enterprise** ausfindig. Drücken Sie die Eingabetaste, um die Startoptionen auf der Management Station anzuzeigen.

2. Aktivieren Sie EMS an einer Windows-Eingabeaufforderung, indem Sie Folgendes eingeben:

   ```
   bootcfg /EMS ON /PORT COM1 /BAUD 115200 /ID <Start-ID>
   ```

   ANMERKUNG: *<Start-ID>* ist die Starteintrags-ID aus Schritt 1.

3. Drücken Sie die Eingabetaste, um zu überprüfen, ob die EMS- Konsoleneinstellung wirksam ist.

Beispiel von originalem bootcfg setting:

```
_____________________________________________________________________

      Boot Loader Settings

      --------------------

      timeout:30

      default:multi(0)disk(0)rdisk(0)partition(1)\WINDOWS


      Boot Entries
```

```
      ------------

      Boot entry ID: 1

      OS Friendly Name: Winodws Server 2003, Enterprise

      Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

      OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect

_____________________________________________________________________
```

Beispiel von modifizierter bootcfg-Einstellung:

```
_____________________________________________________________________

      Boot Loader Settings

      --------------------

      timeout: 30

      default: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

      redirect: COM1

      redirectbaudrate:115200


      Boot Entries

      ------------

      Boot entry ID: 1

      Os Friendly Name: Windows Server 2003, Enterprise

      Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

      OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect

_____________________________________________________________________
```

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

GUI-Konsolenumleitung verwenden

Controller-Firmware Version 1.4 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 9-1 listet die unterstützten Bildschirmauflösungen und entsprechenden Bildwiederholfrequenzen für eine Konsolenumleitungssitzung auf, die auf dem verwalteten Server ausgeführt wird.

Tabelle 9-1. Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

Bildschirmauflösung	Bildwiederholfrequenz (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60

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 Installation einer Java-Laufzeitumgebung (JRE).

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 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 9-2 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 9-3.

Tabelle 9-2. 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** 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 9-5 sind auf der Seite **Konsolenumleitungskonfiguration** verfügbar.

Tabelle 9-3. 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 9-4 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 iDRAC-Webschnittstelle.

Tabelle 9-4. 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: Für Informationen zur Verwendung des virtuellen Datenträgers mit Konsolenumleitung siehe Virtuellen Datenträger konfigurieren und verwenden.

Die Schaltflächen in Tabelle 9-5 sind auf der Seite **Konsolenumleitungskonfiguration** verfügbar.

Tabelle 9-5. 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 9-6 beschreibt die Menüoptionen, die im Viewer zum Gebrauch verfügbar sind.

Tabelle 9-6. Auswahlmöglichkeiten auf der Viewer-Menüleiste

Menüelement	Element	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.
Mouse (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	-	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 9-7 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 9-7. 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. Der Videotreiber muss unter Verwendung der DVD *Dell Systems Management Tools and Documentation* aktualisiert werden.
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 ist, wird neben der Auswahl im **Maus**-Menü ein Häkchen eingeblendet.
Warum kann ich keine Tastatur oder Maus verwenden, während ich Windows 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

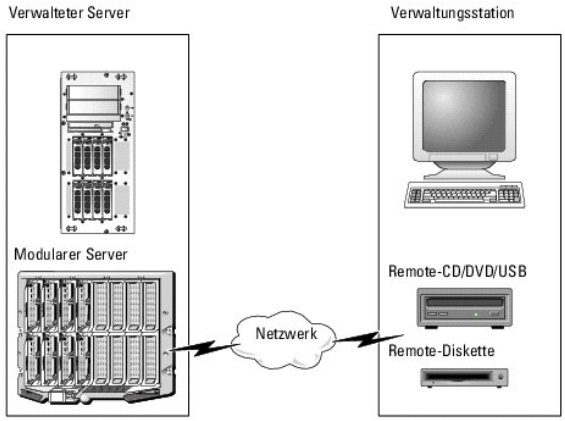
Virtuellen Datenträger konfigurieren und verwenden

Controller-Firmware Version 1.4 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 eine Verbindung zum **virtuellen Datenträger** hergestellt wird, 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 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 die System-Startsequenz anhalten.

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 (Mindestgröße 128 MB)	

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 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 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. 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 10-3. 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

ANMERKUNG: 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.

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 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 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 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→ Virtueller Datenträger-Assistent...**.

   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 **Close** (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 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.

