Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

Anmerkungen und Vorsichtshinweise

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

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

März 2009 Rev. A00

Zurück zum Inhaltsverzeichnis

Übersicht der RACADM-Unterbefehle

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

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

Hilfe

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

Tabelle A-1. Befehl help

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

Zusammenfassung

```
racadm help

racadm help <Unterbefehl>
```

Beschreibung

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

Ausgabe

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

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

Unterstützte Schnittstellen

- lokaler RACADM

---

config

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

Tabelle A-2. config/getconfig

Unterbefehl	Definition
config	Konfiguriert iDRAC6.
getconfig	Ruft die iDRAC6-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 von iDRAC6 einzeln einstellen oder sie als Teil einer Konfigurationsdatei stapelverarbeiten. Wenn sich die Daten unterscheiden, wird das iDRAC6-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 iDRAC6 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 zu iDRAC6 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 iDRAC6 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 iDRAC6-Konfigurationsparameter einzeln abrufen oder alle iDRAC6-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 iDRAC6-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 von iDRAC6 in **myrac.cfg**.

- `racadm getconfig -h`

  Zeigt eine Liste der verfügbaren Konfigurationsgruppen auf iDRAC6.

- `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 iDRAC6 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	Virtual KVM

- `racadm getssninfo -A`

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

- `racadm getssninfo -A -u *`

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

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

---

getsysinfo

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

Tabelle A-8. getsysinfo

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

Zusammenfassung

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

Beschreibung

Mit dem Unterbefehl **getsysinfo** werden Informationen bezüglich iDRAC6, 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 iDRAC6-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 iDRAC6, verwaltetem Server und Watchdog-Konfiguration angezeigt.

Beispielausgabe

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

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

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

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

Beispiele

- `racadm getsysinfo -A -s`

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

- `racadm getsysinfo -w -s`

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


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

Einschränkungen

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

---

getractime

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

Tabelle A-10. getractime

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

Zusammenfassung

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

Beschreibung

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

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

Ausgabe

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

Beispielausgabe

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20071208201542.000000
```

Unterstützte Schnittstellen

- lokaler RACADM

---

setniccfg

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

Tabelle A-11. setniccfg

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

Zusammenfassung

```
racadm setniccfg -d

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

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

Beschreibung

Der Unterbefehl **setniccfg** stellt die iDRAC6-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 iDRAC6 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 Enable      = 1

DHCP Enable     = 1

IP Adress       = 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 iDRAC6 zurück.

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

Zusammenfassung

```
racadm racreset
```

Beschreibung

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

Beispiele

- `racadm racreset`

  Starten Sie die Soft-Reset-Sequenz für iDRAC6.

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 von iDRAC6 verwendet werden.

ANMERKUNG: Mit diesem Befehl wird die aktuelle iDRAC6-Konfiguration gelöscht und die iDRAC6-Konfiguration wird 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 iDRAC6-Protokoll an.
getraclog	Zeigt die iDRAC6-Protokolleinträge an.

Zusammenfassung

```
racadm getraclog -i

racadm getraclog [-A] [-o] [-c count] [-s startrecord]

[-m]
```

Beschreibung

Der Befehl **getraclog -i** zeigt die Anzahl der Einträge im iDRAC6-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
Data/Time:   Dec 8 08:10:11
Source:      login[433]
Description: root login from 143.166.157.103
```

Unterstützte Schnittstellen

- lokaler RACADM

---

clrraclog

Zusammenfassung

```
racadm clrraclog
```

Beschreibung

Mit dem Unterbefehl **clrraclog** werden alle vorhandenen Einträge aus dem iDRAC6-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

Data/Time: Dec 8 08:21:30
```

```
Source: ssnmgrd[175]

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

Unterstützte Schnittstellen

- lokaler RACADM

---

sslcsrgen

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

Tabelle A-24. sslcsrgen

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

Zusammenfassung

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

racadm sslcsrgen -s
```

Beschreibung

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

Optionen

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

Tabelle A-25. Optionen des Unterbefehls sslcsrgen

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

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

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

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

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

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

Beispiele

```
racadm sslcsrgen -s

oder

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

Unterstützte Schnittstellen

- lokaler RACADM

---

sslcertupload

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

Tabelle A-26. sslcertupload

Unterbefehl	Beschreibung
sslcertupload	Lädt ein benutzerdefiniertes SSL-Server- oder Zertifizierungsstellenzertifikat vom Client zu iDRAC6 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 iDRAC6 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 iDRAC6.

Zusammenfassung

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

Beschreibung

Sendet eine Test-E-Mail von iDRAC6 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 user1@mycompany.com
Legen Sie die benutzerdefinierte Nachricht fest, die zur Ziel-E-Mail-Adresse gesendet werden soll	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "This is a test!" ("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 iDRAC6-SNMP.

Zusammenfassung

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

Beschreibung

Mit dem Unterbefehl **testtrap** wird die SNMP-Trap-Warnmeldungsfunktion von iDRAC6 geprüft, indem ein Test-Trap von iDRAC6 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

---

vmdisconnect

Zusammenfassung

```
racadm vmdisconnect
```

Beschreibung

Mit dem Unterbefehl **vmdisconnect** können virtuelle Datenträgerverbindungen getrennt werden.

---

clrasrscreen

Zusammenfassung

```
racadm clrasrscreen
```

Beschreibung

Löscht den letzten ASR-Bildschirm (Bildschirm letzter Absturz)

---

localconredirdisable

Zusammenfassung

```
racadm localconredirdisable [0, 1]
```

Beschreibung

Führt eine lokale kVM-Deaktivierung vom lokalen System durch

Zulässige Werte

`0` = Aktivieren

1 = Deaktivieren

---

vmkey

Zusammenfassung

racadm vmkey [reset]

Beschreibung

Mit dem Unterbefehl **vmkey** wird der virtuelle Datenträgerschlüssel auf die Standardgröße von 256 MB zurückgesetzt.

Zulässige Werte

reset = Setzt den Schlüssel auf die Standardgröße (256 MB) zurück

---

Version

Zusammenfassung

racadm-Version

Beschreibung

Zeigt die RACADM-Version an

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Gruppen- und Objektdefinitionen der iDRAC6 Enterprise Eigenschaften-Datenbank

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

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

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

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 maximal 63 ASCII-Zeichen.

Standardeinstellung

Integrierter Dell Remote Access Controller

Beschreibung

Eine Textzeichenkette, die das Produkt identifiziert.

idRacDescriptionInfo (Nur Lesen)

Zulässige Werte

Zeichenkette mit maximal 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 maximal 63 ASCII-Zeichen.

Standardeinstellung

1

Beschreibung

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

idRacBuildInfo (schreibgeschützt)

Zulässige Werte

Zeichenkette mit maximal 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 maximal 15 ASCII-Zeichen

Standardeinstellung

iDRAC

Beschreibung

Ein vom Benutzer vergebener Name zur Identifizierung dieses Controllers.

idRacType (Nur-Lesen)

Zulässige Werte

Produkt-ID

Standardeinstellung

8

Beschreibung

Identifiziert den Typ des Remote Access Controllers als iDRAC6.

---

cfgOobSnmp

Diese Gruppe enthält Parameter zur Konfiguration des SNMP-Agenten und der Trap-Fähigkeiten des iDRAC.

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

cfgOobSnmpAgentCommunity (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 31

Standardeinstellung

public

Beschreibung

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

cfgOobSnmpAgentEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert den SNMP-Agenten im RAC

---

cfgLanNetworking

Diese Gruppe enthält Parameter zum Konfigurieren der iDRAC6-NIC.

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

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 mit bis zu 254 ASCII-Zeichen Mindestens ein Zeichen muss ein alphabetisches Zeichen sein. Zeichen sind auf die alphanumerischen Zeichen, '-' und '.' beschränkt.

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

Standardeinstellung

(leer)

Beschreibung

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

iDRAC-*Service-Tag-Nummer*

Beschreibung

Zeigt den RAC-Namen an, der standardmäßig die iDRAC-*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 iDRAC6-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.

Standardeinstellung

0.0.0.0

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 iDRAC6-Netzwerkschnittstellen-Controller. Wenn der NIC deaktiviert wird, ist der Zugriff auf die Remote-Netzwerkschnittstellen zum iDRAC6 nicht mehr möglich, und der iDRAC6 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 iDRAC6-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 iDRAC6-IP-Adresse verwendet wird. Wenn diese Eigenschaft auf 1 (TRUE) eingestellt ist, wird die iDRAC6-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 iDRAC6-NIC. Beispiel: 00:12:67:52:51:A3.

Beschreibung

Die iDRAC6-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.

cfgUserAdminIndex (Nur Lesen)

Zulässige Werte

Dieser Parameter wird beruhend auf den vorhandenen Instanzen bestückt.

Standardeinstellung

1 - 16

Beschreibung

Der eindeutige Index eines Benutzers

cfgUserAdminIpmiLanPrivilege (Lesen/Schreiben)

Zulässige Werte

2 (**Benutzer**)

3 (Operator)

4 (**Administrator**)

15 (**Kein Zugriff**)

Standardeinstellung

4 (Benutzer 2)

15 (Alle anderen)

Beschreibung

Die maximale Berechtigung auf dem IPMI-LAN-Kanal

cfgUserAdminPrivilege (Lesen/Schreiben)

Zulässige Werte

0x00000000 bis 0x000001ff und 0x0

Standardeinstellung

0x00000000

Beschreibung

Diese Eigenschaft legt die für den Benutzer zugelassenen rollenbasierten Autoritätsberechtigungen fest. Der Wert wird als Bitmaske dargestellt, wodurch beliebige Kombinationen von Berechtigungswerten möglich 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 iDRAC6 anmelden	0x0000001
iDRAC6 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
Der Benutzer ist nicht zum Zugriff auf den iDRAC6 berechtigt.	0x00000000
Der Benutzer kann sich nur am iDRAC6 anmelden und iDRAC6- und Server-Konfigurationsinformationen anzeigen.	0x00000001
Der Benutzer kann sich am iDRAC6 anmelden und die Konfiguration ändern.	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

(leer)

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 maximal 20 ASCII-Zeichen

Standardeinstellung

(leer)

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

(leer)

Beschreibung

Die E-Mail-Adresse der Warnungsquelle

cfgEmailAlertCustomMsg

Zulässige Werte

Eine Zeichenkette von maximal 32 Zeichen

Standardeinstellung

(leer)

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 iDRAC6 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 - 4

Standardeinstellung

4

Beschreibung

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

cfgSsnMgtWebserverTimeout (Lesen / Schreiben)

Zulässige Werte

60 - 10800

Standardeinstellung

1800

Beschreibung

Definiert das Web Server-Zeitlimit. 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 - 10800

Standardeinstellung

1800

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 - 10800

Standardeinstellung

1800

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 iDRAC6-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 iDRAC6.

cfgSerialTelnetEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Telnet-Konsolenschnittstelle auf dem iDRAC6

---

cfgRemoteHosts

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

cfgRhostsSmtpServerIpAddr (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette, die eine gültige SMTP-Server-IP-Adresse darstellt. Beispiel: 192.168.0.56.

Standardeinstellung

0.0.0.0

Beschreibung

Die IP-Adresse des Netzwerk-SMTP-Servers. Der SMTP-Server überträgt E-Mail-Warnungen vom RAC, wenn die Warnungen konfiguriert und aktiviert sind.

---

cfgUserDomain

Diese Gruppe dient zur Konfiguration der Benutzer-Domänennamen für das aktive Verzeichnis. Es können maximal 40 Domänennamen auf einmal konfiguriert werden.

cfgUserDomainIndex (schreibgeschützt)

Zulässige Werte

1 - 40

Standardeinstellung

<instance>

Beschreibung

Stellt ein spezifisches Domain dar

cfgUserDomainName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von maximal 255 Zeichen

Standardeinstellung

(leer)

Beschreibung

Spezifiziert den Benutzer-Domänennamen des aktiven Verzeichnisses.

---

cfgServerPower

Diese Gruppe bietet verschiedene Energieverwaltungsfunktionen.

cfgServerPowerStatus (schreibgeschützt)

Zulässige Werte

1 = TRUE

0 = FALSE

Standardeinstellung

0

Beschreibung

Stellt den Stromstatus des Servers dar, entweder **EIN** oder **AUS (ON / OFF)**

cfgServerPowerServerAllocation (schreibgeschützt)

Zulässige Werte

Zeichenkette von maximal 32 Zeichen

Standardeinstellung

(leer)

Beschreibung

Stellt die verfügbare Stromversorgung zur Verwendung durch den Server dar

cfgServerPowerActualPowerConsumption (schreibgeschützt)

Zulässige Werte

Zeichenkette von maximal 32 Zeichen

Standardeinstellung

(leer)

Beschreibung

Stellt den vom Server zum derzeitigen Zeitpunkt verwendeten Strom dar

cfgServerPowerPeakPowerConsumption (schreibgeschützt)

Zulässige Werte

Zeichenkette von maximal 32 Zeichen

Standardeinstellung

(leer)

Beschreibung

Stellt die maximale Stromaufnahme des Servers bis zum aktuellen Zeitpunkt dar.

cfgServerPowerPeakPowerTimestamp (schreibgeschützt)

Zulässige Werte

Zeichenkette von maximal 32 Zeichen

Standardeinstellung

(leer)

Beschreibung

Zeit, zu der die maximale Leistungsaufnahme aufgezeichnet wurde.

cfgServerPowerConsumptionClear (Nur Schreiben)

Zulässige Werte

0,1

Standardeinstellung

0

Beschreibung

Setzt die **cfgServerPeakPowerConsumption** Eigenschaft auf 0 und die **cfgServerPeakPowerConsumptionTimestamp** Eigenschaft auf die aktuelle iDRAC6-Zeit zurück

cfgServerPowerCapWatts (schreibgeschützt)

Zulässige Werte

Zeichenkette von maximal 32 Zeichen

Standardeinstellung

(leer)

Beschreibung

Stellt den Leistungsschwellenwert des Servers in Watt dar.

cfgServerPowerCapBtuhr (schreibgeschützt)

Zulässige Werte

Zeichenkette von maximal 32 Zeichen

Standardeinstellung

(leer)

Beschreibung

Stellt den Leistungsschwellenwert des Servers in BTU/h dar.

cfgServerPowerCapPercent (schreibgeschützt)

Zulässige Werte

Zeichenkette von maximal 32 Zeichen

Standardeinstellung

(leer)

Beschreibung

Stellt den Leistungsschwellenwert des Servers in Prozent dar.

---

cfgRacTuning

Diese Gruppe wird verwendet, um verschiedene iDRAC6-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 iDRAC6 zu verwenden ist.

cfgRacTuneIpRangeEnable

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die IP-Adressenbereichs-Überprüfungsfunktion des iDRAC6

cfgRacTuneIpRangeAddr

Zulässige Werte

Eine als IP-Adresse formatierte Zeichenkette 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

Eine als IP-Adresse formatierte Zeichenkette 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 iDRAC6 SSH-Schnittstelle verwendete Anschlussnummer an.

cfgRacTuneConRedirEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Konsolenumleitung

cfgRacTuneTelnetPort (Lesen / Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

23

Beschreibung

Gibt die für die iDRAC6 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 iDRAC6 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 iDRAC6 zu verwenden ist.

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

cfgRacTuneAsrEnable (Lesen / Schreiben)

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

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

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

cfgRacTuneWebserverEnable (Lesen / Schreiben)

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert und deaktiviert den iDRAC6 Web Server Wird diese Eigenschaft deaktiviert, ist der Zugriff auf iDRAC6 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 iDRAC6-Konfigurationsdaten. Standardmäßig ist der Zugriff aktiviert.

ANMERKUNG: Der Zugriff kann mit dem lokalen RACADM oder der iDRAC6-Webschnittstelle deaktiviert werden. Sobald er jedoch deaktiviert ist, kann der Zugriff nur über die iDRAC6-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 (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von maximal 255 Zeichen.

Standardeinstellung

(leer)

Beschreibung

Der Host-Name des verwalteten Servers

ifcRacMnOsOsName (schreibgeschützt)

Zulässige Werte

Eine Zeichenkette von maximal 255 Zeichen.

Standardeinstellung

(leer)

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 iDRAC6 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

Eine Zeichenkette von maximal 254 Zeichen.

Standardeinstellung

Beschreibung

Gibt den allgemeinen Namen (CN) der CSR an

cfgSecCsrOrganizationName (Lesen / Schreiben)

Zulässige Werte

Eine Zeichenkette von maximal 254 Zeichen.

Standardeinstellung

(leer)

Beschreibung

Gibt den CSR-Organisationsnamen (O) an

cfgSecCsrOrganizationUnit (Lesen / Schreiben)

Zulässige Werte

Eine Zeichenkette von maximal 254 Zeichen.

Standardeinstellung

(leer)

Beschreibung

Gibt die CSR-Organisationseinheit (OU) an

cfgSecCsrLocalityName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von maximal 254 Zeichen

Standardeinstellung

(leer)

Beschreibung

Gibt den CSR-Standort (L) an

cfgSecCsrStateName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von maximal 254 Zeichen

Standardeinstellung

(leer)

Beschreibung

Gibt den CSR-Zustandsnamen (S) an

cfgSecCsrCountryCode (Lesen/Schreiben)

Zulässige Werte

Ein Zeichenkette von zwei Zeichen

Standardeinstellung

(leer)

Beschreibung

Gibt den CSR-Landescode (CC) an

cfgSecCsrEmailAddr (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette von maximal 254 Zeichen

Standardeinstellung

(leer)

Beschreibung

Legt die CSR-E-Mail-Adresse fest.

cfgSecCsrKeySize (Lesen/Schreiben)

Zulässige Werte

512

1024

2048

Standardeinstellung

1024

Beschreibung

Gibt die asymmetrische SSL-Schlüsselgröße für die CSR an

---

cfgRacVirtual

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

cfgVirMediaAttached (Lesen/Schreiben)

Zulässige Werte

0 = Trennen

1 = Verbinden

2 = Autom. verbinden

Standardeinstellung

0

Beschreibung

Dieses Objekt wird verwendet, um virtuelle Geräte über den USB-Bus mit dem System zu verbinden. Wenn die Geräte angeschlossen sind, erkennt der Server gültige, am System angeschlossene USB-Massenspeichergeräte. Dies entspricht dem Anschließen eines lokalen USB-CDROM-/Disketten-Laufwerks am USB-Anschluss eines Systems. Wenn die Geräte angeschlossen sind, können Sie im Remote-Zugriff über die iDRAC6-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.

cfgVirMediaBootOnce (Lesen / Schreiben)

Zulässige Werte

1 (Aktiviert)

0 (Deaktiviert)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Einmal-Start-Funktion des virtuellen iDRAC6-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.

cfgVirMediaKeyEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

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 iDRAC6-Active Directory.

cfgADRacDomain (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 der DRAC befindet.

cfgADRacName (Lesen / Schreiben)

Zulässige Werte

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

Standardeinstellung

(leer)

Beschreibung

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

cfgADEnable (Lesen / Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Active Directory-Benutzerauthentifizierung auf dem iDRAC6. Wenn diese Eigenschaft deaktiviert ist, wird statt dessen lokale iDRAC6-Authentifizierung 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.

cfgADDomainController1 (Lesen / Schreiben)

Zulässige Werte

Gültige IP-Adresse oder vollqualifizierter Domänenname (FQDN)

Standardeinstellung

Kein Standardwert

Beschreibung

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

cfgADDomainController2 (Lesen / Schreiben)

Gültige IP-Adresse oder vollqualifizierter Domänenname (FQDN)

Standardeinstellung

Kein Standardwert

Beschreibung

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

cfgADDomainController3 (Lesen / Schreiben)

Gültige IP-Adresse oder vollqualifizierter Domänenname (FQDN)

Standardeinstellung

Kein Standardwert

Beschreibung

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

cfgADGlobalCatalog1 (Lesen / Schreiben)

Zulässige Werte

Gültige IP-Adresse oder vollqualifizierter Domänenname (FQDN)

Standardeinstellung

Kein Standardwert

Beschreibung

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

cfgADGlobalCatalog2 (Lesen/Schreiben)

Zulässige Werte

Gültige IP-Adresse oder vollqualifizierter Domänenname (FQDN)

Standardeinstellung

Kein Standardwert

Beschreibung

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

cfgADGlobalCatalog3 (Lesen/Schreiben)

Zulässige Werte

Gültige IP-Adresse oder vollqualifizierter Domänenname (FQDN)

Standardeinstellung

Kein Standardwert

Beschreibung

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

cfgADType (Lesen/Schreiben)

Zulässige Werte

1 = Aktiviert das aktive Verzeichnis mit dem erweiterten Schema

2 = Aktiviert das aktive Verzeichnis mit dem Standardschema

Standardeinstellung

1

Beschreibung

Bestimmt den Schematyp, der mit dem aktiven Verzeichnis verwendet werden soll

cfgADCertValidationEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Zertifikatvalidierung des aktiven Verzeichnisses

---

cfgStandardSchema

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

cfgSSADRoleGroupIndex (schreibgeschützt)

Zulässige Werte

1 - 5

Beschreibung

Index der Rollengruppe, wie im aktiven Verzeichnis enthalten

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 Gesamtstruktur des aktiven Verzeichnisses enthalten

cfgSSADRoleGroupDomain (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

(leer)

Beschreibung

Domäne des aktiven Verzeichnisses, 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 iDRAC6 anmelden	0x00000001
iDRAC6 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

9600, 19200, 57600, 115200

Standardeinstellung

115200

Beschreibung

Die Baudrate für die serielle Datenübertragung über LAN

cfgIpmiSolMinPrivilege (Lesen/Schreiben)

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

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

cfgIpmiSolAccumulateInterval (Lesen/Schreiben)

Zulässige Werte

1 - 255

Standardeinstellung

10

Beschreibung

Gibt die typische Zeitdauer an, während der der iDRAC6 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 40 Zeichen ohne Leerstellen

Standardeinstellung

0000000000000000000000000000000000000000

Beschreibung

IPMI-Verschlüsselungsschlüssel

cfgIpmiPetCommunityName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette mit maximal 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

Eine Zeichenkette mit maximal 255 Zeichen

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

iDRAC6 SM-CLP-Eigenschaftendatenbank

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 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 keine der folgenden Zeichen enthalten: Schrägstrich (/), Punkt (.) und at-Symbol (@), Anführungszeichen ("). 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
An iDRAC6 anmelden	0x0000001
iDRAC6 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
Der Benutzer darf nicht auf iDRAC6 zugreifen.	0x00000000
Der Benutzer kann sich nur am iDRAC6 anmelden und iDRAC6- und Server-Konfigurationsinformationen anzeigen.	0x00000001
Der Benutzer kann sich am iDRAC6 anmelden und die Konfiguration ändern.	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 iDRAC6-NIC. Es ist eine Instanz der Gruppe zulässig. Für alle Objekte in dieser Gruppe ist ein Reset des iDRAC6-NIC erforderlich, wodurch ein kurzzeitiger Verlust der Verbindungen auftreten kann. Objekte, die die iDRAC6-NIC-IP-Adresseneinstellungen ändern, schließen alle aktiven Benutzersitzungen und erfordern, dass Benutzer mit den aktualisierten IP-Adresseneinstellungen eine neue Verbindung herstellen.

macaddress (schreibgeschützt)

Zulässige Werte

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

Standardeinstellung

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

Beschreibung

Enthält die iDRAC6-NIC-MAC-Adresse.

/system1/sp1/enetport1/lanendpt1/ipendpt1

oemdell_nicenable (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die iDRAC6-NIC. Wenn die NIC deaktiviert ist, werden die Remote-Netzwerkschnittstellen zu iDRAC6 unzugänglich und sorgen dafür, dass iDRAC6 nur über die lokale RACADM-Schnittstelle verfügbar ist.

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 iDRAC6-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 iDRAC6-IP-Adresse verwendet wird. Wenn diese Eigenschaft auf 1 (aktiviert) eingestellt ist, werden die iDRAC6-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/ dnsendpt1

oemdell_domainnamefromdhcp (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

Legt fest, dass der iDRAC6-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 iDRAC6-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. Dieser Parameter ist nur gültig, wenn oemdell_dnsregisterrac auf 1 (registriert) 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/ dnsendpt1/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/ dnsendpt1/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/ remotesap1

defaultgatewayaddress (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

192.168.0.1

Beschreibung

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

/system1/sp1/group<1-5>

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

oemdell_groupname (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette mit bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

""

Beschreibung

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

oemdell_groupdomain (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette mit bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

""

Beschreibung

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

oemdell_groupprivilege (Lesen/Schreiben)

Zulässige Werte

0x00000000 bis 0x000001ff

Standardeinstellung

""

Beschreibung

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

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

Rollengruppe	Berechtigungs-Bitmaske
An iDRAC6 anmelden	0x00000001
iDRAC6 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 iDRAC6 Active Directory-Funktion.

enabledstate (Lesen/Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Active Directory-Benutzerauthentifizierung auf iDRAC6. Falls diese Eigenschaft deaktiviert ist, wird stattdessen die Authentifizierung des lokalen iDRAC6 für Benutzeranmeldungen verwendet.

oemdell_adracname (Lesen/Schreiben)

Zulässige Werte

Jede druckbare Textzeichenkette mit bis zu 254 Zeichen ohne Leerzeichen.

Standardeinstellung

""

Beschreibung

Name des iDRAC6, 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 iDRAC6 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 iDRAC6 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 iDRAC6 zum Durchsuchen des LDAP-Servers nach Benutzernamen verwendet.

/system1/sp1/oemdell_racsecurity1

Diese Gruppe wird für die Konfiguration von Einstellungen verwendet, die mit der iDRAC6-SSL-CSR-Funktion (Zertifikatsignierungsanforderung) in Beziehung stehen. Alle Eigenschaften in dieser Gruppe müssen konfiguriert werden, bevor von iDRAC6 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 iDRAC6-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 iDRAC6-Webschnittstelle oder die CLI eine Verbindung zu den virtuellen Geräten herstellen. Einstellen dieser Eigenschaft auf 0 bewirkt, dass die Komponenten die Verbindung zum USB-Bus aufheben.

oemdell_singleboot (Lesen / Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Einmal-Start-Funktion des virtuellen iDRAC6-Datenträgers. Wenn diese Eigenschaft beim Neustart des Hostservers aktiviert wirdt, wird der Server versuchen, von den virtuellen Datenträgergeräten zu starten.

oemdell_floppyemulation (Lesen / Schreiben)

Zulässige Werte

0 (Deaktiviert)

1 (Aktiviert)

Standardeinstellung

0

Beschreibung

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

/system1/sp1/oemdell_vmservice1/tcpendpt1

portnumber (Lesen / Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

3668

Beschreibung

Gibt die Anschlussnummer an, die für verschlüsselte Verbindungen virtueller Datenträger zum iDRAC6 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 die Anschlussnummer an, die für verschlüsselte Verbindungen virtueller Datenträger zum iDRAC6 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

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 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 der Standardeinstellung: **0**
cfgADRacName	oemdell_adracname	Zeichenkette von bis zu 254 Zeichen.
cfgADRacDomain	oemdell_adracdomain	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**
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 globalen Katalogservers
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 des NIC, 1 zum Aktivieren des NIC Standardeinstellung: **0**
cfgNicUseDHCP	oemdell_usedhcp	0 zur Konfiguration statischer Netzwerkadressen, 1 zur Verwendung von DHCP Standardeinstellung: **0**
cfgNicIpAddress	ipaddress	Die iDRAC6-IP-Adresse, Standardeinstellung: **192.168.0.120** plus Serversteckplatznummer.
cfgNicNetmask	subnetmask	Subnetzmaske für das iDRAC6-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 iDRAC6-Namen im DNS anzumelden, 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	1 zum Aktivieren des Benutzers, 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	password	Eine Zeichenkette von 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		Anschluss für Konsolenumleitung, Standardeinstellung: **5900**
cfgRacTuneConRedirVideoPort		Anschluss für Konsolen-Videoumleitung, Standardeinstellung: **5901**
cfgRacTuneHttpPort		Anschluss für Webschnittstellen-HTTP, Standardeinstellung: **80**
cfgRacTuneHttpsPort		Anschluss für sicheres Webschnittstellen-HTTPS, 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		Die auf die Basisadresse angewandte Bitmaske, um gültige IP-Adressen auszuwählen, Standardeinstellung: **255.255.255.0**
cfgRacTuneLocalServerVideo		Auf 1 einstellen, um lokale iKVM-Konsole zu aktivieren Standardeinstellung: **1**
cfgRacTuneSshPort		Anschluss für den SSH-Dienst Standardeinstellung: **22**
cfgRacTuneTelnetPort		Anschluss für den Telnet-Dienst Standardeinstellung: **23**
cfgRacTuneWebserverEnable		Auf 1 einstellen, um die webbasierten iDRAC6-Schnittstelle 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. Zwei 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 partielles 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: **00000000000000000000000000000000000000000000**
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 (Zurücksetzen), 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 den Status eines CSR-Erstellungsverfahrens zurück
sslcertupload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <iDRAC-Serverzertifikat-TFTP-URI> /system1/sp1/oemdell_ssl1	Lädt das iDRAC6-Serverzertifikat auf den iDRAC6 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 auf den iDRAC6 hoch
sslcertdownload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <iDRAC-Serverzertifikat-TFTP-URI> /system1/sp1/oemdell_ssl1	Lädt das Zertifikat des iDRAC6-Servers vom iDRAC6 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 iDRAC6 herunter

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Übersicht iDRAC6 Enterprise

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

Der Integrated Dell™ Remote Access Controller (iDRAC6) ist eine Systemverwaltungs-Hardware- und -Software-Lösung, die Remote-Verwaltungsfähigkeiten, Wiederherstellung für abgestürzte Systeme sowie Stromsteuerungsfunktionen für Dell PowerEdge™-Systeme bietet.

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

iDRAC6 kann so konfiguriert werden, dass er Ihnen bei Warnungen oder Fehlern eine E-Mail oder eine des SNMP-Trap-Warnung (Simple Network Management Protocol) sendet. Um Ihnen bei der Diagnose der wahrscheinlichen Ursache eines Systemabsturzes behilflich zu sein, kann iDRAC6 Ereignisdaten protokollieren und einen Screenshot erzeugen, 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 Zugriff auf iDRAC6-Geräte, lokale Konsolenverbindungen sowie seine Webschnittstelle.

Alle Netzwerkverbindungen zum iDRAC6 erfolgen über die CMC-Netzwerkschnittstelle (CMC-RJ45-Anschluss "Gb"). Der CMC leitet Datenverkehr über ein privates, internes Netzwerk zu den iDRAC6-Geräten auf seinen Servern. Dieses private Verwaltungsnetzwerk befindet sich außerhalb des Serverdatenpfads und untersteht nicht der Steuerung des Betriebssystems, d. h. *bandextern*. Die *bandinternen* Netzwerkschnittstellen des verwalteten Servers sind über im Gehäuse installierte E/A-Module (IOMs) zugänglich.

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

---

iDRAC6-Verwaltungsfunktionen

iDRAC6 enthält die folgenden Verwaltungsfunktionen:

- Registrierung des dynamischen Domänennamensystems (DDNS)
- Remote-Systemverwaltung und -überwachung über eine Webschnittstelle, die lokale RACADM-Befehlszeilenoberfläche über Konsolenumleitung sowie die SM-CLP-Befehlszeile über eine Telnet/SSH-Verbindung
- Unterstützung für Microsoft Active Directory®-Authentifizierung - Fasst iDRAC6-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 - Bietet Zugriff auf das Systemereignisprotokoll, das iDRAC6-Protokoll und den letzten Absturzbildschirm des abgestürzten oder nicht reagierenden Systems, unabhängig vom Zustand des Betriebssystems
- Dell OpenManage™ Software-Integration - Sie können damit die iDRAC6-Webschnittstelle vom Dell OpenManage Server Administrator oder IT Assistent starten
- Start-Capture - Enthält bis zu drei erfasste Bildschirme des Stratvorgangs für späteres Debugging.
- iDRAC6-Warnungen - Warnt Sie anhand einer E-Mail-Benachrichtigung oder eines SNMP-Traps über potenzielle Problemen verwalteter Knoten
- Remote-Stromverwaltung - Remote-Stromverwaltungsfunktionen wie Herunterfahren und Reset von einer Verwaltungskonsole aus
- Einfache Anmeldung über die CMC-Webschnittstelle - Sobald Sie sich beim CMC angemeldet haben, können Sie auf beliebige iDRACs im Gehäuse zugreifen, ohne sich noch einmal anmelden zu müssen
- One-to-Many-Firmware-Aktualisierung - Ermöglicht eine automatische Aktualisierung von mehr als einem iDRAC6, ohne dass ein Benutzer eingreifen muss
- 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 - Bietet zuweisbare Berechtigungen für verschiedene Systemverwaltungs-Tasks

---

iDRAC-Sicherheitsfunktionen

iDRAC6 enthält die folgenden Sicherheitsfunktionen:

- Benutzerauthentifizierung durch Microsoft Active Directory (optional) oder durch hardwaregespeicherte Benutzer-IDs und Kennwörter
- Rollenbasierte Berechtigung, die einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren
- Benutzer-ID- und Kennwort-Konfiguration über die Webschnittstelle, SM-CLP oder lokalen RACADM
- 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 zu iDRAC6 herstellen

---

Verbesserungen der iDRAC6-Firmware

Zusätzlich wurden wichtige Verbesserungen im Code implementiert

- Bedeutende Verbesserungen der Leistung beim Einsehen des Active Directory
- Verbesserte Reaktionsfähigkeit des TCP-IP-Netzwerkbetriebs-Stacks
- Verbesserte Funktionszustandsschnittstelle zwischen iDRAC6 und CMC
- Sicherheitsverbesserungen unter Verwendung von Analyse-Tools von Fremdherstellern

---

Unterstützte Plattformen

iDRAC6 unterstützt die folgenden PowerEdge-Systeme im Dell PowerEdge M1000e-Systemgehäuse:

- PowerEdge M610
- PowerEdge M710

Informationen zu den neuesten unterstützten Plattformen finden Sie in der Infodatei (Readme) zu iDRAC6 auf Dell Support-Website unter **support.dell.com/manuals**.

Unterstützte Betriebssysteme

Tabelle 1-1 führt die Betriebssysteme auf, die iDRAC6 unterstützen.

Die *Dell Systems Software Support Matrix* auf der Dell Support-Website unter **support.dell.com/manuals** enthält die neuesten Informationen.

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 MS HyperV 2008 **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® Enterprise	Enterprise Linux WS, ES und AS (Version 4) (x86 und x86_64)

Linux®	Enterprise Linux 5 (x86 und x86_64)
SUSE® Linux	Enterprise Server 10 (Gold) (x86_64)
VMware	ESX 3.5 U4

Unterstützte Webbrowser

Tabelle 1-2 führt die als iDRAC6-Clients unterstützten Webbrowser auf.

Neueste Informationen befinden sich in der iDRAC6-Infodatei (Readme) und der *Dell Systems Software Support Matrix* auf der Dell Support-Website unter **support.dell.com/manuals**.

ANMERKUNG: Aufgrund von ernsthaften Sicherheitslücken wird SSL 2.0 nicht mehr unterstützt. Damit Ihr Browser ordnungsgemäß funktioniert, müssen Sie SSL 3.0 aktivieren.

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 2.0/3.0 für Windows (nur Java vKVM/vMedia-Konsole)
Linux	Mozilla Firefox 2.0/3.0 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-Zugriffsverbindungen

Verbindung	Funktionen
iDRAC6-NIC	• 10Mbps/100Mbs/1Gbps Ethernet über CMC Gb Ethernet-Schnittstelle • DHCP-Unterstützung • SNMP-Traps und E-Mail-Ereignis-Benachrichtigung • Unterstützung für SM-CLP-Befehls-Shell (Telnet oder SSH), für Verfahren wie iDRAC6-Konfigurations-, Systemstart-, Reset- sowie Einschalt- und Herunterfahren-Befehle • Unterstützung für IPMI-Dienstprogramme, wie IPMitool und ipmish

iDRAC6-Anschlüsse

Tabelle 1-4 führt die Anschlüsse auf, die iDRAC6 auf Verbindungen abhört. Tabelle 1-5 kennzeichnet die Anschlüsse, die iDRAC6 als Client verwendet. Diese Informationen sind erforderlich, wenn Firewalls für den Remote-Zugriff auf einen iDRAC6 geöffnet werden.

Tabelle 1-4. Abhöranschlüsse des iDRAC6-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. iDRAC6 Client-Anschlüsse

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

Weitere nützliche Dokumente

Zusätzlich zu diesem *Benutzerhandbuch* enthalten die folgenden Dokumente weitere Informationen zum Setup und Betrieb des iDRAC6 auf Ihrem System:

- Die iDRAC6-Online-Hilfe enthält Informationen zur Verwendung der Webschnittstelle.
- Das *Dell Chassis Management Controller Firmware Version 2.0-Benutzerhandbuch* und das *Dell Chassis Management Controller Firmware Version 2.0-Administrator-Referenzhandbuch* enthalten Informationen zur Verwendung des Controllers, der alle Module in dem Gehäuse verwaltet, das Ihren 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 *Dell Update Packages-Benutzerhandbuch* enthält Informationen zum Abrufen und Verwenden von Dell Update Packages als Teil Ihrer Systemaktualisierungsstrategie.
- Das *Dell Unified Server Configurator-Benutzerhandbuch* enthält Informationen zur Installation und Ausführung des Unified Server Configurator.

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

- In den mit dem System gelieferten Sicherheitshinweisen finden Sie wichtige Informationen zur Sicherheit und zu den Betriebsbestimmungen. Weitere Betriebsbestimmungen finden Sie auf der Website zur ?Einhaltung gesetzlicher Normen unter **www.dell.com/regulatory_compliance.** Garantiebestimmungen können als separates Dokument beigelegt sein.
- Der *Getting Started Guide* (das Handbuch zum Einstieg) enthält eine Übersicht über die Systemfunktionen, die Einrichtung des Systems und technische Daten.
- Im *Hardware-Benutzerhandbuch* erhalten Sie Informationen über Systemfunktionen, zur Fehlerbehebung am System und zum Installieren oder Austauschen von Systemkomponenten.
- In der Dokumentation zur Systemverwaltungssoftware sind die Merkmale, die Anforderungen, die Installation und der grundlegende Einsatz der Software beschrieben.
- In der Dokumentation zum Betriebssystem ist beschrieben, wie das Betriebssystem installiert (sofern erforderlich), konfiguriert und verwendet wird.
- Dokumentationen für alle separat erworbenen Komponenten enthalten Informationen zur Konfiguration und zur Installation dieser Zusatzgeräte.
- Möglicherweise sind auch aktualisierte Dokumente beigelegt, in denen Änderungen am System, an der Software und/oder an der Dokumentation beschrieben sind.

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

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6 Enterprise konfigurieren

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

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

Bevor Sie beginnen

Legen Sie vor der Konfiguration von iDRAC6 Folgendes zurecht:

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

Die *DVD Dell Systems Management Tools and Documentation* ist bei den folgenden Komponenten enthalten:

- DVD root - Enthält das Dell Systems Build and Update Utility, welches Informationen zur Einrichtung des Servers und der Systeminstallation enthält.
- SYSMGMT - Enthält die Systemmanagement-Softwareprodukte einschließlich Dell OpenManage Server Administrator.
- DOCS - Enthält die Dokumentation für Systeme, Softwareprodukte zur Systemverwaltung, Peripheriegeräte und RAID-Controller.
- SERVICE - Enthält die Hilfsmittel, die Sie benötigen, um Ihr System zu konfigurieren, und liefert die neuesten Diagnosen und Dell-optimierte Treiber für Ihr System.

Weitere Informationen finden Sie im *Server Administrator-Benutzerhandbuch*, im *IT Assistant-Benutzerhandbuch* und im *Unified Server Configurator-Benutzerhandbuch* auf der Dell Support-Website unter **support.dell.com\manuals**.

Schnittstellen zur Konfiguration des iDRAC6

Sie können iDRAC6 mithilfe des iDRAC6-Konfigurationsdienstprogramms, der iDRAC6-Webschnittstelle, der lokalen RACADM-CLI oder der SM-CLP-CLI konfigurieren. Die lokale RACADM-CLI steht nach der Installation des Betriebssystems und der Dell OpenManage-Server Management-Software auf dem verwalteten Server zur Verfügung. Tabelle 2-1 beschreibt diese Schnittstellen.

Für höhere Sicherheit kann der Zugang zur iDRAC6-Konfiguration über das iDRAC6-Konfigurationsdienstprogramm oder die lokale RACADM-CLI durch einen RACADM-Befehl (siehe "Übersicht der RACADM-Unterbefehle") 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
iDRAC6 Konfiguration Dienstprogramm	Das iDRAC6-Konfigurationshilfsprogramm wird zum Startzeitpunkt des Starts verwendet. Das Programm ist dieses beim Installieren eines neuen PowerEdge-Servers nützlich. Verwenden Sie es zum Einrichten des Netzwerks und grundlegender Sicherheitsfunktionen sowie zum Aktivieren anderer Funktionen.
iDRAC6-Webschnittstelle	Die iDRAC6-Webschnittstelle ist eine browser-basierte Verwaltungsanwendung, die Sie zur interaktiven Verwaltung des iDRAC6 und zur Überwachung des verwalteten Servers verwenden können. Sie stellt die primäre Schnittstelle für alltägliche Aufgaben wie die Überwachung des Systemzustands, die Anzeige des Systemereignisprotokolls, die Verwaltung lokaler iDRAC6-Benutzer und das Starten der CMC-Webschnittstelle und der 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, iDRAC6-Netzwerkeinstellungen zu konfigurieren, sowie den Managed Server zu starten, anzuhalten oder zurückzusetzen.
Gehäuse-LCD-Bedienfeld	Das LCD-Bedienfeld des Gehäuses, welches iDRAC6 enthält, kann zur Anzeige des High-Level-Status der Server im Gehäuse verwendet werden. Während der erstmaligen Konfiguration des CMC erlaubt Ihnen der Konfigurationsassistent, die DHCP-Konfiguration des iDRAC6-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 iDRAC6-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 iDRAC6. Sie können Sensordaten, Protokolleinträge von Systemereignissen sowie die im iDRAC6 geführten aktuellen Status- und Konfigurationswerte untersuchen. Sie können iDRAC6-Konfigurationswerte verändern, lokale Benutzer verwalten, Funktionen aktivieren und deaktivieren sowie Stromfunktionen wie das Herunterfahren oder Neustarten des verwalteten Servers ausführen.
iVMCLI	Die iDRAC6-Befehlszeilenoberfläche des virtuellen Datenträgers (iVM-CLI) bietet dem verwalteten Server Zugriff auf Datenträger auf der Verwaltungsstation. Sie ist hilfreich beim Entwickeln von Scripts zum Installieren von Betriebssystemen auf mehreren verwalteten Servern.

SM-CLP	SM-CLP ist die Implementierung des in iDRAC6 umgesetzten Server Management Workgroup Server Management-Command Line Protocol. Auf die SM-CLP-Befehlszeile kann durch die Anmeldung an iDRAC6 über Telnet oder SSH zugegriffen werden. SM-CLP-Befehle setzen einen nützlichen Teilsatz der Befehle des lokalen RACADM um. Die Befehle sind beim Scripting nützlich, 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 iDRAC6, um mit anderen integrierten Systemen und Verwaltungsanwendungen zu kommunizieren. Sie können die iDRAC6-Webschnittstellen-, SM-CLP- oder RACADM-Befehle zur Konfiguration von IPMI-Plattformereignisfiltern (PEF) und Plattformereignis-Traps (PET) verwenden. PEF bewirken, dass iDRAC6 bestimmte Maßnahmen ausführt (z. B. den Neustart des verwalteten Servers), wenn ein entsprechender Zustand festgestellt wird. PET weisen das iDRAC6 an, E-Mail- oder IPMI-Warnungen zu senden, wenn bestimmte Ereignisse oder Zustände festgestellt werden. Sie können auch standardmäßige IPMI-Hilfsprogramme wie **IPMItool** und **ipmish** mit iDRAC6 verwenden, wenn Sie IPMI-über-LAN aktivieren.

Konfigurations-Tasks

Dieser Abschnitt stellt eine Übersicht der Konfigurations-Tasks für die Verwaltungsstation, den iDRAC6 und den verwalteten Server dar. Die auszuführenden Tasks schließen die Konfiguration des iDRAC6 ein, damit es im Remote-Zugriff eingesetzt werden kann, die Konfiguration der iDRAC6-Funktionen, die Sie verwenden möchten, die Installation des Betriebssystems auf dem verwalteten Server sowie 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".

iDRAC6-Netzwerkbetrieb konfigurieren

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

ANMERKUNG: Der Zugang zur iDRAC6-Konfiguration über das iDRAC6-Konfigurationsdienstprogramm oder die lokale RACADM-CLI kann mit einem RACADM-Befehl (siehe "Übersicht der RACADM-Unterbefehle") oder von der GUI aus (siehe "Lokalen Konfigurationszugriff aktivieren oder deaktivieren") deaktiviert werden.

ANMERKUNG: Eine Änderung der iDRAC6-Netzwerkeinstellungen unterbricht alle aktuellen Netzwerkverbindungen zum iDRAC6.

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 iDRAC6 nicht mehr über das LCD-Bedienfeld neu konfiguriert werden.

ANMERKUNG: Das LCD-Bedienfeld kann zum Aktivieren des DHCP zur Konfiguration des iDRAC6-Netzwerks verwendet werden. Wenn Sie statische Adressen zuweisen möchten, ist es erforderlich, dass Sie das iDRAC6-Konfigurationshilfsprogramm oder die CMC-Webschnittstelle verwenden.

- LCD-Bedienfeld des Gehäuses - siehe *Benutzerhandbuch zur Dell Chassis Management Controller-Firmware*
- iDRAC6-Konfigurationsdienstprogramm - siehe "iDRAC6-Konfigurationsdienstprogramm verwenden"
- CMC-Webschnittstelle - siehe "Netzwerkbetrieb mittels der CMC-Webschnittstelle konfigurieren"
- RACADM - siehe "cfgLanNetworking"

iDRAC6-Benutzer konfigurieren

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

- iDRAC6-Konfigurationsdienstprogramm (konfiguriert nur den Benutzer auf Administratorebene) - siehe "LAN-Benutzerkonfiguration"
- iDRAC6-Webschnittstelle - siehe "iDRAC6-Benutzer hinzufügen und konfigurieren"
- RACADM - siehe "Einen iDRAC6-Benutzer hinzufügen"

ANMERKUNG: Wenn iDRAC6 in einer Active Directory-Umgebung verwendet wird, müssen die von Ihnen erstellten Benutzernamen mit der gültigen Active Directory-Benennungsregel übereinstimmen.

Active Directory konfigurieren

Zusätzlich zu den lokalen Benutzern des iDRAC6 können Sie Microsoft® Active Directory® zum Authentifizieren von iDRAC6-Benutzeranmeldungen verwenden.

Weitere Informationen finden Sie unter "iDRAC6 mit Microsoft Active Directory verwenden".

ANMERKUNG: Wenn iDRAC6 in einer Active Directory-Umgebung verwendet wird, müssen Sie sicherstellen, dass Ihre Benutzernamen mit der gültigen 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.

- iDRAC6-Webschnittstelle - siehe "IP-Filterung und IP-Blockierung konfigurieren"
- RACADM - siehe "IP-Filterung konfigurieren (IP-Bereich)" und "IP-Blockierung konfigurieren"

Plattformereignisse konfigurieren

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

Konfigurieren Sie Plattformereignisfilter (PEF) zum Auswählen der Ereignisse, die Sie feststellen möchten, z. B. Neustarten eines verwalteten Servers bei Feststellung eines Ereignisses.

- iDRAC6-Webschnittstelle - siehe "Plattformereignisfilter (PEF) konfigurieren"
- RACADM - siehe "PEF konfigurieren"

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

- iDRAC6-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 iDRAC6-Konfigurationsdienstprogramm (beim Start) blockiert. Internetzugriff auf Konfigurationsparameter wird nicht behindert und Konfigurationsdaten stehen immer zur Ansicht zur Verfügung. Informationen über die iDRAC6-Webschnittstelle finden Sie unter "Lokalen Konfigurationszugriff aktivieren oder deaktivieren". cfgRac-Tuning-Befehle siehe "cfgRacTuning".

iDRAC6-Dienste konfigurieren

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

- iDRAC6-Webschnittstelle - siehe "iDRAC6-Dienste konfigurieren"
- RACADM - siehe "iDRAC6-Telnet- und SSH-Dienste mittels lokalem RACADM konfigurieren"

SSL konfigurieren

SSL für den iDRAC6-Web-Server konfigurieren.

- iDRAC6-Webschnittstelle - siehe "Secure Sockets Layer (SSL)"
- RACADM - siehe "cfgRacSecurity," "sslcsrgen," "sslcertupload," "sslcertdownload," und "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.

- iDRAC6-Webschnittstelle - siehe "Virtuellen Datenträger konfigurieren und verwenden"
- iDRAC6-Konfigurationsdienstprogramm - siehe "Virtuellen Datenträger konfigurieren"

Konfigurieren einer VFlash-Medienkarte

VFlash--Medienkarte für Verwendung mit iDRAC6 installieren und konfigurieren.

- iDRAC6-Webschnittstelle - siehe "Eine VFlash-Medienkarte zur Verwendung mit iDRAC6 konfigurieren"

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"
- iVMCLI - Siehe "Befehlszeilenoberflächen-Dienstprogramm des virtuellen Datenträgers verwenden"

Verwalteten Server für die Funktion Bildschirm Letzter Absturz konfigurieren

Richten Sie den verwalteten Server so ein, dass iDRAC6 nach Absturz oder Blockierung des Betriebssystems einen Screenshot erstellen kann.

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

Netzwerkbetrieb mittels der CMC- Webschnittstelle konfigurieren

ANMERKUNG: Sie müssen Administratorrechte für die Gehäusekonfiguration (Chassis Configuration Administrator) besitzen, um iDRAC6-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 iDRAC6-Webschnittstelle zur Verfügung, wenn Sie auf **System**→ **Remote-Zugriff**→ **CMC** klicken. Es ist auch möglich, die CMC-Webschnittstelle von diesem Bildschirm aus zu starten.

Die webbasierte iDRAC6-Schnittstelle von CMC aus starten

Der CMC bietet eine eingeschränkte Verwaltung von individuellen Gehäusekomponenten, wie z. B. Server. Zur kompletten Verwaltung dieser individuellen Komponenten bietet der CMC einen Startpunkt für die webbasierte iDRAC6-Schnittstelle des Servers.

iDRAC6 vom Bildschirm des **Servers** aus starten:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Server** aus.

   Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf das Symbol **iDRAC GUI starten** für den Server, den Sie verwalten wollen.

Sie können die webbasierte iDRAC6-Schnittstelle für einen einzelnen Server mittels der **Server**-Liste in der Systemstruktur starten:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Erweitern Sie in der Systemstruktur **Server**.

   Es werden alle Server (1-16) in der erweiterten Liste der **Server** angezeigt.
3. Klicken Sie auf den Server, den Sie anzeigen möchten.

   Der **Serverstatus**-Bildschirm für den ausgewählten Server wird angezeigt.
4. Klicken Sie auf das Symbol **iDRAC GUI starten**.

Einzelanmeldung

Über die Funktion der einfachen Anmeldung können Sie die webbasierte iDRAC6-Schnittstelle aus dem CMC starten, ohne dass Sie sich erneut anmelden müssen. Die Richtlinien der Einzelanmeldung sind nachfolgend beschrieben.

- Ein CMC-Benutzer, dessen **Benutzerberechtigungen** auf **Serveradministrator** eingestellt sind, wird automatisch mit der Einzelanmeldung an der

webbasierten Schnittstelle von iDRAC6 angemeldet. Nach der Anmeldung werden dem Benutzer automatisch iDRAC6 Administratorrechte zugewiesen. Dies gilt sogar dann, wenn derselbe Benutzer kein Konto auf iDRAC6 besitzt oder das Konto keine Administratorrechte hat.

- Ein CMC-Benutzer, dessen **Benutzerberechtigungen** nicht auf **Serveradministrator** eingestellt sind, der aber dasselbe Konto auf iDRAC6 besitzt, wird automatisch mit der Einzelanmeldung bei iDRAC6 angemeldet. Nach der Anmeldung auf der webbasierten Schnittstelle von iDRAC6 werden diesem Benutzer die Berechtigungen zugewiesen, die für das iDRAC6-Konto erstellt wurden.

ANMERKUNG: Die Bezeichnung "dasselbe Konto" bedeutet in diesem Zusammenhang, dass der Benutzer denselben Anmeldenamen mit einem übereinstimmenden Kennwort für CMC und für iDRAC6 besitzt. Der Benutzer, der denselben Anmeldenamen, jedoch ein anderes Kennwort hat, wird nicht als gültiger Benutzer erkannt.

- Ein CMC-Benutzer, dessen **Benutzerberechtigungen** nicht auf **Serveradministrator** bzw. das selbe Konto auf iDRAC6 eingestellt sind, wird *nicht* automatisch mit der Einzelanmeldung bei iDRAC6 angemeldet. Dieser Benutzer wird zur iDRAC6-Anmeldebildschirm umgeleitet, wenn die Schaltfläche **iDRAC6 GUI starten** geklickt wird.

ANMERKUNG: In diesem Fall werden Benutzer eventuell aufgefordert, sich bei iDRAC6 anzumelden.

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

ANMERKUNG: Wenn der Server vom Gehäuse entfernt wird, die iDRAC6-IP-Adresse geändert wird oder die iDRAC6-Netzwerkverbindung ein Problem aufweist, kann das Klicken auf das Symbol **iDRAC6 GUI starten** zur Anzeige eines Fehlerbildschirms führen.

Netzwerkbetrieb für iDRAC6 konfigurieren

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

2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit**:

   Aktivieren oder Deaktivieren von Seriell über LAN:

   a. Klicken Sie auf **Seriell über LAN**.

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

   b. Wählen Sie das Kontrollkästchen **Seriell über LAN aktivieren** aus. Sie können auch die Einstellungen **Baudrate** und **Beschränkung der Channel-Berechtigungsebene** ändern.

   c. Klicken Sie auf **Anwenden**.

   Aktivieren oder Deaktivieren von IPMI über LAN:

   a. Klicken Sie auf **Netzwerk**.

      Die Anzeige **Netzwerkkonfiguration** wird eingeblendet.

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

   c. Wählen Sie das Kontrollkästchen **IPMI-Über-LAN aktivieren** aus. Sie können auch die Einstellungen **Verschlüsselungsschlüssel** und **Beschränkung der Channel-Berechtigungsebene** ändern.

   d. Klicken Sie auf **Anwenden**.

   Aktivieren oder Deaktivieren von DHCP:

   a. Klicken Sie auf **Netzwerk**.

      Die Anzeige **Netzwerkkonfiguration** wird eingeblendet.

   b. Klicken Sie auf **Netzwerkeinstellungen**.

      - Um DHCP für NIC-IP Adressen zu verwenden, wählen Sie das Kontrollkästchen **DHCP verwenden (für NIC-IP-Adresse)** aus.
      - Um DHCP zum Abrufen von DNS-Serveradressen zu verwenden, wählen Sie das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** aus.

   c. Klicken Sie auf **Anwenden**.

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

Verbindungen der FlexAddress-Mezzanine- Kartenarchitektur anzeigen

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

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

Die Konfiguration der Funktion FlexAddress wird mithilfe der CMC-Webschnittstelle ausgeführt. Weitere Informationen zur Funktion FlexAddress und deren Konfiguration finden Sie im *Benutzerhandbuch Dell Chassis Management Controller-Firmware Version 2.0*.

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, der Lage des Architekturanschlusses, des Architekturtyps und

der server-konfigurierten oder gehäuse-zugewiesenen MAC-Adressen für jedes installierte, 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.

---

iDRAC6-Firmware aktualisieren

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

- SM-CLP-Befehl **load**
- iDRAC6-Webschnittstelle
- Dell Update Package (für Linux oder Microsoft Windows)
- DOS-iDRAC6-Firmware-Aktualisierungsdienstprogramm
- CMC-Webschnittstelle

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 iDRAC6-Firmware über die iDRAC6-Webschnittstelle oder SM-CLP oder zum Wiederherstellen des iDRAC6 mittels der CMC-Webschnittstelle das als selbstextrahierendes Archiv verpackte Binärbild herunter.

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

Laden Sie zum Aktualisieren der iDRAC6-Firmware anhand des DOS-iDRAC6-Firmware-Aktualisierungsdienstprogramms sowohl das Aktualisierungsdienstprogramm als auch das Binärbild herunter, die in selbstextrahierenden Archivdateien verpackt sind.

Firmware-Aktualisierung ausführen

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

ANMERKUNG: Während der iDRAC6-Firmware-Aktualisierung laufen die Gehäuselüfter bei 100% Kapazität. Nach Abschluss der Aktualisierung wird die normale 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 iDRAC6 weiterleiten kann. Siehe iDRAC6-Firmware mittels SM-CLP aktualisieren".

Legen Sie das Firmware-Binärbild bei Verwendung der iDRAC6-Webschnittstelle oder der CMC-Webschnittstelle auf einer Festplatte ab, auf die die Verwaltungsstation zugreifen kann, von der aus Sie die Webschnittstelle ausführen. Siehe Aktualisiert die iDRAC6-Firmware".

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

Die iDRAC6-Firmware kann mit der CMC-Webschnittstelle oder CMC RACADM aktualisiert werden. Diese Funktion ist sowohl im Normalbetrieb der iDRAC6-Firmware verfügbar als auch dann, wenn diese beschädigt ist. Siehe Aktualisieren der iDRAC6-Firmware mittels CMC".

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

ANMERKUNG: Wenn Sie die iDRAC6-Firmware von Version 1.20 auf eine frühere Version zurückdatieren, muss das vorhandene Internet Explorer ActiveX® Browser-Plug-in auf jeder Windows-basierten Management Station gelöscht werden, damit die Firmware eine kompatible Version des ActiveX-Plug-in installieren kann. Weitere Informationen finden Sie unter ActiveX Plug-in löschen".

ActiveX Plug-in löschen

Sie müssen das vorhandene Internet Explorer ActiveX Browser-Plug-in auf jeder Windows-basierten Management Station löschen, damit die Firmware eine kompatible Version des ActiveX-Plug-in installieren kann.

Das ActiveX Plug-in in Internet Explorer 6 löschen:

1. Wechseln Sie zu **C:\WINDOWS\Downloaded Program Files**.
2. Löschen Sie die Datei **DELL IDRAC 11G AVCView**.

Das ActiveX Plug-in in Internet Explorer 7 löschen:

1. Öffnen Sie Internet Explorer 7.
2. Betätigen Sie die <Alt> Taste, um bei Bedarf die Menüleiste einzublenden.
3. Klicken Sie auf **Extras**→ **Add-Ons verwalten**→ **Add-Ons aktivieren und deaktivieren**.
4. Wählen Sie im Fenster **Add-Ons verwalten Heruntergeladene ActiveX Controls (32-Bit)** aus dem Drop-Down-Menü **Show** aus.
5. Klicken Sie in der **Aktiviert** Liste auf **DELL IDRAC 11G AVCView** und klicken Sie anschließend die Schaltfläche **Löschen** im Abschnitt **ActiveX löschen**.
6. Klicken Sie auf **OK**.

iDRAC6-Webschnittstelle verwenden

VORSICHT: Wenn die iDRAC6-Firmware beschädigt wird, was eintreten könnte, wenn der iDRAC6-Firmware-Aktualisierungsvorgang vor seinem Abschluss abgebrochen wird, können Sie iDRAC6 mithilfe der iDRAC6-Webschnittstelle wiederherstellen.

ANMERKUNG: Die Firmware-Aktualisierung behält standardmäßig die aktuellen iDRAC6-Einstellungen bei. Während des Aktualisierungsvorgangs haben Sie die Möglichkeit, die iDRAC6-Konfiguration auf die 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 iDRAC6-Konfigurationshilfsprogramms aktiviert und konfiguriert werden.

1. Starten Sie die iDRAC6-Webschnittstelle.
2. Wählen Sie in der Systemstruktur **System**→ **Remote-Zugriff**→ **iDRAC** aus.
3. Klicken Sie auf die Registerkarte **Update** (Aktualisieren).

   Die Anzeige **Firmware Update** (Firmwareaktualisierung) wird eingeblendet.

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

4. Klicken Sie im Abschnitt **Hochladen (Schritt 1 bis 4)** auf **Durchsuchen, um nach den** von Ihnen heruntergeladenen Firmware-Image zu suchen. Sie können auch den Dateipfad im Textfeld eingeben. Zum Beispiel:

   `C:\Updates\V2.0\<Image-Name>`.

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

5. Klicken Sie auf **Hochladen**.

   Die Datei wird auf iDRAC6 hochgeladen. Dieser Vorgang kann mehrere Minuten beanspruchen.

   ANMERKUNG: Sie können während des Hochladevorgangs das Firmware-Upgrade abbrechen, indem Sie auf **Abbrechen** klicken. Klicken Sie auf **Abbrechen**, wird iDRAC6 in den normalen Betriebsmodus zurückgesetzt.

   Ist der Hochladevorgang abgeschlossen, wird die Anzeige **Firmware Update - Validierung (Seite 2 von 4)** eingeblendet..

   - Wenn die Image-Datei erfolgreich hochgeladen wurde und alle Überprüfungsvorgänge durchlaufen sind, wird eine Meldung mit dem Inhalt, dass das Firmware-Image überprüft wurde, eingeblendet.
   - Wenn das Image nicht erfolgreich hochgeladen wurde oder die Überprüfungsvorgänge nicht bestanden hat, wechselt die Firmware-Aktualisierung zur Anzeige **Firmware-Aktualisierung** zurück. Sie können versuchen, iDRAC6 erneut zu aktualisieren oder auf **Abbrechen** klicken, um iDRAC6 in den normalen Betriebsmodus zurückzusetzen.

   ANMERKUNG: Wenn Sie die Markierung im Kontrollkästchen Konfiguration beibehalten entfernen, wird iDRAC6 auf seine Standardeinstellungen zurückgesetzt. In der Standardeinstellung ist LAN deaktiviert und Sie können sich nicht über die iDRAC6-Webschnittstelle anmelden. Sie müssen die LAN-Einstellungen während des BIOS POST mittels dem iDRAC6-Konfigurationsdienstprogramm neu konfigurieren.

6. Standardmäßig ist die Option **Konfiguration sichern** ausgewählt (markiert), um die aktuellen Einstellungen auf iDRAC6 nach einem Upgrade zu sichern. Wenn die Einstellungen nicht beibehalten werden sollen, entfernen Sie die Markierung im Kontrollkästchen **Konfiguration beibehalten**.
7. Klicken Sie auf **Aktualisierung starten**, um den Aktualisierungsvorgang zu starten. Unterbrechen Sie den Aktualisierungsvorgang nicht.
8. 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.
9. Sobald die Firmware-Aktualisierung abgeschlossen ist, wird das Fenster **Firmware-Aktualisierung - Aktualisierungsergebnisse (Seite 4 von 4)** angezeigt und iDRAC6 automatisch zurückgesetzt. Sie müssen das aktuelle Browserfenster schließen und eine neue iDRAC6-Verbindung in einem neuen Browserfenster herstellen.

DOS-Aktualisierungsdienstprogramm verwenden

Starten Sie zum Aktualisieren der iDRAC6-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 iDRAC6-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>` - Gibt den Dateinamen des Firmware-Images an. Diese Option ist erforderlich, wenn der Firmware-Dateiname geändert wurde und jetzt vom Standardnamen **firmimg.imc** abweicht.
- `-l=<Protokolldatei>` - Protokolliert die Ausgabe der Aktualisierungsaktivität. Diese Option wird für das Debuggen verwendet.

ANMERKUNG: Wenn Sie zum Befehl **idrac16d** falsche Argumente eingeben oder die Option -h angeben, 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 iDRAC6-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 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. (Product Group) <linux-security@dell.com> Primary key fingerprint: 4172 E2CE 955A 1776 A5E6
      1BB7 CA77 951D 23B6 6A9D (pub 1024D/23B66A9D 2001-04-16 Dell, Inc. (Produktgruppe) <linux-security@dell.com> Primärer
      Schlüsselfingerabdruck: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D)
      ```

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

   c. 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 ein und betätigen Sie die <Eingabetaste>. 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 <Eingabetaste> ein, um Ihre Auswahl zu bestätigen.

f. Geben Sie quit <Eingabetaste> 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**. Das iDRAC6-Firmware-Image hat beispielsweise eine zugeordnete **.sign** Datei (**IDRAC_FRMW_LX_2.0.BIN.sign**), die im selbstextrahierenden Archiv mit dem Firmware-Image enthalten ist (**IDRAC_FRMW_LX_2.0.BIN**). 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™ M610-iDRAC6-Aktualisierungspakets dargestellt:

1. Laden Sie die beiden folgenden Dateien von **support.dell.com** herunter:
   - IDRAC_FRMW_LX_2.0.BIN.sign
   - IDRAC_FRMW_LX_2.0.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) <linuxsecurity@ 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>" 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 <Eingabetaste> ein, um I trust ultimately (Ich habe absolutes Vertrauen) aus dem Menü auszuwählen.

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

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

Damit ist die Validierung des öffentlichen Schlüssels von Dell abgeschlossen.

4. Überprüfen Sie die Digitalsignatur des PowerEdge-M610-iDRAC-Pakets durch Ausführen des folgenden Befehls:

```
gpg --verify IDRAC_FRMW_LX_2.0.BIN.sign IDRAC_FRMW_LX_2.0.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 iDRAC6 verwendet werden können, muss der Browser-Cache zum Entfernen/Löschen aller *alter* Webseiten, die eventuell im System gespeichert sind, gelöscht werden.

Internet Explorer 6

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

   Das Fenster **Internetoptionen** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Allgemein**.
4. Klicken Sie unter **Temporäre Internetdateien** auf **Dateien löschen**.

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

Internet Explorer 7

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

   Das Fenster **Internetoptionen** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Allgemein**.
4. Klicken Sie unter **Browserverlauf** auf **Löschen ...**.

   Das Fenster **Dateien löschen** wird angezeigt.
5. Klicken Sie neben **Temporäre Internetdateien** auf **Dateien löschen**.
6. Klicken Sie auf **Schließen** und anschließend 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).

Aktualisieren des USC Reparatur-Pakets

Weitere Informationen zur Aktualisierung des USC Reparatur-Pakets über die iDRAC6-Webschnittstelle finden Sie im *Dell Unified Server Configurator Benutzerhandbuch*.

---

iDRAC6 zur Verwendung mit IT Assistant konfigurieren

Dell™ OpenManage™ IT Assistant dient zur Ermittlung verwalteter Geräte, welche die Anforderungen für SNMP-v1 und -v2c (Einfaches Netzwerkverwaltungsprotokoll) und IPMI-Version 2.0 (Intelligente Plattform-Managementschnittstelle) erfüllen.

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

iDRAC6-Konfigurationsdienstprogramm zum Aktivieren von Ermittlung und Überwachung verwenden

Um einen iDRAC6 für die IPMI-Ermittlung sowie das Senden von Warnungs-Traps auf der Stufe des iDRAC6-Konfigurationsdienstprogramms einzurichten, müssen Sie Ihren verwalteten Server (Blade) neu starten und sein Einschalten über das iKVM sowie entweder einen Remote-Monitor und eine Konsolentastatur oder eine SOL-Verbindung (Seriell über LAN) beobachten. Wird `Press<Ctrl-E> for Remote Access Setup (Drücken Sie <Strg-E> für Setup im Remote-Zugriff)` angezeigt, betätigen Sie die Tasten <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 Pfeiltasten Nach-oben- und Nach-unten.
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 **iDRAC6-Name** ein. Die Standardeinstellung lautet `iDRAC6-{Service- Tag-Nummer}`.

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

iDRAC6-Webschnittstelle zum Aktivieren von Ermittlung und Überwachung verwenden

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

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der iDRAC6 webbasierten Schnittstelle als Administrator mit dem entsprechenden Kennwort an.
3. Wählen Sie in der Systemstruktur **System**→ **Remote-Zugriff**→ **iDRAC** aus.
4. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit**.

   Die Anzeige **Netzwerkkonfiguration** wird eingeblendet.
5. Klicken Sie auf **IPMI LAN-Einstellungen**.
6. Stellen Sie sicher, dass das Kontrollkästchen **IPMI-Über-LAN aktivieren** ausgewählt (aktiviert) ist.
7. Wählen Sie aus dem Drop-Down-Menü **Berechtigungen auf Kanalebene Administrator** aus.

8. Geben Sie, falls verwendet, den **Verschlüsselungsschlüssel** für RMCP+ Ihrer Site ein.
9. Klicken Sie auf **Anwenden**, falls Sie Änderungen in diesem Bildschirm vorgenommen haben.
10. Wählen Sie in der Systemstruktur **System** aus.
11. Klicken Sie auf das Register **Warnungsverwaltung** und dann auf **Plattformereignisse**.

    Die Anzeige **Plattformereignisse** wird eingeblendet und zeigt die Liste der Ereignisse an, für die Sie iDRAC6 zum Erzeugen von E-Mail-Warnungen konfigurieren können.
12. Aktivieren Sie die E-Mail-Warnungen für ein oder mehrere Ereignisse, indem Sie das Kontrollkästchen in der Spalte **Warnungen erzeugen** auswählen.
13. Klicken Sie auf **Anwenden**, falls Sie Änderungen in diesem Bildschirm vorgenommen haben.
14. Klicken Sie auf **Trap-Einstellungen**.

    Der Bildschirm **Plattformereigniswarnungsziele** wird eingeblendet.
15. Wählen Sie im ersten verfügbaren Feld **Ziel-IP-Adresse** im Abschnitt **IPv4 Zielliste** das Kontrollkästchen **Aktiviert** aus und geben Sie anschließend die IP-Adresse Ihrer Management-Station ein.
16. Klicken Sie auf **Anwenden**, falls Sie Änderungen in diesem Bildschirm vorgenommen haben.

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

Dell empfiehlt dringend, dass Sie zu Sicherheitszwecken für IPMI-Befehle einen separaten Benutzer mit eigenem Benutzernamen, IPMI-über-LAN-Berechtigungen und Kennwort einrichten.

1. Wählen Sie in der Systemstruktur **System**→ **Remote-Zugriff**→ **iDRAC** aus.
2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit** und dann auf **Benutzer**.

   Die Anzeige **Benutzer** wird eingeblendet und zeigt die Liste aller Benutzer an (definiert oder nicht definiert).
3. Klicken Sie auf die **Benutzer-ID** eines nicht definierten Benutzers.

   Die Anzeige **Benutzerkonfiguration** der ausgewählten Benutzer-ID wird eingeblendet.
4. Wählen Sie das Kontrollkästchen **Benutzer aktivieren** und geben Sie anschließend den Benutzernamen und das Kennwort ein.
5. Stellen Sie sicher, dass im Abschnitt **IPMI LAN Berechtigung Maximale LAN-Benutzerberechtigung gewährt** auf **Administrator** eingestellt ist.
6. Legen Sie weitere Benutzerberechtigungen nach Bedarf fest.
7. Klicken Sie auf **Anwenden**, um die neuen Benutzereinstellungen zu speichern.

Dell IT Assistant zum Anzeigen des iDRAC6-Status und -Ereignissen verwenden

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

iDRAC6-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 Dell OpenManage IT Assistant* zur Verfügung.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Konfiguration der Verwaltungsstation

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 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 iDRAC6-Enterprise eingerichtet wird. Befolgen Sie vor dem Konfigurieren von iDRAC6 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 iDRAC6 zugreifen kann, muss sie sich auf demselben Netzwerk wie der mit "GB1" bezeichnete CMC RJ45-Anschluss 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 iDRAC6 hat.

Durch die Verwendung der iDRAC6-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. Neustart des Computers unter Verwendung von iDRAC6-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 iDRAC6-Webschnittstelle. Eine Liste unterstützter Web-Browser erhalten Sie unter "Unterstützte Webbrowser".

Webbrowser öffnen

Die iDRAC6-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 u. U. die Meldung **Done, with errors (mit Fehlern abgeschlossen)** in der Statusleiste des Browsers zusammen mit einer teilweise erstellten Anzeige im Hauptfenster des Browsers angezeigt. Dieser Fehler kann auch bei Konnektivitätsproblemen auftreten. Es handelt sich dabei um ein bekanntes Problem bei Internet Explorer 6. Schließen Sie den Browser und starten Sie ihn erneut.

Webbrowser zur Verbindung mit der Webschnittstelle konfigurieren

Wenn Sie eine Verbindung zur iDRAC6-Webschnittstelle von einer Verwaltungsstation aus herstellen, die über einen Proxyserver mit dem Internet verbunden ist, muss der Webbrowser so konfiguriert sein, 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**.
4. Klicken Sie auf die **Benutzerdefinierte Stufe**.
5. Wählen Sie aus dem Dropdown-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 dann nach unten zum Abschnitt mit der Bezeichnung "ActiveX-Steuerelemente und -Plug-ins" und markieren Sie alle Einstellungen, da verschiedene Versionen von Internet Explorer unterschiedliche Einstellungen im Zustand **Mittel-Niedrig** aufweisen:
   - 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

- Wählen Sie **Extras**→ **Internetoptionen**→ **Erweitert**.
- 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: nicht markiert
- 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, empfiehlt Dell, dass Sie sich zuerst über die Konsequenzen, die dies nach sich ziehen würde, informieren und diese verstehen. Wenn Sie z. B. wählen, Popups zu blockieren, werden gewisse Bereiche der iDRAC6-Webschnittstelle nicht funktionieren.

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

iDRAC6 zur Liste vertrauenswürdiger Domänen hinzufügen

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

Lokalisierte Versionen der Webschnittstelle anzeigen

Die iDRAC6-Webschnittstelle wird in den folgenden Betriebssystemsprachen unterstützt:

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

Die ISO-Sprachcodes, 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 iDRAC6-Webschnittstelle wurde für den Einsatz mit lokalisierten Tastaturen für die oben aufgeführten spezifischen Sprachvarianten entwickelt. Einige Funktionen der iDRAC6-Webschnittstelle, wie z. B. Konsolenumleitung, können zusätzliche Schritte für den Zugriff auf bestimmte Funktionen/Buchstaben erfordern. Weitere Einzelheiten, wie lokalisierte Tastaturen in diesen Situationen verwendet werden, finden Sie unter "Video Viewer verwenden". Die Verwendung anderer Tastaturen wird nicht unterstützt und könnte unerwartete Probleme verursachen.

Internet Explorer 6.0 (Windows)

Um eine lokalisierte Version der iDRAC6-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 2.0 (Linux oder Windows)

Um eine lokalisierte Version der iDRAC6-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.

Zeichensatz auf einem Linux-Client mit einer GUI in vereinfachtem Chinesisch einrichten:

1. Öffnen Sie einen Befehls-Terminal.
2. Geben Sie locale ein und betätigen Sie die <Eingabetaste>. 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 zh_CN.UTF-8 nicht 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 iDRAC6 erforderlich, den Sie besuchen, 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 betätigen Sie die <Eingabetaste>:

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

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

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

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

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 iDRAC6-Webschnittstelle konfigurieren, bevor Sie den Viewer starten. Weitere Informationen finden Sie unter Konsolenumleitung und Virtuellen Datenträger in der iDRAC6-Webschnittstelle konfigurieren".

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 iDRAC6-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 iDRAC6-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 zu iDRAC6 existieren. Wenn eine aktive Verbindung besteht, werden andere Verbindungsversuche abgelehnt.

Telnet mit iDRAC6

Telnet ist in Windows- und Linux-Betriebssystemen eingeschlossen und kann von einer Befehls-Shell 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 SP1 oder Windows 2003 ausführt, kann ein Problem mit den Zeichen in einer iDRAC6-Telnet-Sitzung auftreten. Dieses Problem kann sich als blockierende 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.

ANMERKUNG: Der Hotfix wird nur für Windows XP mit Service Pack 1 und Windows 2003 benötigt. Windows XP SP2 behebt dieses Problem.

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 an der Eingabeaufforderung 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 eine Shell und geben Sie Folgendes ein:

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

   ```
   telnet
   ```

SSH mit iDRAC6

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

Sie können auf einer Verwaltungsstation PuTTY (Windows) oder OpenSSH (Linux) verwenden, um eine Verbindung zum iDRAC6 eines verwalteten Servers herzustellen. Wenn während des Anmeldeverfahrens ein Fehler auftritt, gibt der **ssh**-Client eine Fehlermeldung aus. Der Meldungstext hängt vom Client ab und wird nicht von iDRAC6 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 iDRAC6 Enterprise Eigenschaften-Datenbank" beschrieben.

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

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 iDRAC6-Webschnittstelle lediglich zur Übertragung von SSL-Zertifikaten und zum Hochladen neuer iDRAC6-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 und von iDRAC6 verwendet.

Es ist nur dann notwendig, Dateien an den oder vom iDRAC6 zu kopieren, wenn Sie die iDRAC6-Firmware aktualisieren oder Zertifikate auf iDRAC6 installieren. Wenn Sie beim Ausführen dieser Tasks SM-CLP oder RACADM auswählen, muss ein TFTP-Server auf einem Computer ausgeführt werden, auf den iDRAC6 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*
- 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 *Dell OpenManage Software-Schnellinstallationshandbuch* enthalten.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Verwalteten Server konfigurieren

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

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

Softwareinstallation auf dem Managed Server

Die Verwaltungssoftware von Dell schließt die folgenden Funktionen ein:

- Lokale RACADM-CLI - Damit können Sie iDRAC6 vom verwalteten System aus konfigurieren und verwalten. Sie stellt ein leistungsfähiges Tool für Scripting-Konfiguration und Verwaltungs-Tasks dar.
- Server Administrator - Muss die iDRAC-Bildschirmfunktion "Letzter Absturzbildschirm" verwenden.
- Server Administrator Instrumentation Service - Bietet Zugriff auf detaillierte Fehler- und Leistungsinformationen, die von Systemverwaltungsagenten (Industriestandard) 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 Startseite anzeigen, drucken oder als Berichte speichern und sie als E-Mail an einen festgelegten Dienstkontakt 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

iDRAC6 kann den letzten Absturzbildschirm erfassen, damit Sie ihn in der Webschnittstelle anzeigen und die Ursache des Absturzes des verwalteten Servers feststellen und beheben können. Führen Sie folgende Schritte aus, um die Funktion "Bildschirm Letzter Absturz" zu aktivieren.

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

2. Wenn Sie ein Windows ausführen, ist sicherzustellen, dass **Automatischer Neustart** 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 iDRAC6-Webschnittstelle.

   Klicken Sie zum Aktivieren des **Bildschirms Letzter Absturz** in der iDRAC6-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 letzten Absturzbildschirms unter Verwendung von lokalem RACADM eine Eingabeaufforderung auf dem verwalteten Server, und geben Sie den folgenden Befehl ein:

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

4. Aktivieren Sie in der webbasierten Server Administrator-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 beträgt 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 iDRAC6 in der Lage ist, den letzten Absturzbildschirm zu erfassen, deaktivieren Sie die Option **Automatischer Neustart** auf verwalteten Servern, auf denen 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

iDRAC6 mittels der Enterprise-Webschnittstelle konfigurieren

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

iDRAC6 enthält eine Webschnittstelle, mit der Sie die iDRAC-Eigenschaften und -Benutzer konfigurieren, Remote-Verwaltungs-Tasks ausführen sowie Fehlerbehebungsmaßnahmen auf ein (verwaltetes) Remote-System anwenden können. Verwenden Sie die iDRAC6-Webschnittstelle für routinemäßige Systemverwaltung. Dieses Kapitel enthält Informationen darüber, wie allgemeine Systemverwaltungs-Tasks über die iDRAC6-Webschnittstelle ausgeführt werden, und Links zu zugehörigen 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 "iDRAC6-Enterprise verwenden SM-CLP-Befehlszeilenschnittstelle".

Zugriff auf die Webschnittstelle

Führen Sie zum Zugriff auf die iDRAC6-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 <Eingabe>.

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

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

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

   Das iDRAC6-**Anmelde**-Fenster wird eingeblendet.

Anmeldung

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

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

Um sich anzumelden, führen Sie die folgenden Schritte aus.

