Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

---

Anmerkungen und Hinweise

ANMERKUNG: Eine ANMERKUNG zeigt wichtige Informationen an, die Ihnen helfen, Ihren Computer effektiver einzusetzen.

HINWEIS: Ein HINWEIS zeigt entweder einen eventuellen Hardwareschaden oder Datenverlust an und weist darauf hin, wie das Problem vermieden werden kann.

Januar 2007 Rev. A00

Zurück zum Inhaltsverzeichnis

RACADM-Unterbefehlsübersicht

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

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

---

help

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **An DRAC 5 anmelden** haben.

In Tabelle A-1 wird der Unterbefehl **help** beschrieben.

Tabelle A-1. Befehl Help

Befehl	Definition
help	Listet alle verfügbaren Unterbefehle auf, die mit **racadm** verwendet werden und zeigt eine kurze Beschreibung für jeden Befehl an.

Zusammenfassung

```
racadm help

racadm help <Unterbefehl>
```

Beschreibung

Der Unterbefehl **help** listet alle Unterbefehle, die unter dem Befehl **racadm** verfügbar sind, zusammen mit einer einzeiligen Beschreibung auf. Es kann ebenfalls

ein Unterbefehl nach dem Befehl **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 zur Verwendung des angegebenen Unterbefehls an.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

arp

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **Diagnosebefehle ausführen** haben.

In Tabelle A-2 wird der Unterbefehl **arp** beschrieben.

Tabelle A-2. arp-Befehl

Befehl	Definition
arp	Zeigt den Inhalt der ARP-Tabelle an. ARP-Tabellen dürfen nicht hinzugefügt oder gelöscht werden.

Zusammenfassung

```
racadm arp
```

Unterstützte Schnittstellen

- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

clearasrscreen

ANMERKUNG: Um diesen Unterbefehl zu verwenden, müssen Sie die Berechtigung **Protokolle löschen** haben.

In Tabelle A-3 wird der Unterbefehl **clearasrscreen** beschrieben.

Tabelle A-3. clearasrscreen

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

Zusammenfassung

```
racadm clearasrscreen
```

Unterstützte Schnittstellen

- Lokaler RACADM

- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

config

ANMERKUNG: Zur Anwendung des Befehls **getconfig** müssen Sie die Berechtigung **An DRAC 5 anmelden** haben.

In Tabelle A-4 werden die Unterbefehle **config** und **getconfig** beschrieben.

Tabelle A-4. config / getconfig

Unterbefehl	Definition
config	Konfiguriert den DRAC 5.
getconfig	Erhält die DRAC 5-Konfigurationsdaten.

Zusammenfassung

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

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

Beschreibung

Mit dem Unterbefehl **config** kann der Benutzer die Konfigurationsparameter des DRAC 5 einzeln einstellen oder die Parameter stapelweise als Teil einer Konfigurationsdatei ausführen. Wenn sich die Daten unterscheiden, wird das DRAC 5-Objekt mit dem neuen Wert geschrieben.

Eingabe

In Tabelle A-5 werden die Unterbefehlsoptionen für **config** beschrieben.