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 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 Virtuellen 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 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 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 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 iDRAC 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 (Mindestgröße 128 MB) • 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 Disketten-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-Diskette 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 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.
Welche Dateisystemtypen werden auf meinem virtuellen Disketten-Laufwerk unterstützt?	Ihr virtuelles Disketten-Laufwerk 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?	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

Controller-Firmware Version 1.4 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:

```
racadm-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 11-1 enthält eine Beschreibung der einzelnen RACADM-Unterbefehle, die Sie in RACADM ausführen können. Für eine ausführliche Auflistung von RACADM-Unterbefehlen einschließlich der Syntax und gültiger Einträge siehe Übersicht der RACADM-Unterbefehle.

Tabelle 11-1. RACADM-Unterbefehle

Befehl	Beschreibung
clrraclog	Löscht das iDRAC-Protokoll. Nach dem Löschvorgang wird ein einzelner Eintrag vorgenommen, um dem 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

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

ANMERKUNG: Wenn Sie einen neuen 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.

ANMERKUNG: Benutzer und Gruppen, die für Active Directory-Umgebungen erstellt wurden, müssen mit der in Ihrer Umgebung vorherrschenden Active Directory-Benennungsregel übereinstimmen.

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 11-2 gezeigten Werten konstruiert ist:

Tabelle 11-2. 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 <*Stufe*> eine der Folgenden ist:

- 2 (**Benutzer**)
- 3 (**Operator**)
- 4 (**Administrator**)

Beispiel: Um die IPMI-LAN-Kanalberechtigung auf 2 (Benutzer) einzustellen, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
```

b. Stellen Sie, falls erforderlich, den Verschlüsselungsschlüssel des IPMI- LAN-Kanals ein, indem Sie einen Befehl wie den folgenden eingeben:

ANMERKUNG: 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 11-3 führt die möglichen Maßnahmen sowie den Wert auf, mithilfe derer sie in RACADM identifiziert werden können.

Tabelle 11-3. 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 5-7 und <*Maßnahmenwert*> ein Wert von Tabelle 11-3.

   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, welches 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 11-4. 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 verwenden finden Sie weitere Informationen zu RACADM- und RACADM-Befehlen.

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

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

   racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57
   ```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

2. Zur Beschränkung von Anmeldungen auf einen kleinen Satz von vier angrenzenden IP-Adressen (z. B. 192.168.0.212 bis 192.168.0.215) wählen Sie alle außer den niederwertigsten zwei 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 11-5. 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

ANMERKUNG: Bearbeiten Sie die Konfigurationsdatei mit einem Klartext- Bearbeitungsprogramm, z. B. Notepad (Windows) oder vi (Linux). Das Dienstprogramm racadm parst nur ASCII-Text. Formatierung verwirrt den Parser, wodurch die 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:

  ```
  #

  # This is a comment

  [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=192.168.133.121 (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:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

This file will be updated as follows:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored

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.

ANMERKUNG: 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 `racresetcfg` 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

Controller-Firmware Version 1.4 Benutzerhandbuch

Dieser Abschnitt enthält Informationen zum im iDRAC 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 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 12-1 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 12-1. 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
help	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, -version, -wait
version	Zeigt die Versionsattribute eines Ziels an. Syntax: version [*Optionen*]	-examine, -help, -output, -version

Tabelle 12-2 beschreibt die SM-CLP-Optionen. Einige Optionen haben abgekürzte Formen, wie in der Tabelle gezeigt.

Tabelle 12-2. Unterstützte SM-CLP-Optionen

SM-CLP-Option	Beschreibung
-all, -a	Beauftragt das Verb, alle möglichen Funktionen auszuführen.
-destination	Bestimmt den Speicherort, an dem ein Image im Dump-Befehl gespeichert wird. Syntax: -destination <URI>
-display, -d	Filtert die Befehlsausgabe. Syntax: -display <Eigenschaften | Ziele | Verben>[, <Eigenschaften | Ziele | Verben>]*
-examine, -x	Weist den Befehlsprozessor an, die Befehlssyntax zu validieren, ohne den Befehl auszuführen.

-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 12-3 enthält eine Liste von Zielen, die über das SM-CLP zur Verfügung stehen.