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

   - Ihren iDRAC6-Benutzernamen.

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

   - Ihren Active Directory-Benutzernamen.

     Active Directory-Namen können in einem der folgenden Formate eingegeben werden: *<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`. Sie können alternativ auch die Domäne in das Feld **Domäne** eingeben.

2. Geben Sie im Feld **Kennwort** Ihr iDRAC6-Benutzerkennwort oder 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 iDRAC6-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 beheben, 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 unterschiedliches 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 iDRAC6-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 iDRAC6-Webschnittstelle ab.

Das Verhalten der Register in Firefox 2 ist identisch mit dem Registerverhalten in Internet Explorer 7; neue Register sind neue Sitzungen. Das Fensterverhalten 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 sind, haben **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

---

iDRAC6-NIC konfigurieren

Für diesen Abschnitt wird angenommen, dass der iDRAC6 bereits konfiguriert wurde und über das Netzwerk auf darauf zugegriffen werden kann. Hilfe für die erste iDRAC6-Netzwerkkonfiguration finden Sie unter "iDRAC6-Netzwerkbetrieb konfigurieren".

Netzwerk und IPMI-LAN-Einstellungen konfigurieren

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

ANMERKUNG: Für die meisten DHCP-Server ist ein Server zum Speichern eines Client-Bezeichner-Tokens in der Reservierungstabelle erforderlich. Der Client (z. B. iDRAC) muss dieses Token während der DHCP-Verhandlung zur Verfügung stellen. iDRAC6 liefert die Option 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 die Registerkarte **Netzwerk/Sicherheit**.

   Der Bildschirm **Netzwerkkonfiguration** wird eingeblendet.

3. Netzwerk- und IPMI-LAN-Einstellungen nach Bedarf konfigurieren. Siehe Tabelle 5-2 und Tabelle 5-3 zur Beschreibung der Optionen der **Netzwerkeinstellungen** und **IPMI LAN-Einstellungen**.

4. Klicken Sie auf **Anwenden**.

5. 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 iDRAC6 über das Netzwerk blockiert. Die Standardeinstellung ist **aus**.

MAC-Adresse	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 iDRAC6 auf, eine IP-Adresse für die NIC vom DHCP-Server (dynamisches Host-Konfigurationsprotokoll) 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 iDRAC6-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 iDRAC6-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, ein statisches Gateway für die iDRAC6-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 iDRAC6-Namen auf dem DNS-Server. Die Standardeinstellung ist **Deaktiviert**.
DNS iDRAC Name	Zeigt den iDRAC6-Namen nur an, wenn **iDRAC6 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, wird diese Option abgeblendet und das Feld kann nicht geändert werden.

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 des Bildschirms "Netzwerkkonfiguration"

Schaltfläche	Beschreibung
Erweiterte Einstellungen	Öffnet den Bildschirm **Netzwerksicherheit**, auf dem Benutzer den IP-Bereich sowie IP-Blockierungsattribute eingeben können.
Drucken	Druckt die Werte der **Netzwerkkonfiguration** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt den Bildschirm **Netzwerkkonfiguration** neu.
Anwenden	Speichert alle neuen Einstellungen, die Sie auf dem Bildschirm Netzwerkkonfiguration vorgenommen haben. **ANMERKUNG:** Wenn Sie Änderungen an den Einstellungen der NIC-IP-Adresse vornehmen, werden alle Benutzersitzungen geschlossen und Benutzer müssen unter Verwendung der aktualisierten IP-Adresseneinstellungen eine neue Verbindung zur iDRAC6-Webschnittstelle herstellen. Alle anderen Änderungen erfordern, dass die NIC zurückgesetzt wird, was 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.**
2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit.**

   Der Bildschirm **Netzwerkkonfiguration** wird eingeblendet.
3. Klicken Sie auf **Erweiterte Einstellungen**.

   Der Bildschirm **Netzwerksicherheit** wird eingeblendet.
4. IP-Filterung und IP-Blockierung nach Bedarf konfigurieren. Siehe Tabelle 5-5 zur Beschreibung der **IP-Filterung und IP-Blockierung**.
5. Klicken Sie auf **Anwenden**.
6. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-6.

Tabelle 5-5. Netzwerksicherheitseinstellungen

Einstellungen	Beschreibung
IP-Bereich aktiviert	Aktiviert die Funktion zum Prüfen des IP-Bereichs, mit dem eine Reihe von IP-Adressen definiert werden, die auf den iDRAC6 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 der Form einer Netzmaske sein, wobei die signifikanteren Bits alles Einsen (1) sind, mit einem einzigen Übergang zu alles 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 aufgrund übermäßiger Fehler abgewiesen werden. Die Standardeinstellung ist **3600.**

Tabelle 5-6. Schaltflächen des Bildschirms "Netzwerksicherheit"

Schaltfläche	Beschreibung
Drucken	Druckt die Werte der **Netzwerksicherheit** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt den Bildschirm **Netzwerksicherheit** neu.
Anwenden	Speichert alle neuen Einstellungen, die Sie auf dem Bildschirm **Netzwerksicherheit** vorgenommen haben.
Zurück zur Netzwerkseite	Wechselt zum Bildschirm **Netzwerk** zurück.

Plattformereignisse konfigurieren

Die Plattformereigniskonfiguration bietet einen Mechanismus zur Konfiguration des iDRAC6, damit bei bestimmten Ereignismeldungen 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.

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

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

Plattformereignisfilter (PEF) konfigurieren

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

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

   Der Bildschirm **Plattformereignisse** wird eingeblendet.
3. Markieren Sie neben jedem Ereignis das Kontrollkästchen **Warnung erstellen**, für welches Sie eine Warnung erzeugen möchten.

   ANMERKUNG: Die Warnungserstellung kann für alle Ereignisse aktiviert oder deaktiviert werden, indem Sie das Kontrollkästchen neben der Spaltenüberschrift **Warnung erstellen** markieren oder die Markierung entfernen.
4. Wählen Sie die Optionsschaltfläche unter der Maßnahme aus, die Sie für die einzelnen Ereignisse aktivieren möchten. Für jedes Ereignis kann nur eine Maßnahme ausgewählt 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 bei der iDRAC6-Webschnittstelle an.
2. Vergewissern Sie sich, dass Sie die unter "Plattformereignisfilter (PEF) konfigurieren" beschriebenen Verfahren befolgt haben.
3. Klicken Sie auf **System** und dann auf das Register **Warnungsverwaltung**.

   Der Bildschirm **Plattformereignisse** wird eingeblendet.
4. Klicken Sie auf **Trap-Einstellungen**.

   Der Bildschirm **Plattformereigniswarnungsziele** wird eingeblendet.
5. Konfigurieren Sie die PET-Ziel-IP-Adresse:
   a. Wählen Sie das Kontrollkästchen **Aktivieren** neben der **Zielnummer** aus, die Sie aktivieren möchten.
   b. Geben Sie eine IP-Adresse im Kästchen **Ziel-IP-Adresse** ein.

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

   c. Klicken Sie auf **Anwenden**.

   ANMERKUNG: Der Wert der **Community-Zeichenkette** muss auf dem Bildschirm **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 verwendet werden soll, das vom iDRAC6 gesendet wird. SNMP-Warnungs-Traps werden vom iDRAC6 übertragen, wenn ein Plattformereignis auftritt. Die Standardeinstellung für die **Community-Zeichenkette** ist **Öffentlich**.

   d. Klicken Sie auf **Senden**, um die konfigurierte Warnung zu testen.
   e. Wiederholen Sie die Schritte Schritt a bis Schritt d, um eine zusätzliche IP-Zieladresse hinzuzufügen. Sie können bis zu vier IP- Zieladressen

angeben.

Konfiguration von E-Mail-Warnungen

1. Melden Sie sich bei der iDRAC6-Webschnittstelle an.
2. Vergewissern Sie sich, dass Sie die unter "Plattformereignisfilter (PEF) konfigurieren" beschriebenen Verfahren befolgt haben.
3. Klicken Sie auf **System** und dann auf das Register **Warnungsverwaltung**.

   Der Bildschirm **Plattformereignisse** wird eingeblendet.
4. Klicken Sie auf **E-Mail-Warnungseinstellungen**.

   Der Bildschirm **E-Mail-Warnungseinstellungen** wird eingeblendet.
5. Konfigurieren Sie das E-Mail-Warnungsziel.
   a. Wählen Sie das Kontrollkästchen **Aktiviert** für die erste undefinierte E-Mail-Warnung aus.
   b. Geben Sie eine gültige E-Mail-Adresse in das Feld **Ziel-E-Mail- Adresse** ein.
   c. Klicken Sie auf **Anwenden**.

   ANMERKUNG: Die **SMTP-Server-Adresse** muss im Abschnitt **SMTP- (E-Mail-) Serveradresseinstellungen** des Bildschirms **E-Mail-Warnungseinstellungen** konfiguriert sein, um eine Test-E-Mail erfolgreich senden zu können. Die IP-Adresse des **SMTP-Servers** kommuniziert mit dem iDRAC6, um im Falle eines Plattformereignisses E-Mail-Warnungen zu senden.

   d. Klicken Sie auf **Senden**, um die konfigurierte E-Mail-Warnung zu testen (falls gewünscht).
   e. Wiederholen Sie die Schritte Schritt a bis Schritt d, um eine weitere Zieladresse für E-Mail-Warnmeldungen hinzuzufügen. Sie können bis zu vier Zieladressen für E-Mail-Warnmeldungen angeben.

IPMI-über-LAN konfigurieren

1. Melden Sie sich bei der iDRAC6-Webschnittstelle an.
2. Konfigurieren Sie IPMI über LAN:
   a. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Netzwerk/Sicherheit**.

      Der Bildschirm **Netzwerkkonfiguration** wird eingeblendet.
   b. Klicken Sie auf **IPMI LAN-Einstellungen**.
   c. Wählen Sie das Kontrollkästchen **IPMI-über-LAN aktivieren** aus.
   d. Aktualisieren Sie die IPMI-LAN-Kanalberechtigungen, falls erforderlich.

   ANMERKUNG: Diese Einstellung bestimmt die IPMI-Befehle, die von der IPMI-über-LAN-Schnittstelle ausgeführt werden können. Weitere Informationen finden Sie in den IPMI 2.0-Angaben.

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

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

   ANMERKUNG: Die iDRAC6-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.

   f. Klicken Sie auf **Anwenden**.
3. IPMI-Seriell-über-LAN (SOL) konfigurieren.
   a. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Netzwerk/Sicherheit**.

      Der Bildschirm **Netzwerkkonfiguration** wird eingeblendet.
   b. Öffnen Sie den Bildschirm **Seriell über LAN**.
   c. Wählen Sie das Kontrollkästchen **Seriell über LAN aktivieren** aus.
   d. Aktualisieren Sie bei Bedarf die IPMI-SOL-Baudrate, indem Sie aus dem Baudraten-Dropdown-Menü eine Datengeschwindigkeit auswählen.

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

e. Klicken Sie auf **Anwenden**.

---

iDRAC6-Benutzer hinzufügen und konfigurieren

Erstellen Sie zur Verwaltung des Systems mit dem iDRAC6 und zur Aufrechterhaltung der Systemsicherheit eindeutige Benutzer mit spezifischen Administrationsberechtigungen (oder *rollenbasierter Autorität*).

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

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

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Netzwerk/Sicherheit**.
2. Öffnen Sie den Bildschirm **Benutzer**, um einzelne Benutzer zu konfigurieren.

   Der Bildschirm **Benutzer** zeigt für jeden 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 dem Bildschirm **Benutzerkonfiguration**.

   Tabelle 5-8 beschreibt die **allgemeinen** Einstellungen zur Konfiguration eines Benutzernamens und -kennworts für iDRAC6.

   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 iDRAC6 aktiviert ist. Wenn das Feld nicht markiert ist, ist der Benutzerzugriff deaktiviert.
Benutzername	Gibt einen iDRAC6-Benutzernamen von bis zu 16 Zeichen an. Jeder Benutzer muss einen eindeutigen Benutzernamen besitzen. **ANMERKUNG:** Benutzernamen für den iDRAC6 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 iDRAC6-Benutzers. Geben Sie ein **Kennwort** mit bis zu 20 Zeichen ein. Die Zeichen werden nicht angezeigt.
Neues Kennwort bestätigen	Geben Sie das Kennwort des iDRAC6-Benutzers erneut ein, um es zu bestätigen.

Tabelle 5-9. IPMI-LAN-Benutzerberechtigungen

Eigenschaft	Beschreibung
Maximale LAN-Benutzerberechtigung	Legt die maximale Berechtigung des Benutzers auf dem IPMI-LAN-Kanal auf eine der folgenden Benutzergruppen

gewährt	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. iDRAC6-Benutzerberechtigungen

Eigenschaft	Beschreibung
iDRAC-Gruppe	Legt die maximale iDRAC6-Benutzerberechtigung als eine der Folgenden fest: **Administrator**, **Hauptbenutzer**, **Gastbenutzer**, **Benutzerdefiniert** oder **Keine**. Siehe Tabelle 5-11 zu **iDRAC6-Gruppen**berechtigungen.
Bei iDRAC anmelden	Ermöglicht dem Benutzer, sich am iDRAC6 anzumelden.
iDRAC konfigurieren	Ermöglicht dem Benutzer, den iDRAC6 zu konfigurieren.
Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern zu erlauben, auf das System zuzugreifen.
Protokolle löschen	Ermöglicht dem Benutzer, die iDRAC6-Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer, RACADM-Befehle auszuführen.
Auf die Konsolenumleitung zugreifen	Ermöglicht dem Benutzer, die Konsolenumleitung auszuführen.
Zugriff auf virtuelle Datenträger	Ermöglicht dem Benutzer, virtuelle Datenträger auszuführen und zu verwenden.
Testwarnungen	Ermöglicht dem Benutzer, einem bestimmten Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Tabelle 5-11. iDRAC6-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 des Bildschirms "Benutzerkonfiguration"

Schaltfläche	Abhilfe
Drucken	Druckt die Werte der **Benutzerkonfiguration** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt den Bildschirm **Benutzerkonfiguration** neu.
Anwenden	Speichert alle neuen Einstellungen, die an der Benutzerkonfiguration vorgenommen wurden.
Zurück zum Bildschirm "Benutzer"	Kehrt zum **Bildschirm Benutzer** zurück.

---

iDRAC6-Datenübertragung mit SSL und digitalen Zertifikaten sichern

Dieser Abschnitt enthält Informationen über die folgenden Datensicherheitsfunktionen, die in iDRAC6 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)

iDRAC6 beinhaltet einen Web-Server, der zur Verwendung des SSL-Sicherheitsprotokolls (Industriestandard) 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. iDRAC6 verwendet den SSL-128-Bit-Verschlüsselungsstandard, die sicherste Form der Verschlüsselung, die für Webbrowser in Nordamerika allgemein verfügbar ist.

Der iDRAC6-Web-Server enthält standardmäßig ein selbst-signiertes 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 iDRAC6-Webschnittstelle zum Erstellen einer Zertifikatsignierungsanforderung (CSR) mit den Informationen 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 (CA) ist eine Unternehmenseinheit, die in der IT-Industrie dafür bekannt 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 für Transaktionen über Netzwerke und das Internet eindeutig identifiziert.

Nachdem die Zertifizierungsstelle die Zertifikatssignierungsanforderung genehmigt und das Zertifikat gesendet hat, muss das Zertifikat zur iDRAC6-Firmware hochgeladen werden. Die auf der iDRAC6-Firmware gespeicherten CSR-Informationen müssen mit den im Zertifikat enthaltenen Informationen übereinstimmen.

Zugriff auf das SSL-Hauptmenü

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

Verwenden Sie den Bildschirm **SSL-Hauptmenü** zum Erstellen einer CSR, die an eine Zertifizierungsstelle gesendet werden soll. Die CSR-Informationen werden in der iDRAC6-Firmware gespeichert.

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

Tabelle 5-14 beschreibt die auf dem Bildschirm **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 den Bildschirm **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 den Bildschirm **Zertifikat hochladen** zu öffnen und das Zertifikat hochzuladen, das Ihnen die Zertifizierungsstelle zugesandt hat. **ANMERKUNG:** iDRAC6 akzeptiert lediglich X509-Base-64-codierte Zertifikate. DER-kodierte Zertifikate werden nicht angenommen.
Serverzertifikat anzeigen	Wählen Sie die Option aus und klicken Sie auf **Weiter**, um den Bildschirm **Serverzertifikat anzeigen** zu öffnen und ein vorhandenes Serverzertifikat anzuzeigen.

Tabelle 5-14. SSL-Hauptmenüschaltflächen

Schaltfläche	Beschreibung
Drucken	Druckt die Werte des **SSL-Hauptmenüs** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt den Bildschirm **SSL-Hauptmenü** neu.
Weiter	Verarbeitet die Informationen auf dem Bildschirm **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 iDRAC6 das Zertifikat nicht an.

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

   Tabelle 5-15 beschreibt die Optionen des Bildschirms **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 des Bildschirms "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/der Kanton, in dem sich das Unternehmen befindet, das sich für eine Zertifizierung bewirbt (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 des Bildschirms "Zertifikatsignierungsanforderung (CSR) erstellen"

Schaltfläche	Beschreibung
Drucken	Druckt die Werte **Zertifikatsignierungsanforderung erstellen** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt den Bildschirm **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 zum Bildschirm **SSL-Hauptmenü** zurück.

Ein Serverzertifikat hochladen

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

   Der Bildschirm **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 Dateipfad des Zertifikats an, das Sie hochladen. Sie müssen den vollständigen Dateipfad eingeben, der den vollen Pfad und den vollständigen 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. Schaltflächen des Bildschirms "Zertifikat hochladen"

Schaltfläche	Beschreibung
Drucken	Druckt die Werte aus, die auf dem Bildschirm **Zertifikat hochladen** angezeigt werden.

Aktualisieren	Lädt den Bildschirm **Zertifikat hochladen** neu.
Anwenden	Wendet das Zertifikat auf die iDRAC6-Firmware an.
Zurück zum SSL-Hauptmenü	Bringt den Benutzer zum Bildschirm **SSL-Hauptmenü** zurück

Serverzertifikat anzeigen

1. Wählen Sie auf dem Bildschirm **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 des Bildschirms "Serverzertifikat anzeigen"

Schaltfläche	Beschreibung
Drucken	Druckt die Werte für **Serverzertifikat anzeigen** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt den Bildschirm **Serverzertifikat anzeigen** neu.
Zurück zum SSL-Hauptmenü	Zurück zum Bildschirm **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 "iDRAC6 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 den Bildschirm **Active Directory- Hauptmenü** zu öffnen.

   Tabelle 5-20 führt die Optionen des Bildschirms **Active Directory-Hauptmenü** auf.

3. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-20.

Tabelle 5-20. Optionen des Hauptmenüs 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 iDRAC6 hoch.
Active Directory-CA-Zertifikat anzeigen	Zeigt ein Active Directory-Zertifikat an, das zum iDRAC6 hochgeladen wurde.

Tabelle 5-21. Schaltflächen des Bildschirms "Active Directory-Hauptmenü"

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

Active Directory konfigurieren (Standardschema und erweitertes Schema)

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

   Tabelle 5-22 beschreibt die Einstellungen des Bildschirms **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 dem Bildschirm **Active Directory-Konfiguration** auf **Anwenden**, bevor Sie mit dem Bildschirm **Benutzerdefinierte Rollengruppe** fortfahren.

Tabelle 5-22. Einstellungen des Bildschirms 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 iDRAC6 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-iDRAC6-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 iDRAC6 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, zu dem iDRAC6 zugehört. Diese Standardeinstellung ist leer.
Gruppendomäne	Der Domänentyp, bei dem sich die Rollengruppe befindet.

Tabelle 5-23. Schaltflächen des Bildschirms "Active Directory-Konfiguration"

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

Tabelle 5-24. Rollengruppenberechtigungen

Einstellung	Beschreibung
Zugriffsstufe der Rollengruppe	Legt die maximale iDRAC6-Benutzerberechtigung als eine der Folgenden fest: **Administrator**, **Hauptbenutzer**, **Gastbenutzer**, **Keine** oder **Benutzerdefiniert**. Siehe Tabelle 5-25 zu **Rollengruppen**-Berechtigungen.
Bei iDRAC anmelden	Erlaubt der Gruppe den Anmeldezugriff auf iDRAC6.
iDRAC konfigurieren	Gibt der Gruppe die Berechtigung, iDRAC6 zu konfigurieren.
Benutzer konfigurieren	Gibt der Gruppe die Berechtigung, Benutzer zu konfigurieren.
Protokolle löschen	Erlaubt der Gruppenberechtigung, Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Erlaubt der Gruppenberechtigung, Serversteuerungsbefehle auszuführen.
Auf die 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 dem Bildschirm **Active Directory-Hauptmenü** die Option **Active Directory-CA-Zertifikat hochladen** aus und klicken Sie auf **Weiter**.
2. Geben Sie auf dem **Bildschirm 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 Dateipfad des Zertifikats an, das Sie hochladen. Sie müssen den vollständigen Dateipfad eingeben, der den vollen Pfad und den vollständigen Dateinamen und die Dateierweiterung enthält.

Stellen Sie sicher, dass die SSL-Zertifikate des Domänen-Controllers von derselben Zertifizierungsstelle (CA) signiert wurden und dass dieses Zertifikat auf der Management Station verfügbar ist, die auf iDRAC6 zugreift.

3. Klicken Sie auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-26.

Tabelle 5-26. Schaltflächen des Bildschirms "Zertifikat hochladen"

Schaltfläche	Beschreibung
Drucken	Druckt die Werte zu **Zertifikat hochladen** aus, die auf dem Bildschirm angezeigt werden
Aktualisieren	Lädt den Bildschirm **Zertifikat hochladen** neu.
Anwenden	Wendet das Zertifikat auf die iDRAC6-Firmware an.
Zurück zum Active Directory-Hauptmenü	Kehrt zum Bildschirm **Active Directory-Hauptmenü** zurück.

Active Directory-CA-Zertifikat anzeigen

Verwenden Sie den Bildschirm **Active Directory-Hauptmenü**, um ein CA-Serverzertifikat für iDRAC6 anzuzeigen.

1. Wählen Sie auf dem Bildschirm **Active Directory-Hauptmenü Active Directory-CA-Zertifikat hochladen** 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. Schaltflächen des Bildschirms "Active Directory CA-Zertifikat"

Schaltfläche	Beschreibung
Drucken	Druckt die **Werte des Active Directory-Zertifizierungsstellenzertifikats, die auf dem Bildschirm angezeigt werden**, aus.
Aktualisieren	Lädt den Bildschirm **Active Directory-CA-Zertifikat neu**.
Zurück zum Active Directory-Hauptmenü	Leitet den Benutzer auf den Bildschirm **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. Siehe Tabelle 5-34.

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. Siehe Tabelle 5-34.

---

iDRAC6-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 den Bildschirm "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
   - SNMP Agent - siehe Tabelle 5-32 für die Einstellungen des SNMP-Agents
   - Automatisierter Systemwiederherstellungsagent - siehe Tabelle 5-33 für die Einstellungen des automatisierten Systemwiederherstellungsagenten

4. Klicken Sie auf **Anwenden**.

5. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe Tabelle 5-34.

Tabelle 5-29. Web-Server-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert den iDRAC6-Web-Server. Weist, falls markiert, darauf hin, dass der Web-Server aktiviert ist. Standardmäßig ist der Wert auf **aktiviert** eingestellt.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger Sitzungen, die für dieses System zulässig sind. Dieses Feld kann nicht bearbeitet werden. Es können vier Sitzungen gleichzeitig ausfgeführt werden.
Aktuelle Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich **Max. Sitzungen**. Dieses Feld kann nicht bearbeitet werden.
Zeitüberschreitung	Die Zeit in Sekunden, für die eine Verbindung ungenutzt bleiben kann. Die Sitzung wird abgebrochen, wenn das Zeitlimit erreicht wird. Änderungen an der Einstellung zur Zeitüberschreitung werden sofort wirksam und führen zu einem Reset des Web-Servers. Der Zeitüberschreitungsbereich beträgt 60 bis 10800 Sekunden. Die Standardeinstellung ist **1800** Sekunden.
HTTP-Anschlussnummer	Der Anschluss, den iDRAC6 abhört, um ggf. eine Browser-Verbindung festzustellen. Die Standardeinstellung ist **80.**
HTTPS-Anschlussnummer	Der Anschluss, den iDRAC6 abhört, um ggf. eine sichere Browser-Verbindung festzustellen. 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. Der Zeitüberschreitungsbereich beträgt 60 bis 10800 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitlimit-Funktion zu deaktivieren. Die Standardeinstellung ist **1800**.
Anschlussnummer	Der Anschluss, den iDRAC6 abhört, um ggf. eine SSH-Verbindung festzustellen. Die Standardeinstellung ist **22.**

Tabelle 5-31. Telnet-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert Telnet. Wenn markiert, ist Telnet aktiviert. Standardmäßig ist der Wert auf **deaktiviert** eingestellt.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger Sitzungen, die für dieses System zulässig sind. Es wird nur eine einzige Sitzung unterstützt.
Aktive Sitzungen	Die Anzahl der aktuellen Sitzungen auf dem System.
Zeitüberschreitung	Die telnet-Zeitüberschreitung wegen Leerlauf, in Sekunden. Der Zeitüberschreitungsbereich beträgt 60 bis 10800 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitlimit-Funktion zu deaktivieren. Die Standardeinstellung ist **1800**.
Anschlussnummer	Der Anschluss, den iDRAC6 abhört, um ggf. eine Telnet-Verbindung festzustellen. Die Standardeinstellung ist **23.**

Tabelle 5-32. SNMP-Agent

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert E-Mail-Warnungen.
SNMP-Community-Name	Der Name der Community, die die IP-Adresse für das SNMP-Warnungsziel enthält. Der Community-Name kann bis zu 31 Zeichen (keine Leerzeichen) lang sein. Standardwert=public.

Tabelle 5-33. Einstellung des automatisierten Systemwiederherstellungs-Agenten

Einstellung	Beschreibung

Aktiviert	Aktiviert den automatisierten Systemwiederherstellungs-Agenten.

Tabelle 5-34. Schaltflächen des Bildschirms "Dienste"

Schaltfläche	Beschreibung
Drucken	Druckt den Bildschirm **Dienste**.
Aktualisieren	Aktualisiert den Bildschirm **Dienste**.
Änderungen anwenden	Wendet die Einstellungen auf dem Bildschirm **Dienste** an.

Aktualisiert die iDRAC6-Firmware

ANMERKUNG: Wenn die iDRAC6-Firmware beschädigt wird, was eintreten könnte, wenn der iDRAC6-Firmware-Aktualisierungsvorgang vor seinem Abschluss abgebrochen wird, können Sie den iDRAC6 mithilfe des CMC wiederherstellen. Anleitungen hierzu finden Sie im *CMC Firmware-Benutzerhandbuch*.

ANMERKUNG: Die Firmware-Aktualisierung behält standardmäßig die aktuellen iDRAC6-Einstellungen bei. Während des Aktualisierungsvorgangs haben Sie die Möglichkeit, die iDRAC6-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 iDRAC6-Konfigurationshilfsprogramms oder der CMC-Webschnittstelle aktiviert und konfiguriert werden.

1. Starten Sie die iDRAC6-Webschnittstelle.
2. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Aktualisieren**.

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

3. Klicken Sie auf dem Bildschirm **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\V2.0\<Image_Name>`.

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

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

   - Die Datei wird auf den iDRAC6 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 iDRAC6 in den normalen Betriebsmodus zurückgesetzt.

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

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

    ODER

  - Wenn das Image nicht erfolgreich hochgeladen wurde oder die Überprüfungsvorgänge nicht bestanden hat, wechselt die Firmware-Aktualisierung zum Fenster **Firmware-Aktualisierung - Hochladen (Seite 1 von 4)** zurück. Sie können versuchen, iDRAC6 erneut zu aktualisieren, oder klicken Sie auf **Abbrechen**, um iDRAC6 in den normalen Betriebsmodus zurückzusetzen.

  ANMERKUNG: Wenn Sie die Markierung aus dem Kontrollkästchen **Konfiguration beibehalten** entfernen, wird iDRAC6 auf seine Standardeinstellungen zurückgesetzt. Das LAN ist in den Standardeinstellungen deaktiviert. Sie werden nicht in der Lage sein, sich an der iDRAC6-Webschnittstelle anzumelden. Es wird erforderlich sein, die LAN-Einstellungen unter Verwendung der CMC-Webschnittstelle oder iKVM unter Verwendung des iDRAC6-Konfigurationshilfsprogramms während des BIOS-POST neu zu konfigurieren.

7. Standardmäßig ist das Kontrollkästchen **Konfiguration sichern** markiert, um die aktuellen Einstellungen auf iDRAC6 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 iDRAC6 wird automatisch zurückgesetzt. Sie müssen das aktuelle Browserfenster schließen und eine neue iDRAC6-Verbindung in einem neuen Browserfenster herstellen.

Aktualisieren der iDRAC6-Firmware mittels CMC

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

Die iDRAC6-Firmware kann mit der CMC-Webschnittstelle oder CMC RACADM aktualisiert werden. Diese Funktion ist sowohl im Normalbetrieb der iDRAC6-Firmware verfügbar als auch dann, wenn diese beschädigt ist. Siehe "Aktualisieren der iDRAC6-Firmware mittels CMC."]

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

Um die iDRAC6-Firmware zu aktualisieren, führen Sie folgende Schritte aus:

1. Laden Sie die neueste iDRAC6-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.
5. Klicken Sie auf **Server-*n***, wobei ***n*** die Nummer des Servers ist, dessen iDRAC6 Sie aktualisieren möchten.
6. Klicken Sie auf **Durchsuchen,** und suchen Sie nach dem von Ihnen heruntergeladenen iDRAC6-Firmware-Image. Klicken Sie dann auf **Öffnen**.
7. Klicken Sie auf **Firmware-Aktualisierung beginnen**.

Wenn die Firmware-Image-Datei zum CMC hochgeladen wurde, aktualisiert sich der iDRAC6 anhand des Images selbst.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6 mit Microsoft Active Directory verwenden

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

Ein Verzeichnisdienst wird verwendet, um eine allgemeine Datenbank aller Informationen aufrechtzuerhalten, die erforderlich sind, um Benutzer, Computer, Drucker etc. auf einem Netzwerk zu steuern. Wenn Ihre Firma die Microsoft® Active Directory® Service-Software bereits verwendet, kann die Software so konfiguriert werden, dass sie Zugriff auf den iDRAC6 bietet. Sie können dann bestehenden Benutzern in der Active Directory-Software iDRAC6-Benutzerberechtigungen zuteilen und diese steuern.

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

Tabelle 6-1 zeigt die neun Active Directory-Benutzerberechtigungen des iDRAC6 an.

Tabelle 6-1. iDRAC6-Benutzerberechtigungen

Berechtigung	Beschreibung
Bei iDRAC anmelden	Ermöglicht dem Benutzer, sich am iDRAC6 anzumelden.
iDRAC konfigurieren	Ermöglicht dem Benutzer, iDRAC6 zu konfigurieren.
Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern den Zugriff auf das System zu gewähren.
Protokolle löschen	Ermöglicht dem Benutzer, die iDRAC6-Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer, RACADM-Befehle auszuführen.
Auf die Konsolenumleitung zugreifen	Ermöglicht dem Benutzer, die Konsolenumleitung auszuführen.
Zugriff auf virtuelle Datenträger	Ermöglicht dem Benutzer, virtuelle Datenträger auszuführen und zu verwenden.
Testwarnungen	Ermöglicht dem Benutzer, Testwarnungen (E-Mail und PET) an einen bestimmten Benutzer zu senden.
Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Voraussetzungen zum Aktivieren der Active Directory-Authentifizierung für den iDRAC6.

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

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

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

Um eine korrekte Authentifizierung in allen Domänen-Controllern vornehmen zu können, müssen Sie auch die SSL-Verschlüsselung auf sämtlichen Domänen-Controllern aktivieren, zu denen der iDRAC6 eine Verbindung herstellt. Unter "SSL auf einem Domänen-Controller aktivieren" finden Sie detailliertere Informationen.

Unterstützte Active Directory- Authentifizierungsmechanismen

Sie können Active Directory zum Festlegen von Benutzerzugriffen auf den iDRAC6 mithilfe von zwei Verfahren verwenden. Entweder verwenden Sie die Lösung *Erweitertes Schema*, die Dell zum Hinzufügen von Dell-definierten Active Directory-Objekten angepasst hat. Oder Sie verwenden die Lösung *Standardschema*, die lediglich Active Directory-Gruppenobjekte verwendet. Weitere Informationen über diese Lösungen finden Sie in den nachfolgenden Abschnitten.

Bei der Verwendung von Active Directory zur Konfiguration des Zugriffs auf den iDRAC6 müssen Sie entweder die Lösund Erweitertes Schema oder Standardschema auswählen.

Die Vorteile bei der Verwendung des erweiterten Schemas sind:

- Alle Zugriffssteuerungsobjekte werden im Active Directory verwahrt.
- Bei der Konfiguration des Benutzerzugriffs auf unterschiedliche iDRAC6-Karten mit verschieden Berechtigungsebenen steht Ihnen maximale Flexibilität zur Verfügung.

Der Vorteil bei der Verwendung der Standardschema-Lösung besteht darin, dass keine Schemaerweiterung erforderlich ist, weil alle notwendigen Objektklassen von Microsofts Standardkonfiguration des Active Directory-Schemas zur Verfügung gestellt werden.

Übersicht des Active Directory mit erweitertem Schema

Die Verwendung der Lösung Erweitertes Schema erfordert die Active Directory-Schemaerweiterung, wie im folgenden Abschnitt dargestellt.

Erweiterung des Active Directory-Schemas

Wichtig: Die Schemaerweiterung für dieses Produkt unterscheidet sich von der vorigen Generation der Dell Remote-Verwaltungsprodukte. Sie müssen das neue Schema erweitern und das neue **Active Directory-Benutzer- und Computer Snap-In** der **Microsoft-Verwaltungskonsole (MMC)** in Ihrem Verzeichnis installieren. Das alte Schema funktioniert nicht mehr mit diesem Produkt.

ANMERKUNG: Eine Erweiterung des neuen Schemas oder Installation der neuen Erweiterung im Active Directory-Benutzer- und Computer-Snap-In hat keine Auswirkungen auf vorherige Versionen dieses Produkts.

Die Erweiterung des Schema Extenders und Active Directory-Benutzer- und Computer-Snap-Ins stehen auf der DVD *Dell Systems Management Tools and Documentation* zur Verfügung. Weitere Informationen finden Sie unter "Active Directory-Schema erweitern" und "Dell Erweiterung im Active Directory-Benutzer- und Computer-Snap-In installieren". Weitere Details zum Erweitern des Schemas für den iDRAC6 und zum Installieren des Active Directory-Benutzer- und Computer-MMC-Snap-Ins finden Sie im *Dell OpenManage-Installations- und Sicherheitsbenutzerhandbuch*, das unter **support.dell.com\manuals** zur Verfügung steht.

ANMERKUNG: Stellen Sie sicher, dass Sie bei der Erstellung von iDRAC6-Zuordnungsobjekten **Erweitertes Dell Remote-Verwaltungsobjekt** auswählen.

Active Directory-Schemaerweiterungen

Bei den Active Directory-Daten handelt es sich um eine dezentrale Datenbank von Attributen und Klassen. Das Active Directory-Schema enthält die Regeln, die den Typ der Daten bestimmen, die der Datenbank hinzugefügt bzw. darin aufgenommen werden können. Die Benutzerklasse ist ein Beispiel einer Klasse, die in der Datenbank gespeichert wird. Einige Beispiel-Attribute der Benutzerklasse sind Vorname, Nachname, Telefonnummer usw. des Benutzers. Firmen können die Active Directory-Datenbank erweitern, indem sie ihre eigenen eindeutigen Attribute und Klassen hinzufügen, um sich an umgebungsspezifische Bedürfnisse zu richten. Dell hat das Schema erweitert, um die erforderlichen Änderungen zur Unterstützung der Remote-Verwaltung-Authentifizierung und Autorisierung einzuschließen.

Jedes Attribut bzw. jede Klasse, die einem vorhandenen Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert werden. Um einzigartige IDs über den Industriezweig hinaus aufrechtzuerhalten, hält Microsoft eine Datenbank von Active Directory-Objektbezeichnern (OIDs), damit diese die Gewährleistung haben, einzigartig zu sein und nicht miteinander in Konflikt zu stehen, wenn Unternehmen dem Schema Erweiterungen hinzufügen. Um das Schema im Active Directory von Microsoft zu erweitern, erhielt Dell eindeutige OIDs, eindeutige Namenserweiterungen und eindeutig verbundene Attribut-IDs für die Attribute und Klassen, die dem Verzeichnisdienst hinzugefügt werden.

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

Übersicht der iDRAC6-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 iDRAC6-Geräten verwendet. Dieses Modell bietet dem Administrator höchste Flexibilität über die verschiedenen Kombinationen von Benutzern, iDRAC6-Berechtigungen und iDRAC6-Geräten auf dem Netzwerk, ohne zu viel Komplexität hinzuzufügen.

Active Directory - Objekt-Übersicht

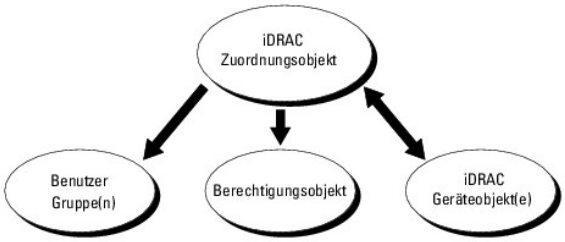
Für jedes der physischen iDRAC6-Geräte auf dem Netzwerk, das Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein iDRAC6-Geräteobjekt erstellen. Sie können verschiedene Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt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

Jedoch darf jedes Zuordnungsobjekt nur mit einem Berechtigungsobjekt verbunden werden bzw. darf jedes Zuordnungsobjekt Benutzer, Benutzergruppen oder iDRAC6-Geräteobjekte nur mit einem Berechtigungsobjekt verbinden. Dieses Beispiel ermöglicht dem Administrator, die Berechtigungen jedes Benutzers auf spezifischen iDRAC6-Geräten zu steuern.

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

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

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



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

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

Mit der Dell-Erweiterung zum ADUC-MMC-Snap-In ist es nur möglich, das Berechtigungsobjekt und iDRAC6-Objekt von derselben Domäne aus mit dem Zuordnungsobjekt zuzuordnen. Die Dell-Erweiterung erlaubt, dass weder ein Gruppen- noch ein iDRAC6-Objekt von anderen Domänen aus als Produktmitglied des Zuordnungsobjekts hinzugefügt wird.

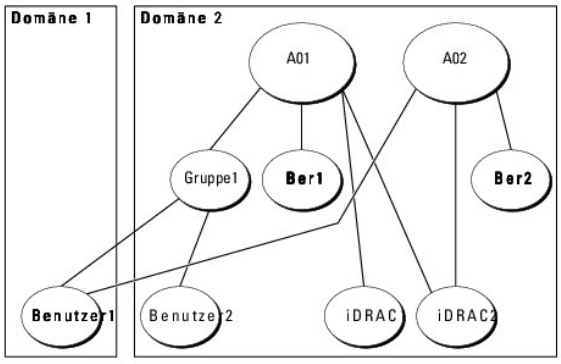
Benutzer, Benutzergruppen oder verschachtelte Benutzergruppen jeglicher Domäne können dem Zuordnungsobjekt hinzugefügt werden. Lösungen des Erweiterten Schemas unterstützen jeden Benutzergruppentyp und jede Benutzergruppenverschachtelung über mehrere von Microsoft Active Directory erlaubte Domänen hinaus.

Unter Verwendung des erweiterten Schemas Berechtigungen ansammeln

Die Methode der Authentifizierung des erweiterten Schemas unterstützt das Ansammeln von Berechtigungen über unterschiedliche Berechtigungsobjekte, die mit demselben Benutzer durch verschiedene Zuordnungsobjekte in Verbindung stehen. Mit anderen Worten sammelt die Authentifizierung des erweiterten Schemas Berechtigungen an, um dem Benutzer den Super-Satz aller zugewiesener Berechtigungen zur Verfügung stellen zu können, die den verschiedenen, mit demselben Benutzer in Verbindung stehenden, Berechtigungsobjekten entsprechen.