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

Tabelle A-5. config-Unterbefehlsoptionen und -Beschreibungen

Option	Beschreibung
-f	Mit der Option **-f <Dateiname>** kann **config** den Inhalt der von **<Dateiname>** angegebenen Datei lesen und DRAC 5 konfigurieren. Die Datei muss Daten im "Parsing-Regeln" angegebenen Format enthalten.
-p	Die Option **-p** bzw. die Kennwortoption weist **config** an, die Kennworteinträge in der config-Datei **-f <Dateiname>** zu löschen, sobald die Konfiguration abgeschlossen wurde.
-g	Die Option **-g <Gruppenname>** bzw. die Gruppenoption muss zusammen mit der Option **-o** verwendet werden. Der <*Gruppenname*> gibt die Gruppe an, in der das einzustellende Objekt enthalten ist.
-o	Der **-o <Objektname> <Wert>** oder die Objektoption muss 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 Index-Option ist nur für indizierte Gruppen gültig und kann zur Angabe einer eindeutigen Gruppe verwendet werden. Der <*Index*> ist eine dezimale Ganzzahl von 1 bis 16. Der Index wird hier durch den Indexwert angegeben und nicht durch einen "Benennungs"-Wert.
-c	Die Option **-c** bzw. die Überprüfungsoption wird zusammen mit dem Unterbefehl **config** verwendet und ermöglicht dem Benutzer, die **.cfg**-Datei auf Syntaxfehler zu analysieren. Falls Fehler gefunden werden, wird die Zeilennummer zusammen mit einer kurzen Beschreibung des Fehlers angezeigt. Schreibvorgänge zum DRAC 5 kommen nicht 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 Gesamtobjekten in der **.cfg**-Datei befanden.

Beispiele

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

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

- `racadm config -f myrac.cfg`

  Konfiguriert oder konfiguriert den DRAC 5 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 Kennwortinformationen. Um diese Informationen in der Datei zu speichern, müssen sie manuell eingegeben werden. Wenn Sie Kennwort-Informationen von der **myrac.cfg**-Datei während der Konfiguration entfernen wollen, verwenden Sie die Option **-p**.

---

getconfig

Beschreibung des Unterbefehls getconfig

Mit dem Unterbefehl **getconfig** kann der Benutzer DRAC 5-Konfigurationsparameter einzeln oder alle RAC-Konfigurationsgruppen erhalten und sie in einer Datei speichern.

Eingabe

In Tabelle A-6 werden die Unterbefehlsoptionen für **getconfig** beschrieben.

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

Tabelle A-6. getconfig-Unterbefehlsoptionen

Option	Beschreibung
-f	Die Option **-f <*Dateiname*>** leitet getconfig an, die gesamte RAC-Konfiguration in eine Konfigurationsdatei zu schreiben. Diese Datei kann für Batch-Konfigurationsvorgänge verwendet werden, die den Unterbefehl **config** verwenden. **ANMERKUNG:** Die Option **-f** erstellt keine Einträge für die Gruppen **cfgIpmiPet** und **cfgIpmiPef**. Sie müssen mindestens ein Trap-Ziel einstellen, um die **cfgIpmiPet**-Gruppe zur Datei zu erfassen.
-g	Die Option **-g <*Gruppenname*>** oder **Gruppe** kann zur Anzeige der Konfiguration einer einzelnen Gruppe verwendet werden. Der **Gruppenname** ist der Name der Gruppe, die in den **racadm.cfg**-Dateien verwendet wird. Wenn es sich bei der Gruppe um eine indizierte Gruppe handelt, verwenden Sie die Option **-i**.
-h	Die Option **-h** oder **Hilfe** zeigt eine Liste aller vorhandenen Konfigurationsgruppen, die Sie verwenden können, an. Diese Option ist nützlich, wenn die genauen Gruppennamen nicht bekannt sind.
-i	Die Option **-i** <***Index***> oder **Index** ist nur für mit einem Inhaltsverzeichnis versehene Gruppen gültig und kann verwendet werden, um eine einzigartige Gruppe anzugeben. Der <*Index*> ist eine dezimale Ganzzahl von 1 bis 16. Wenn die Option **-i <***Index***>** nicht angegeben wird, wird ein Wert von 1 für Gruppen angenommen, wobei es sich um Tabellen mit mehreren Einträgen handelt. Der Index wird durch den Indexwert angegeben und nicht durch einen "Benennungs"-Wert.
-o	Der -o **<*Objektname*>** oder die Objektoption gibt den Objekt-Namen an, der in der Abfrage verwendet wird. Diese Option ist wahlweise und kann mit der Option -g verwendet werden.
-u	Die Option **-u <*Benutzername*>** oder **Benutzername** kann verwendet werden, um die Konfiguration für den angegebenen Benutzer anzuzeigen. Die Option **<*Benutzername*>** ist der Anmeldename des Benutzers.
-v	Die Option **-v** zeigt zusätzliche Details mit der Anzeige der Eigenschaften an und wird mit der Option **-g** verwendet.