Tabelle 12-3. 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 Managed 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 an, untergeordnete Ziele sowie eine Liste der SM-CLP-Verben, 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 wird:

```
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 12-4 enthält Beispiele für die Verwendung des SM-CLP zum Ausführen von Stromverwaltungsvorgängen auf einem verwalteten Server.

Tabelle 12-4. Server-Stromverwaltungsvorgänge

Operation	Syntax

Anmeldung am iDRAC über die SSH-Schnittstelle	`>ssh 192.168.0.120`
	`>login: root`
	`>password:`

Schalten Sie den Server aus.	`->stop /system1` `system1 has been stopped successfully`
Server aus dem ausgeschalteten Zustand hochfahren	`->start /system1` `system1 has been started successfully`
Server neu starten	`->reset /system1`

	system1 has been reset successfully

SEL-Verwaltung

Tabelle 12-5 enthält Beispiele für die Verwendung des SM-CLP zum Ausführen von SEL-bezogenen Vorgängen auf dem Managed System.

Tabelle 12-5. 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 defined 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=4 MessageTimeStamp=16:37:10,January 13,2007 Verbs: cd exit help show version
SEL löschen	->delete /system1/sp1/logs1 All records deleted successfully

MAP-Zielnavigation

Tabelle 12-6 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 12-6. 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 12-7 zeigt Beispiele zum Einstellen der iDRAC-Eigenschaften unter Verwendung des SM-CLP.

Tabelle 12-7. 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.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Betriebssystemmithilfe von iVM-CLI bereitstellen

Controller-Firmware Version 1.4 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 Informationen an 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-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 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.

   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 Script) 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 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 RACADM-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 Beispielscript **ivmdeploy**, das illustriert, wie die iVM-CLI- und RACADM-Dienstprogramme zum Bereitstellen von Software an mehrere Remote-Systeme verwendet werden.

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 das 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 an, welche 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 der 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.

Diskette/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 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)

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:\` (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 (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 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

Controller-Firmware Version 1.4 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, welche 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.)`

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 14-1. LAN-Parameter

Element	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 14-2. LAN-Benutzerkonfigurationsseite

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 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:

```
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.

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

Controller-Firmware Version 1.4 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 15-1 beschreibt die Bedeutungen der LED-Anzeigen des PowerEdge-Servers:

Tabelle 15-1. 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 15-2. 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 15-3 beschreibt die Bedeutung der Systemzustandsanzeigen.

Tabelle 15-3. 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 15-3), einen Zeitstempel sowie eine Beschreibung des Ereignisses ein.
3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Systemereignisprotokoll**, um fortzufahren (siehe Tabelle 15-4).

Tabelle 15-4. Schaltflächen der SEL-Seite

Schaltfläche	Abhilfe
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 15-3), einen Hexadezimalcode sowie eine Beschreibung des Codes ein.
2. Klicken Sie auf die entsprechende Schaltfläche der Seite **POST-Codes**, um fortzufahren (siehe Tabelle 15-5).

Tabelle 15-5. POST-Code-Schaltflächen

Schaltfläche	Abhilfe
Drucken	Druckt die Seite **POST-Codes aus.**
Aktualisieren	Lädt die Seite **POST-Codes** neu.

Bildschirm Letzter Systemabsturz anzeigen

ANMERKUNG: 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 15-6 gezeigten Schaltflächen auf:

ANMERKUNG: Die Schaltflächen Speichern und Löschen werden nicht angezeigt, wenn kein gespeicherter Absturzbildschirm vorhanden ist.

Tabelle 15-6. Schaltflächen der Seite Bildschirm Letzter Absturz

Schaltfläche	Abhilfe
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 15-7 führt die verfügbaren Steuerungsmaßnahmen auf.

ANMERKUNG: Sie müssen über Administratorrechte verfügen, um die Wiedergabe der Start-Capture-Sequenzen anzuzeigen.

Tabelle 15-7. 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 15-8. Serverstatusbildschirm

Severity	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 15-9 aufgeführten Informationen zur Verfügung.

Tabelle 15-9. 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 15-10).

Tabelle 15-10. iDRAC-Protokoll-Schaltflächen

Schaltfläche	Abhilfe
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 15-11 und Tabelle 15-12 beschreiben die Eigenschaften des Hauptsystemgehäuses.

Tabelle 15-11. 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 15-12. 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 15-13 beschreibt die iDRAC-Eigenschaften.

Tabelle 15-13. 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. 192.168.154.127.
Gateway	Die IP-Adresse des Gateways, die als Brücke zu anderen Netzwerken dient. Dieser Wert wird im *Punkttrennungs*-Format angegeben, z. B. 192.168.150.5.
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 15-14), 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 15-14 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 15-14. 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 15-15 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 15-15.

Tabelle 15-15. 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).

ANMERKUNG: Ein ordentliches Herunterfahren des Serverbetriebssystems ist eventuell nicht möglich, wenn die Serversoftware nicht mehr reagiert, oder wenn ein Administrator nicht an der lokalen Konsole eines Windows 2000 Servers oder eines neueren Systems angemeldet ist. In solchen Fällen müssen Sie aufgrund des Windows-Sicherheitsdesigns ein erzwungenes Herunterfahren anstatt eines ordentlichen Herunterfahrens festlegen. Windows Server 2003 und neuere Versionen enthalten eine Gruppenrichtlinien-Sicherheitseinstellung, die ein ordentliches Herunterfahrne ohne Administratoranmeldung ermöglicht. Ziehen Sie die Microsoft-Dokumentation zurate, um sich über die Richtlinie "Shutdown: Allow system to be shut down without having to login" (Herunterfahren: System ohne Anmeldung herunterfahren lassen) zu lokalen Computern zu informieren.