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

Abbildung 6-2. Ansammeln von Berechtigungen für einen Benutzer



Die Abbildung stellt zwei Zuordnungsobjekte dar - A01 und A02. Benutzer1 wird über beide Zuordnungsobjekte mit iDRAC2 assoziiert. Benutzer1 hat daher Berechtigungen angesammelt, die das Ergebnis der Kombination der Berechtigungen sind, die für die Objekte Priv1 und Priv2 auf iDRAC2 eingerichtet wurden.

Zum Beispiel besitzt Priv1 die Berechtigungen Anmeldung, Virtueller Datenträger und Protokolle löschen, und Priv2 besitzt die Berechtigungen Anmeldung am iDRAC, iDRAC konfigurieren und Testwarnungen. Daraus ergibt sich, dass Benutzer1 nun über den folgenden Berechtigungssatz verfügt: Anmeldung am iDRAC, Virtueller Datenträger, Protokolle löschen, iDRAC konfigurieren und Testwarnungen, was den kombinierten Berechtigungssatz von Priv1 und Priv2 darstellt.

Mit anderen Worten sammelt die Authentifizierung des erweiterten Schemas Berechtigungen an, um dem Benutzer den maximalen Satz aller möglichen Berechtigungen zur Verfügung stellen zu können, wobei die zugewiesenen Berechtigungen der verschiedenen Berechtigungsobjekte, die mit demselben Benutzer in Verbindung stehen, berücksichtigt werden.

Bei dieser Konfiguration besitzt Benutzer1 sowohl die Priv1- als auch die Priv2-Berechtigungen auf iDRAC2. Benutzer1 verfügt nur auf iDRAC1 über Priv1-Berechtigungen. Benutzer2 verfügt sowohl auf iDRAC1 als auch auf iDRAC2 über Priv1-Berechtigungen. Zusätzlich zeigt diese Abbildung, dass sich Benutzer1 in einer anderen Domäne befinden und Mitglied einer Gruppe sein kann.

Erweitertes Schema von Active Directory konfigurieren, um auf den iDRAC6 zuzugreifen

Konfigurieren Sie vor der Verwendung von Active Directory zum Zugriff auf iDRAC6 die Active Directory-Software und den iDRAC6, indem Sie die folgenden Schritte in der vorgegebenen Reihenfolge durchführen:

1. Erweitern Sie das Active Directory-Schema (s. "Erweiterung des Active Directory-Schemas").

2. Erweitern Sie das Snap-In von Active Directory-Benutzer und -Computer (s. "Dell Erweiterung zum Active Directory-Benutzer und -Computer-Snap-In installieren").

3. Fügen Sie Active Directory iDRAC6-Benutzer und deren Berechtigungen hinzu (siehe "iDRAC6-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 iDRAC6 entweder über die webbasierte iDRAC6-Schnittstelle oder über RACADM (siehe "Active Directory mit Erweitertem Schema unter Verwendung der webbasierten iDRAC6-Schnittstelle konfigurieren" oder "Active Directory mit Erweitertem Schema unter Verwendung von RACADM konfigurieren").

Mit der Erweiterung des Active Directory-Schemas werden dem Active Directory-Schema eine Dell-Organisationseinheit, Schemaklassen und -attribute sowie Beispielberechtigungen und Zuordnungsobjekte hinzugefügt. Bevor Sie das Schema erweitern, ist sicherzustellen, dass Sie Schema-Admin-Rechte auf dem Schema Master-FSMO-Rollenbesitzer (Flexible Single Master Operation) der Domänenstruktur besitzen.

Sie können das Schema mit einer der folgenden Methoden erweitern:

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

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

Die LDIF-Dateien und Dell Schema Extender befinden sich auf der DVD *Dell Systems Management Tools and Documentation* in den folgenden jeweiligen Verzeichnissen:

- *DVD-Laufwerk*:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- *<DVD-Laufwerk>*:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender**

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Dateien**. Informationen zur Verwendung von Dell Schema Extender zum Erweitern des Active Directory-Schemas befinden sich unter "Dell Schema Extender verwenden".

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

Dell Schema Extender verwenden

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

1. Klicken Sie auf dem **Willkommen**-Bildschirm auf **Weiter**.

2. Lesen Sie die Warnung und vergewissern Sie sich, dass Sie sie verstehen, und klicken Sie auf **Weiter**.

3. Wählen Sie **Aktuelle Anmeldeinformationen verwenden** aus, oder geben Sie einen Benutzernamen und ein Kennwort mit Schema-Administratorrechten ein.

4. Klicken Sie auf **Weiter**, um den Dell Schema Extender auszuführen.

5. Klicken Sie auf **Fertig stellen**.

   Das Schema wird erweitert. Zur Überprüfung der Schema-Erweiterung verwenden Sie die Microsoft Verwaltungskonsole (MMC) und das Active Directory Schema-Snap-In, um zu überprüfen, ob folgende Elemente vorhanden sind:

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

   Details über die Verwendung der MMC und des Active Directory-Schema-Snap-Ins finden Sie in Ihrer Microsoft Dokumentation.

Tabelle 6-2. Klassendefinitionen für zum Active Directory-Schema hinzugefügte Klassen

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabelle 6-3. dellRacDevice Class

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

Tabelle 6-4. delliDRACAssociationObject-Klasse

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

Tabelle 6-5. dellRAC4Privileges Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
Beschreibung	Legt die Berechtigungen (Autorisierungsrechte) für den iDRAC6 fest
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 Liste der dellRacDevice- und DelliDRACDevice-Objekte, die zu dieser Rolle 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 besitzt.	1.2.840.113556.1.8000.1280.1.1.2.4 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.5 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE, wenn der Benutzer Protokolllöschungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.7 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE, wenn der Benutzer Konsolenumleitungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.8 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE, wenn der Benutzer Rechte für den virtuellen Datenträger auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE, wenn der Benutzer Testwarnungsbenutzerrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.10 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE, wenn der Benutzer Debug-Befehl-Administratorrechte auf dem Gerät besitzt.	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 delliDRACDevice-Objekt und der Rückwärtslink zum dellAssociationObjectMembers-Vorwärtslink.	1.2.840.113556.1.8000.1280.1.1.2.13 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Die Liste von dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist das Rückwärtslink zum dellProductMembers-verknüpften Attribut. Link-ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Definierter Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

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

Wenn Sie die Systems Management Software von der **DVD** *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsvorgangs die Option Active Directory-Benutzer- und -Computer-Snap-In auswählen. Das *Schnellinstallationshandbuch zu Dell OpenManage-Software* enthält zusätzliche Anleitungen zur Installation von Systemverwaltungssoftware. Bei 64-Bit-Betriebssystemen von Windows befindet sich des Snap-In-Installationsprogramm unter:

<DVD-Laufwerk>: \SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

Weitere Informationen über Active Directory-Benutzer- und Computer-Snap-In erhalten Sie in Ihrer Dokumentation von Microsoft.

Administratorpaket installieren

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

Weitere Informationen finden Sie unter Snap-In von Active Directory-Benutzer und -Computer öffnen".

Snap-In von Active Directory-Benutzer und -Computer öffnen

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

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

   Wenn Sie nicht auf dem Domänen-Controller angemeldet sind, muss das entsprechende Microsoft Administratorpaket auf dem lokalen System installiert sein. Klicken Sie zur Installation des Administratorpakets auf **Start→ Ausführen**, geben Sie `MMC` ein und drücken Sie **Eingabe**.

   Die MMC wird angezeigt.

2. Klicken Sie im Fenster **Konsole 1** auf **Datei** (oder auf **Konsole** bei Systemen, auf denen Windows 2000 ausgeführt wird).

3. Klicken Sie auf **Snap-In hinzufügen/entfernen**.

4. Wählen Sie **Active Directory-Benutzer- und Computer-Snap-In** aus und klicken Sie auf **Hinzufügen**.

5. Klicken Sie auf **Schließen** und dann auf **OK**.

iDRAC6-Benutzer und -Berechtigungen zum Active Directory hinzufügen

Mit dem von Dell erweiterten Active Directory-Benutzer- und Computer-Snap-In können Sie iDRAC6-Benutzer und -Berechtigungen hinzufügen, indem Sie iDRAC6-, Zuordnungs- und Berechtigungsobjekte erstellen. Führen Sie zum Hinzufügen der einzelnen Objektarten folgende Verfahren aus:

- Erstellen Sie ein iDRAC6-Geräteobjekt
- Berechtigungsobjekt erstellen
- Zuordnungsobjekt erstellen
- Einem Zuordnungsobjekt Objekte hinzufügen

iDRAC6-Geräteobjekt erstellen

1. Klicken Sie im Fenster MMC-**Console Root** mit der rechten Maustaste auf einen Container.

2. Wählen Sie **Neu→ Erweitertes Dell Remote-Verwaltungsobjekt** aus.

   Das Fenster **Neues Objekt** wird geöffnet.

3. Geben Sie einen Namen für das neue Objekt ein. Der Name muss mit dem iDRAC6-Namen übereinstimmen, den Sie in Schritt A von "Active Directory mit Erweitertem Schema unter Verwendung der webbasierten iDRAC6-Schnittstelle konfigurieren" eingeben.

4. Wählen Sie **iDRAC-Geräteobjekt** aus.

5. Klicken Sie auf **OK**.

Berechtigungsobjekt erstellen

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

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.

2. Wählen Sie **Neu→ Erweitertes Dell Remote-Verwaltungsobjekt** aus.

   Das Fenster **Neues Objekt** wird geöffnet.

3. Geben Sie einen Namen für das neue Objekt ein.

4. Wählen Sie **Berechtigungsobjekt** aus.
5. Klicken Sie auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf das Berechtigungsobjekt, das Sie erstellt haben, und wählen Sie **Eigenschaften** aus.
7. Klicken Sie auf das Register **Remote-Verwaltungsberechtigung** und wählen Sie die Berechtigungen aus, die Sie für den Benutzer oder die Gruppe vorgesehen haben (siehe Tabelle 5-10).

Zuordnungsobjekt erstellen

ANMERKUNG: Das iDRAC6-Zuordnungsobjekt wird von einer Gruppe abgeleitet und seine Reichweite ist auf lokale Domäne eingestellt.

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu→ Erweitertes Dell Remote-Verwaltungsobjekt** aus.

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

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

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

Benutzer oder Benutzergruppen hinzufügen

1. Klicken Sie mit der rechten Maustaste auf **Zuordnungsobjekt** und wählen Sie **Eigenschaften**.
2. Wählen Sie die Registerkarte **Benutzer** und klicken Sie auf **Hinzufügen**.
3. Geben Sie den Namen des Benutzers oder der Benutzergruppe ein und klicken Sie auf **OK**.

Berechtigungen hinzufügen

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

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

iDRAC6-Geräte oder oder iDRAC6-Gerätegruppen hinzufügen

Um iDRAC6-Geräte oder iDRAC6-Gerätegruppen hinzuzufügen:

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

Klicken Sie auf die Registerkarte **Produkte**, um ein mit dem Netzwerk verbundenes iDRAC6-Gerät hinzuzufügen, das für festgelegte Benutzer oder Benutzergruppen verfügbar ist. Einem Zuordnungsobjekt können mehrere iDRAC6-Geräte hinzugefügt werden.

Active Directory mit Erweitertem Schema unter Verwendung der webbasierten iDRAC6-Schnittstelle konfigurieren

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der webbasierten iDRAC6-Benutzerschnittstelle an.
3. Wählen Sie in der Systemstruktur **System**→ **Remote-Zugriff**→ **iDRAC** aus.

   Die Seite **iDRAC-Informationen** wird angezeigt.
4. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit** und dann auf **Active Directory**.

   Die Seite **Active Directory-Konfiguration und Verwaltung** wird angezeigt.
5. Scrollen Sie zum unteren Bildschirmrand und klicken Sie auf **Active Directory konfigurieren**.

   Die Seite **Schritt 1 von 4 Active Directory - Konfiguration und Verwaltung** wird angezeigt.
6. Wählen Sie zum Überprüfen des SSL-Zertifikats Ihres Active Directory- Servers das Kontrollkästchen **Zertifikat-Validierung aktivieren** unter **Zertifikatseinstellungen** aus.

   Wenn Sie das SSL-Zertifikat Ihres Active Directory-Servers nicht überprüfen möchten, ergreifen Sie keine Maßnahme, sondern fahren mit Schritt 8 fort.
7. Geben Sie unter **Active Directory-CA-Zertifikat hochladen** den Dateipfad des Zertifikats ein oder durchsuchen das System, um die Zertifikatsdatei zu finden, und klicken dann auf **Hochladen**.

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

   Die Zertifikatsinformationen für das von Ihnen hochgeladene Active Directory-CA-Zertifikat wird im Abschnitt **Aktuelles Active Directory-CA-Zertifikat** angezeigt.
8. Klicken Sie auf **Next** (Weiter).

   Die Seite **Schritt 2 von 4 Active Directory - Konfiguration und Verwaltung** wird angezeigt.
9. Wählen Sie das Kontrollkästchen **Active Directory aktivieren** aus.
10. Klicken Sie zum Eingeben des Benutzerdomänennamens auf **Hinzufügen**, geben Sie den Benutzerdomänennamen im Textfeld ein und klicken Sie dann auf **OK**.
11. Geben Sie den Benutzerdomänennamen in der Eingabeaufforderung ein und klicken Sie auf **OK**. Beachten Sie, dass dieser Schritt optional ist. Wenn Sie eine Liste von Benutzerdomänen konfigurieren, wird diese Liste auf dem Anmeldebildschirm der webbasierten Schnittstelle verfügbar sein. Sie können von dieser Liste auswählen und brauchen dann nur noch den Benutzernamen einzugeben.
12. Geben Sie im Feld **Zeitüberschreitung** die Sekunden ein, die iDRAC6 abwarten soll, bevor Active Directory antwortet. Der Standardwert beträgt 120 Sekunden.
13. Geben Sie die **Serveradresse des Domain-Controllers** ein. Es können bis zu drei Active Directory-Server zur Verarbeitung der Anmeldung eingegeben werden, jedoch müssen Sie mindestens einen Server konfigurieren, indem Sie die IP-Adresse oder den vollständig qualifizierten Domänennamen (FQDN) eingeben. iDRAC6 versucht, mit jedem konfigurierten Server zu verbinden, bis eine Verbindung hergestellt ist.

    ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie für dieses Feld festlegen, sollte mit den Feldern **Bewerber** oder **Alternativer Bewerbername** Ihres Domänen-Controller-Zertifikats übereinstimmen, wenn die Zertfikatsüberprüfung aktiviert ist.
14. Klicken Sie auf **Next** (Weiter).

    Die Seite **Schritt 3 von 4 Active Directory - Konfiguration und Verwaltung** wird angezeigt.
15. Wählen Sie das Kontrollkästchen **Erweitertes Schema** unter **Schemaauswahl.**
16. Klicken Sie auf **Next** (Weiter).

    Die Seite **Schritt 4 von 4 Active Directory - Konfiguration und Verwaltung** wird angezeigt.
17. Geben sie unter **Erweitertes Schema - Einstellungen** den iDRAC6-Namen und -Domänennamen ein, um das iDRAC6-Geräteobjekt und seinen

Speicherort im Active Directory zu konfigurieren.

18. Klicken Sie zum Speichern der Änderungen auf **Fertigstellen** und dann auf **Done (Fertig)**.

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

19. Scrollen Sie zum unteren Bildschirmrand und klicken Sie auf **Einstellungen testen**.

    Die Seite **Active Directory-Einstellungen testen** wird angezeigt.

20. Geben Sie Ihren iDRAC6-Benutzernamen und Ihr -Kennwort ein und klicken Sie dann auf **Test starten**.

    Die Testergebnisse und das Testprotokoll werden angezeigt. Weitere Informationen finden Sie unter "Konfigurationen testen".

ANMERKUNG: Der DNS-Server muss ordnungsgemäß auf dem iDRAC6 konfiguriert sein, damit er die Anmeldung am Active Directory unterstützen kann. Wechseln Sie zur Seite **Netzwerkkonfiguration** (klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Netzwerk/Sicherheit**), um den/die DNS-Server manuell zu konfigurieren, oder verwenden Sie DHCP, um den/die DNS-Server zu erhalten.

Sie haben die Konfiguration von Active Directory mit Erweitertem Schema abgeschlossen.

Active Directory mit Erweitertem Schema unter Verwendung von RACADM konfigurieren

Verwenden Sie die folgenden Befehle zum Konfigurieren der Active Directory-Funktion des iDRAC6 mit erweitertem Schema unter Verwendung des RACADM-CLI-Hilfsprogramms statt der webbasierten Schnittstelle.

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

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

   racadm config -g cfgActiveDirectory -o cfgADType 1

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

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

   racadm config -g cfgActiveDirectory -o cfgDomainController1 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>

   racadm config -g cfgActiveDirectory -o cfgDomainController2 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>

   racadm config -g cfgActiveDirectory -o cfgDomainController3 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
   ```

   ANMERKUNG: Mindenstens eine der drei Adressen muss konfiguriert werden. iDRAC6 versucht, mit jeder der konfigurierten Adressen nacheinander zu verbinden, bis eine Verbindung erfolgreich hergestellt ist. Diese sind die FQDN oder IP-Adressen des Domänen-Controllers mit Erweitertem Schema, auf denen sich das iDRAC6-Gerät befindet. Globale Katalogserver werden im Erweiterten Schema überhaupt nicht verwendet.

   Wenn Sie die Zertifikatsvalidierung während des SSL-Handshaking deaktivieren möchten, geben Sie den folgenden RACADM-Befehl ein:

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

   In diesem Fall müssen Sie das CA-Zertifikat nicht hochladen.

   Wenn Sie die Zertifikatsvalidierung während des SSL-Handshaking erzwingen möchten, geben Sie den folgenden RACADM-Befehl ein:

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

   In diesem Fall müssen Sie ein CA-Zertifikat mithilfe des folgenden RACADM-Befehls hochladen:

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

   Die Verwendung des folgenden RACADM-Befehls ist eventuell optional. Weitere Informationen finden Sie unter "SSL-Zertifikat der iDRAC6-Firmware importieren".

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

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

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

3. Wenn DHCP auf dem iDRAC6 deaktiviert ist oder Sie Ihre DNS-IP- Adresse manuell eingeben möchten, geben Sie die folgenden RACADM- Befehle ein:

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

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

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

4. Wenn Sie eine Liste der Benutzerdomänen konfigurieren möchten, um lediglich den Benutzernamen während der Anmeldung an der webbasierten iDRAC6-Schnittstelle eingeben zu brauchen, geben sie den folgenden Befehl ein:

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

   Es können bis zu 40 Benutzerdomänen mit Indexnummern zwischen 1 und 40 konfiguriert werden.

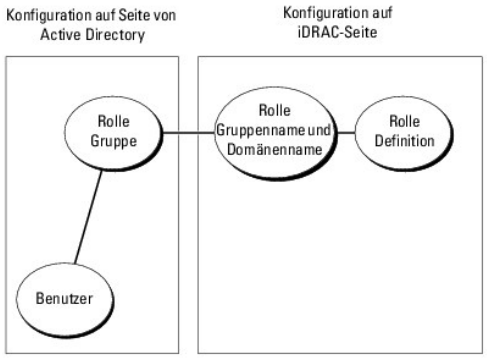
   Details zu Benutzerdomänen finden Sie unter "Active Directory zur Anmeldung beim iDRAC6 verwenden".

5. Drücken Sie **Eingabe**, um die Active Directory-Konfiguration mit Erweitertem Schema abzuschließen.

Übersicht des Standardschema-Active Directory

Wie in Abbildung 6-3dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration unter Active Directory als auch unter iDRAC6.

Abbildung 6-3. Konfiguration des iDRAC6 mit Microsoft Active Directory und Standardschema



Auf der Seite des Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der Zugang zum iDRAC6 hat, wird ein Mitglied der Rollengruppe sein. Um diesem Benutzer Zugriff auf eine spezifische iDRAC6-Karte zu gewähren, müssen der Rollengruppenname und sein Domänenname auf der spezifischen iDRAC6-Karte konfiguriert werden. Im Unterschied zur Lösung des erweiterten Schemas, sind die Rollen- und Berechtigungsebenen auf jeder iDRAC6-Karte und nicht im Active Directory festgelegt. Bis zu fünf Rollengruppen können in jedem iDRAC6 konfiguriert und definiert werden. Tabelle 6-9 zeigt die Standardeinstellung der Rollengruppenberechtigungen.

Tabelle 6-9. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppen	Standard-Zugriffsstufe	Gewährte Berechtigungen	Bit-Maske
Rollengruppe 1	Administrator	**Beim iDRAC anmelden**, **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **auf Konsolenumleitung zugreifen**, **auf Virtuellen Datenträger zugreifen**, **Warnungen testen**, **Diagnosebefehle ausführen**	0x000001ff
Rollengruppe 2	Operator	**Beim iDRAC anmelden**, **iDRAC konfigurieren, Serversteuerungsbefehle ausführen**, **auf Konsolenumleitung zugreifen**, **auf Virtuellen Datenträger zugreifen**, **Warnungen testen, Diagnosebefehle ausführen**	0x000000f9
Rollengruppe 3	Schreibgeschützt.	Bei iDRAC anmelden	0x00000001
Rollengruppe 4	Keine	Keine zugewiesenen Berechtigungen	0x00000000
Rollengruppe 5	Keine	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bitmasken-Werte werden nur verwendet, wenn das Standardschema mit dem RACADM eingerichtet wird.

Einzeldomänen- vs. Mehrdomänenszenarien

Wenn sich alle anmeldenden Benutzer und Rollengruppen sowie verschachtelte Gruppen in derselben Domäne befinden, müssen lediglich die Adressen der Domänen-Controller auf dem iDRAC6 konfiguriert werden. Jeder Gruppentyp wird in diesem Einzeldomänenszenario unterstützt.

Wenn alle anmeldenden Benutzer und Rollengruppen oder jedwede der verschachtelten Gruppen von mehreren Domänen kommen, müssen Adressen des globalen Katalogservers auf dem iDRAC6 konfiguriert werden. Alle Rollengruppen und verschachtelten Gruppen, falls vorhanden, müssen in diesem Mehrdomänenszenario vom Typ Universalgruppen sein.

Standardschema von Active Directory konfigurieren, um auf den iDRAC6 zuzugreifen

Bevor ein Active Directory-Benutzer auf den iDRAC6 zugreifen kann, müssen die folgenen Schritte zur Konfiguration des Active Directory durchgeführt 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 Gruppen- und der Domänenname müssen auf dem iDRAC6 entweder mithilfe der webbasierten Schnittstelle oder RACADM konfiguriert werden (siehe "Active Directory mit Standardschema unter Verwendung der webbasierten iDRAC6-Schnittstelle konfigurieren" oder "Active Directory mit Standardschema unter Verwendung von RACADM konfigurieren").
3. Fügen Sie den Active Directory-Benutzer als ein Mitglied der Active Directory-Gruppe hinzu, um auf den iDRAC6 zuzugreifen.

Active Directory mit Standardschema unter Verwendung der webbasierten iDRAC6-Schnittstelle konfigurieren

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich an der iDRAC6-Benutzerschnittstelle an.
3. Wählen Sie in der Systemstruktur **System**→ **Remote-Zugriff**→ **iDRAC** aus.
4. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit** und dann auf **Active Directory**.

   Die Seite **Active Directory-Konfiguration und Verwaltung** wird angezeigt.
5. Scrollen Sie zum unteren Bildschirmrand und klicken Sie auf **Active Directory konfigurieren**.

   Die Seite **Schritt 1 von 4 Active Directory - Konfiguration und Verwaltung** wird angezeigt.
6. Wählen Sie **Active Directory aktivieren** unter **Zertifikatseinstellungen** aus.
7. Geben Sie unter **Active Directory-CA-Zertifikat hochladen** den Dateipfad des Zertifikats ein oder durchsuchen das System, um die Zertifikatsdatei zu finden, und klicken dann auf **Hochladen**.

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

   Die Zertifikatsinformationen für das von Ihnen hochgeladene Active Directory-CA-Zertifikat wird im Abschnitt **Aktuelles Active Directory-CA-Zertifikat** angezeigt.
8. Klicken Sie auf Next (Weiter).

   Die Seite **Schritt 2 von 4 Active Directory - Konfiguration und Verwaltung** wird angezeigt.
9. Wählen Sie das Kontrollkästchen **Active Directory aktivieren** aus.
10. Klicken Sie zum Eingeben des Benutzerdomänennamens auf **Hinzufügen**, geben Sie den Benutzerdomänennamen im Textfeld ein und klicken Sie dann auf **OK**.
11. Geben Sie im Feld **Zeitüberschreitung** die Sekunden ein, die iDRAC6 abwarten soll, bevor Active Directory antwortet. Der Standardwert beträgt 120 Sekunden.
12. Geben Sie die **Serveradresse des Domain-Controllers** ein. Es können bis zu drei Active Directory-Server zur Verarbeitung der Anmeldung eingegeben werden, jedoch müssen Sie mindestens einen Server konfigurieren, indem Sie die IP-Adresse oder den vollständig qualifizierten Domänennamen (FQDN) eingeben. iDRAC6 versucht, mit jedem konfigurierten Server zu verbinden, bis eine Verbindung hergestellt ist.
13. Klicken Sie auf **Next** (Weiter).

    Die Seite **Schritt 3 von 4 Active Directory - Konfiguration und Verwaltung** wird angezeigt.
14. Wählen Sie das Kontrollkästchen **Standardschema** unter **Schemaauswahl** aus.
15. Klicken Sie auf **Next** (Weiter).

    Die Seite **Schritt 4a von 4 Active Directory - Konfiguration und Verwaltung** wird angezeigt.
16. Geben Sie unter **Standardschemaeinstellungen** die Adresse(n) des globalen Katalogservers ein.

ANMERKUNG: Der globale Katalogserver ist nur für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen in unterschiedlichen Domänen befinden. In diesem Mehrdomänen-Fall kann nur die Universalgruppe verwendet werden.

17. Klicken Sie auf eine **Rollengruppe-**Schaltfläche, um eine Rollengruppe hinzuzufügen.

    Die Seite **Schritt 4b von 4 Rollengruppe 1 konfigurieren** wird angezeigt.

18. Geben Sie den **Gruppennamen** ein. Der Gruppenname identifiziert die Rollengruppe in dem Active Directory, das dem iDRAC6 zugeordnet ist.

19. Geben Sie die **Gruppendomäne** ein. Die **Gruppendomäne** ist der vollständig qualifizierte root-Domänenname der Gesamtstruktur.

20. Richten Sie im Abschnitt **Rollengruppenberechtigungen** die Gruppenberechtigungen ein. Informationen zu Rollengruppenberechtigungen finden Sie unter Tabelle 5-11.

    ANMERKUNG: Wenn Sie eine Berechtigung modifizieren, wird die vorhandene Rollengruppenberechtigung (Administrator, Hauptbenutzer oder Gastbenutzer) auf Grundlage der modifizierten Berechtigungen entweder zur benutzerdefinierten Gruppe oder zur entsprechenden Rollengruppenberechtigung verändert.

21. Klicken Sie auf **OK**, um die Einstellungen der Rollengruppe zu speichern.

    Ein Warnungsdialogfeld wird eingeblendet und weist darauf hin, dass die Einstellungen verändert wurden. Klicken Sie auf OK, um zur Seite **Schritt 4a von 4 Active Directory - Konfiguration und Verwaltung** zurückzukehren.

22. Um eine weitere Rollengruppe hinzuzufügen, wiederholen Sie Schritt 17 bis Schritt 21.

23. Klicken Sie auf **Fertigstellen** und dann auf **Done (Fertig)**.

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

24. Scrollen Sie zum unteren Bildschirmrand und klicken Sie auf **Einstellungen testen**.

    Die Seite **Active Directory-Einstellungen testen** wird angezeigt.

25. Geben Sie Ihren iDRAC6-Benutzernamen und Ihr -Kennwort ein und klicken Sie dann auf **Test starten**.

    Die Testergebnisse und das Testprotokoll werden angezeigt. Weitere Informationen finden Sie unter "Konfigurationen testen".

ANMERKUNG: Der DNS-Server muss ordnungsgemäß auf dem iDRAC6 konfiguriert sein, damit er die Anmeldung am Active Directory unterstützen kann. Wechseln Sie zur Seite **Remote-Zugriff→ Konfiguration→ Netzwerk**, um DNS-Server manuell zu konfigurieren oder DHCP zu verwenden, um DNS-Server zu erhalten.

Sie haben die Konfiguration von Active Directory mit Standardschema abgeschlossen.

Active Directory mit Standardschema unter Verwendung von RACADM konfigurieren

Verwenden Sie die folgenden Befehle zum Konfigurieren der Active Directory-Funktion des IDRAC6 mit Standardschema unter Verwendung der RACADM-CLI statt der webbasierten Schnittstelle.

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

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

racadm config -g cfgActiveDirectory -o cfgADType 2

racadm config -g cfgStandardSchema -i <Index> -o
cfgSSADRoleGroupName <allgemeiner Name der Rollengruppe>

racadm config -g cfgStandardSchema -i <Index>-o
cfgSSADRoleGroupDomain <vollständig qualifizierter Domänenname>

racadm config -g cfgStandardSchema -i <Index>-o
cfgSSADRoleGroupPrivilege <Bitmaskenwert für
spezifische Benutzerberechtigungen>
```

    ANMERKUNG: Siehe Tabelle B-1für Bitmasken-Zahlenwerte.

```
racadm config -g cfgActiveDirectory -o cfgDomainController1 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-
Controllers>

racadm config -g cfgActiveDirectory -o cfgDomainController2 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-
Controllers>

racadm config -g cfgActiveDirectory -o cfgDomainController3 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-
```

Controllers>

ANMERKUNG: Geben Sie den FQDN des Domänen-Controllers an, aber *nicht* den FQDN der Domäne. Geben Sie zum Beispiel servername.dell.com statt dell.com ein.

ANMERKUNG: Mindestens eine der drei Adressen muss konfiguriert werden. iDRAC6 versucht, mit jeder der konfigurierten Adressen nacheinander zu verbinden, bis eine Verbindung erfolgreich hergestellt ist. Dies sind die Adressen des Domänen-Controllers mit Standardschema, auf denen sich die Benutzerkonten und Rollengruppen befinden.

```
racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>

racadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>

racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
```

ANMERKUNG: Der globale Katalogserver ist nur für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen in unterschiedlichen Domänen befinden. In diesem Mehrdomänen-Fall kann nur die Universalgruppe verwendet werden.

ANMERKUNG: Der FQDN oder die IP-Adresse, die Sie für dieses Feld festlegen, sollte mit den Feldern **Bewerber** oder **Alternativer Bewerbername** Ihres Domänen-Controller-Zertifikats übereinstimmen, wenn die Zertfikatsüberprüfung aktiviert ist.

Wenn Sie die Zertifikatsvalidierung während des SSL-Handshaking deaktivieren möchten, geben Sie den folgenden RACADM-Befehl ein:

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

In diesem Fall muss kein Zertifizierungsstellen-(CA)-Zertifikat hochgeladen werden.

Wenn Sie die Zertifikatsvalidierung während des SSL-Handshaking erzwingen möchten, geben Sie den folgenden RACADM-Befehl ein:

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

In diesem Fall müssen Sie auch das CA-Zertifikat mithilfe des folgenden RACADM-Befehls hochladen:

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

Die Verwendung des folgenden RACADM-Befehls ist eventuell optional. Weitere Informationen finden Sie unter "SSL-Zertifikat der iDRAC6-Firmware importieren".

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

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

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

3. Wenn DHCP auf dem iDRAC6 deaktiviert ist oder Sie Ihre DNS-IP- Adresse manuell eingeben möchten, geben Sie die folgenden RACADM- Befehle ein:

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

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

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

4. Wenn Sie eine Liste der Benutzerdomänen konfigurieren möchten, um lediglich den Benutzernamen während der Anmeldung an der webbasierten Schnittstelle eingeben zu brauchen, geben sie den folgenden Befehl ein:

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

   Es können bis zu 40 Benutzerdomänen mit Indexnummern zwischen 1 und 40 konfiguriert werden.

   Details zu Benutzerdomänen finden Sie unter "Active Directory zur Anmeldung beim iDRAC6 verwenden".

Konfigurationen testen

Wenn Sie überprüfen möchten, ob Ihre Konfiguration funktioniert, oder wenn Sie das Problem bei der fehlgeschlagenen Active Directory-Anmeldung diagnostizieren müssen, können Sie Ihre Einstellungen von der webbasierten iDRAC6-Schnittstelle aus testen.

Klicken Sie, nachdem die Konfiguration der Einstellungen in der webbasierten iDRAC6-Schnittstelle abgeschlossen sind, auf **Einstellungen testen** an der Unterkante der Seite. Es ist erforderlich, einen Test-Benutzernamen (z. B. Benutzername@Domäne.de) und ein Kennwort zur Ausführung des Tests einzugeben. Abhängig von der Konfiguration dauert es eine gewisse Zeit, bis der Test abgeschlossen ist und die Ergebnisse angezeigt werden können. Am Ende der Ergebnisseite wird ein ausführliches Testprotokoll angezeigt.

Wenn ein Fehler in irgendeinem Schritt auftritt, überprüfen Sie das Testprotokoll, um das Problem herauszufinden und zu lösen. Informationen zu den meisten allgemeinen Fehlern finden Sie unter "Häufig gestellte Fragen".

Wenn Sie an Ihren Einstellungen Änderungen vornehmen müssen, klicken Sie auf die Registerkarte **Active Directory** und ändern Sie die Konfiguration schrittweise.

SSL auf einem Domänen-Controller aktivieren

Wenn Benutzer durch den iDRAC6 gegen einen Active Directory-Domänen-Controller authentifiziert werden, wird eine SSL-Sitzung mit dem Domänen-Controller gestartet. Der Domänen-Controller sollte jetzt ein von der Zertifizierungsstelle (CA) signiertes Zertifikat veröffentlichen. Und zwar das Stammzertifikat, das auch in den iDRAC6 hochgeladen wird. Damit, anders ausgedrückt, die iDRAC6-Authentifizierung auf einen *beliebigen* Domänen-Controller möglich ist - egal, ob es sich um den Stamm-Domänen-Controller oder den untergeordneten Domänen-Controller handelt - muss dieser Domänen-Controller ein SSL-aktiviertes von der CA der Domäne signiertes Zertifikat besitzen.

Wenn Sie die Microsoft Enterprise-Stamm-CA verwenden, um alle Domänen-Controller *automatisch* einem SSL-Zertifikat zuzuweisen, müssen Sie die folgenden Schritte ausführen, um SSL auf den einzelnen Domänen-Controllern zu aktivieren.

1. Aktivieren Sie SSL auf jedem einzelnen Domänen-Controller, indem Sie das SSL-Zertifikat für jeden Controller installieren.
   a. Klicken Sie auf **Start**→ **Verwaltung**→ **Domänensicherheitsregeln**.
   b. Erweitern Sie den Ordner **Richtlinien öffentlicher Schlüssel** klicken Sie mit der rechten Maustaste auf **Automatische Zertifikatanforderungs-Einstellungen** und klicken Sie auf **Automatische Zertifikatanforderung**.
   c. Klicken Sie im **Setup-Assistent der automatischen Zertifikatanforderung** auf **Weiter** und wählen Sie **Domänen- Controller** aus.
   d. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

Stammzertifizierungsstellenzertifikat des Domänen-Controllers in den iDRAC6 exportieren

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

ANMERKUNG: Wenn Sie in Kontakt mit einer eigenständigen Zertifizierungsstelle stehen, können die folgenden Schritte abweichen.

1. Machen Sie den Domänen-Controller ausfindig, der den Microsoft Enterprise-CA -Dienst ausführt.
2. Wählen Sie **Start**→ **Ausführen**.
3. Geben Sie im Feld **Ausführen** den Befehl `mmc` ein und klicken Sie auf **OK.**
4. Klicken Sie im Fenster **Konsole 1** (MMC) auf **Datei** (oder auf **Konsole** auf Windows 2000-Systemen**)** 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. Machen Sie das Stammzertifizierungsstellenzertifikat ausfindig und klicken Sie mit der rechten Maustaste darauf, wählen Sie **Alle Aufgaben** aus und klicken Sie dann 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 in den iDRAC6 hoch.

    Informationen zum Hochladen des Zertifikats unter Verwendung von RACADM finden Sie unter "Active Directory mit Standardschema unter Verwendung von RACADM konfigurieren".

    Wie Sie das Zertifikat mithilfe der webbasierten Schnittstelle hochladen, finden Sie unter "Active Directory mit Standardschema unter Verwendung der webbasierten iDRAC6-Schnittstelle konfigurieren".

SSL-Zertifikat der iDRAC6-Firmware importieren

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

Wenden Sie das folgende Verfahren an, um das SSL-Zertifikat der iDRAC6-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 SSL-Zertifikat der iDRAC6-Firmware von einer bekannten CA signiert wird und sich das Zertifikat dieser CA bereits in der Liste der Vertrauenswürdigen Stammzertifizierungsstellen des Domänen-Controllers befindet, müssen Sie die Schritte in diesem Abschnitt nicht ausführen.

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

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

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

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

   Wenn Sie Ihr eigenes Zertifikat installiert haben, stellen Sie sicher, dass die Zertifizierungsstelle, die das Zertifikat signiert hat, in der Liste **Vertrauenswürdige Stammzertifizierungsstellen** aufgeführt ist. Wenn die Zertifizierungsstelle nicht auf der Liste enthalten ist, muss sie auf allen Ihren Domänen-Controllern installiert werden.
5. Klicken Sie auf **Weiter** und wählen Sie aus, ob Windows automatisch einen Zertifikatspeicher aussuchen soll, der vom Zertifikattyp abhängt, oder ob Sie nach einem eigenen Speicher suchen wollen.
6. Klicken Sie auf **Fertig stellen** und dann auf **OK**.

Active Directory zur Anmeldung beim iDRAC6 verwenden

Sie können Active Directory zum Anmelden am iDRAC6 mithilfe eines der folgenden Verfahren verwenden:

- Web-basierte Schnittstelle
- lokaler RACADM
- SSH oder Telnet-Konsole für die SM-CLP-CLI

Die Anmeldungssyntax ist für alle drei Methoden gleich:

<*Benutzername@Domäne*>

oder

<*Domäne*>\<*Benutzername*> oder <*Domäne*>/<*Benutzername*>

wobei *username* eine ASCII-Zeichenkette von 1 - 256 Byte ist.

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

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

Wenn Sie sich an der webbasierten Schnittstelle anmelden und Benutzerdomänen konfiguriert haben, führt der Anmeldebildschirm der webbasierten Schnittstelle alle Benutzerdomänen im Pulldown-Menü zur Auswahl für Sie auf. Wenn Sie eine Benutzerdomäne aus dem Pulldown-Menü auswählen, geben Sie nur den Benutzernamen ein. Wenn Sie **Dieser iDRAC** auswählen, können Sie sich immer noch als Active Directory-Benutzer anmelden, wenn Sie die Anmeldesyntax, wie oben in "Active Directory zur Anmeldung beim iDRAC6 verwenden" beschrieben, verwenden.

Häufig gestellte Fragen

Probleme beim Anmelden am Active Directory

Meine Anmeldung am Active Directory ist fehlgeschlagen. Was kann ich dagegen tun?

iDRAC6 bietet ein Diagnosehilfsprogramm für die webbasierte Schnittstelle.

1. Melden Sie sich als lokaler Benutzer mit Administratorrechten an der webbasierten Schnittstelle an.

2. Wählen Sie in der Systemstruktur **System→ Remote-Zugriff→ iDRAC** aus.

3. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit** und dann auf das **Active Directory-Unterregister**.

   Die Seite **Active Directory-Konfiguration und Verwaltung** wird angezeigt.

4. Scrollen Sie zum unteren Bildschirmrand und klicken Sie auf **Einstellungen testen**.

   Die Seite **Active Directory-Einstellungen testen** wird angezeigt.

5. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein und klicken Sie dann auf **Test starten**.

   iDRAC6 führt die Tests schrittweise durch und zeigt das Ergebnis jedes Schritts an. iDRAC6 erstellt auch ein ausführliches Protokoll über die Testergebnisse, um beim Lösen jeglicher Probleme behilflich zu sein.

   Wenn Probleme bestehen bleiben:

   a. Klicken Sie auf der Seite **Einstellungen testen** auf das Unterregister **Active Directory**, um zur Seite **Active Directory - Konfiguration und Verwaltung** zurückzukehren.

   b. Scrollen Sie zum unteren Bildschirmrand und klicken Sie auf **Active Directory konfigurieren**.

   c. Ändern Sie die Benutzerkonfiguration und führen Sie den Test erneut durch, bis der Testbenutzer den Autorisierungsschritt besteht.

Obwohl die Zertifikatsvalidierung aktiviert ist, konnte ich mich nicht am Active Directory anmelden. Ich habe eine Diagnose von der GUI aus durchgeführt, dennoch zeigt das Testergebnis die folgende Fehlermeldung an:

```
ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been 144 Using iDRAC6 With Microsoft Active Directory uploaded to iDRAC. Please also check if the iDRAC date is within the valid period of the certificates and if the Domain Controller Address configured in iDRAC matches the subject of the Directory Server Certificate.

(FEHLER: Kann keine Verbindung mit LDAP-Server herstellen, Fehler:14090086:SSL-Routinen:SSL3_GET_SERVER_CERTIFICATE:Zertifikatsüberprüfung fehlgeschlagen: Bitte überprüfen Sie, ob das korrekte Zertifizierungsstellen-(CA)-Zertifikat auf den iDRAChochgeladen wurde. Überprüfen Sie bitte auch, ob das iDRAC-Datum innerhalb der gültigen Zeitspanne der Zertifikate liegt und ob die im iDRAC konfigurierte Adresse des Domänen-Controllers mit dem Berwerber des Directory-Serverzertifikats übereinstimmt.)
```

Was könnte das Problem sein und wie kann ich es beheben?

Wenn die Zertifikatsvalidierung aktiviert ist, verwendet der iDRAC6 das hochgeladene CA-Zertifikat zur Überprüfung des Directory-Serverzertifikats, sobald der iDRAC6 eine SSL-Verbindung zum Directory-Server herstellt. Die häufigsten Ursachen für das Versagen einer Zertifikatsvalidierung sind:

- Das iDRAC6-Datum liegt nicht innerhalb der gültigen Zeitspanne des Serverzertifikats oder CA-Zertifikats. Überprüfen Sie die Uhrzeit des iDRAC6 und den Zeitraum des Zertifikats auf Gütligkeit.
- Die im iDRAC6 konfigurierten Adressen des Domänen-Controllers stimmen nicht mit dem Bewerber oder dem alternativen Bewerbernamen des Directory-Serverzertifikats überein.
  - Wenn Sie eine IP-Adresse verwenden, schauen Sie unter "Ich verwende eine IP-Adresse für eine Domänen-Controlleradresse und die Zertifikatsvalidierung schlug bei mir fehl. Woran liegt das?" nach.
  - Stellen Sie bei der Verwendung eines FQDN sicher, dass Sie den FQDN des Domängen-Controllers und nicht der Domäne selbst verwenden. Zum Beispiel verwenden Sie servername.example.com und *nicht* example.com.

Was sollte ich überprüfen, wenn ich mich nicht mithilfe des Active Directory am iDRAC6 anmelden kann?

Bestimmen Sie zuerst das Problem mithilfe der Funktion Einstellungen testen. Anweisungen finden Sie unter "Meine Anmeldung am Active Directory ist fehlgeschlagen. Was kann ich dagegen tun?".

Beheben Sie dann das von den Testergebnissen angezeigte spezifische Problem. Weitere Informationen finden Sie unter "Konfigurationen testen".

Die häufigsten Problem werden in diesem Abschnitt geklärt. Dennoch sollten Sie üblicherweise Folgendes überprüfen:

1. Stellen Sie sicher, dass Sie während einer Anmeldung den korrekten Benutzerdomänennamen statt des NetBIOS-Namens verwenden.

2. Wenn Sie ein lokales iDRAC6-Benutzerkonto haben, melden Sie sich mit Ihren lokalen Anmeldeinformationen beim iDRAC6 an.

3. Überprüfen Sie die folgenden Einstellungen:

   a. Wechseln Sie zur Seite **Active Directory - Konfiguration und Verwaltung**. Wählen Sie **System→ Remote-Zugriff→ iDRAC** aus, klicken Sie auf das Register **Netzwerk/Sicherheit** und dann auf das Unterregister **Active Directory**.

   b. Stellen Sie sicher, dass das Kontrollkästchen **Active Directory aktiviert** ausgewählt ist.

   c. Wenn Zertifikatsvalidierung aktiviert ist, stellen Sie sicher, dass das richtige Active Directory-Stammzertifizierungsstellenzertifikat auf den iDRAC6 hochgeladen wurde. Das Zertifikat wird im Bereich **Active Directory-CA-Zertifikat** angezeigt. Versichern Sie, dass die iDRAC6- Uhrzeit innerhalb des gültigen Zeitraums des CA-Zertifikats liegt.

   d. Stellen Sie bei Verwendung des Erweiterten Schemas sicher, dass der **iDRAC-Name** und der **iDRAC-Domänenname** mit der

Umgebungskonfiguration des Active Directory übereinstimmen.

Stellen Sie bei Verwendung des Standardschemas sicher, dass der **Gruppenname** und der **Gruppendomänenname** mit der Active Directory-Konfiguration übereinstimmen.

e. Wechseln Sie zur Seite Netzwerkkonfiguration. Wählen Sie **System→ Remote-Zugriff→ iDRAC** aus und klicken Sie dann auf **Netzwerk/ Sicherheit**.
Stellen Sie sicher, dass die DNS-Einstellungen korrekt sind.

f. Überprüfen Sie die SSL-Zertifikate des Domänen-Controllers, um sicherzustellen, dass die iDRAC6-Uhrzeit innerhalb des gültigen Zeitraums des Zertifikats liegt.

Active Directory-Zertifikatsvalidierung

Ich verwende eine IP-Adresse für eine Domänen-Controlleradresse und die Zertifikatsvalidierung schlug bei mir fehl. Woran liegt das?

Überprüfen Sie das Feld Bewerber oder alternativer Berwerbername in Ihrem Domänen-Controllerzertifikat. Normalerweise verwendet Active Directory den Hostnamen des Domänen-Controllers, aber nicht die IP-Adresse, im Feld Bewerber oder alternativer Bewerbername des Domänen-Controllerzertifikats. Sie können dieses Problem beheben, indem Sie eine der folgenden Maßnahmen durchführen:

- Konfigurieren Sie den Hostnamen (FQDN) des Domänen-Controllers als *Domänen-Controlleradresse(n)* auf dem iDRAC6, damit der Bewerber mit dem alternativen Bewerbernamen des Serverzertifikats übereinstimmt.
- Stellen Sie das Zertifikat erneut aus, um eine IP-Adresse im Feld Bewerber oder alternativer Bewerbername zu verwenden, damit es mit der im iDRAC6 konfigurierten IP-Adresse übereinstimmt.
- Deaktivieren Sie die Zertifikatsvalidierung, wenn Sie wählen, diesem Domänen-Controller ohne Zertifikatsvalidierung während des SSL-Handshaking zu vertrauen.

Warum aktiviert iDRAC6 standardmäßig die Zertifikatsvalidierung?

iDRAC6 erzwingt hohe Sicherheit, um die Identität des mit dem iDRAC6 verbundenen Domänen-Controllers sicherzustellen. Ohne Zertifikatsvalidierung könnte ein Hacker einen Domänen-Controller täuschen und die SSL-Verbindung gewaltsam übernehmen. Wenn Sie wählen, allen Domänen-Controllern in Ihrem Sicherheitsbereich ohne Zertifikatsvalidierung zu vertrauen, können Sie diesen durch die GUI oder CLI deaktivieren.

Erweitertes und Standardschema

I verwende das Erweiterte Schema in einer Mehrdomänenumgebung. Wie wird/ werden die Adresse/n des Domänen-Controllers konfiguriert?

Verwenden Sie den Hostnamen (FQDN) oder die IP-Adresse des/der Domänen-Controller/s, der der Domäne dient, in der sich das iDRAC6-Objekt befindet.

Muss ich die globale(n) Katalogadresse(n) konfigurieren?

Bei der Verwendung des Erweiterten Schemas können Sie globale Katalogadressen nicht konfigurieren, weil sie nicht im Erweiterten Schema verwendet werden.

Wenn bei der Verwendung des Standardschemas Benutzer und Rollengruppen von verschieden Domänen kommen, müssen Sie die globale(n) Katalogadresse (n) konfigurieren. In diesem Fall kann nur die Universalgruppe verwendet werden.

Wenn sich bei der Verwendung des Standardschemas alle Benutzer und Rollengruppen in derselben Domäne befinden, müssen Sie die globale(n) Katalogadresse(n) nicht konfigurieren.

Wie funktioniert die Standardschema-Abfrage?

iDRAC6 stellt zuerst eine Verbindung mit den konfigurierten Domänen-Controlleradressen her. Wenn sich Benutzer und Rollengruppen in dieser Domäne befinden, werden die Berechtigungen gespeichert.

Wenn globale Controlleradressen konfiguriert werden, fährt iDRAC6 mit der Abfrage des globalen Katalogs fort. Beim Abrufen zusätzlicher Berechtigungen vom globalen Katalog werden diese angesammelt.

Verschiedenes

Verwendet iDRAC6 immer LDAP-über-SSL?

Ja. Die Übertragungen laufen über den sicheren Anschluss 636 und/oder 3269 ab.

Während der Option *Einstellung testen* stellt iDRAC6 eine LDAP-VERBINDUNG nur her, um das Problem zu isolieren, jedoch baut er keine LDAP BIND an einer unsicheren Verbindung auf.

Unterstützt iDRAC6 den NetBIOS-Namen?

Nicht in dieser Version.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Anzeige der Konfiguration und des Zustands des verwalteten Servers

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 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 iDRAC6-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 iDRAC6-Webschnittstelle erhalten Sie die folgenden Informationen über die E/A-Mezzanine-Karten, die auf dem verwalteten Server installiert sind:

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

Integrierte Speicherkarte

Dieser Abschnitt der iDRAC6-Webschnittstelle bietet Informationen über die auf dem verwalteten Server installierte integrierte Speichercontrollerkarte:

- Kartentyp - zeigt den Modellnamen der installierten Speicherkarte

Automatische Wiederherstellung

In diesem Abschnitt der iDRAC6-Webschnittstelle wird der aktuelle Betriebsmodus der Funktion "Automatische Wiederherstellung" auf dem verwalteten Server, wie zuvor von Open Manage Server Administrator eingestellt, beschrieben:

- Wiederherstellungsmaßnahme - Die Maßnahme wird durchgeführt, wenn ein Systemfehler oder *Hängen des Systems* erkannt wird. Verfügbare Maßnahmen sind **Keine Maßnahme**, **Kaltstart**, **Herunterfahren** oder **Aus- und Einschalten**.
- Anfänglicher Countdown - Die Zeitdauer (in Sekunden) nachdem ein Hängen des Systems erkannt wurde, bis iDRAC6 eine Wiederherstellungsmaßnahme durchführt.
- Vorhandener Countdown - Der aktuelle Wert (in Sekunden) des Countdown-Zeitgebers.

Integrated Dell Remote Access Controller 6 - Enterprise

iDRAC6 Information

Dieser Abschnitt der iDRAC-Webschnittstelle enthält folgende grundlegende Informationen über iDRAC6 selbst:

- Datum/Uhrzeit - Das aktuelle Datum und die Uhrzeit (ab Aktualisierung der letzten Seite) von iDRAC6.
- Firmware-Version - Die aktuelle Version der auf dem verwalteten Server installierten iDRAC6-Firmware.
- Firmware aktualisiert - Das Datum und die Uhrzeit der letzten erfolgreichen Aktualisierung der iDRAC6-Firmware.
- Hardware-Version - Die Versionsnummer der der Platine des verwalteten Servers.
- IP-Adresse - Die mit dem iDRAC6 (nicht dem verwalteten Server) verbundene IP-Adresse.
- Gateway - Die IP-Adresse des für iDRAC6 konfigurierten Netzwerk-Gateways.
- Subnetzmaske - Die für iDRAC6 konfigurierte TCP/IP-Subnetzmaske.
- MAC-Adresse - Die MAC-Adresse, die mit dem LOM-NIC von iDRAC6 verbunden ist (LOM = LAN auf der Hauptplatine).
- DHCP aktiviert - Ist aktiviert, wenn iDRAC6 zum Abrufen seiner IP-Adresse und zugehöriger 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 iDRAC6 und die überwachten Komponenten zu erhalten. Die Spalte **Schweregrad** zeigt den Status jeder Komponente. Eine Liste von Zustandssymbolen und deren Bedeutung finden Sie unter Tabelle 17-3. 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.

iDRAC6

Die **iDRAC6-Informations**anzeige führt eine Reihe wichtiger Einzelheiten über den iDRAC6 auf, z. B. Funktionszustand, Name, Firmware, Revision und Netzwerkparameter. Zusätzliche Einzelheiten stehen zur Verfügung, wenn Sie oben auf der Anzeige auf das entsprechende Register klicken.

CMC

Die **CMC**-Anzeige zeigt den Funktionszustand, die Firmware-Version und die IP-Adresse des Gehäuseverwaltungscontrollers an. Durch Klicken auf die Schaltfläche **CMC-Webschnittstelle starten** kann die CMC-Webschnittstelle ebenfalls gestartet werden. Siehe *Benutzerhandbuch zur Chassis Management Controller-Firmware*.

Batterien

Die **Batterie**-Anzeige zeigt den Status und die Werte der Systemplatinen-Knopfzellenbatterie an, die die Echtzeituhr (RTC) und den Datenspeicher für die CMOS-Konfiguration auf dem verwalteten System mit Strom versorgt.

Temperaturen

Die **Informationsanzeige 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 **Informationsanzeige für Spannungssonden** zeigt den Status und Messwert der Spannungssonden an und liefert Informationen wie 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 Anzeige zur **Stromüberwachung** ermöglicht Ihnen, die folgenden Informationen zur Überwachungs- und Stromstatistik anzuzeigen:

- 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-Informationsanzeige** 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**-Anzeige zeigt den letzten POST-Code des Systems (hexadezimal) an, bevor das Betriebssystem des verwalteten Servers gestartet wird.

Sonstige Zustände

Die Anzeige **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

Stromüberwachung und Energieverwaltung

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

Dell™ PowerEdge™-Systeme umfassen viele neue und verbesserte Energieverwaltungsfunktionen. Bei dem Design der gesamten Plattform, angefangen bei der Hardware über die Firmware bis hin zur Systemverwaltungssoftware, standen Energieeffizienz, Überwachung und Energieverwaltung stets im Mittelpunkt.

PowerEdge-Systeme bieten viele Funktionen zur Überwachung und Verwaltung der Energie:

- **Stromüberwachung:** iDRAC6 erstellt einen Verlauf über Strommesswerte und errechnet ausführende Durchschnittswerte, Spitzenwerte usw. Mit der webbasierten iDRAC6-Schnittstelle können Sie die Daten auf der Seite **Stromüberwachung** einsehen. Durch Klicken auf **Grafik anzeigen** am Ende der Seite **Stromüberwachung** können Sie die Informationen auch als Grafik einsehen. Weitere Informationen finden Sie unter "Stromregelung".
- **Strombudgetierung:** Beim Einschalten ermöglicht eine Bestandsaufnahme des Systems, dass ein Budget des Systemstroms anhand der aktuellen Konfiguration berechnet wird. Weitere Informationen finden Sie unter Stromüberwachung".
- **Stromregelung:** Mit dem iDRAC6 können verschiedene Energieverwaltungsmaßnahmen auf dem verwalteten System per Remote-Funktion ausgeführt werden. Weitere Informationen finden Sie unter Stromregelung".

Konfiguration und Verwaltung der Energieeinstellungen

Sowohl die webbasierte iDRAC6-Schnittstelle als auch die RACADM-Befehlszeilenschnittstelle (CLI) ermöglichen die Verwaltung und Konfiguration von Stromregelungen auf dem PowerEdge-System. Genauer gesagt können Sie:

- den Stromstatus des Servers anzeigen. Siehe Stromüberwachung anzeigen".
- die Strombudgetinformationen für den Server, einschließlich der minimal möglichen und maximal möglichen Leistungsaufnahme, anzeigen. Siehe Strombudgets anzeigen".
- den Schwellenwert des Strombudgets für den Server anzeigen. Siehe Strombudgetschwellenwert anzeigen".
- den Stromsteuerungsvorgang auf dem Server (z. B. Einschalten, Ausschalten, Systemreset, Aus- und Einschalten) ausführen. Siehe Stromregelungsmaßnahmen am Server durchführen".

Stromüberwachung

iDRAC6 überwacht fortwährend die Leistungsaufnahme in PowerEdge-Servern. iDRAC6 berechnet die folgenden Stromwerte und liefert die Informationen über die webbasierte Schnittstelle oder RACADM-CLI:

- Gesamtstrom
- Durchschnitts-, Mindest- und Höchststrom
- Leistungsaufnahme (auch als Grafik auf der webbasierten Schnittstelle angezeigt)
- Schwellenwerte des Strombudgets

Stromüberwachung anzeigen

Webschnittstelle verwenden

Zum Einsehen der Stromüberwachungsdaten:

1. Melden Sie sich bei der iDRAC6-Webschnittstelle an.
2. Wählen Sie **Stromüberwachung** in der Systemstruktur aus.

   Die Seite **Stromüberwachung** erscheint mit folgenden Informationen:

Stromüberwachung

- **Status**: Ein **grünes Häkchen** zeigt einen normalen Stromstatus an, **Warnung** bedeutet, dass eine Warnungsmeldung ausgegeben wurde und **Schwerwiegend** bedeutet, dass eine Fehlerwarnung ausgegeben wurde.
- **Sondenname**: Systemebene der Systemplatine. Diese Beschreibung weist darauf hin, dass die Sonde anhand ihrer Position im System überwacht wird.

- **Messwert**: Die aktuelle Leistungsaufnahme in Watt.

Stromstärke

- **Position:** Derzeitiger Überwachungsstrom der Systemplatine
- **Messwert**: Die aktuelle Leistungsaufnahme in Ampere

Stromüberwachungsstatistik

- Statistik:
  - **Kumulative Systemleistung** zeigt die aktuelle kumulative Leistungsaufnahme (in kWh) für den Server an. Der Wert stellt die gesamte vom System verbrauchte Energie dar. Dieser Wert kann durch Klicken auf **Zurücksetzen** am Ende der Tabellenzeile auf 0 gestellt werden.
  - **Spitzenstrom des Systems** gibt den Spitzenwert des Systems in Watt innerhalb des Zeitraums an, der von der **Startzeit der Messung** und der **Aktuellen Messung** festgelegt wird. Dieser Wert kann durch Klicken auf **Zurücksetzen** am Ende der Tabellenzeile auf 0 gestellt werden.
  - **Spitzenstromstärke des Systems** gibt die Spitzenstromstärke des Systems in Watt innerhalb des Zeitraums an, der von der **Startzeit der Messung** und der **Aktuellen Messung** festgelegt wird. Dieser Wert kann durch Klicken auf **Zurücksetzen** am Ende der Tabellenzeile auf 0 gestellt werden.
- **Startzeit der Messung** zeigt das Datum und die gespeicherte Zeit an, zu der der Wert für den Systemenergieverbrauch zuletzt gelöscht wurde und der neue Messzyklus begann. Für die Statistik von **Kumulativer Systemleistung**, **Spitzenstromstärke des Systems** und **Spitzenstrom des Systems** kann jeder Wert durch Klicken auf **Rücksetzen** am Ende der Tabellenzeile auf 0 zurückgesetzt werden. Dieser bleibt jedoch bei einem Zurücksetzen des Systems oder im CMC-Failover-Betrieb erhalten.
- **Aktuelle Messung** für **Kumulative Systemleistung** zeigt das aktuelle Datum und die Uhrzeit an, zu der die Leistungsaufnahme des Systems für die Anzeige berechnet wurde. Für **Spitzenstromstärke des Systems und Spitzenstrom des Systems** zeigen die Felder **Spitzenzeit** die Zeit an, zu der die Spitzenwerte auftraten.
- **Messwert**: Die Strommenge (in kWh), die seit dem Start des Zählers verbraucht wurde.

ANMERKUNG: Stromverfolgungsstatistiken werden trotz Systemrücksetzung erhalten und geben somit sämtliche Aktivitäten in der Zeitspanne zwischen den angegebenen Start- und Endzeiten an. Die Taste **Max. Spitzenwerte zurücksetzen** dient zum Zurücksetzen auf statistische Spitzenwerte. In der nächsten Tabelle werden die Stromverbrauchsdaten nicht beim Zurücksetzen des Systems beibehalten, sondern auf Spitzenstatistikwerte zurückgesetzt. Die angezeigten Leistungswerte stellen kumulative Durchschnittswerte über den jeweiligen Zeitraum hinweg dar (vorhergehende Minute, Stunde, Tag und Woche). Da sich die Zeiträume von Start bis Ende hier von den Stromverfolgungsstatistiken unterscheiden können, kann es zu unterschiedlichen Spitzenstromwerten kommen (Max. Spitzenstrom in Watt im Vergleich zu Max. Leistungsaufnahme).

Leistungsaufnahme

- **Durchschnittliche Leistungsaufnahme**: Der Durchschnitt der vorhergehenden Minute, vorhergehenden Stunde, des vorhergehenden Tags und der vorhergehenden Woche.
- **Max. Leistungsaufnahme** und **Min. Leistungsaufnahme**: Die höchste und geringste Leistungsaufnahme, die im gegebenen Zeitraum beobachtet wurden.
- **Max. Stromzeit** und **Min. Stromzeit**: Die Zeiten (in Minuten, Stunden, Tagen und Wochen), zu denen die höchste und geringste Leistungsaufnahme erfolgte.

Grafik anzeigen

Klicken Sie auf **Grafik anzeigen**, um die Leistungsaufnahme des iDRAC6 der letzten Stunde, der letzten 24 Stunden, der letzten drei Tage und der letzten Woche in Watt darzustellen. Verwenden Sie das Drop-Down-Menü über der Grafik zur Auswahl des Zeitraums.

ANMERKUNG: Jeder verzeichnete Datenpunkt in der Grafik stellt den Durchschnitt der über 5 Minuten hinweg gemessenen Werte dar. Folglich können die Grafiken keine momentanen Schwankungen der Leistungs- oder Stromaufnahme wiedergeben.

Strombudgetierung

iDRAC6 kann so konfiguriert werden, dass die minimalen und maximalen vom CMC eingestellten Stromgrenzwerte für die derzeitige Systemkonfiguration erzwungen werden. Auf der Seite **Strombudget** erscheinen diese Stromschwellenwerte, die den Bereich der Netzstrom-Leistungsaufnahmen decken, die ein begrenztes System bei starker Auslastung für das Datenzentrum darstellen. Diese Grenzwerte sind nicht konfigurierbar.

Strombudgets anzeigen

Der Server bietet auf der Seite **Strombudgetinformationen** einen Überblick über den Strombudgetstatus des Stromsubsystems.

Webschnittstelle verwenden

ANMERKUNG: Zur Ausführung von Energieverwaltungsaufgaben müssen Sie über **Administrationsrechte** verfügen.

1. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
2. Wählen Sie in der Systemstruktur **System** aus**.**
3. Klicken Sie auf die Registerkarte **Energieverwaltung** und dann auf **Strombudget**.

   Die Seite **Strombudget-Information** wird angezeigt.

Die Tabelle **Strombudgetinformationen** zeigt die minimalen und maximalen Stromschwellenwerte für die aktuelle Systemkonfiguration an. Diese decken den Bereich des Netzstromverbrauchs, die ein begrenztes System bei starker Auslastung für ein Datenzentrum darstellen.

- **Minimal mögliche Leistungsaufnahme** stellt den kleinsten Strombudgetschwellenwert dar.
- **Maximal mögliche Leistungsaufnahme** stellt den größten Strombudgetschwellenwert dar. Dieser Wert ist zugleich der absolute Höchstwert für die Leistungsaufnahme des aktuellen Systems.

RACADM verwenden

Öffnen Sie eine Befehlszeile auf einem verwalteten Knoten und geben Sie Folgendes ein:

```
racadm getconfig -g cfgServerPower
```

ANMERKUNG: Weitere Informationen über sfgServerPower, einschließlich Ausgabedetails, finden Sie unter "cfgServerPower".

Strombudgetschwellenwert anzeigen

Der Strombudgetschwellenwert erzwingt, sofern aktiviert, Stromschwellenwerte für das System. Die Systemleistung wird dynamisch angepasst, um die Leistungsaufnahme nahe dem spezifischen Schwellenwert zu behalten.

ANMERKUNG: Der Strombudgetschwellenwert ist schreibgeschützt und kann im iDRAC6 nicht aktiviert oder konfiguriert werden.

Die tatsächliche Leistungsaufnahme kann bei schwacher Auslastung niedriger sein und momentan den Schwellenwert übersteigen, bis die Leistungsanpassung erfolgt ist.

Verwendung der webbasierten Schnittstelle

1. Melden Sie sich an der webbasierten iDRAC6-Schnittstelle an.
2. Wählen Sie in der Systemstruktur **System** aus**.**
3. Klicken Sie auf die Registerkarte **Energieverwaltung** und dann auf **Strombudget**.

   Die Seite **Strombudgetinformationen** wird angezeigt.
4. Klicken Sie auf **Strombudgetschwellenwert**

Die Tabelle **Strombudgetschwellenwert** zeigt Informationen zu den Stromgrenzwerten für das System an:

- **Aktiviert** zeigt an, ob das System den Strombudgetschwellenwert erzwingt.
- **Schwellenwert in Watt** und **Schwellenwert in BTU/h** zeigen jeweils die Grenzwerte in Watt und BTU/h an.
- **Schwellenwertprozentsatz** zeigt den Prozentsatz des Strombereichs an.

RACADM verwenden

Öffnen Sie eine Befehlszeile auf einem verwalteten Knoten und geben Sie Folgendes ein:

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts <power cap value in Watts>

racadm getconfig -g cfgServerPower -o cfgServerPowerCapBTUhr <hr>

racadm getconfig -g cfgServerPower -o cfgServerPowerCapPercent <power cap value in %>
```

ANMERKUNG: Weitere Informationen über sfgServerPower, einschließlich Ausgabedetails, finden Sie unter "cfgServerPower".

Stromregelung

Mit dem iDRAC6 können folgende Funktionen im Remote-Zugriff ausgeführt werden: Einschalten, Zurücksetzen, ordentliches Herunterfahren, nicht-maskierbarer Interrupt (NMI) oder Aus-/Einschalten. Verwenden Sie die Seite **Stromregelung,** um während eines Neustarts und beim Ein- und Ausschalten des

Systems ein ordentliches Herunterfahren durch das Betriebssystem durchzuführen.

Stromregelungsmaßnahmen am Server durchführen

ANMERKUNG: Um Energieverwaltungsmaßnahmen durchführen zu können, müssen Sie über **Administratorrechte für die Gehäusesteuerung** verfügen.

Mit dem iDRAC6 können folgende Funktionen im Remote-Zugriff ausgeführt werden: Einschalten, Zurücksetzen, ordentliches Herunterfahren, nicht-maskierbarer Interrupt (NMI) oder Aus-/Einschalten.

Webschnittstelle verwenden

1. Melden Sie sich bei der iDRAC6-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **System** aus.
3. Klicken Sie auf die Registerkarte **Power Management** (Energieverwaltung).

   Die Seite **Stromregelung** erscheint.
4. Wählen Sie eine der folgenden **Stromregelungsmaßnahmen** aus, indem Sie auf die entsprechende Optionsschaltfläche klicken:
   - **System einschalten** schaltet den Server ein (entspricht dem Drücken des Netzschalters, wenn der Serverstrom ausgeschaltet ist). Diese Option ist deaktiviert, wenn das System bereits eingeschaltet ist.
   - **System ausschalten** schaltet den Server aus. Diese Option ist deaktiviert, wenn das System bereits heruntergefahren wurde.
   - **NMI (nicht-maskierbarer Interrupt)** erzeugt einen NMI, um den Betrieb des Systems anzuhalten. Ein NMI 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. Für Ordentliches Herunterfahren ist ein ACPI-abhängiges Betriebssystem (Advanced Configuration and Power Interface) erforderlich, das systemgesteuerte Energieverwaltung ermöglicht.
   - **System zurücksetzen (Softwareneustart)** startet das System neu, ohne es auszuschalten. Diese Option ist deaktiviert, wenn das System bereits heruntergefahren wurde.
   - **System aus- und einschalten**(**Hardwareneustart)** schaltet das System aus und dann wieder ein. Diese Option ist deaktiviert, wenn das System bereits heruntergefahren wurde.
5. Klicken Sie auf **Anwenden**.

   Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
6. Klicken Sie auf **OK**, um die gewählte Energieverwaltungsmaßnahme auszuführen.

RACADM verwenden

Öffnen Sie erst einen verwalteten Knoten, dann eine Textkonsole der Befehlszeilenschnittstelle für den Server, melden Sie sich an und geben Sie Folgendes ein:

```
racadm serveraction <Maßnahme>
```

wobei `<Maßnahme>` `powerup`, `powerdown`, `powercycle`, `hardreset` oder `powerstatus` ist.

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Seriell über LAN konfigurieren und verwenden

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 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 bandexterne Ethernet-Verwaltungsnetzwerk des iDRAC 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. Vorteile von SOL:

- 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 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. iDRAC6 für Seriell über LAN konfigurieren
3. Eine Methode zum Initialisieren von Seriell über LAN auswählen (SSH, Telnet, SOL Proxy oder IPMI-Hilfsprogramm)
4. Das BS 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 iDRAC6-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 9-1. Seriell über LAN-Konfigurationseinstellungen

Einstellung	Beschreibung
Seriell über LAN aktivieren	Ein markiertes Kontrollkästchen bedeutet, 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 9-2. Seriell über LAN-Konfigurationsschaltflächen

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 beim Betrachten 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 9-3. Seriell über LAN-Konfiguration auf der Seite Erweiterte Einstellungen

Einstellung	Beschreibung
?Intervall der Zeichenakkumulation	Die typische Zeitspanne, die der iDRAC6 abwartet, bevor ein SOL-Datenpaket teilweise gesendet wird. 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 iDRAC6 akzeptierten Zeichen gleich oder größer dem Schwellenwert für gesendete Zeichen ist, beginnt der iDRAC6, 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. Dies führt zu einer bedeutend herabgesetzten Leistung.

Tabelle 9-4. 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 **Seriell 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 das SSH- oder 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 einem Remote-System.

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

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 bandexterne iDRAC6-Schnittstelle (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 iDRAC6 in die Konsole Ihrer Management Station umzuleiten.

Modell zum Umleiten von SOL über Telnet oder SSH

Telnet (Anschluss 23)/ SSH (Anschluss 22) Client←→WAN-Anschluss←→iDRAC6-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/soll** aus gestartet werden.

Weitere 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 (Anschluss 623) ←→WAN-Anschluss ←→SOL Proxy ←→iDRAC6-Server

Wenn der SOL Proxy mit dem Telnet-Client auf einer Management Station kommuniziert, verwendet er das TCP/IP-Protokoll. Der SOL Proxy kommuniziert jedoch mit dem iDRAC6 des verwalteten Servers über das RMCP/IPMI/SOL-Protokoll, das ein UDP-basiertes Protokoll ist. Wenn Sie daher mit dem iDRAC6 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 iDRAC6-Server auf demselben LAN befinden. Die Management Station mit dem Telnet-Client kann dann über einen WAN-Anschluss eine Verbindung zum SOL Proxy herstellen. In diesem Verwendungsmodell wird der SOL Proxy wie gewünscht funktionieren.

Modell zum Umleiten von SOL über IMPItool

IPMItool ←→WAN-Anschluss ←→iDRAC6-Server

Das IPMI-basierte SOL-Dienstprogramm, IPMItool, verwendet das Protokoll RMCP+, das unter Verwendung von UDP-Datengrammen an Schnittstelle 623 geliefert wird. iDRAC6 erfordert, dass diese RMCP+-Verbindung verschlüsselt ist. Der Verschlüsselungsschlüssel (KG-Schlüssel) muss Nullzeichen oder NULL enthalten, die in der iDRAC6-Web-GUI oder im iDRAC6-Konfigurationsdienstprogramm konfiguriert werden können. Sie haben auch die Möglichkeit, den Verschlüsselungsschlüssel zu löschen, indem Sie die Rücktaste drücken, sodass der iDRAC6 als Verschlüsselungsschlüssel standardmäßig NULL-Zeichen ausgibt. 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 finden Sie unter "SOL über IPMItool verwenden" oder auf der IPMItool-Website: **http://ipmitool.sourceforge.net/manpage.html**.

SOL-Sitzung in SM-CLP abbrechen

Bei Verwendung eines SSH- oder Telnet-Protokolls zum Zugriff auf die Seriell über LAN-Funktion, stellen Sie zuerst eine Verbindung zum SM-CLP-Dienst des iDRAC her, von der Sie die SOL-Sitzung mit einem SM-CLP-Befehl (`start /system1/sol1`) starten können. 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. Lesen Sie diesen Abschnitt genau durch. Erst wenn die SOL-Sitzung vollständig beendet ist, können Sie das Dienstprogramm verlassen.

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 Management Station von Windows 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 mit folgendem Befehl in der Befehlseingabeaufforderung eine Verbindung zum iDRAC6 her:

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

   ANMERKUNG: Die Nummer des Anschlusses ist optional. Sie ist nur dann erforderlich, wenn die Anschlussnummer neu zugeordnet wird.

2. 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 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 iDRAC6 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 Kennwort ein, um eine Verbindung zu SM-CLP des iDRAC6 herzustellen.
4. Geben Sie an der SM-CLP-Eingabeaufforderung den folgenden Befehl ein um SOL zu starten:

   ```
   start /system1/sol1
   ```

5. Um eine SOL-Sitzung von Telnet auf Linux zu beenden, drücken Sie <Strg>+] (halten Sie die Strg-Taste gedrückt, drücken Sie die Taste für die rechte eckige Klammer und lassen sie los). 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 iDRAC6 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 (siehe "SOL-Sitzung in SM-

CLP abbrechen" zum Schließen einer aktiven SOL-Sitzung) und eine neue Sitzung starten, um SM-CLP verwenden zu können.

SOL über IPMItool verwenden

Die DVD *Dell Systems Management Tools and Documentation* enthält IPMItool, 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** unter **System→ Remote-Zugriff→ iDRAC→ Netzwerk/Sicherheit→ Netzwerk→ IPMI- LAN-Einstellungen** nur aus Nullen besteht.

3. Geben Sie bei der Windows-Eingabeaufforderung oder bei 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 ein, um iDRAC neu zu starten. Geben Sie iDRAC6 1-2 Minuten Zeit, um den Start auszuführen. Weitere Informationen finden Sie unter "Übersicht der RACADM-Unterbefehle".

   ```
   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-Befehl telnet, der von einer MS-DOS ®-Eingabeaufforderung ausgeführt wird, unterstützt ANSI-Terminalemulation. Das BIOS muss auf ANSI-Emulation eingestellt sein, um alle Bildschirme richtig anzuzeigen.

Vor der Verwendung des SOL Proxy

Bevor Sie den SOL Proxy verwenden, lesen Sie bitte im *Benutzerhandbuch zu den Dienstprogrammen des Baseboard-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/ipmish

SOL Proxy-Sitzung einleiten

Für Windows 2003

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

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

   Das Fenster **Computerverwaltung** wird angezeigt.

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

   Verfügbare Dienste werden rechts angezeigt.

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

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

Für Linux

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

```
solproxy status

dsm_bmu_solproxy32d start

dsm_bmu_solproxy32d stop

solproxy restart
```

Telnet mit SOL Proxy verwenden

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

Für Windows 2003:

1. Öffnen Sie ein Eingabeaufforderungsfenster auf Ihrer Management Station.

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

   ```
   telnet localhost 623
   ```

Für Linux:

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

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

   ```
   telnet localhost 623
   ```

   ANMERKUNG: Egal, ob das Hostbetriebssystem Windows oder Linux ist, geben Sie statt localhost die IP-Adresse des SOL Proxy-Servers ein, 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 gestellt:

1. Connect to the Remote Server's BMC (1. Eine Verbindung zum BMC des Remote-Servers herstellen)
2. Configure the Serial-Over-LAN for the Remote Server (2. Seriell über LAN für den Remote-Server konfigurieren)
3. Activate Console Redirection (3. Konsolenumleitung aktivieren)
4. Reboot and Activate Console Redirection (4. 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: Verwenden Sie zum Beenden einer aktiven SOL-Sitzung die Zeichenfolge <~><.> Mit dieser Folge wird SOL beendet und das Hauptmenü 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 iDRAC6-**Benutzernamen** und das **Kennwort** für iDRAC6 auf dem verwalteten System an. Der iDRAC6-Benutzername und das Kennwort müssen im nicht-flüchtigen Speicher des iDRAC6 zugewiesen und gespeichert werden.

   ANMERKUNG: Es ist nur eine SOL-Konsolenumleitungssitzung mit iDRAC6 auf einmal zulässig.

   ANMERKUNG: Falls erforderlich, können Sie die SOL-Sitzungsdauer auf unendlich erweitern, indem Sie den **Telnet-Zeitüberschreitung**swert auf der iDRAC6-Web-GUI-Seite unter **System**→ **Remote-Zugriff**→ **iDRAC**→ **Netzwerk/Sicherheit**→ **Dienste** auf Null ändern.

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

   ANMERKUNG: Sie können den IPMI-Verschlüsselungsschlüssel in der iDRAC6-GUI unter **System**→ **Remote-Zugriff**→**iDRAC**→**Netzwerk/Sicherheit**→**Netzwerk**→**IPMI-LAN-Einstellungen**→ **Verschlüsselungsschlüssel** ausfindig machen.

   ANMERKUNG: Der standardmäßige IPMI-Verschlüsselungsschlüssel besteht ausschließlich aus Nullen. Wenn Sie für die Verschlüsselungsoption die Eingabetaste drücken, wird iDRAC6 diesen standardmäßigen Verschlüsselungsschlüssel verwenden.

5. Wählen Sie **Seriell über LAN für den Remote Server konfigurieren** (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 Ihnen stehen drei Möglichkeiten zur Auswahl:

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

   - Wenn SOL aktiviert ist, stellen Sie sicher, dass die SOL-Baudrate mit dem von iDRAC übereinstimmt und dass die unterste iDRAC6-Berechtigungsebene des **Administrators** zur Aktivierung der Konsolenumleitung erforderlich ist.
   - Wenn SOL gegenwärtig deaktiviert ist, geben Sie Y ein, um SOL zu aktivieren, oder N, um SOL deaktiviert zu lassen.

- Wählen Sie **Konsolenumleitung aktivieren** (Option 3) im Hauptmenü aus.

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

7. Wählen Sie **Neustart und Konsolenumleitung aktivieren** (Option 4) im Hauptmenü aus.

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

8. Wählen Sie im Hauptmenü **Hilfe** (Option 5) aus, um eine detaillierte Beschreibung der einzelnen Optionen anzuzeigen.

9. Wählen Sie im Hauptmenü **Beenden** (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. Geben Sie iDRAC6 1-2 Minuten Zeit, um den Start auszuführen. Weitere Einzelheiten stehen unter "Übersicht der 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` section.