Ausgabe

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

- Ungültige Syntax, ungültiger Gruppenname, Objektname, Index oder andere ungültige Datenbankmitglieder
- Racadm-Befehlszeilen-Dienstprogramm (CLI)-Fehler

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

Beispiele

- `racadm getconfig -g cfgLanNetworking`

  Anzeige aller Konfigurationseigenschaften (Objekte), die in der Gruppe **cfgLanNetworking** enthalten sind.

- `racadm getconfig -f myrac.cfg`

  Speichert alle Gruppenkonfigurationsobjekte vom RAC zu **myrac.cfg**.

- `racadm getconfig -h`

  Anzeige einer Liste der verfügbaren Konfigurationsgruppen auf dem DRAC 5.

- `racadm getconfig -u root`

  Zeigt die Konfigurationseigenschaften für den Benutzer 'root' an.

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

  Zeigt das Benutzergruppen-Beispiel an Index 2 mit wortreichen Informationen für die Eigenschaftswerte.

Zusammenfassung

`racadm getconfig -f <Dateiname>`

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

`racadm getconfig -u <Benutzername>`

`racadm getconfig -h`

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

coredump

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

In Tabelle A-7 wird der Unterbefehl **coredump** beschrieben.

Tabelle A-7. coredump

Unterbefehl	Definition
coredump	Zeigt den letzten Coredump des DRAC 5 an.

Zusammenfassung

`racadm coredump`

Beschreibung

Mit dem Unterbefehl **coredump** werden detaillierte Informationen bezüglich vor Kurzem aufgetretener kritischer Probleme am RAC angezeigt. Die coredump-Informationen können zur Diagnose dieser kritischen Probleme eingesetzt werden.

Wenn verfügbar, sind die coredump-Informationen beständig über Betriebs-Zyklen des RAC und werden verfügbar bleiben, bis eine der folgenden Bedingungen eintritt:

- Die coredump-Informationen werden mit dem Unterbefehl **coredumpdelete** gelöscht.
- Eine andere kritische Bedingung tritt auf dem RAC ein. In diesem Fall beziehen sich die coredump-Informationen auf den zuletzt aufgetretenen kritischen Fehler.

Der Unterbefehl **coredumpdelete** enthält weitere Informationen über das Löschen des **coredump**.

Unterstützte Schnittstellen

- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

coredumpdelete

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

In Tabelle A-8 wird der Unterbefehl **coredumpdelete** beschrieben.

Tabelle A-8. coredumpdelete

Unterbefehl	Definition
coredumpdelete	Löscht den im DRAC 5 gespeicherten Coredump.

Zusammenfassung

```
racadm coredumpdelete
```

Beschreibung

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

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

Weitere Information über die Ansicht eines Coredump finden Sie im Unterbefehl **coredump**.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

fwupdate

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

ANMERKUNG: Bevor Sie mit der Firmware-Aktualisierung beginnen, sollten Sie die zusätzlichen Anleitungen unter "DRAC 5-Firmware aktualisieren" beachten.

In Tabelle A-9 wird der Unterbefehl **fwupdate** beschrieben.

Tabelle A-9. fwupdate

Unterbefehl	Definition
fwupdate	Aktualisiert die Firmware des DRAC 5.