Tabelle 15-16. Schaltflächen der Stromverwaltungs-Seite

Schaltfläche	Abhilfe
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 15-17 enthält häufig gestellte Fragen zu Problemen bei der Störungsbehebung.

Tabelle 15-17. 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 Enabled = 1 IP Address = 192.168.0.1 Subnet Mask = 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 Enabled = 1 DHCP Enabled = 1 Static IP Address = 192.168.0.120 Static Subnet Mask = 255.255.255.0 Static Gateway = 192.168.0.1 Current IP Address = 10.35.155.151 Current Subnet Mask = 255.255.255.0 Current Gateway = 10.35.155.1 Speed = Autonegotiate Duplex = Autonegotiate
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.	Entfernen 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

Controller-Firmware Version 1.4 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.

AGP

Abkürzung für Accelerated Graphics Port (Beschleunigter Grafik-Port), wobei es sich um eine Bus-Spezifikation handelt, mit der Grafikkarten schneller auf den Hauptsystemspeicher zugreifen können.

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).

CMC

Abkürzung für Enclosure Management Controller (Gehäuseverwaltungs-Controller), die Controller-Schnittstelle zwischen dem iDRAC und dem CMC des verwalteten Systems.

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 iDRAC; 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 durch den iDRAC und den CMC 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.

iDRAC

Abkürzung für Dell Remote Access Controller 5.

iDRAC

Akronym für Integrated Dell Remote Access Controller, das integrierte System-auf-Chip-Überwachungs-/Steuerungssystem für die Dell 10G-PowerEdge-Server.

IMPItool

Ein Dienstprogramm zum Verwalten und Konfigurieren von Geräten, die IMPI Version 1.5 und Version 2.0 unterstützen.

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.

Kbps

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).

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 Verwaltungsstation ist ein System, das im Remote-Zugriff auf den iDRAC zugreift.

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).

OpenSSH

Ein Open Source-Dienstprogramm zur Verwendung des SSH-Protokolls.

OSCAR

Akronym für On Screen Configuration and Reporting (Onscreen-Konfiguration und -Berichterstattung). OSCAR ist das durch die Avocent iKVM angezeigte Menü, wenn Sie auf <Druck> drücken. Es ermöglicht Ihnen, die CMC-Konsole oder die iDRAC-Konsole für einen im CMC installierten Server auszuwählen.

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.

PuTTY

Eine Terminalemulatoranwendung, die als Client für SSH, Telnet, rlogin und Roh-TCP-Computerprotokolle eingesetzt wird.

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.

RAM-Platte

Ein speicherresidentes Programm, das ein Festplattenlaufwerk emuliert. Der iDRAC 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.

SAC

Akronym für Microsoft Special Administration Console.

SAP

Abkürzung für Service Access Point (Service-Zugriffspunkt).

SEL

Akronym für System Event Log (Systemereignisprotokoll).

SM-CLP

Das im iDRAC integrierte Serververwaltungs-Befehlszeilenprotokoll (Server Management-Command Line Protocol, SM-CLP) der verteilten Management Task Force (Distributed Management Task Force).

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 oder vom CMC erzeugte Meldung (Ereignis), die Informationen über Statusänderungen auf dem verwalteten Server oder über mögliche Hardwarestörungen enthält.

SOL

Eine IPMI-Funktion, über die die textbasierten Konsolendaten eines verwalteten Servers über das dedizierte Out-of-Band-Ethernet-Verwaltungsnetzwerk des iDRACs umgeleitet werden.

SOL Proxy

Ein Telnet-Dämon, der eine LAN-basierte Verwaltung von Remote-Systemen mit SOL- und IPMI-Protokollen ermöglicht.

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 iDRAC; verwendet nur Active Directory-Gruppenobjekte.

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.

Telnet

Ein Netzwerkprotokoll, das für Internetverbindungen oder für Verbindungen des lokalen Netzwerks verwendet wird.

TFTP

Abkürzung für Trivial File Transfer Protocol (Trivial-Dateiübertragungsprotokoll). Ein einfaches Dateiübertragungsprotokoll, das zum Herunterladen von Startcode auf datenträgerlose Geräte oder Systeme verwendet wird.

U/min

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.

USB

Akronym für Universal Serial Bus (Universeller serieller Bus).

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 integriert ist.

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).

Zurück zum Inhaltsverzeichnis