   ```
   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.

# (Diese Dateibeschreibt, wie das INIT-Verfahren das System auf

# einer bestimmten Ausführungsstufe einrichten sollte.)

#


SKIP this part of file (Diesen Teil der Datei ÜBERSPRINGEN)


# Run gettys in standard runlevels (# gettys in Standard-Ausführungsstufen ausführen)

1:2345:respawn:/sbin/migetty tty1

2:2345:respawn:/sbin/migetty tty1

3:2345:respawn:/sbin/migetty tty1

4:2345:respawn:/sbin/migetty tty1

5:2345:respawn:/sbin/migetty tty1

6:2345:respawn:/sbin/migetty tty1


# Run xdm in runlevel 5 (# xdm in Ausführungsstufe 5 ausführen)

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.

# (Diese Dateibeschreibt, wie das INIT-Verfahren das System auf

# einer bestimmten Ausführungsstufe einrichten sollte.)

#
```

```
SKIP this part of file (Diesen Teil der Datei ÜBERSPRINGEN)

# Run gettys in standard runlevels (# gettys in Standard-Ausführungsstufen ausführen)
1:2345:respawn:/sbin/migetty tty1
2:2345:respawn:/sbin/migetty tty1
3:2345:respawn:/sbin/migetty tty1
4:2345:respawn:/sbin/migetty tty1
5:2345:respawn:/sbin/migetty tty1
6:2345:respawn:/sbin/migetty tty1
7:2345:respawn:/sbin/agetty -h ttyS0 115200 vt220

# Run xdm in runlevel 5 (# xdm in Ausführungsstufe 5 ausführen)
x:5:respawn:/etc/X11/prefdm -nodaemon
```

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

   ```
   ttyS0
   ```

Beispiel von originalem /etc/securetty:

```
console (Konsole)
vc/1
vc/2
vc/3
vc/4

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

Beispiel von modifiziertem /etc/securetty:

```
console (Konsole)
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 Original /boot/grub/grub.conf in RHEL 5:

```
# grub.conf generated by anaconda (grub.conf erstellt durch anaconda)

#

# Note that you do not have to return grub after making changes

to this (Beachten Sie, dass grub nicht zurückgegeben werden muss, nachdem Sie Änderungen an dieser)

# file (Datei vorgenommen haben)

# NOTICE: You have a /boot partition. This means that all kernel and initrd paths are relative to /boot/,eg.(Sie haben
eine /Startpartition. Dies bedeutet, dass alle Kernel- und initrd-Pfade im Verhältnis zu /boot/ stehen, z. B.)

#

# root (hd0,0)

# kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00

# initrd /initrd-version.img

#boot=/dev/sda

default=0

timeout=5

splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu


title Red Hat Enterprise Linux 5

     root (hd0,0)

     kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet

     initrd /initrd-2.6.18-8.el5.img
```

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

```
# grub.conf generated by anaconda (grub.conf erstellt durch anaconda)

#

# Note that you do not have to return grub after making changes

to this (Beachten Sie, dass grub nicht zurückgegeben werden muss, nachdem Sie Änderungen an dieser)

# file (Datei vorgenommen haben)

# NOTICE: You have a /boot partition. This means that all kernel and initrd paths are relative to /boot/,eg.(Sie haben
eine /Startpartition. Dies bedeutet, dass alle Kernel- und initrd-Pfade im Verhältnis zu /boot/ stehen, z. B.)

#

# root (hd0,0)

# kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00

# initrd /initrd-version.img

#boot=/dev/sda
```

```
default=0

timeout=5

#splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu


# Redirect the OS boot via SOL (# BS-Start über SOL umleiten)

title Red Hat Enterprise Linux 5 SOL redirection (SOL-Umleitung)

     root (hd0,0)

     kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet console=tty1 console=ttyS0,115200

     initrd /initrd-2.6.18-8.el5.img
```

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

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

Default 0

Timeout 8

gfxmenu (hd0.5)/boot/message


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

title SUSE Linux Enterprise Server 10 SP1

     root (hd0,5)

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

     initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

Beispiel von 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 bei der Windows- Eingabeaufforderung bootcfg eingeben. Suchen Sie die Starteintrags- ID für den Abschnitt mit dem BS-freundlichen Namen **Windows Server 2003 Enterprise**. Drücken Sie die Eingabetaste, um die Startoptionen auf der Management Station anzuzeigen.

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

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

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

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

Beispiel von Original 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

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

Dieser Abschnitt enthält Informationen über die Verwendung der iDRAC6-Konsolenumleitungsfunktion.

Übersicht

Mit der Konsolenumleitungsfunktion des iDRAC6 ist Fernzugriff auf lokale Konsolen im Grafik- oder Textmodus möglich, was die Steuerung eines oder mehrerer iDRAC6-aktivierter Systeme von einer einzigen Position aus ermöglicht.

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 10-1 listet die unterstützten Bildschirmauflösungen und entsprechenden Bildwiederholfrequenzen für eine Konsolenumleitungssitzung auf, die auf dem verwalteten Server ausgeführt wird.

Tabelle 10-1. Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

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

Konfiguration der Verwaltungsstation

Zur Verwendung der Konsolenumleitung auf der Management Station gehen Sie wie folgt vor:

1. Installieren und konfigurieren Sie einen unterstützten Internet-Browser. Siehe Unterstützte Webbrowser" und 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. Dell empfiehlt, dass Sie die Auflösung Ihres Monitors auf 1280x1024 Pixel einstellen.

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 umgeschaltet.

Konsolenumleitung und Virtuellen Datenträger in der iDRAC6-Webschnittstelle konfigurieren

Um auf der iDRAC6-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 10-2 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 10-3.

Tabelle 10-2. Konfigurationseigenschaften der Konsolenumleitung

Eigenschaft	Beschreibung
Enabled	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 Sessions	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.**
Active Sessions	Zeigt die Anzahl der Sitzungen Aktiver Konsolen an. Dieses Feld ist schreibgeschützt.
Keyboard and Mouse Port Number	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.**
Video Port Number	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.**
Video Encryption Enabled	**Markiert** zeigt an, dass die Videoverschlüsselung aktiviert ist. Aller 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.**
Mouse Mode	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 Zugang**, wenn der Server weder auf einem Windows- noch auf einem Linux-Betriebssystem ausgeführt wird. **ANMERKUNG:** Wählen Sie **Kein Mauszugangsmodus** in HyperV, Dell Diagnostics oder USC. Die Standardeinstellung ist **Windows**.
Console Plug-In Type for 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.

Local Server Video Enabled	**Markiert** weist darauf hin, dass die Ausgabe an den iKVM-Monitor während der Konsolenumleitung deaktiviert ist. **Nicht markiert** stellt sicher, 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 siehe "Virtuellen Datenträger konfigurieren und verwenden".

Die Schaltflächen in Tabelle 10-5sind auf der Seite **Konsolenumleitungskonfiguration** verfügbar.

Tabelle 10-3. Schaltflächen zur 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.

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 10-4, um sicherzustellen, dass eine Konsolenumleitungssitzung verfügbar ist.

   Sollten Sie einige der angezeigten Eigenschaftswerte neu konfigurieren wollen, finden Sie entsprechende Informationen unter "Konsolenumleitung und Virtuellen Datenträger in der iDRAC6-Webschnittstelle konfigurieren".

Tabelle 10-4. Informationen zur Konsolenumleitung

Eigenschaft	Beschreibung
Console Redirection Enabled	Ja/Nein
Video Encryption Enabled	Ja/Nein
Max Sessions	Zeigt die maximale Anzahl unterstützter Konsolenumleitungssitzungen an
Current Sessions	Zeigt die aktuelle Anzahl aktiver Konsolenumleitungssitzungen an
Mouse Mode	Zeigt die aktuell geltende Mausbeschleunigung an. Der Modus **Mausbeschleunigung** sollte auf der Grundlage des auf dem verwalteten Server installierten Betriebssystems ausgewählt werden.
Console Plug-in Type	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 iDRAC6 zugreifen, können Sie entweder Active-X oder Java als Plugin-Typ auswählen.
Local Server Video Enabled	Markiert weist darauf hin, dass die Ausgabe an den iKVM-Monitor während der Konsolenumleitung deaktiviert ist. Unmarkiert stellt sicher, 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 siehe "Virtuellen Datenträger konfigurieren und verwenden".

Die Schaltflächen in Tabelle 10-5sind auf der Seite **Konsolenumleitungskonfiguration** verfügbar.

Tabelle 10-5. Schaltflächen zur Konsolenumleitungskonfiguration

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 Management Station wird mit dem iDRAC6 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 10-6 beschreibt die Menüoptionen, die im Viewer zum Gebrauch verfügbar sind.

Tabelle 10-6. Auswahlmöglichkeiten auf der Viewer-Menüleiste

Menüelement	Element	Beschreibung
Grafik	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	Synchronisiert den Cursor, damit die Maus auf dem Client zur Maus auf dem Server umgeleitet wird.
	Lokalen Cursor ausblenden	Es wird nur der Cursor vom KVM angezeigt. Dell empfiehlt diese Einstellung, wenn USC in einem vKVM ausgeführt 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 Enterprise oder Novell SUSE Linux sicher, dass der Mausmodus für Linux konfiguriert ist, bevor Sie den Viewer starten. Hilfe bei der Konfiguration steht unter "Konsolenumleitung und Virtuellen Datenträger in der iDRAC6-Webschnittstelle konfigurieren" zur Verfügung. Die Standardmauseinstellungen des Betriebssystems werden zur Steuerung des Mauspfeils auf dem Seite iDRAC6-**Konsolenumleitung** verwendet.

Lokale Konsole deaktivieren oder aktivieren

Sie können den iDRAC6 so konfigurieren, dass iKVM-Verbindungen über die iDRAC6-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 iDRAC6 gesperrt ist. Wenn die lokale Konsole aktiviert ist, ist der Statuspunkt grün.

Wenn Sie sicherstellen möchten, dass Sie exklusiven Zugriff auf die Konsole des verwalteten Servers haben, müssen Sie die lokale Konsole deaktivieren *und* die **Max. Sitzungen** auf der **Seite** Konsolenumleitung auf 1 *einstellen*.

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 Management Station einen unterstützten Webbrowser, und melden Sie sich am iDRAC6 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 Sie das lokale Video auf dem Server deaktivieren (ausschalten) möchten, heben Sie auf der Seite **Konsolenumleitungskonfiguration** die Markierung des Kontrollkästchens **Lokales Servervideo aktiviert** auf und klicken dann auf **Änderungen übernehmen**. Die Standardeinstellung ist **Aktiviert (markiert)**.
4. Wenn Sie auf dem Server das lokale Video aktivieren (einschalten) möchten, wählen Sie auf der Seite **Konsolenumleitungskonfiguration** das Kontrollkästchen **Lokales Servervideo aktiviert** aus und klicken dann auf **Änderungen übernehmen**.

Die Anzeige **Konsolenumleitung** zeigt den Status des lokalen Servervideos an.

Häufig gestellte Fragen

Tabelle 10-7 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 10-7. Konsolenumleitung verwenden: Häufig gestellte Fragen

Frage	Antwort
Kann eine neue Remote-Konsolen-Videositzung gestartet werden, wenn das lokale Video auf dem Server ausgeschaltet	Ja.

ist?	
Warum dauert es 15 Sekunden, um das lokale Video auf dem Server auszuschalten, nachdem eine Aufforderung zum Ausschalten des lokalen Vidoes erteilt wurde?	Hierdurch wird einem lokalen Benutzer die Gelegenheit gegeben, Maßnahmen durchzuführen, bevor das Video ausgeschaltet wird.
Gibt es beim Einschalten des lokalen Videos eine Zeitverzögerung?	Nein. Sobald der iDRAC6 eine Aufforderung zum **EIN**schalten des lokalen Videos erhält, wird das Video sofort eingeschaltet.
Kann der lokale Benutzer das Video auch ausschalten?	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 iDRAC6-Benutzer erforderlich, um das lokale Server-Video ein- oder auszuschalten?	Jeder Benutzer mit iDRAC6-Konfigurationsberechtigungen kann die lokale Konsole ein- oder ausschalten.
Wie kann ich den aktuellen Status des lokalen Servervideos abrufen?	Der Status wird auf der Seite **Konsolenumleitungskonfiguration** der iDRAC6-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 iDRAC6 gesperrt ist.
Ich kann vom Konsolenumleitungsfenster aus den unteren Teil des Systembildschirms nicht sehen.	Stellen Sie sicher, dass die Bildschirmauflösung der Management Station auf 1280 x 1024 eingestellt ist.
Das Konsolenfenster ist entstellt.	Für den Konsolen-Viewer auf Linux ist ein UTF-8-Zeichensatz erforderlich. Überprüfen Sie Ihr Gebietsschema und setzen Sie den Zeichensatz ggf. zurück. Weitere Informationen finden Sie unter "Gebietsschema in Linux einstellen".
Warum wird auf dem verwalteten Server ein leerer Bildschirm eingeblendet, wenn das Windows 2000-Betriebssystem lädt?	Auf dem verwalteten Server befindet sich nicht der richtige ATI-Videotreiber. Es ist erforderlich, den Videotreiber unter Verwendung der CD *Dell PowerEdge Installation and Server Management* zu aktualisieren.
Warum synchronisiert die Maus nicht in DOS, wenn die Konsolenumleitung ausgeführt wird?	Das Dell-BIOS emuliert den Maustreiber als PS/2-Maus. Die PS/2-Maus ist so konzipiert, dass sie die Relativposition für den Mauszeiger verwendet, was die Verzögerung in der Synchronisation verursacht. Der iDRAC6 enthält einen USB-Maustreiber, der eine absolute Position und ein genaueres Verfolgen des Mauszeigers ermöglicht. Selbst wenn der iDRAC6 die absolute USB-Mausposition auf das Dell-BIOS überträgt, 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 **Kein Zugang** 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 ein Microsoft®-Betriebssystem mithilfe einer iDRAC6-Konsolenumleitung im Remote-Zugriff installiere?	Wenn Sie im Remote-Zugriff auf ein unterstütztes Microsoft-Betriebssystem auf einem System auf dem die Konsolenumleitung im BIOS aktiviert ist, installieren, erhalten Sie eine EMS-Verbindungsmeldung, die verlangt, dass Sie **OK** wählen, bevor Sie fortfahren können. Sie können nicht die Maus verwenden, um **OK** im Remote-Zugriff auszuwählen. Sie müssen entweder auf dem lokalen System **OK** auswählen, oder den im Remote-Zugriff verwalteten Server neu starten und neu installieren und dann die Konsolenumleitung im BIOS ausschalten. Diese Nachricht wird durch Microsoft erstellt, um den Benutzer darauf hinzuweisen, dass die Konsolenumleitung aktiviert ist. Um sicherzustellen, dass diese Meldung nicht eingeblendet wird, schalten Sie die Konsolenumleitung im BIOS immer aus, bevor Sie ein Betriebssystem im Remote-Zugriff installieren.
Warum zeigt die Num-Tasten-Anzeige auf meiner Management Station nicht den Status der Num-Taste auf dem Remote-Server an?	Wenn über den iDRAC6 auf die Num-Taste zugegriffen wird, stimmt die Num-Taste auf der Management Station nicht unbedingt mit dem Zustand der Num-Taste auf dem Remote-Server überein. Der Zustand der Num-Taste hängt von der Einstellung auf dem Remote-Server ab, wenn die Remote-Sitzung verbunden wird, unabhängig vom Zustand der Num-Taste auf der Management Station.
Warum werden mehrere Session Viewer-Fenster eingeblendet, wenn ich vom lokalen Host aus eine Konsolenumleitungssitzung aufbaue?	Eine Konsolenumleitungssitzung wird vom lokalen System aus konfiguriert. Dies wird nicht unterstützt.
Erhalte ich eine Warnungsmeldung, wenn ich eine Konsolenumleitungssitzung ausführe und ein lokaler Benutzer auf den verwalteten Server zugreift?	Nein. Wenn ein lokaler Benutzer auf das System zugreift, haben 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

Eine VFlash-Medienkarte zur Verwendung mit iDRAC6 konfigurieren

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

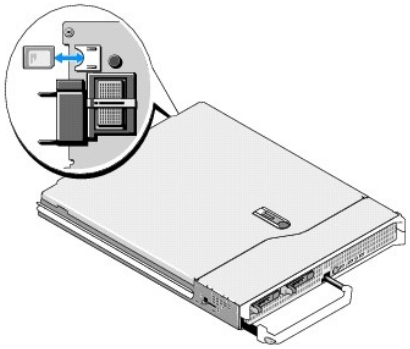
Die VFlash-Medienkarte ist eine SD-Karte (Secure Digital), die an der optionalen iDRAC6-Enterprise-Karte in der hinteren Ecke des Systems eingesetzt wird. Sie bietet Speicherplatz, der sich wie ein herkömmlicher USB-Speicherstick verhält.

Installieren einer VFlash-Medienkarte

ANMERKUNG: Für die vFlash-Medien von Dell ist die virtuelle Flash-Partition erforderlich.

1. Entfernen Sie das Blade aus dem Gehäuse.
2. Lokalisieren Sie den VFlash-Mediensteckplatz in der hinteren Ecke des Systems.

   ANMERKUNG: Sie müssen die Blade-Abdeckung nicht entfernen, um die Karte zu installieren oder herauszunehmen.



3. Führen Sie das SD-Kartenende mit den Kontakten in den Steckplatz ein, wobei die Etikettseite nach oben weist.

   ANMERKUNG: Der Steckplatz ist kodiert, um ein korrektes Einsetzen der Karte zu gewährleisten.

4. Drücken Sie die Karte nach innen, um sie im Steckplatz zu sichern.
5. Setzen Sie das Blade wieder im Gehäuse ein.

Entfernen einer VFlash-Medienkarte

Um das VFlash-Medium zu entfernen, drücken Sie die Karte nach innen, um sie freizugeben, und ziehen Sie dann die Karte aus dem Steckplatz.

Die VFlash-Medienkarte mit der iDRAC6- Webschnittstelle konfigurieren

Aktivieren oder Deaktivieren der VFlash-Medienkarte

ANMERKUNG: Das Kontrollkästchen **VFlash aktivieren** ist nur dann aktiv, wenn eine VFlash-Karte vorhanden ist. Ohne eine solche Karte erscheint die folgende Meldung:

```
SD Card not inserted. Please insert an SD card of size greater than 256MB. (Keine SD-Karte eingesetzt. Bitte setzen Sie eine SD-Karte mit mindestens 256 MB ein.)
```

1. Stellen Sie sicher, dass die VFlash-Karte installiert wurde.

2. Öffnen Sie einen unterstützten Webbrowser.
3. Melden Sie sich bei der iDRAC6-Webschnittstelle an.
4. Wählen Sie in der Systemstruktur **System** aus.
5. Klicken Sie auf die Registerkarte **VFlash.**

   Die Seite **VFlash** wird angezeigt.
6. Wählen Sie das Kontrollkästchen **VFlash aktivieren** aus, um die VFlash- Medienkarte zu aktivieren. Zum Deaktivieren, das Kontrollkästchen abwählen.
7. Klicken Sie auf **Anwenden**.

VFlash-Medienkarte formatieren

ANMERKUNG: Die Option **Formatieren** ist nur dann aktiv, wenn eine VFlash-Karte vorhanden ist.

1. Melden Sie sich bei der iDRAC6-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **System** aus.
3. Klicken Sie auf die Registerkarte **VFlash.**

   Die Seite **VFlash** wird angezeigt.
4. Stellen Sie sicher, dass VFlash deaktiviert ist. Das Kontrollkästchen **VFlash aktivieren** sollte nicht markiert sein.
5. Klicken Sie auf **Formatieren**.

   Es erscheint eine Warnungsmeldung, dass jegliches vorhandene Image auf der Karte während der Formatierung gelöscht wird. Dann wird um Bestätigung gebeten. Klicken Sie auf **OK**, um fortzufahren.

   Es erscheint ein Statusbalken, der den Formatierungsfortschritt anzeigt.

Laufwerk-Image hochladen

1. Stellen Sie sicher, dass die Imagedatei die Erweiterung .img aufweist und dass das Image nicht größer als 256 MB ist.

   ANMERKUNG: Auch wenn Ihre VFlash-Karte mehr als 256 MB Speicher bietet, so kann zurzeit nur auf 256 MB zugegriffen werden.
2. Melden Sie sich bei der iDRAC6-Webschnittstelle an.
3. Wählen Sie in der Systemstruktur **System** aus.
4. Klicken Sie auf die Registerkarte **VFlash.**

   Die Seite **VFlash** wird angezeigt.
5. Stellen Sie sicher, dass VFlash deaktiviert ist. Das Kontrollkästchen **VFlash aktivieren** sollte nicht markiert sein.
6. Geben Sie im Abschnitt **VFlash-Laufwerk** den Pfad zur Imagedatei ein oder klicken Sie auf **Durchsuchen**, um an deren Speicherort auf Ihrem System zu wechseln.

   Klicken Sie auf **Hochladen**.

   Es erscheint ein Statusbalken, der den Hochladefortschritt anzeigt.

VFlash-Speicherstickgröße anzeigen

Das Drop-Down-Menü **Größe des virtuellen Flash-Speichersticks** zeigt die aktuelle Größeneinstellung an.

VFlash-Medienkarte mit RACADM konfigurieren

Aktivieren oder Deaktivieren der VFlash-Medienkarte

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

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

wobei `1` aktiviert und `0` deaktiviert bedeutet.

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

VFlash-Medienkarte formatieren

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

```
racadm vmkey reset
```

VORSICHT: Die Formatierung der VFlash-Medienkarte löscht sämtliche vorhandene Daten.

ANMERKUNG: Weitere Informationen über vmkey finden Sie unter "vmkey".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Virtuellen Datenträger konfigurieren und verwenden

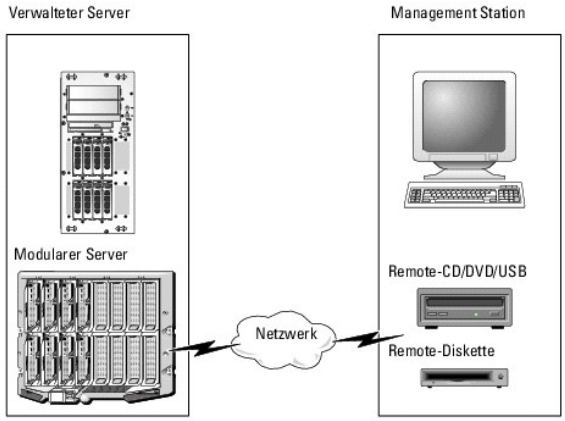
Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

---

Übersicht

Die Funktion **Virtueller Datenträger**, auf die über den Konsolenumleitungs-Viewer zugegriffen werden kann, bietet dem verwalteten Server Zugriff auf Datenträger, die mit einem Remote-System auf dem Netzwerk verbunden sind. Abbildung 12-1 zeigt die gesamte Architektur des **virtuellen Datenträgers**.

Abbildung 12-1. Gesamte Architektur des virtuellen Datenträgers



Mit dem **virtuellen Datenträger** können Administratoren im Remote-Zugriff verwaltete Server starten, Anwendungen installieren, Treiber aktualisieren oder sogar neue Betriebssysteme von virtuellen CD/DVD- und 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 12-1 führt die unterstützten Laufwerkverbindungen für virtuelle Floppy-Laufwerke und virtuelle optische Laufwerke auf.

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

Tabelle 12-1. 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 Management Station mit dem Windows-Betriebssystem 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 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 an der iDRAC6-Webschnittstelle an.
2. Klicken Sie auf das Register **Konsole/Datenträger**.
3. Klicken Sie auf **Konfiguration und dann auf Virtueller Datenträger**.

   Die Seite **Konsolenumleitungskonfiguration** wird eingeblendet.
4. Klicken Sie auf **Virtueller Datenträger**.
5. Wählen Sie im Abschnitt **Virtueller Datenträger** Werte für die Einstellungen aus. Unter Tabelle 12-2 finden Sie weitere Informationen über die Konfigurationswerte des **Virtuellen Datenträgers.**
6. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

   Die folgende Warnungmeldung wird eingeblendet: `You are about to change device configuration. All existing redirection sessions will be closed. Do you want to continue? (Sie sind dabei, die Gerätekonfiguration zu ändern. Alle bestehenden Umleitungssitzungen werden geschlossen. Möchten Sie fortfahren?)`
7. Klicken Sie auf **OK**, um fortzufahren.

   Die folgende Warnungsmeldung wird eingeblendet: `Virtual Media Configuration successfully set. (Konfiguration des virtuellen Datenträgers erfolgreich abgeschlossen.)`

Tabelle 12-2. Konfigurationswerte des virtuellen Datenträgers

Attribut	Wert
Attach Virtual Media	Attach - Schließt den **Virtuellen Datenträger** umgehend an den Server an.

	Detach - Trennt den **Virtuellen Datenträger** umgehend vom Server ab. Auto-Attach - Schließt den **virtuellen Datenträger** nur dann am Server an, wenn eine Sitzung des virtuellen Datenträgers gestartet wird.
Maximum Sessions	Zeigt die maximale Anzahl zulässiger **Virtueller Datenträger**-Sitzungen an. Dieser Wert beträgt immer **1**. **ANMERKUNG:** Es ist nur eine Benutzersitzung für virtuelle Datenträger zulässig; es können jedoch mehrere Geräte in einer Sitzung verbunden werden. Siehe Virtuellen Datenträger ausführen".
Active Sessions	Zeigt die aktuelle Anzahl von Sitzungen des virtuellen Datenträgers an.
Virtual Media Encryption Enabled	Aktiviert (markiert) oder deaktiviert (nicht markiert) Verschlüsselung auf den Verbindungen des **Virtuellen Datenträgers.**
Virtual Media Port Number	Die Netzwerkanschlussnummer, die zur Verbindung mit dem Dienst des **virtuellen Datenträgers** ohne Verschlüsselung verwendet wird. Zwei aufeinander folgende 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 iDRAC6-Dienst konfiguriert werden. Die Standardeinstellung ist **3668**.
Virtual Media SSL Port Number	Die Netzwerkanschlussnummer, die für verschlüsselte Verbindungen zum **Virtueller Datenträger**-Dienst verwendet wird. Zwei aufeinander folgende 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 iDRAC6-Dienst konfiguriert werden. Die Standardeinstellung ist **3670**.
Floppy Emulation	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.
Enable Boot Once	Aktiviert (markiert) oder deaktiviert (nicht markiert) die Option Einzelstart, bei der die **Virtuelle Datenträger**-Sitzung automatisch nach dem einmaligen Start des Servers abschaltet. Diese Option ist nützlich für automatische Bereitstellungen.

Virtuellen Datenträger ausführen

VORSICHT: Geben Sie keinen racreset-Befehl aus, wenn eine virtueller Datenträger-Sitzung ausgeführt wird. Andernfalls kann es zu unerwünschten Folgen kommen, z. B. Datenverlust.

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.
2. Melden Sie sich an der iDRAC6-Webschnittstelle an.
3. Klicken Sie auf die Registerkarte **Konsole / Datenträger**.

   Die Seite **Konsolenumleitungskonfiguration** 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 beheben, ziehen Sie die Dokumentation für Ihr Microsoft-Betriebssystem zurate oder setzen Sie 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. Wählen Sie **Datenträger** → **Virtueller Datenträger Assistent...**

   Der **Assistent zur Datenträgerumleitung** wird eingeblendet.

6. Sehen Sie das Fenster **Status** am Ende der Seite **Assistent** ein. Wenn eine Datenträgerverbindung besteht, muss diese vor dem Verbinden mit einer anderen Datenträgerquelle zuerst unterbrochen werden. Um Datenträger zu trennen, klicken Sie auf die Schaltfläche **Trennen** neben dem Datenträger im Fenster **Status**.
7. Wählen Sie die Optionsschaltfläche neben den Datenträgertypen aus, zu denen eine Verbindung hergestellt werden soll.

   Sie können sowohl die Optionsschaltfläche **Diskettenabbild** als auch eine der Optionsschaltflächen im Abschnitt **CD / DVD-Laufwerk** auswählen.

   Um ein Disketten- oder ISO-Abbild zu verbinden, geben Sie den Pfad zum Abbildspeicherplatz auf Ihrem lokalen Computer ein oder klicken Sie auf die

Schaltfläche **Durchsuchen**, um zum Speicherort des Abbilds zu wechseln.

8. Klicken Sie **neben jedem ausgewählten Datenträgertyp auf die Schaltfläche Verbinden.**

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

9. Klicken Sie auf **Schließen.**

Verbindung des virtuellen Datenträgers unterbrechen

1. Wählen Sie **Datenträger** → **Virtueller Datenträger-Assistent...**

   Der **Assistent zur Datenträgerumleitung** wird eingeblendet.

2. Klicken Sie neben dem Datenträger, dessen Verbindung unterbrochen werden soll, auf **Trennen**.

   Die Verbindung zum Datenträger wird unterbrochen und das Fenster **Status** 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 kann unter Verwendung des **virtuellen Datenträgers** bis zum Abschluss weniger als 15 Minuten in Anspruch nehmen. Weitere Informationen finden Sie unter Betriebssystem bereitstellen".

1. Überprüfen Sie folgende Punkte:

   - Die Installations-DVD/CD des Betriebssystems wird in das DVD/CD-Laufwerk der Management Station eingelegt.
   - Das lokale DVD/CD-Laufwerk ist ausgewählt.
   - Sie sind mit den virtuellen Laufwerken verbunden.

2. Befolgen Sie die Schritte zum Starten vom virtuellen Datenträger, die im Abschnitt "Starten vom virtuellen Datenträger" enthalten sind, um sicherzustellen, dass das BIOS so eingestellt ist, dass es von dem DVD/ 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 **mount** manuell.

Häufig gestellte Fragen

Tabelle 12-3 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 12-3. Virtuelle Datenträger verwenden: Häufig gestellte Fragen

Frage	Antwort
Manchmal bemerke ich, dass die Client-Verbindung meines virtuellen Datenträgers unterbrochen wird. Warum?	Wenn eine Netzwerk-Zeitüberschreitung eintritt, trennt die iDRAC6-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Wenn die Konfigurationseinstellungen des virtuellen Datenträgers in der iDRAC6-Webschnittstelle oder durch Befehle des lokalen RACADM geändert werden, wird die Verbindung aller verbundener Datenträger bei Übernahme der Konfigurationsänderung unterbrochen. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie den Virtuellen Datenträger-Assistenten.
Welche Betriebssysteme unterstützen iDRAC6?	Eine Liste unterstützter Betriebssysteme finden Sie unter "Unterstützte Betriebssysteme".
Welche Webbrowser unterstützen iDRAC6?	Eine Liste unterstützter Internet-Browser erhalten Sie unter "Unterstützte Webbrowser".
Warum bricht meine Client-Verbindung manchmal ab?	• Ihre Client-Verbindung kann manchmal abbrechen, wenn das Netzwerk langsam ist, oder wenn Sie die CD im CD-Laufwerk des Client-Systems wechseln. Beispiel: Wenn Sie die CD im CD-Laufwerk des Client-Systems wechseln, weist die neue CD eventuell eine Autostart-Funktion auf. Wenn dies der Fall ist, kann für die Firmware eine Zeitüberschreitung eintreten und die Verbindung kann verloren gehen, wenn das Client-System zu lange braucht, bis es zum Lesen der CD bereit ist. Wenn eine Verbindung verloren geht, können Sie sie über die GUI wiederherstellen und mit dem vorherigen Vorgang fortfahren. • Wenn eine Netzwerk-Zeitüberschreitung eintritt, trennt die iDRAC6-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Es 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?	Wenn Sie das Windows-Betriebssystem über die CD *Dell PowerEdge Installation and Server Management* und über eine langsame Netzwerkverbindung installieren, ist für das Installationsverfahren aufgrund der Netzwerklatenzzeit eventuell ein höherer Zeitaufwand erforderlich, um auf die iDRAC6-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?	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 iDRAC6 können Sie von den folgenden startfähigen Datenträgern aus starten: • CDROM/DVD-Datenträger • ISO 9660-Abbild • 1,44 Zoll-Diskette oder Diskette-Abbild • USB-Schlüssel, der vom Betriebssystem als Wechselplatte erkannt wird (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. bei 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 zu Dells Support-Website unter **support.dell.com** und suchen nach der Datei **R122672.exe**.
Ich kann mein virtuelles Disketten-Gerät auf einem 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?	Bei einigen Linux-Versionen erfolgt die automatische Ladung des virtuellen Floppy-Laufwerks und des virtuellen CD-Laufwerks auf unterschiedliche Weise. Um das virtuelle Diskettenlaufwerk zu laden, machen Sie den Geräteknoten ausfindig, den Linux dem virtuellen Diskettenlaufwerk zuweist. Führen Sie die folgenden Schritte aus, um das virtuelle Diskettenlaufwerk korrekt ausfindig zu machen und zu laden: 1. Öffnen Sie eine Linux-Eingabeaufforderung und führen Sie den folgenden Befehl aus: grep "Virtual Floppy" /var/log/messages 2. Machen Sie den letzten Eintrag zu dieser Meldung ausfindig und notieren Sie die Zeit. 3. Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus: grep "*hh:mm:ss*" /var/log/messages wobei *hh:mm:ss* der Zeitstempel der Meldung ist, die von grep in Schritt 1 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 Diskettenlaufwerk unterstützt?	Ihr virtuelles Disketten-Laufwerk unterstützt FAT16- oder FAT32-Dateisysteme.
Als ich im Remote-Zugriff anhand der iDRAC6-Webschnittstelle eine Firmwareaktualisierung ausgeführt habe, wurden meine virtuellen Laufwerke vom Server getrennt. Warum?	Firmwareaktualisierungen führen zum Zurücksetzen des iDRAC6, zum Trennen der Remote-Verbindung und zum Trennen der virtuellen Datenträger. Die Laufwerke erscheinen wieder, wenn der iDRAC6-Reset abgeschlossen ist.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Befehlszeilenoberfläche des lokalen RACADM verwenden

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

Die lokale RACADM-Befehlszeilenschnittstelle (CLI) bietet Zugriff auf die iDRAC6-Verwaltungsfunktionen vom verwalteten Server aus. RACADM bietet Zugriff auf dieselben Funktionen wie die iDRAC6-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 keine Netzwerkverbindungen zum Zugriff auf den iDRAC6 vom verwalteten Server aus. Dies bedeutet, dass Sie Befehle des lokalen RACADM verwenden können, um den anfänglichen iDRAC6-Netzwerkbetrieb zu konfigurieren.

Weitere Informationen zur Konfiguration mehrerer iDRACs finden Sie unter "Mehrere iDRACs gleichzeitigkonfigurieren".

Dieser Abschnitt enthält die folgenden Informationen:

- RACADM von einer Eingabeaufforderung aus verwenden
- iDRAC6 mit dem **racadm**-Befehl 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 der RACADM-Unterbefehlliste Folgendes ein:

```
racadm-Help
```

Die Liste der Unterbefehle enthält alle Befehle, die vom iDRAC6 unterstützt werden.

Um für einen Unterbefehl Hilfe zu erhalten, geben Sie Folgendes ein:

```
racadm help-<Unterbefehl>
```

Der Befehl zeigt die Syntax- und Befehlszeilenoptionen für den Unterbefehl an.

RACADM-Unterbefehle

Tabelle 13-1 enthält eine Beschreibung der einzelnen RACADM-Unterbefehle, die Sie in RACADM ausführen können. Eine ausführliche Auflistung aller RACADM-Unterbefehle einschließlich der Syntax und gültiger Einträge finden Sie unter "Übersicht der RACADM-Unterbefehle."

Tabelle 13-1. RACADM-Unterbefehle

Befehl	Beschreibung
clrasrscreen	Löscht die Seite Bildschirm Letzter Absturz (ASR).
clrraclog	Löscht das iDRAC6-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 iDRAC6.
getconfig	Zeigt die aktuellen iDRAC6-Konfigurationseigenschaften an.
getniccfg	Zeigt die derzeitige IP-Konfiguration für den Controller an.
getraclog	Zeigt das iDRAC6-Protokoll an.
getractime	Zeigt die iDRAC6-Zeit an.
getssninfo	Zeigt Informationen über aktive Sitzungen an
getsvctag	Zeigt Service-Tag-Nummern an.
getsysinfo	Zeigt Informationen zum iDRAC6 und dem verwalteten Server, einschließlich IP-Konfiguration, Hardwaremodell, Firmware-Versionen und Betriebssysteminformationen, an.

gettracelog	Zeigt das iDRAC6-Ablaufverfolgungsprotokoll an. Bei Verwendung mit -i zeigt der Befehl die Anzahl von Einträgen im iDRAC6-Ablaufverfolgungsprotokoll an.
help	Listet die iDRAC6-Unterbefehle auf.
help <*Unterbefehl*>	Listet die Verwendungsaussage für den angegebenen Unterbefehl auf.
localconredirdisable	Führt die lokale kVM-Deaktivierung vom lokalen System aus durch.
racreset	Setzt den iDRAC6 zurück.
racresetcfg	Setzt den iDRAC6 auf die Standardkonfiguration zurück.
serveraction	Führt Energieverwaltungsvorgänge auf dem verwalteten Server aus.
setniccfg	Stellt die IP-Konfiguration für den Controller ein.
sslcertdownload	Lädt ein CA-Zertifikat herunter.
sslcertupload	Lädt ein CA-Zertifikat oder Serverzertifikat auf den iDRAC6 hoch.
sslcertview	Zeigt ein CA-Zertifikat oder Serverzertifikat im iDRAC6 an.
sslcsrgen	Erstellt die SSL-CSR und lädt sie herunter.
testemail	Zwingt den iDRAC6, eine E-Mail über den iDRAC6-NIC zu senden.
testtrap	Zwingt den iDRAC6, einen SNMP-Alarm über den iDRAC6-NIC zu senden.
vmkey	Setzt den virtuellen Medienschlüssel auf die Standardgröße von 256 MB zurück.

RACADM-Dienstprogramm zur Konfiguration des iDRAC6 verwenden

In diesem Abschnitt wird beschrieben, wie RACADM zum Ausführen verschiedener iDRAC6-Konfigurations-Tasks verwendet wird.

Aktuelle iDRAC6-Einstellungen anzeigen

Der RACADM-Unterbefehl **getconfig** ruft aktuelle Konfigurationseinstellungen vom iDRAC6 ab. Die Konfigurationswerte werden in *Gruppen* organisiert, die ein oder mehrere *Objekt(e)* enthalten, wobei die Objekte *Werte* haben.

Eine vollständige Beschreibung der Gruppen und Objekte finden Sie unter "Gruppen- und Objektdefinitionen der iDRAC6 Enterprise Eigenschaften-Datenbank".

Geben Sie zum Anzeigen einer Liste aller iDRAC6-Gruppen den folgenden Befehl ein:

```
racadm getconfig -h
```

Geben Sie zum Anzeigen der Objekte und Werte für eine bestimmte Gruppe den folgenden Befehl ein:

```
racadm getconfig -g <Gruppe>
```

Beispiel: Um eine Liste aller **cfgLanNetworking**-Gruppenobjekteinstellungen anzuzeigen, geben Sie den folgenden Befehl ein:

```
racadm getconfig -g cfgLanNetworking
```

iDRAC6-Benutzer mit RACADM verwalten

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

ANMERKUNG: Wenn Sie einen neuen iDRAC6 konfigurieren oder den Befehl **racadm racresetcfg** ausgeführt haben, ist der einzige aktuelle Benutzer **root** mit dem Kennwort **calvin**.

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

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

Sie können in der iDRAC6-Eigenschaftendatenbank bis zu 15 Benutzer konfigurieren. (Ein 16. Benutzer ist für den IPMI-LAN-Benutzer reserviert.) Überprüfen Sie, ob bereits aktuelle Benutzer vorhanden sind, bevor Sie einen iDRAC6-Benutzer manuell aktivieren.

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

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

ODER

Geben Sie den folgenden Befehl einmal für jeden Index von 1 bis 16 ein:

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

ANMERKUNG: Sie können auch racadm getconfig -f <*Dateiname*> eingeben und die erstellte Datei <*Dateiname*> anzeigen, die alle Benutzer sowie alle anderen iDRAC6-Konfigurationsparameter einschließt.

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

Einen iDRAC6-Benutzer hinzufügen

Um dem iDRAC6 einen neuen Benutzer hinzuzufügen, gehen Sie wie folgt vor:

1. Legen Sie den Benutzernamen fest.
2. Legen Sie das Kennwort fest.
3. Stellen Sie die Benutzerberechtigung zum Anmelden am iDRAC6 ein.
4. Aktivieren Sie den Benutzer.

Beispiel

Das folgende Beispiel beschreibt, wie man dem iDRAC6 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
```

iDRAC6-Benutzer mit Berechtigungen aktivieren

Um einem Benutzer bestimmte administrative (rollenbasierte) Berechtigungen zu erteilen, stellen Sie die Eigenschaft **cfgUserAdminPrivilege** auf eine Bitmaske ein, die aus den unter Tabelle 13-2gezeigten Werten konstruiert ist:

Tabelle 13-2. Bit-Masken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
Bei iDRAC6 anmelden	0x0000001
iDRAC6 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
```

Einen iDRAC6-Benutzer entfernen

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

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

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

Eine Null-Kette mit doppelten Anführungszeichen ("") weist den iDRAC6 an, die Benutzerkonfiguration am angegebenen Index zu entfernen und die Benutzerkonfiguration auf die ursprünglichen Werkseinstellungen zurückzusetzen.

Testen von E-Mail-Warnmeldungen

Mit der iDRAC6-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 iDRAC6 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".

iDRAC6-SNMP-Trap-Warnungsfunktion testen

Die iDRAC6-SNMP-Trap-Warnungsfunktion ermöglicht den SNMP-Trap-Abhörkonfigurationen, Traps für Systemereignisse zu empfangen, die auf dem verwalteten Server auftreten.

Das folgende Beispiel zeigt, wie ein Benutzer die SNMP-Trap-Warnungsfunktion testen kann.

```
racadm testtrap -i 2
```

ANMERKUNG: Stellen Sie vor dem Testen der iDRAC6-SNMP-Trap-Warnungsfunktion sicher, dass die SNMP- und Trap-Einstellungen ordnungsgemäß konfiguriert sind. Diese Einstellungen können anhand der Beschreibungen zu den Unterbefehlen **testtrap** und **testemail** konfiguriert werden.

iDRAC6-Netzwerkeigenschaften konfigurieren

Geben Sie Folgendes ein, um eine Liste verfügbarer Netzwerkeigenschaften zu erstellen:

```
racadm getconfig -g cfgLanNetworking
```

Wenn DHCP zum Erhalt einer IP-Adresse verwendet werden soll, kann der folgende Befehl zum Schreiben des Objekts **cfgNicUseDhcp** und zum Aktivieren dieser Funktion verwendet werden:

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

Die Befehle bieten dieselbe Konfigurationsfunktionalität wie das iDRAC6-Konfigurationsdienstprogramm, wenn Sie dazu aufgefordert werden, <Strg><E> zu drücken. Weitere Informationen zum Konfigurieren von Netzwerkeigenschaften mit dem iDRAC6-Konfigurationsdienstprogramm finden Sie unter "iDRAC6 LAN".

Im folgenden Beispiel wird gezeigt, wie der Befehl zur Konfiguration gewünschter LAN-Netzwerkeigenschaften verwendet werden kann.

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

ANMERKUNG: Wenn **cfgNicEnable** auf **0** gesetzt wird, wird das iDRAC6-LAN selbst dann deaktiviert, wenn DHCP aktiviert ist.

IPMI Über LAN konfigurieren

1. Konfigurieren Sie IPMI über LAN, indem Sie folgenden Befehl eingeben:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
   ```

ANMERKUNG: Diese Einstellung bestimmt die IPMI-Befehle, die von der IPMI-über-LAN-Schnittstelle ausgeführt werden können. Weitere Informationen finden Sie in den IPMI 2.0-Angaben.

   a. Aktualisieren Sie die IPMI-Kanalberechtigungen, indem Sie folgenden Befehl eingeben:

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <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 iDRAC6-IPMI unterstützt das RMCP+-Protokoll. Die IPMI 2.0-Spezifikationen enthalten weitere Informationen.

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <Schlüssel>
      ```

      wobei <*Schlüssel*> ein aus 20 Zeichen bestehender Verschlüsselungsschlüssel in einem gültigen Hexadezimal-Format ist.

2. Konfigurieren Sie IPMI Seriell über LAN (SOL), 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 iDRAC6 bei jeder einzelnen Plattformwarnung ergreifen soll. Tabelle 13-3 führt die möglichen Maßnahmen sowie den Wert auf, mithilfe derer sie in RACADM identifiziert werden können.

Tabelle 13-3. Plattformereignismaßnahme

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 (Tabelle 5-7) und <*Maßnahmenwert*> ein Wert von "Tabelle 13-3".

   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 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 an der Eingabeaufforderung 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 (IP-Bereich)

Die IP-Adressenfilterung (oder *IP-Bereichsüberprüfung*) gestattet den iDRAC6-Zugriff nur von Clients oder Verwaltungsstationen aus, deren IP-Adressen innerhalb eines vom Benutzer angegebenen Bereichs liegen. Alle anderen Anmeldeaufforderungen werden abgewiesen.

Die IP-Filterung vergleicht die IP-Adresse einer eingehenden Anmeldung mit dem IP-Adressenbereich, der in den folgenden **cfgRacTuning**-Eigenschaften angegeben ist:

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

Die Eigenschaft **cfgRacTuneIpRangeMask** wird sowohl auf die eingehende IP-Adresse als auch auf die **cfgRacTuneIpRangeAddr**-Eigenschaften angewendet. Sind die Ergebnisse identisch, wird für die eingehende Anmeldeaufforderung der Zugriff auf den iDRAC6 zugelassen. Anmeldungen von IP-Adressen außerhalb dieses Bereichs erhalten eine Fehlermeldung.

Die Anmeldung wird fortgeführt, wenn der folgende Ausdruck Null entspricht:

```
cfgRacTuneIpRangeMask & (<eingehende-IP-Adresse> ^ cfgRacTuneIpRangeAddr)
```

wobei & das binäre UND der Mengen und ^ das binäre ausschließliche ODER ist.

Eine vollständige Liste von **cfgRacTuning**-Eigenschaften steht unter "cfgRacTuning" zur Verfügung.

Tabelle 13-4. Eigenschaften der IP-Adressenfilterung (IP-Bereich)

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*und*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 die Form einer Netzmaske haben, 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: "Befehlszeilenoberfläche des lokalen RACADM verwenden" enthält weitere Informationen über RACADM und RACADM-Befehle.

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 Anmeldefehler auftreten und die Adresse blockiert bzw. daran gehindert wird, eine bestimmte Zeit lang eine Anmeldung am iDRAC6 durchzuführen.

Die Funktionen der IP-Blockierung schließen ein:

- Die Anzahl zulässiger Anmeldefehlschläge (**cfgRacTuneIpBlkFailcount**)
- Die Zeitspanne in Sekunden, während der diese Fehler auftreten müssen (**cfgRacTuneIpBlkFailWindow**)
- Die Zeitdauer in Sekunden, während der die blockierte IP-Adresse daran gehindert wird, eine Sitzung herzustellen, nachdem die zulässige Anzahl von Fehlern überschritten wurde (**cfgRacTuneIpBlkPenaltyTime**)

Wenn sich Anmeldefehler von einer spezifischen IP-Adresse aus ansammeln, werden sie durch einen internen Schalter registriert. Wenn sich der Benutzer erfolgreich anmeldet, wird die Aufzeichnung der Fehlversuche gelöscht und der interne Zähler zurückgesetzt.

ANMERKUNG: Wenn Anmeldeversuche von der Client-IP-Adresse abgelehnt werden, können einige SSH-Clients die folgende Meldung anzeigen: ssh exchange identification: Connection closed by remote host. (Verbindung vom Remote-Host geschlossen.)

Eine vollständige Liste von **cfgRacTune**-Eigenschaften steht unter "Gruppen- und Objektdefinitionen der iDRAC6 Enterprise Eigenschaften-Datenbank" zur Verfügung.

Anmeldungswiederholungs-Beschränkungseigenschaften (IP-Blockierung)" führt die vom Benutzer definierten Parameter auf.

Tabelle 13-5. Anmeldungswiederholungs-Beschränkungseigenschaften (IP-Blockierung)

Eigenschaft	Definition
cfgRacTuneIpBlkEnable	Aktiviert die IP-Blockierungsfunktion. Wenn innerhalb eines bestimmten Zeitraums (**cfgRacTuneIpBlkFailWindow**) aufeinander folgende Fehler (**cfgRacTuneIpBlkFailCount**) von einer einzelnen IP-Adresse aus festgestellt werden, werden alle weiteren Versuche, von dieser Adresse aus eine Sitzung herzustellen, während eines bestimmten Zeitraums zurückgewiesen (**cfgRacTuneIpBlkPenaltyTime**).
cfgRacTuneIpBlkFailCount	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche zurückgewiesen werden.
cfgRacTuneIpBlkFailWindow	Die Zeitspanne in Sekunden, während der die fehlgeschlagenen Versuche gezählt werden. Wenn die Fehlversuche diese Grenze überschreiten, werden sie aus dem Zähler gelöscht.
cfgRacTuneIpBlkPenaltyTime	Definiert den Zeitraum in Sekunden, 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
```

iDRAC6-Telnet- und SSH-Dienste mittels lokalem RACADM konfigurieren

Die Telnet-/SSH-Konsole kann lokal (auf dem verwalteten Server) unter Verwendung von RACADM-Befehlen konfiguriert werden.

ANMERKUNG: Um die Befehle in diesem Abschnitt ausführen zu können, müssen Sie über die Berechtigung **iDRAC6 konfigurieren** verfügen.

ANMERKUNG: Eine Neukonfiguration von Telnet- oder SSH-Einstellungen im iDRAC6 führt dazu, dass alle aktuellen Sitzungen ohne Warnung beendet werden.

Um Telnet und SSH vom lokalen RACADM zu aktivieren, melden Sie sich am verwalteten Server an und geben bei einer entsprechende Eingabeaufforderung die folgenden Befehle ein:

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

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

Ändern Sie zum Deaktivieren des Telnet- oder SSH-Diensts den Wert von `1` zu `0`:

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

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

Geben Sie den folgenden Befehl ein, um die Telnet-Anschlussnummer auf dem iDRAC6 zu ändern.

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <neue Anschlussnummer>
```

Geben Sie z. B. zum Ändern des Telnet-Anschlusses 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".

Eine iDRAC6-Konfigurationsdatei verwenden

Eine iDRAC6-Konfigurationsdatei ist eine Textdatei, die eine Darstellung der Werte in der iDRAC6-Datenbank enthält. Der RACADM-Unterbefehl **getconfig** kann zum Erstellen einer Konfigurationsdatei verwendet werden, die die aktuellen Werte des iDRAC6 enthält. Sie können dann die Datei bearbeiten und den RACADM-Unterbefehl **config -f** zum Zurückladen der Datei in den iDRAC6 verwenden, oder die Konfiguration auf andere iDRACs kopieren.

Eine iDRAC6-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
- Vom iDRAC6 mit dem RACADM-Unterbefehl **getconfig** erhalten
- Vom iDRAC6 mit dem RACADM-Unterbefehl **getconfig** und Bearbeitung erhalten

Geben Sie zum Abrufen einer Konfigurationsdatei unter Verwendung des RACADM-Befehls **getconfig** den folgenden Befehl bei 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 iDRAC6-Datenbank beschädigt werden kann.

In diesem Abschnitt wird das Format der Konfigurationsdatei beschrieben.

- Zeilen, die mit einem # beginnen, sind Kommentare.

  Ein Kommentar *muss* in der ersten Spalte der Zeile beginnen. Ein #-Zeichen wird in jeder anderen Spalte als normales #-Zeichen behandelt.

  Beispiel:

  ```
  #

  # This is a comment (Dies ist eine Anmerkung)

  [cfgUserAdmin]

  cfgUserAdminPrivilege=4
  ```

- Alle Gruppeneinträge müssen sich zwischen den Zeichen **[** und **]** befinden.

  Das Anfangszeichen **[**, das einen Gruppennamen anzeigt, *muss* in Spalte eins beginnen. Der Gruppenname *muss* vor allen anderen Objekten in dieser Gruppe angegeben werden. Objekte, die keinen zugewiesenen Gruppennamen enthalten, erzeugen Fehler. Die Konfigurationsdaten werden in Gruppen organisiert, wie unter "Gruppen- und Objektdefinitionen der iDRAC6 Enterprise Eigenschaften-Datenbank"definiert.

  Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objekts an.

  Beispiel:

  ```
  [cfgLanNetworking] (Gruppenname)

  cfgNicIpAddress=143.154.133.121 (Objektname)
  ```

- Parameter werden als *Objekt*=*Wert*-Paare ohne Leerzeichen zwischen Objekt, = und Wert angegeben.

  Auf den Wert folgende Leerzeichen werden ignoriert. Ein Leerzeichen innerhalb einer Wertezeichenkette bleibt unverändert. Alle Zeichen rechts neben = werden unverändert übernommen (z. B. ein zweites = oder ein #, *[*, *]* usw.).

- Der Parser ignoriert einen Index-Objekteintrag.

  Benutzer können *nicht* angeben, welcher Index verwendet werden soll. Wenn der Index bereits vorhanden ist, wird dieser entweder verwendet, oder es wird ein neuer Eintrag im ersten verfügbaren Index für diese Gruppe erstellt.

  Der Befehl racadm getconfig -f *<Dateiname>* setzt einen Kommentar vor die Index-Objekte, wodurch die enthaltenen Kommentare sichtbar werden.

  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 iDRAC6 an, den Index für die angegebene Gruppe zu löschen.

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

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

- 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 alle Indizes aus dem iDRAC6 für diese Gruppe aus. Alle Objekte innerhalb dieser Gruppe sind einfache Modifizierungen, wenn der iDRAC6 konfiguriert wird. Wenn ein modifiziertes Objekt einen neuen Index darstellt, wird der Index während der Konfiguration auf dem iDRAC6 erstellt.

- 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 iDRAC6 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.

Die iDRAC6-IP-Adresse in einer Konfigurationsdatei modifizieren

Wenn Sie die IDRAC6-IP-Adresse in der Konfigurationsdatei modifizieren, entfernen Sie alle unnötigen Einträge von **<***Variable***>=**<*Wert*>. 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 (Objektgruppe) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Die Datei wird wie folgt aktualisiert:

```
#

# Object Group (Objektgruppe) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored (Anmerkung, der Rest dieser Zeile wird ignoriert)

cfgNicGateway=10.35.9.1
```

Die Konfigurationsdatei in den iDRAC6 laden

Der Befehl `racadm config -f <Dateiname>` parst die Konfigurationsdatei, um zu überprüfen, ob gültige Gruppen- und Objektnamen vorhanden sind und Syntaxregeln befolgt werden. Weist die Datei keine Fehler auf, aktualisiert der Befehl die iDRAC6-Datenbank mit dem Dateiinhalt.

ANMERKUNG: Wenn Sie nur die Syntax überprüfen, jedoch nicht die iDRAC6-Datenbank aktualisieren möchten, fügen Sie dem Unterbefehl **config** die Option **-c** hinzu.

Fehler in der Konfigurationsdatei werden mit der Zeilennummer sowie einer Meldung markiert, die das Problem beschreibt. Bevor die Konfigurationsdatei den iDRAC6 aktualisieren kann, müssen alle Fehler korrigiert worden sein.

ANMERKUNG: Verwenden Sie den Unterbefehl **racresetcfg**, um die Datenbank und die iDRAC6-NIC-Einstellungen auf die ursprünglichen Standardeinstellungen zurückzusetzen und alle Benutzer und Benutzerkonfigurationen zu entfernen. Während der Stammbenutzer verfügbar ist, werden die Einstellungen anderer Benutzer ebenfalls auf die Standardeinstellungen zurückgesetzt.

Bevor Sie den Befehl `racadm config -f <Dateiname>` ausführen, können Sie den Unterbefehl `racresetcfg` ausführen, um den iDRAC6 auf seine Standardeinstellungen zurückzusetzen. Stellen Sie sicher, dass die zu ladende Konfigurationsdatei alle gewünschten Objekte, Benutzer, Indizes und anderen Parameter enthält.

Um den iDRAC6 mit der Konfigurationsdatei zu aktualisieren, führen Sie bei 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 iDRAC6 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 iDRAC6-Eigenschaften ist, wie z. B. **myconfig.cfg**.

Weitere Informationen finden Sie unter Eine iDRAC6-Konfigurationsdatei erstellen".

ANMERKUNG: Einige Konfigurationsdateien enthalten eindeutige iDRAC6-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, wo sie für alle verwalteten Server, deren iDRAC6 konfiguriert werden soll, zugänglich ist.

4. Führen Sie für jeden iDRAC6, den Sie konfigurieren möchten, Folgendes aus:

   a. Melden Sie sich am verwalteten Server an und öffnen Sie eine Eingabeaufforderung.

   b. Wenn Sie den iDRAC6 von den Standardeinstellungen aus neu konfigurieren möchten, geben Sie folgenden Befehl ein:

      ```
      racadm racreset
      ```

   c. Laden Sie die Konfigurationsdatei mit folgendem Befehl in den iDRAC6:

      ```
      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 iDRAC6 mit dem folgenden Befehl zurück:

      ```
      racadm reset
      ```

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iDRAC6-Enterprise verwenden SM-CLP-Befehlszeilenschnittstelle

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

Dieser Abschnitt enthält Informationen zum SMWG-SM-CLP (Serververwaltungs-Workgroup, Serververwaltungs-Befehlszeilenprotokoll), das im iDRAC6 integriert ist.

ANMERKUNG: Für diesen Abschnitt wird angenommen, dass Sie mit der SMASH-Initiative (Systemverwaltungsarchitektur für Serverhardware) und den SMWG SM-CLP-Angaben vertraut sind. Weitere Information zu diesen Angaben finden Sie auf der Website zur Distributed Management Task Force (DMTF) unter **www.dmtf.org**.

Das iDRAC6-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 iDRAC6 ausgeführt, während RACADM auf dem verwalteten Server ausgeführt wird. 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 iDRAC6-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
- iDRAC6-Benutzerkontoverwaltung
- Active Directory-Konfiguration
- iDRAC6-LAN-Konfiguration
- Erstellung einer SSL-Zertifikatsignaturanforderung (CSR)
- Konfiguration des virtuellen Datenträgers
- SOL-Umleitung (Seriell über LAN) über Telnet oder SSH

---

iDRAC6-SM-CLP-Support

SM-CLP wird von der iDRAC6-Firmware gehostet und unterstützt Telnet- und SSH-Verbindungen. Die iDRAC6-SM-CLP-Schnittstelle basiert auf der SM-CLP-Spezifikation Version 1.0, bereitgestellt von der DMTF-Organisation.

Die folgenden Abschnitte enthalten eine Übersicht der SM-CLP-Funktion, die vom iDRAC6 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 14-1 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 14-1. 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 -destination *<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 14-2 beschreibt die SM-CLP-Optionen. Einige Optionen haben abgekürzte Formen, wie in der Tabelle gezeigt.

Tabelle 14-2. 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 iDRAC6 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 14-3 enthält eine Liste von Zielen, die über das SM-CLP zur Verfügung stehen.

Tabelle 14-3. 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 iDRAC6-Benutzerkonten. account1 ist das Stammkonto.
/system1/sp1/enetport1	Die iDRAC6-NIC-MAC-Adresse.
/system1/sp1/enetport1/lanendpt1/ ipendpt1	Die Einstellungen für iDRAC6-IP, -Gateway und -Netzmaske.
/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1	Die Einstellungen des iDRAC6-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 für iDRAC6-SM-CLP

Die folgenden Unterabschnitte enthalten Beispiele zur Verwendung des SM-CLP, um folgende Vorgänge auszuführen:

- Serverstromverwaltung
- SEL-Verwaltung
- MAP-Zielnavigation
- Eigenschaften des Anzeigesystems
- iDRAC6-IP-Adresse, -Subnetzmaske und -Gateway-Adresse einstellen

Informationen zur Verwendung der iDRAC6 SM-CLP-Schnittstellen finden Sie unter "iDRAC6 SM-CLP-Eigenschaftendatenbank".

Server-Stromverwaltung

Tabelle 14-4 enthält Beispiele für die Verwendung des SM-CLP zum Ausführen von Stromverwaltungsvorgängen auf einem verwalteten Server.

Tabelle 14-4. Server-Energieverwaltungsvorgänge

Operation	Syntax

Anmeldung am iDRAC6 über die SSH-Schnittstelle	`>ssh 192.168.0.120`
	`>login: root`
	`>password:`

Schalten Sie den Server aus.	`->stop /system1`
	`system1 has been stopped successfully`
	`(system1 wurde erfolgreich angehalten)`

Server aus dem ausgeschalteten Zustand hochfahren	`->start /system1`

	system1 has been started successfully (system1 wurde erfolgreich gestartet)
Server neu starten	->reset /system1 system1 has been reset successfully (system1 wurde erfolgreich zurückgesetzt)

SEL-Verwaltung

Tabelle 14-5 enthält Beispiele für die Verwendung des SM-CLP zum Ausführen von SEL-bezogenen Vorgängen auf dem Managed System.

Tabelle 14-5. 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 (Alle Einträge wurden erfolgreich gelöscht)

MAP-Zielnavigation

Tabelle 14-6 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 14-6. 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

iDRAC6-IP-Adresse, -Subnetzmaske und -Gateway-Adresse einstellen

Die Verwendung des SM-CLP zum Aktualisieren der iDRAC6-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 iDRAC6-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 einen lokalen RACADM zum Einstellen der iDRAC6-Netzwerkeigenschaften verwenden, werden Ihre Änderungen sofort wirksam, da ein lokaler 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 14-7 zeigt Beispiele zum Einstellen der iDRAC6-Eigenschaften unter Verwendung des SM-CLP.

Tabelle 14-7. iDRAC6-Netzwerkeigenschaften mit SM-CLP einstellen

Operation	Syntax
Wechseln Sie zum Speicherort der iDRAC6-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

iDRAC6-Firmware mittels SM-CLP aktualisieren

Um die iDRAC6-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 iDRAC6 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

Betriebssystem mithilfe von iVMCLI bereitstellen

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

Das integrierte Dienstprogramm Befehlszeilenschnittstelle des virtuellen Datenträgers (iVMCLI) ist eine Befehlszeilenschnittstelle, die die Funktionen des virtuellen Datenträgers von der Management Station zum iDRAC6 im Remote-System bereitstellt. Mit iVMCLI und geskripteten Methoden können Sie Ihr Betriebssystem auf mehreren Remote-Systemen in Ihrem Netzwerk einsetzen.

Dieser Abschnitt liefert Informationen 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 iDRAC6 ist auf jedem Remote-System konfiguriert.

Netzwerkanforderungen

Eine Netzwerkfreigabe muss die folgenden Komponenten enthalten:

- Betriebssystemdateien
- Erforderliche Treiber
- Startabbilddatei(en) des Betriebssystems

  Die Image-Datei muss das ISO-Image einer Betriebssystem-CD oder einer CD/DVD mit einem dem Industriestandard entsprechenden startfähigen Format sein.

Startfähige Abbilddatei erstellen

Bevor Sie die Abbilddatei für die Remote-Systeme bereitstellen, ist sicherzustellen, dass ein unterstütztes System von der Datei starten kann. Um die Image-Datei zu prüfen, übertragen Sie sie mithilfe der iDRAC6-Webschnittstelle auf ein Testsystem und führen Sie dann einen Neustart des Systems durch.

Die folgenden Abschnitte enthalten spezifische Informationen über das Erstellen von Abbilddateien für Linux- und Windows-Systeme.

Abbilddatei für Linux-Systeme erstellen

Verwenden Sie das Datenvervielfältigungs-Dienstprogramm (dd), um eine startfähige Image-Datei für das Linux-System zu erstellen.

Um das Dienstprogramm auszuführen, öffnen Sie eine Eingabeaufforderung und geben Sie Folgendes ein:

```
dd if=<Eingabekomponente> of=<Ausgabedatei>
```

Zum Beispiel:

```
dd if=/dev/sdc0 of=mycd.img
```

Abbilddatei für Windows-Systeme erstellen

Achten Sie bei der Auswahl eines Daten-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:
  - **IPMItool** und die Befehlszeilenschnittstelle des virtuellen Datenträgers (VMCLI) in Ihre vorhandene Betriebssystem-Bereitstellungsanwendung integrieren. 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 im 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 iDRAC6-IP-Adressen der Remote-Systeme auf, die in der Textdatei **ip.txt** bereitgestellt werden (eine IP-Adresse pro Zeile).
2. Legen Sie eine startfähige Betriebssystem-CD oder -DVD in das Laufwerk des Client-Datenträgers ein.
3. Führen Sie an der Befehlszeile **ivmdeploy** aus.

Geben Sie zum Ausführen des ivmdeploy-Skripts den folgenden Befehl an der Befehlszeile ein:

```
ivmdeploy -r ip.txt -u <idrac-Benutzer> -p <idrac-Kennwt> -c {<iso9660-img> | <Pfad>}
```

wobei

- *<idrac-Benutzer>* ist der iDRAC6-Benutzername, z. B. **root**
- *<idrac-Kennwt>* ist das Kennwort für den iDRAC6-Benutzer, z. B. **calvin**
- *<iso9660-img>* ist der Pfad zu einem ISO9660-Image der Betriebssystem-Installations-CD-ROM oder -DVD
- *<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 iDRAC6-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 iDRAC6 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 Befehlszeilenschnittstelle des virtuellen Datenträgers (iVMCLI) ist eine scriptfähige Befehlszeilenschnittstelle, die die Funktionen des virtuellen Datenträgers von der Management Station zum iDRAC6 bereitstellt.

Das iVMCLI-Dienstprogramm enthält 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 iDRAC6-Firmware aktiviert ist.
- Sichere Datenübertragung zum iDRAC6 mittels SSL-Verschlüsselung

Stellen Sie vor dem Ausführen des Dienstprogramms sicher, dass Sie für den iDRAC6 über Benutzerberechtigungen des virtuellen Datenträgers verfügen.

Wenn das Betriebssystem Administratorrechte oder eine betriebssystemspezifische Berechtigung oder Gruppenmitgliedschaft unterstützt, sind 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 Befehl **sudo** 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 Befehl **visudo**. Benutzer ohne Administratorrechte können den Befehl **sudo** als Präfix zur iVM-CLI-Befehlszeile (oder zum iVMCLI-Skript) hinzufügen, um Zugriff auf den iDRAC6 im Remote-System zu erhalten und das Dienstprogramm auszuführen.

Das 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 zur Installation des Dienstprogramms die *DVD* in das DVD-Laufwerk des Systems ein und folgen Sie den Bildschirmanweisungen.

Die *DVD Dell Systems Management Tools and Documentation* enthält die neuesten Systemverwaltungs-Softwareprodukte einschließlich Diagnose, Speicherverwaltung, Remote-Zugriffs-Dienst und das RACADM-Dienstprogramm. Diese DVD enthält auch Infodateien mit den neuesten Produktinformationen über die Systems Management Software.

Darüber hinaus enthält die *DVD Dell Systems Management Tools and Documentation* das 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 iDRAC6-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 iVMCLI-Parameter".

Wenn das Remote-System die Befehle akzeptiert und der iDRAC6 die Verbindung genehmigt, wird der Befehl weiterhin ausgeführt, bis eine der folgenden Situationen zutrifft:

- Die 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.

iVMCLI-Parameter

iDRAC6-IP-Adresse

`-r <iDRAC-IP-Adresse>[:<iDRAC-SSL-Port>]`

Dieser Parameter bietet die iDRAC6-IP-Adresse und die SSL-Schnittstelle, welche das Dienstprogramm zum Herstellen einer Verbindung des virtuellen Datenträgers zum Ziel-iDRAC6 benötigt. Wenn Sie eine ungültige IP-Adresse oder einen ungültigen DDNS-Namen eingeben, wird eine Fehlermeldung angezeigt, und der Befehl wird abgebrochen.

wobei <*iDRAC-IP-Adresse*> eine gültige, eindeutige IP-Adresse oder der iDRAC6-DDNS-Name (dynamisches Domänennamenssystem) ist, falls unterstützt. Wenn <*iDRAC-SSL-Anschluss*> ausgelassen wird, wird der Anschluss 443 (Standard-Anschluss) verwendet. Solange der iDRAC6-Standard-SSL-Anschluss nicht geändert wird, ist der optionale SSL-Anschluss nicht erforderlich.

iDRAC6-Benutzername

`-u <iDRAC-Benutzername>`

Dieser Parameter enthält den iDRAC6-Benutzernamen, der den virtuellen Datenträger ausführen wird.

Der *<iDRAC-Benutzername>* muss die folgenden Attribute aufweisen:

- Gültiger Benutzername
- iDRAC6-Benutzerberechtigung für den virtuellen Datenträger

Wenn die iDRAC6-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt und der Befehl wird terminiert.

iDRAC6-Kennwort

`-p <iDRAC-Benutzerkennwort>`

Dieser Parameter enthält das Kennwort für den angegebenen iDRAC6-Benutzer.

Wenn die iDRAC6-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 iVMCLI einen SSL-verschlüsselten Kanal zur Übertragung von Daten zwischen der Management Station und dem iDRAC6 im Remote-System. Wenn dieser Parameter nicht in der Befehlszeile enthalten ist, wird die Datenübertragung nicht verschlüsselt.

iVMCLI-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.

iVMCLI Return Codes

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

iDRAC6-Konfigurationsdienstprogramm verwenden

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

---

Übersicht

Das iDRAC6-Konfigurationsdienstprogramm ist eine Vorstart-Konfigurationsumgebung, die es ermöglicht, Parameter für den iDRAC6 und den verwalteten Server anzuzeigen und einzustellen. Genauer gesagt können Sie:

- die Firmware-Revisionsnummern für die Firmware des iDRAC6 und der primären Rückwandplatine anzeigen
- das lokale Netzwerk (LAN) des iDRAC6 konfigurieren, aktivieren oder deaktivieren
- IPMI über LAN aktivieren oder deaktivieren
- LAN-Parameter konfigurieren
- Systemdienste aktivieren, deaktivieren oder beenden
- die Geräte des virtuellen Datenträgers verbinden oder abtrennen
- den administrativen Benutzernamen bzw. das administrative Kennwort ändern
- die iDRAC6-Konfiguration auf die Werkseinstellungen zurücksetzen
- SEL-Meldungen (Systemereignisprotokoll) anzeigen oder Meldungen aus dem Protokoll löschen

Die Tasks, die Sie anhand des iDRAC6-Konfigurationsdienstprogramms ausführen können, können auch unter Verwendung anderer Dienstprogramme ausgeführt werden, welche durch den iDRAC6 oder die Dell OpenManage-Software zur Verfügung gestellt werden. Dazu gehören die Webschnittstelle, die SM-CLP-Befehlszeilenschnittstelle, die Befehlszeilenschnittstelle des lokalen RACADM und im Falle einfacher Netzwerkkonfiguration während der erstmaligen iDRAC6-Konfiguration, das iDRAC6-LCD.

---

iDRAC6-Konfigurationsdienstprogramm verwenden

Für den ersten Zugriff auf das iDRAC6-Konfigurationsdienstprogramm oder nach dem Zurücksetzen des iDRAC6 auf Werkseinstellungen müssen Sie eine iDRAC6-KVM-verbundene Konsole verwenden.

1. Drücken Sie auf der Tastatur, die mit der iDRAC6-KVM-Konsole verbunden ist, die Taste <Druck>, um das Menü **iDRAC6-KVM- 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 die Aufforderung `Press <Ctrl-E> for Remote Access Setup within 5 sec....., (<Strgl-E> drücken für Remote-Zugriff-Setup innerhalb von 5 Sekunden.....)` erscheint, drücken Sie sofort <Strg><E>. iDRAC6-Konfigurationsdienstprogramm verwenden

ANMERKUNG: Wenn das Betriebssystem zu laden beginnt, bevor Sie auf <Strg><E> gedrückt haben, lassen Sie das System den Startvorgang beenden, starten Sie dann den Server neu starten und wiederholen Sie den Vorgang.

Die ersten zwei Zeilen des Konfigurationsdienstprogramms liefern Informationen über die iDRAC6-Firmware und primäre Rückwandplatinen-Firmware-Revisionen. Die Revisionsstufen können nützlich sein, wenn Sie bestimmen möchten, ob ein Firmware-Upgrade erforderlich ist.

Die iDRAC6-Firmware ist der Teil der Firmware, die für externe Schnittstellen zuständig ist, wie z. B. die webbasierte Schnittstelle, SM-CLP und Webschnittstellen. Die Firmware der primären Rückwandplatine ist der Teil der Firmware, der mit der Serverhardware-Umgebung gekoppelt wird und diese überwacht.

---

iDRAC6-Konfigurationsdienstprogramm verwenden

Unterhalb der Firmware-Revisionsmeldungen besteht der Rest des iDRAC6-Konfigurationsdienstprogramms 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 wählbare Werte bietet, z. B. Ja/Nein oder Aktiviert/Deaktiviert, drücken Sie die Taste <Nach links> und <Nach rechts> bzw. 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 iDRAC6-Konfigurationsdienstprogramms 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 Dienstprogramm zurückkehren möchten.

In den folgenden Abschnitten werden die Menüelemente des iDRAC6-Konfigurationsdienstprogramms beschrieben.

iDRAC6 LAN

Verwenden Sie die Taste <Nach links> und <Nach rechts> bzw. die Leertaste, um zwischen **Aktiviert** und **Deaktiviert** zu wählen.

Das iDRAC6-LAN ist in der Standardkonfiguration deaktiviert. Das LAN muss aktiviert sein, damit die Verwendung der iDRAC6-Einrichtungen, wie z. B. webbasierte Schnittstelle, Telnet/SSH-Zugriff auf die SM-CLP-Befehlszeilenschnittstelle, Konsolenumleitung und virtuelle Medien, 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.)`

Die Meldung informiert Sie darüber, dass zusätzlich zu den Einrichtungen, auf die Sie über die direkte Verbindung zu den iDRAC6-HTTP-, HTTPS-, Telnet- oder SSH-Schnittstellen zugreifen, der bandexterne Verwaltungsnetzwerkdatenverkehr, wie z. B. IPMI-Meldungen, die von einer Verwaltungsstation aus an den iDRAC6 gesendet werden, nicht empfangen werden kann, wenn das LAN deaktiviert ist. Die Schnittstelle des lokalen RACADM bleibt verfügbar und kann zur Neukonfiguration des iDRAC6-LAN verwendet werden.

`Drücken Sie auf eine beliebige Taste, um die Meldung zu löschen und fortzufahren.`

IPMI über LAN

Verwenden Sie die Tasten <Nach links> und <Nach rechts> bzw. die Leertaste, um zwischen **Ein** und **Aus** zu wählen. Wenn **Aus** ausgewählt ist, akzeptiert der iDRAC6 keine IPMI-Meldungen, die über die LAN-Schnittstelle eingehen.

Wenn Sie **Aus** auswählen, wird die folgende Warnung angezeigt:

`iDRAC Out-of-Band interface will be disabled if IPMI Over LAN is OFF. (Bandexterne iDRAC-Schnittstelle wird deaktiviert, wenn IPMI über LAN auf AUS steht.)`

Drücken Sie auf eine beliebige Taste, um die Meldung zu löschen und fortzufahren. Diese Meldung wird im Abschnitt "iDRAC6 LAN " erklärt.

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 16-1. 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 iDRAC6-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 iDRAC6-Namen im DNS-Dienst zu registrieren. Wählen Sie **Aus**, wenn Sie nicht möchten, dass Benutzer in der Lage sein sollen, den iDRAC6-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 iDRAC6-Namen fertig bearbeitet haben. Drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln. Der iDRAC6-Name muss ein gültiger DNS-Host-Name sein.
Domänenname von DHCP	Wählen Sie **Ein** aus, wenn Sie den Domänennamen von einem DHCP-Dienst auf dem Netzwerk abrufen möchten. Wählen Sie **Aus**, wenn Sie den Domänennamen festlegen möchten.
Domänenname	Wenn **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`.

Virtuellen Datenträger konfigurieren

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, sodass sie während **Konsolenumleitungs**-Sitzungen verfügbar werden.
- Wenn Sie **Abgetrennt** auswählen, können Benutzer während **Konsolenumleitungs**-Sitzungen nicht auf virtuelle Datenträgergeräte zugreifen.

ANMERKUNG: Um ein USB-Flashlaufwerk mit der Funktion Virtueller Datenträger zu verwenden, muss der **Emulationstyp des USB-Flashlaufwerks** im BIOS-Setup-Dienstprogramm auf **Festplatte** eingestellt sein. Sie können auf das BIOS-Setup-Dienstprogramm zugreifen, indem Sie während des Serverstarts auf <F2> drücken. Wenn der **Emulationstyp des USB-Flashlaufwerks** auf **Automatisch** eingestellt ist, erscheint das Flashlaufwerk dem System als Diskettenlaufwerk.

Virtual Flash

Verwenden Sie die Tasten <Nach links> und <Nach rechts>, um **Aktiviert** oder **Deaktiviert** auszuwählen.

- **Aktivieren**/**Deaktivieren** löst **Trennen** und **Verbinden** aller virtuellen Datenträgergeräte vom USB-Bus aus.
- **Deaktivieren** trennt den Virtual Flash, sodass dieser nicht länger zur Verfügung steht.

ANMERKUNG: Dieses Feld ist schreibgeschützt, wenn keine SD-Karte mit mehr als 256 MB auf dem AMEA-Kartensteckplatz vorhanden ist.

ANMERKUNG: Für die virtuelle Flash-Partition ist ein vFlash-Datenträger der Marke Dell erforderlich.

Systemdienste-Konfiguration

System Services

Verwenden Sie die Tasten <Nach links> und <Nach rechts>, um **Aktiviert** oder **Deaktiviert** auszuwählen. Im aktivierten Zustand können bestimmte iDRAC6-Funktionen über die Unified Server Configuration (USC) konfiguriert werden. Weitere Informationen finden Sie im *Unified Server Configurator-Benutzerhandbuch* auf der Dell Support-Website unter **support.dell.com**.

ANMERKUNG: Eine Änderung dieser Option startet den Server neu, wenn Sie **Speichern** und **Beenden** wählen, um die neuen Einstellungen zu übernehmen.

Systemdienste beenden

Verwenden Sie die Tasten <Nach links> und <Nach rechts>, um **Ja** oder **Nein** auszuwählen.

Wenn Sie **Ja** wählen, werden alle Sitzungen des Unified Server Configurators geschlossen und der Server start neu, wenn Sie **Speichern** und **Beenden** wählen, um die neuen Einstellungen zu übernehmen.

LAN-Benutzerkonfiguration

Der LAN-Benutzer ist das iDRAC6-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 16-2. LAN-Benutzer-Konfigurationsseite

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 während der Eingabe nicht auf der Anzeige wiedergegeben.
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-Element **Auf Standardwert zurücksetzen**, um alle iDRAC6-Konfigurationselemente auf ihre Werkseinstellungen zurückzusetzen. Zum Beispiel ist dies eventuell dann erforderlich, wenn Sie das Kennwort des administrativen Benutzers vergessen haben oder den iDRAC6 von den Standardeinstellungen aus neu konfigurieren möchten.

ANMERKUNG: In der Standardkonfiguration ist der iDRAC6-Netzwerkbetrieb deaktiviert. Sie können den iDRAC6 erst dann über das Netzwerk neu konfigurieren, wenn Sie das iDRAC6-Netzwerk im iDRAC6-Konfigurationsdienstprogramm 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? (Durch das Zurücksetzen auf die Werkseinstellungen werden die nichtflüchtigen Remote-Benutzereinstellungen wiederhergestellt. Vorgang fortsetzen?)

< NO (Cancel) (NEIN (Abbrechen)) >

< YES (Continue) (JA (Fortfahren)) >
```

Zum Zurücksetzen des iDRAC6 auf seine Standardwerte, wählen Sie **JA** und drücken <Eingabe>.

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>. Zum Navigieren:

- Verwenden Sie die Taste <Nach links> um zur vorherigen (älteren) Meldung zu gelangen und die Taste <Nach rechts> um zur nächsten (neueren) Meldung zu gelangen.
- Geben Sie eine Eintragsnummer an, um zu diesem Eintrag zu wechseln.

Drücken Sie auf <Esc>, um das Systemereignisprotokoll zu verlassen.

ANMERKUNG: Sie können das SEL nur im iDRAC6-Konfigurationsdienstprogramm oder in der webbasierten iDRAC6-Schnittstelle 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.

iDRAC6-Konfigurationsdienstprogramm beenden

Wenn Sie mit den Änderungen der iDRAC6-Konfiguration fertig sind, drücken Sie auf die Taste <Esc>, um das Menü Beenden anzuzeigen.

Wählen Sie **Änderungen speichern und beenden** aus und drücken Sie dann auf <Eingabe>, um Ihre Änderungen beizubehalten.

Wählen Sie **Änderungen ablehnen und beenden** aus und drücken Sie auf <Eingabe>, um alle vorgenommenen Änderungen zu ignorieren.

Wählen Sie **Zum Setup zurückkehren** aus und drücken Sie auf <Eingabe>, um zum iDRAC6-Konfigurationsdienstprogramm zurückzukehren.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Wiederherstellung und Fehlerbehebung des verwalteten Servers

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

In diesem Abschnitt wird erklärt, wie sich Tasks in Bezug auf Diagnose und Fehlerbehebung eines im Remote-Zugriff verwalteten Servers mithilfe der iDRAC6-Dienstprogramme ausführen lassen. Er enthält die folgenden Unterabschnitte:

- Problemanzeichen - hilft Ihnen, Meldungen und andere Systemanzeigen zu finden, die zu einer Problemdiagnose führen können
- Hilfsprogramme zur Problemlösung - beschreibt iDRAC6-Hilfsprogramme, die Sie zur Fehlerbehebung des Systems verwenden können
- Fehlerbehebung und häufig gestellte Fragen - Antworten 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 ein Problem im System vorliegen könnte.

LED-Anzeigen

LEDs am Gehäuse oder an im Gehäuse installierten Bauteilen liefern gewöhnlich die ersten Anzeichen von Systemproblemen. 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 17-1 beschreibt die Bedeutungen der LED-Anzeigen des PowerEdge-Servers:

Tabelle 17-1. 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 iDRAC6 funktioniert fehlerfrei.
blinkt gelb	Der iDRAC6 hat einen Fehlerzustand festgestellt oder aktualisiert gerade die Firmware.
blinkt blau	Ein Benutzer hat die Locator-ID für diesen Server aktiviert.

Anzeigen für Hardwareprobleme

Anzeichen dafür, dass bei einem Modul ein Hardwareproblem vorliegt, schließen folgende ein:

- Gerät kann nicht hochgefahren werden
- Laute Lüfter
- Verlust der Netzwerkkonnektivität
- Warnungen zu Batterie, Temperatur, Spannung oder 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 17-2. 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 iDRAC6-Protokoll	Siehe Das iDRAC6-Protokoll anzeigen".

Hilfsprogramme zum Lösen von Problemen

In diesem Abschnitt werden iDRAC6-Dienstprogramme beschrieben, die Sie zur Diagnose von Problemen im 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
- iDRAC6-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 iDRAC6-Webschnittstelle anmelden, beschreibt die erste angezeigte Seite den Zustand der Systemkomponenten. Tabelle 17-3 beschreibt die Bedeutung der Systemzustandsanzeigen.

Tabelle 17-3. 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 iDRAC6 und CMC enthalten nützliche Informationen zum aktuellen Status und zur Konfiguration.

Systemereignisprotokoll (SEL) überprüfen

Auf der Seite **SEL-Protokoll** werden Meldungen zu Ereignissen angezeigt, die auf dem verwalteten Server auftreten.

Führen Sie zum Anzeigen des **Systemereignisprotokolls** folgende Schritte aus:

1. Klicken Sie auf **System** und dann auf das Register **Protokolle**.

2. Klicken Sie auf **Systemereignisprotokoll**, um die Seite **Systemereignisprotokoll** aufzurufen.

   Die Seite **Systemereignisprotokoll** blendet eine Systemzustandsanzeige (siehe Tabelle 17-3), einen Zeitstempel sowie eine Beschreibung des Ereignisses ein.

3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Systemereignisprotokoll**, um fortzufahren (siehe Tabelle 17-4).

Tabelle 17-4. SEL-Schaltflächen

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** erneut.

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 17-3), einen Hexadezimalcode sowie eine Beschreibung des Codes ein.

2. Klicken Sie auf die entsprechende **POST-Code**-Schaltfläche, um fortzufahren (siehe Tabelle 17-5).

Tabelle 17-5. POST-Code-Schaltflächen

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

Bildschirm Letzter Systemabsturz anzeigen

ANMERKUNG: Die Funktion Bildschirm Letzter Absturz muss im Server Administrator und in der iDRAC6-Webschnittstelle konfiguriert werden. Anleitungen zum Konfigurieren dieser Funktion finden Sie unter "Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz".

Auf 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 iDRAC6 gespeichert und steht im Remote-Zugriff zur Verfügung.

Führen Sie zur Ansicht der Seite **Bildschirm Letzter Absturz** 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 17-6 gezeigten Schaltflächen auf:

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

Tabelle 17-6. Schaltflächen der Seite Bildschirm Letzter Absturz

Schaltfläche	Abhilfe
Drucken	Druckt die Seite **Bildschirm Letzter Absturz** aus.
Speichern	Öffnet ein Pop-Up-Fenster, das es Ihnen ermöglicht, die Seite **Bildschirm Letzter Absturz** in einem Verzeichnis Ihrer Wahl zu speichern.
Löschen	Löscht die Seite **Bildschirm Letzter Absturz.**
Aktualisieren	Lädt die Seite **Bildschirm Letzter Absturz** erneut.

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 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 Seite **Start-Capture** ansehen. Die Wiedergabe der Startbildschirme tritt mit einer Rate von 1 Frame pro Sekunde auf. Tabelle 17-7 führt die verfügbaren Steuerungsmaßnahmen auf.

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

Tabelle 17-7. 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 Seite Start-Capture neu.

Serverstatusbildschirm auf Fehlermeldungen überprüfen

Wenn eine gelbe LED zu blinken beginnt und ein bestimmter Server einen Fehler aufweist, hebt der Hauptserverstatusbildschirm auf dem LCD den betroffenen Server in orange hervor. Verwenden Sie die LCD-Navigationsschaltflächen, um den betroffenen Server hervorzuheben, 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 17-8. Serverstatus-Bildschirm

Severity	Meldung	Ursache
Warnung	System Board Ambient Temp: Temperature sensor for System Board, warning event (Umgebungstemperatur der Systemplatine: Temperatursensor für Systemplatine, Warnungsereignis)	Die Umgebungstemperatur des Servers hat einen Warnungsschwellenwert überschritten
Kritisch	System Board Ambient Temp: Temperature sensor for System Board, failure event (Umgebungstemperatur der Systemplatine: Temperatursensor für Systemplatine, Fehlerereignis)	Die Umgebungstemperatur des Servers hat einen Fehlerschwellenwert überschritten
Kritisch	System Board CMOS Battery: Battery sensor for System Board, failed was asserted (CMOS-Batterie der Systemplatine: Batteriesensor der Systemplatine, Ausfall bestätigt)	CMOS-Batterie nicht vorhanden oder weist keine Spannung auf
Warnung	System Board System Level: Current sensor for System Board, warning event (Systemebene der Systemplatine: Stromsensor für Systemplatine, Warnungsereignis)	Strom hat eine Warnungsschwelle überschritten
Kritisch	System Board System Level: Current sensor for System Board, failure event (Systemebene der Systemplatine: Stromsensor für Systemplatine, Fehlerereignis)	Strom hat eine Fehlerschwelle überschritten
Kritisch	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (CPU<Nummer> <Name des Spannungssensors>: Spannungssensor für CPU<Nummer>, bestätigter Zustand wurde bestätigt)	Spannung außerhalb des Bereichs
Kritisch	System Board <voltage sensor name>: Voltage sensor for System Board, state asserted was asserted (Systemplatine <Name des Spannungssensors>: Spannungssensor für Systemplatine, bestätigter Zustand wurde bestätigt)	Spannung außerhalb des Bereichs
Kritisch	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (CPU<Nummer> <Name des Spannungssensors>: Spannungssensor für CPU<Nummer>, bestätigter Zustand wurde bestätigt)	Spannung außerhalb des Bereichs
Kritisch	CPU<number> Status: Processor sensor for CPU<number, IERR was asserted (CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, IERR wurde bestätigt)	CPU-Fehler
Kritisch	CPU<number> Status: Processor sensor for CPU<number>, thermal tripped was asserted (CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, thermische Auslösung wurde bestätigt)	CPU überhitzt
Kritisch	CPU<number> Status: Processor sensor for CPU<number, configuration error was asserted (CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, Konfigurationsfehler wurde bestätigt)	Falscher Prozessortyp oder an falschem Ort
Kritisch	CPU<number> Status: Processor sensor for CPU<number>, presence was deasserted (CPU<Nummer> Status: Prozessorsensor für CPU<Nummer>, Bestätigung des Vorhandenseins wurde aufgehoben)	Erforderliche CPU fehlt oder ist nicht vorhanden.
Kritisch	System Board Video Riser: Module sensor for System Board, device removed was asserted (Video-Riser-Karte der Systemplatine: Modulsensor der Systemplatine, Entfernen des Geräts wurde bestätigt)	Erforderliches Modul wurde entfernt
Kritisch	Mezz B<slot number> Status: Add-in Card sensor for Mezz B<slot number>, install error was asserted (Mezz B<Steckplatznummer> Status: Add-In-Kartensensor für Mezz B<Steckplatznummer>, Installationsfehler wurde bestätigt)	Falsche Mezzaninkarte für E/A-Architektur installiert
Kritisch	Mezz C<slot number> Status: Add-in Card sensor for Mezz C<slot number>, install error was asserted (Mezz C<Steckplatznummer> Status: Add-In-Kartensensor für Mezz C<Steckplatznummer>, Installationsfehler wurde bestätigt)	Falsche Mezzaninkarte für E/A-Architektur installiert

Kritisch	Backplane Drive <number>: Drive Slot sensor for Backplane, drive removed (Rückwandplatine, Laufwerk <Nummer>: Laufwerksteckplatzsensor für Rückwandplatine, Laufwerk entfernt)	Speicherlaufwerk wurde entfernt
Kritisch	Backplane Drive <number>: Drive Slot sensor for Backplane, drive fault was asserted (Rückwandplatine, Laufwerk <Nummer>: Laufwerksteckplatzsensor für Rückwandplatine, Laufwerkfehler wurde bestätigt)	Speicherlaufwerk fehlerhaft
Kritisch	System Board PFault Fail Safe: Voltage sensor for System Board, state asserted was asserted (Systemplatine, PFault störsicher: Spannungssensor für Systemplatine, bestätigter Zustand wurde bestätigt)	Dieses Ereignis wird erstellt, wenn sich die Systemplatinenspannungen nicht im normalen Bereich befinden.
Kritisch	System Board OS Watchdog: Watchdog sensor for System Board, timer expired was asserted (Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, abgelaufener Zeitgeber wurde bestätigt)	Der iDRAC6-Watchdog-Zeitgeber ist abgelaufen und es wurde keine Maßnahme festgelegt.
Kritisch	System Board OS Watchdog: Watchdog sensor for System Board, reboot was asserted (Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, Neustart wurde bestätigt)	Der iDRAC6-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist), und die Maßnahme wurde auf Neustart festgelegt.
Kritisch	System Board OS Watchdog: Watchdog sensor for System Board, power off was asserted (Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, Ausschalten des Stroms wurde bestätigt)	Der iDRAC6-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist), und die Maßnahme wurde auf Ausschalten des Systems festgelegt.
Kritisch	System Board OS Watchdog: Watchdog sensor for System Board, power cycle was asserted (Systemplatinen-BS-Watchdog: Watchdog-Sensor für Systemplatine, Aus- und Einschalten des Stroms wurde bestätigt)	Der iDRAC6-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist), und die Maßnahme wurde auf Aus-/Einschalten des Systems festgelegt.
Kritisch	System Board SEL: Event Log sensor for System Board, log full was asserted (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 Corr Err: Memory sensor, correctable ECC (<DIMM Location>) was asserted (ECC, korrigierbarer Fehler: Speichersensor, korrigierbarer ECC (<DIMM-Position>) wurde bestätigt)	Korrigierbare ECC-Fehler haben eine kritische Rate erreicht.
Kritisch	ECC Uncorr Err: Memory sensor, uncorrectable ECC (<DIMM Location>) was asserted (ECC, nicht korrigierbarer Fehler: Speichersensor, nicht korrigierbarer ECC (<DIMM-Position>) wurde bestätigt)	Ein nicht korrigierbarer ECC-Fehler wurde festgestellt.
Kritisch	I/O Channel Chk: Critical Event sensor, I/O channel check NMI was asserted (E/A-Kanalüberprüfung: Sensor für kritische Ereignisse, E/A-Kanalüberprüfungs-NMI wurde bestätigt)	Im E/A-Kanal wird ein kritischer Interrupt erstellt.
Kritisch	PCI Parity Err: Critical Event sensor, PCI PERR was asserted (PCI-Paritätsfehler: Sensor für kritische Ereignisse, PCI PERR wurde bestätigt)	Auf dem PCI-Bus wurde ein Paritätsfehler festgestellt.
Kritisch	PCI System Err: Critical Event sensor, PCI SERR (<Slot number or PCI Device ID>) was asserted (PCI-Systemfehler: Sensor für kritische Ereignisse, PCI SERR (<Steckplatznummer oder PCI-Geräte-ID>) wurde bestätigt)	PCI-Fehler durch Gerät festgestellt
Kritisch	SBE Log Disabled: Event Log sensor, correctable memory error logging disabled was asserted (SBE-Protokoll deaktiviert: Ereignisprotokollsensor, Deaktivierung der Protokollierung korrigierbarer Speicherfehler wurde bestätigt)	Einzelbitfehler-Protokollierung wird deaktiviert, wenn zu viele SBE protokolliert werden
Kritisch	Logging Disabled: Event Log sensor, all event logging disabled was asserted (Protokollierung deaktiviert: Ereignisprotokollsensor, Deaktivierung der gesamten Ereignisprotokollierung wurde bestätigt)	Die gesamte Fehlerprotokollierung ist deaktiviert
Nicht wiederherstellbar	CPU Protocol Err: Processor sensor, transition to non-recoverable was asserted	Das Prozessorprotokoll ist in einen nicht wiederherstellbaren Zustand übergegangen.

	(CPU-Protokollfehler: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt)	
Nicht wiederherstellbar	CPU Bus PERR: Processor sensor, transition to non-recoverable was asserted (CPU-Bus-PERR: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt)	Der Prozessor-Bus-PERR ist in einen nicht wiederherstellbaren Zustand übergegangen
Nicht wiederherstellbar	CPU Init Err: Processor sensor, transition to non-recoverable was asserted (CPU-Initialisierungsfehler: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt)	Die Prozessorinitialisierung ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht wiederherstellbar	CPU Machine Chk: Processor sensor, transition to non-recoverable was asserted (CPU-Maschinenüberprüfung: Prozessorsensor, Übergang zu nicht wiederherstellbar wurde bestätigt)	Die Prozessormaschinenüberprüfung ist in einen nicht wiederherstellbaren Zustand übergegangen.
Kritisch	Memory Spared: Memory sensor, redundancy lost (<DIMM Location>) was asserted (Speicher reserviert: Speichersensor, Redundanz verloren (<DIMM-Position>) wurde bestätigt)	Speicherreserve ist nicht mehr redundant
Kritisch	Memory Mirrored: Memory sensor, redundancy lost (<DIMM Location>) was asserted (Speicher gespiegelt: Speichersensor, Redundanz verloren (<DIMM-Position>) wurde bestätigt)	Gespiegelter Speicher ist nicht mehr redundant
Kritisch	Memory RAID: Memory sensor, redundancy lost (<DIMM Location>) was asserted (Speicher-RAID: Speichersensor, Redundanz verloren (<DIMM-Position>) wurde bestätigt)	RAID-Speicher ist nicht mehr redundant
Warnung	Memory Added: Memory sensor, presence (<DIMM Location>) was deasserted (Speicher hinzugefügt: Speichersensor, Bestätigung des Vorhandenseins (<DIMM-Position>) wurde aufgehoben)	Hinzugefügtes Speichermodul wurde entfernt.
Warnung	Memory Removed: Memory sensor, presence (<DIMM Location>) was deasserted (Speicher entfernt: Speichersensor, Bestätigung des Vorhandenseins (<DIMM-Position>) wurde aufgehoben)	Speichermodul wurde entfernt.
Kritisch	Memory Cfg Err: Memory sensor, configuration error (<DIMM Location>) was asserted (Speicherkonfigurationsfehler: Speichersensor, Konfigurationsfehler (<DIMM-Position>) wurde bestätigt)	Falsche Speicherkonfiguration für das System
Warnung	Mem Redun Gain: Memory sensor, redundancy degraded (<DIMM Location>) was asserted (Speicherredundanz-Zunahme: Speichersensor, Redundanz herabgesetzt (<DIMM-Position>) wurde bestätigt)	Speicherredundanz ist herabgesetzt aber nicht verloren
Kritisch	PCIE Fatal Err: Critical Event sensor, bus fatal error was asserted (Schwerwiegender PCIE-Fehler: Sensor für kritische Ereignisse, schwerwiegender Busfehler wurde bestätigt)	Schwerwiegender Fehler auf dem PCIE-Bus festgestellt
Kritisch	Chipset Err: Critical Event sensor, PCI PERR was asserted (Chipset-Fehler: Sensor für kritische Ereignisse, PCI-PERR wurde bestätigt)	Chip-Fehler wurde festgestellt
Warnung	Mem ECC Warning: Memory sensor, transition to non-critical from OK (<DIMM Location>) was asserted (Speicher-ECC-Warnung: Speichersensor, Übergang zu nicht kritisch von OK (<DIMM-Position>) wurde bestätigt)	Die Rate der korrigierbaren ECC-Fehler geht über eine normale Rate hinaus.
Kritisch	Mem ECC Warning: Memory sensor, transition to critical from less severe (<DIMM Location>) was asserted (Speicher-ECC-Warnung: Speichersensor, Übergang zu kritisch von weniger schwerwiegend (<DIMM-Position>) wurde bestätigt)	Korrigierbare ECC-Fehler haben kritische Rate erreicht.
Kritisch	POST Err: POST sensor, No memory installed (POST-Fehler: POST-Sensor, Kein Speicher installiert)	Kein Speicher auf Platine festgestellt
Kritisch	POST Err: POST sensor, Memory configuration error (POST-Fehler: POST-Sensor, Speicherkonfigurationsfehler)	Speicher wurde erkannt, kann jedoch nicht konfiguriert werden.
Kritisch	POST Err: POST sensor, Unusable memory error (POST-Fehler: POST-Sensor, Fehler durch unbrauchbaren	Speicher wurde konfiguriert, ist jedoch unbrauchbar

	Speicher)	
Kritisch	POST Err: POST sensor, Shadow BIOS failed (POST-Fehler: POST-Sensor, Shadow-BIOS fehlerhaft)	System-BIOS, Shadow-Fehler
Kritisch	POST Err: POST sensor, CMOS failed (POST-Fehler: POST-Sensor, CMOS fehlerhaft)	CMOS-Fehler
Kritisch	POST Err: POST sensor, DMA controller failed (POST-Fehler: POST-Sensor, DMA-Controller fehlerhaft)	DMA-Controller-Fehler
Kritisch	POST Err: POST sensor, Interrupt controller failed (POST-Fehler: POST-Sensor, Interrupt-Controller fehlerhaft)	Interrupt-Controller-Fehler
Kritisch	POST Err: POST sensor, Timer refresh failed (POST-Fehler: POST-Sensor, Zeitgeberaktualisierung fehlerhaft)	Fehler bei der Zeitgeberaktualisierung
Kritisch	POST Err: POST sensor, Programmable interval timer error (POST-Fehler: POST-Sensor, Fehler bei programmierbarem Intervallzeitgeber)	Fehler beim programmierbaren Intervallzeitgeber
Kritisch	POST Err: POST sensor, Parity error (POST-Fehler: POST-Sensor, Paritätsfehler)	Paritätsfehler
Kritisch	POST Err: POST sensor, SIO failed (POST-Fehler: POST-Sensor, SIO fehlerhaft)	SIO-Fehler
Kritisch	POST Err: POST sensor, Keyboard controller failed (POST-Fehler: POST-Sensor, Tastatur-Controller fehlerhaft)	Tastatur-Controllerfehler
Kritisch	POST Err: POST sensor, System management interrupt initialization failed (POST-Fehler: POST-Sensor, Interrupt-Initialisierung der Systemverwaltung fehlerhaft)	Initialisierungsfehler bei Systemverwaltungs-Interrupt
Kritisch	POST Err: POST sensor, BIOS shutdown test failed (POST-Fehler: POST-Sensor, Test zum Herunterfahren des BIOS fehlerhaft)	Fehler beim BIOS-Herunterfahren-Test
Kritisch	POST Err: POST sensor, BIOS POST memory test failed (POST-Fehler: POST-Sensor, BIOS-POST-Speichertest fehlerhaft)	BIOS-POST-Speicherüberprüfungsfehler
Kritisch	POST Err: POST sensor, Dell remote access controller configuration failed (POST-Fehler: POST-Sensor, Konfiguration des Dell Remote Access Controller fehlerhaft)	Konfigurationsfehler bei Dell Remote Access Controller
Kritisch	POST Err: POST sensor, CPU configuration failed (POST-Fehler: POST-Sensor, CPU-Konfiguration fehlerhaft)	CPU-Konfigurationsfehler
Kritisch	POST Err: POST sensor, Incorrect memory configuration (POST-Fehler: POST-Sensor, Falsche Speicherkonfiguration)	Falsche Speicherkonfiguration
Kritisch	POST Err: POST sensor, POST failure (POST-Fehler: POST-Sensor, POST-Fehler)	Allgemeiner Fehler nach Video
Kritisch	Hdwar version err: Version Change sensor, hardware incompatibility was asserted (Hardwareversions-Fehler: Sensor für Versionsänderung, Hardware-Inkompatibilität wurde bestätigt)	Inkompatible Hardware wurde festgestellt
Kritisch	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware) was asserted (Hardwareversions-Fehler: Sensor für Versionsänderung, Hardware-Inkompatibilität (BMC-Firmware) wurde bestätigt)	Hardware ist inkompatibel mit Firmware
Kritisch	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware and CPU mismatch) was asserted (Hardwareversions-Fehler: Sensor für Versionsänderung, Hardware-Inkompatibilität (BMC-Firmware und CPU-Übereinstimmungsfehler) wurde bestätigt)	CPU und Firmware nicht kompatibel
Kritisch	Mem Overtemp: Memory sensor, correctable ECC <DIMM Location> was asserted (Speicherübertemperatur: Speichersensor, korrigierbarer ECC <DIMM-Position> wurde bestätigt)	Überhitzung des Speichermoduls

Kritisch	Mem Fatal SB CRC: Memory sensor, uncorrectable ECC was asserted (Speicher, SB-CRC schwerwiegend: Speichersensor, nicht korrigierbarer ECC wurde bestätigt)	Southbridge-Speicher fehlerhaft
Kritisch	Mem Fatal NB CRC: Memory sensor, uncorrectable ECC was asserted (Speicher, NB-CRC schwerwiegend: Speichersensor, nicht korrigierbarer ECC wurde bestätigt)	Northbridge-Speicher fehlerhaft
Kritisch	WatchDog Timer: Watchdog sensor, reboot was asserted (Watchdog-Zeitgeber: Watchdog-Sensor, Neustart wurde bestätigt)	Watchdog-Zeitgeber verursachte Systemneustart
Kritisch	WatchDog Timer: Watchdog sensor, timer expired was asserted (Watchdog-Zeitgeber: Watchdog-Sensor, Ablaufen des Zeitgebers wurde bestätigt)	Watchdog-Zeitgeber abgelaufen, jedoch keine Maßnahme ergriffen
Warnung	Link Tuning: Version Change sensor, successful software or F/W change was deasserted (Link Tuning: Versionsänderungsensor, eine erfolgreiche Software- oder F/W-Änderung wurde nicht bestätigt)	Link-Tuning-Einstellung für ordnungsgemäßen NIC-Betrieb konnte nicht aktualisiert werden
Warnung	Link Tuning: Version Change sensor, successful hardware change <device slot number> was deasserted (Link-Tuning: Sensor für Versionsänderung, Bestätigung der erfolgreichen Hardwareänderung <Gerätesteckplatznummer> wurde aufgehoben)	Link-Tuning-Einstellung für ordnungsgemäßen NIC-Betrieb konnte nicht aktualisiert werden
Kritisch	LinkT/FlexAddr: Link Tuning sensor, failed to program virtual MAC address (Bus # Device # Function #) was asserted (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	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or flex address (Mezz <location>) was asserted (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	LinkT/FlexAddr: Link Tuning sensor, failed to get link tuning or flex address data from BMC/iDRAC6 was asserted (Link-T/Flex-Adr: Link-Tuning-Sensor, Bestätigung, dass Daten zu Link-Tuning oder Flex-Adresse nicht vom BMC/iDRAC6 abgerufen werden konnten)	Informationen zu Link-Tuning oder Flex-Adresse konnten nicht vom BMC/iDRAC6 abgerufen werden
Kritisch	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or flex address (Mezz XX) was asserted (Link-T/Flex-Adr: Link-Tuning-Sensor, Bestätigung, dass Geräte-Options-ROM Link-Tuning oder Flex-Adresse (Mezz <Position>) nicht unterstützen konnte)	Dieses Ereignis wird erstellt, wenn der PCI-Geräte-Options-ROM für einen NIC weder die Funktion Link-Tuning noch die Flex-Adresse unterstützt.
Kritisch	LinkT/FlexAddr: Link Tuning sensor, failed to program the virtual MAC address (<location>) was asserted (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: Fatal IO Group sensor, fatal IO error (<location>) (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: Non Fatal I/O Group sensor, PCIe error (<location>) (PCIE NonFatal Er: Behebbarer E/A-Gruppensensor, PCIe-Fehler (<Position>))	Dieses Ereignis wird in Verbindung mit einem CPU-IERR erstellt.

Das iDRAC6-Protokoll anzeigen

Das **iDRAC6-Protokoll** ist ein dauerhaftes Protokoll, das in der iDRAC6-Firmware unterhalten wird. Das Protokoll enthält eine Liste von Benutzermaßnahmen (wie z. B. An- und Abmelden, Änderungen der Sicherheitsregeln) und Warnungen, die vom iDRAC6 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 iDRAC6 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 17-9 aufgeführten Informationen zur Verfügung.

Tabelle 17-9. iDRAC6-Protokollinformationen

Feld	Beschreibung
Uhrzeit/Datum	Datum und Uhrzeit (z. B. 19. Dez. 16:55:47). iDRAC6 stellt seine Uhr anhand der Uhr des verwalteten Servers ein. Wenn der iDRAC6 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 iDRAC6 angemeldet hat.

Die iDRAC6-Protokoll-Schaltflächen verwenden

Die Anzeige **iDRAC-Protokoll** enthält folgende Schaltflächen (siehe Tabelle 17-10).

Tabelle 17-10. iDRAC6-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** erneut.

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 17-11 und Tabelle 17-12 beschreiben die Eigenschaften des Hauptsystemgehäuses.

Tabelle 17-11. Systeminformationsfelder

Feld	Beschreibung
Beschreibung	Gibt eine Systembeschreibung.
BIOS-Version	Führt die System-BIOS-Version auf.
Service-Tag-Nummer	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 17-12. Felder der Autom. Wiederherstellung

Feld	Beschreibung
Wiederherstellungsmaßnahme	Wenn festgestellt wird, dass das *System hängt*, kann der iDRAC6 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 iDRAC6 eine Wiederherstellungsmaßnahme ausführt.
Vorhandener Countdown	Der aktuelle Wert, in Sekunden, des Countdown-Zeitgebers.

Integrierter Dell Remote Access Controller

Tabelle 17-13 beschreibt die Merkmale des iDRAC6.

Tabelle 17-13. Felder der iDRAC6-Protokollinformationen

Feld	Beschreibung
Uhrzeit/Datum	Zeigt das aktuelle Datum bzw. die aktuelle Uhrzeit auf dem iDRAC6 in MGZ an.
Firmware-Version	Listet die Version der iDRAC6-Firmware auf.
Aktualisierte Firmware	Führt das Datum der letzten Firmware-Aktualisierung auf. Das Datum wird im UTC-Format angezeigt, z. B.: Tue, 8 May 2007, 22:18:21 UTC.
IP-Adresse	Die 32-Bit-Adresse, die die Netzwerkschnittstelle identifiziert. Der Wert wird im *Punkttrennungs*-Format angezeigt, z. B. 143.166.154.127.
Gateway	Die IP-Adresse des Gateways, die als Brücke zu anderen Netzwerken dient. Dieser Wert wird im *Punkttrennungs*-Format angegeben, z. B. 143.166.150.5.
Subnetzmaske	Die Subnetzmaske identifiziert die Abschnitte einer IP-Adresse, bei denen es sich um das erweiterte Netzwerkpräfix und die Host-Nummer handelt. Der Wert wird im *Punkttrennungs*-Format angezeigt, z. B. 255.255.0.0.
MAC-Adresse	Die MAC-Adresse (Medienzugriffssteuerung), die jede NIC im Netzwerk eindeutig identifiziert, z. B. 00-00-0c-ac-08. Hierbei handelt es sich um eine von Dell zugewiesene ID, die nicht bearbeitet werden kann.
DHCP aktiviert	**Aktiviert** weist darauf hin, dass das dynamische Host-Konfigurationsprotokoll (DHCP) aktiviert ist. **Deaktiviert** weist darauf hin, dass DHCP *nicht* aktiviert ist.

Verwalteten Server im Gehäuse identifizieren

In das PowerEdge M1000e-Gehäuse können bis zu 16 Server eingebaut werden. Um einen bestimmten Server im Gehäuse ausfindig zu machen, können Sie mithilfe der iDRAC6-Webschnittstelle eine blaue, blinkende LED auf dem Server einschalten. 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 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 für **Server identifizieren** auf.
3. Klicken Sie auf **Anwenden**.

Diagnosekonsole verwenden

Der iDRAC6 bietet einen Standardsatz von Netzwerkdiagnose-Hilfsprogrammen (siehe Tabelle 17-14), die den mit Microsoft® Windows®- oder Linux-basierten Systemen gelieferten Hilfsprogrammen ähnlich sind. Mit der iDRAC6-Webschnittstelle können Sie auf die Hilfsprogramme zum Netzwerk-Debuggen zugreifen.

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 17-14 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 17-14. 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 iDRAC6 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 iDRAC6-Ablaufverfolgungsprotokoll an. Weitere Informationen finden Sie unter gettracelog".

Netzstrom auf einem Remote-System verwalten

Mit dem iDRAC6 können im Remote-Zugriff mehrere Energieverwaltungsmaßnahmen auf dem verwalteten Server durchgeführt werden. Verwenden Sie die Seite **Energieverwaltung**, um während eines Neustarts und beim 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 "iDRAC6-Benutzer hinzufügen und konfigurieren" finden Sie Hilfe 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 17-15 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 17-15.

Tabelle 17-15. 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. **ANMERKUNG:** Ein ordentliches Herunterfahren des BS des Servers kann u.U. nicht möglich sein, wenn die Serversoftware nicht länger reagiert oder wenn Sie nicht als Administrator auf einer lokalen Windows-Konsole angemeldet sind. In dem Fall müssen Sie einen Neustart erzwingen, anstatt eines ordentlichen Herunterfahrens von Windows. Außerdem ist, je nach Version des Windows-BS, womöglich eine Regel bezüglich des Herunterfahrens konfiguriert, die das Herunterfahrverhalten ändert, wenn die Maßnahme vom iDRAC6 ausgelöst wird. Ziehen Sie die Microsoft-Dokumentation zurate, um sich über die Richtlinie "Shutdown: Allow system to be shut down without having to login" (Herunterfahren: System ohne Anmeldung herunterfahren lassen) zu lokalen Computern zu informieren.
System zurücksetzen (Softwareneustart)	Startet das System neu, ohne es auszuschalten (Softwareneustart).
System aus- und wieder einschalten (Power Cycle)	Schaltet das System aus und startet es dann neu (Hardwareneustart).

Tabelle 17-16. Die Schaltflächen für die Energieverwaltung

Schaltfläche	Abhilfe
Drucken	Druckt die Werte der **Stromverwaltung** aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite **Energieverwaltung** erneut.
Anwenden	Speichert alle neuen Einstellungen, die Sie bei der Betrachtung der Seite Energieverwaltung vornehmen.

Fehlerbehebung und häufig gestellte Fragen

Tabelle 17-17 enthält häufig gestellte Fragen zu Problemen bei der Störungsbehebung.

Tabelle 17-17. Häufig gestellte Fragen/Fehlerbehebung

Frage	Antwort
Die LED auf dem Server blinkt gelb.	Überprüfen Sie das SEL auf Meldungen und löschen Sie das SEL dann, um die blinkende LED zu stoppen. Von der iDRAC6-Webschnittstelle aus: • Siehe Systemereignisprotokoll (SEL) überprüfen" Vom SM-CLP: • Siehe SEL-Verwaltung" Vom iDRAC6-Konfigurationsdienstprogramm aus: • 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 iDRAC6 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 iDRAC6-Konfigurationsdienstprogramm durch Drücken auf <Strg><E> ein ODER • Warten Sie darauf, dass die IP-Adresse während des BIOS-POST angezeigt wird. ODER • Wählen Sie zur Anmeldung über eine lokale serielle Verbindung am CMC im OSCAR die "Dell CMC"-Konsole aus. CMC-RACADM-Befehle können über diese Verbindung ausgegeben werden. Eine vollständige Liste der CMC-RACADM-Unterbefehle finden Sie im *CMC Firmware-Benutzerhandbuch*. Sie können auch den lokalen RACADM-Befehl **getsysinfo** verwenden, um die IP-Adresse des iDRAC6 anzuzeigen.
	Zum Beispiel: $ racadm getniccfg -m server-1 DHCP Enabled = 1 IP Adress = 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 iDRAC6-Webschnittstelle aus: • Klicken Sie auf **System**→ **Remote-Zugriff**→ **CMC**. Die CMC-IP-Adresse wird auf der Seite **Zusammenfassung** angezeigt. ODER

	• Wählen Sie zur Anmeldung über eine lokale serielle Verbindung am CMC im OSCAR die "Dell CMC"-Konsole aus. 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 Enable = 1 DHCP Enable = 1 Static IP Adress = 192.168.0.120 Static Subnet Mask = 255.255.255.0 Static Gateway = 192.168.0.1 Current IP Adress = 10.35.155.151 Current Subnet Mask = 255.255.255.0 Current Gateway = 10.35.155.1 Speed = Autonegotiate Duplex = Autonegotiate
Die iDRAC6-Netzwerkverbindung funktioniert nicht.	• Stellen Sie sicher, dass das LAN-Kabel am CMC angeschlossen ist. • Stellen Sie sicher, dass das iDRAC6-LAN aktiviert ist.
Ich habe den Server in das Gehäuse eingesetzt und den Netzschalter gedrückt, aber nichts ist passiert.	• Der iDRAC6 benötigt etwa 30 Sekunden, um initialisiert zu werden, bevor der Server hochgefahren werden 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 iDRAC6-Administrator vergessen.	Sie müssen die Standardeinstellungen des iDRAC6 wiederherstellen. 1. Starten Sie den Server neu und drücken Sie auf <Strg><E>, wenn Sie zur Eingabe des iDRAC6-Konfigurationsdienstprogramms aufgefordert werden. 2. Markieren Sie im Menü **Konfigurationsdienstprogramm** 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 die Registerkarte **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 iDRAC6-Webschnittstelle aus gestartet wird, erscheint ein ActiveX-Sicherheits-Popup.	Der iDRAC6 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 iDRAC6 einfach der Liste vertrauenswürdiger Sites hinzu: 1. Klicken Sie auf **Extras**→ **Internetoptionen...**→ **Sicherheit**→ **Vertrauenswürdige Sites**. 2. Klicken Sie auf **Sites** und geben Sie die IP-Adresse oder den DNS-Namen des iDRAC6 ein. 3. Klicken Sie auf **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 somit auf die Funktion des virtuellen Datenträgers zugreifen. Jedoch wird hierbei die Konsole des verwalteten Servers nicht angezeigt.
iDRAC6 startet nicht.	Enfernen Sie den Server und setzen Sie ihn erneut ein. Überprüfen Sie die CMC-Webschnittstelle, um zu sehen, ob der iDRAC6 als aktualisierbare Komponente erscheint. Ist dies der Fall, befolgen Sie die Anleitungen unter "Aktualisieren der iDRAC6-Firmware mittels CMC". 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 iDRAC6-Protokoll, von der iDRAC6-Webschnittstelle oder vom LCD.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Glossar

Integrierter Dell™ Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server Version 2.0 Benutzerhandbuch

Active Directory

Active Directory ist ein zentralisiertes, standardisiertes System zur Automatisierung der Netzwerkverwaltung von Benutzerdaten, Sicherheit und verteilten Ressourcen und macht die Zusammenarbeit mit anderen Verzeichnissen möglich. Active Directory richtet sich speziell auf dezentrale Netzwerkumgebungen aus.

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 iDRAC6 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 iDRAC6; 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 iDRAC6 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.

iDRAC6

Abkürzung für Dell Remote Access Controller 6 Enterprise.

iDRAC6

Akronym für Integrated Dell Remote Access Controller 6, das integrierte System-auf-Chip-Überwachungs-/Steuerungssystem für die Dell 10G-PowerEdge-Server.

IP

Abkürzung für Internet Protocol (Internet-Protokoll). Die Netzwerkschicht für TCP/IP. IP ermöglicht Paket-Routing, Fragmentierung und Reorganisation.

IPMB

Abkürzung für Intelligent Platform Management Bus (intelligenter Plattformverwaltungsbus), der ein in der Systemverwaltungstechnologie verwendeter Bus ist.

IPMI

Abkürzung für Intelligent Platform Management Interface (Intelligente Plattformverwaltungsschnittstelle). Ein Teil der Systemverwaltungstechnologie.

kBit/s

Abkürzung für Kilobits per Second (Kilobit pro Sekunde). Eine Datentransferrate.

Konsolenumleitung

Konsolenumleitung ist eine Funktion, die den Anzeigebildschirm sowie die Maus- und Tastaturfunktionen eines verwalteten Servers an die entsprechenden Komponenten einer Management Station weiterleitet. Die Systemkonsole der Management Station kann zur Steuerung des verwalteten Servers verwendet werden.

LAN

Abkürzung für Local Area Network (Lokales Netzwerk).

LDAP

Abkürzung für Lightweight Directory Access Protocol.

LED

Akronym für Light-Emitting Diode (Leuchtdiode).

LOM

Abkürzung für Local Area Network On Motherboard (Lokales Netz auf der Hauptplatine).

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 iDRAC6 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).

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 iDRAC6-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 Internetprotokollstandard zur Übertragung von Netzwerkschicht-Datagrammen (z. B. IP-Pakete) über serielle Punkt-zu-Punkt-Verbindungen.

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 in iDRAC6.

RAM-Platte

Ein speicherresidentes Programm, das ein Festplattenlaufwerk emuliert. iDRAC6 besitzt eine RAM-Platte im Speicher.

ROM

Akronym für Read-Only Memory (Nur-Lese-Speicher). Speicher, von dem Daten gelesen werden können, auf den jedoch keine Daten geschrieben werden können.

RPM

Abkürzung für Red Hat® Package Manager, der ein Paketverwaltungssystem für das Red Hat Enterprise Linux®-Betriebssystem ist, das bei der Installation von Softwarepaketen hilft. Es ist einem Installationsprogramm ähnlich.

SAC

Akronym für Microsoft Special Administration Console.

SAP

Abkürzung für Service Access Point (Service-Zugriffspunkt).

SEL

Akronym für System Event Log (Systemereignisprotokoll).

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 von iDRAC6 oder CMC erzeugte Meldung (Ereignis), die Informationen über Statusänderungen auf dem verwalteten System oder über mögliche Hardwarestörungen enthält.

SSH

Abkürzung für Secure Shell (Sichere Shell).

SSL

Abkürzung für Secure Sockets Layer (Sichere Sockelschicht).

Standardschema

Eine mit Active Directory verwendete Lösung zum Bestimmen von Benutzerzugriffen auf iDRAC6; 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.

TFTP

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

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 iDRAC6 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

Zurück zum Inhaltsverzeichnis

Version 2.0 Benutzerhandbuch

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

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

März 2009 Rev. A00

Zurück zum Inhaltsverzeichnis