Zusammenfassung

```
racadm fwupdate -s

racadm fwupdate -g -u -a <TFTP_Server_IP_Address> -d <Pfad>

racadm fwupdate -p -u -d <Pfad>
```

Beschreibung

Mit dem Unterbefehl **fwupdate** können Benutzer die Firmware auf dem DRAC 5 aktualisieren. Der Benutzer kann:

- Den Status des Firmware-Aktualisierungsverfahrens prüfen
- DRAC 5-Firmware von einem TFTP-Server durch Angabe einer IP-Adresse und eines optionalen Pfads aktualisieren
- DRAC 5-Firmware vom lokalen Dateisystem mittels lokalem RACADM aktualisieren

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

Eingabe

In Tabelle A-10 werden die Unterbefehlsoptionen für **fwupdate** beschrieben.

ANMERKUNG: Die Option **-p** Option wird nur in lokalem RACADM unterstützt, nicht mit der seriell/telnet/ssh-Konsole.

Tabelle A-10. fwupdate-Unterbefehlsoptionen

Option	Beschreibung
-u	Die Option **Aktualisierung** führt einen Prüfsummentest der Firmware-Aktualisierungsdatei durch und startet das aktuelle Aktualisierungsverfahren. Diese Option kann zusammen mit Optionen **-g** oder **-p** verwendet werden. Nach der Aktualisierung führt der DRAC 5 einen weichen Reset durch.
-s	Die Option **Status** kehrt zum derzeitigen Status des Vorgangs im Aktualisierungsverfahren zurück. Diese Option wird immer allein verwendet.
-g	Die Option **get** weist die Firmware an, die Firmware-Aktualisierungsdatei vom TFTP-Server abzurufen. Der Benutzer muss auch die Optionen **-a** und **-d** angeben. Ohne die Option **-a** werden die Standardeinstellungen der Eigenschaften in der Gruppe **cfgRemoteHosts** gelesen, wobei die Eigenschaften **cfgRhostsFwUpdateIpAddr** und **cfgRhostsFwUpdatePath** verwendet werden.
-a	Die Option **IP-Adresse** gibt die IP-Adresse des TFTP-Servers an.
-d	Die Option **-d** oder **Verzeichnis** bestimmt das Verzeichnis auf dem TFTP-Server oder auf dem Host-Server des DRAC 5, wo sich die Firmware-Aktualisierungsdatei befindet.
-p	Die Option **-p** oder **put** wird zum Aktualisieren der Firmwaredatei vom verwalteten System zum DRAC 5 verwendet. Die Option **-u** muss zusammen mit der Option **-p** verwendet werden.

Ausgabe

Zeigt durch eine Meldung an, welcher Vorgang ausgeführt wird.

Beispiele

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

  In diesem Beispiel wird die Firmware durch die Option **-g** angewiesen, die Firmware-Aktualisierungsdatei von einem Speicherort (durch die Option **-d** angegeben) auf dem TFTP-Server unter einer bestimmten IP-Adresse (durch die Option **-a** angegeben) herunterzuladen. Nachdem die Abbilddatei vom TFTP Server heruntergeladen ist, beginnt das Update-Verfahren. Wenn dies abgeschlossen ist, wir der DRAC 5 zurückgesetzt.

  Wenn der Download länger als 15 Minuten dauert und das Zeitlimit überschreitet, übertragen Sie das Firmware-Flash-Image auf ein lokales Laufwerk auf dem Server. Stellen Sie dann anhand der Konsolenumleitung eine Verbindung zum Remote-System her, und nehmen Sie unter Verwendung des lokalen RACADM eine lokale Installation der Firmware vor.

- `racadm fwupdate -s`

  Diese Option liest den derzeitigen Status der Firmware-Aktualisierung.

- `racadm fwupdate -p -u -d c:\ <Images>`

  In diesem Beispiel wird das Firmware-Image für die Aktualisierung vom Dateisystem des Hosts geliefert.

- `racadm -r 192.168.0.120 -u root -p racpassword fwupdate -g -u -a 192.168.0.120 -d <Images>`

  In diesem Beispiel wird RACADM verwendet, um im Remote-Zugriff mit dem vorgegebenen DRAC-Benutzernamen und Kennwort die Firmware eines angegebenen DRAC zu aktualisieren. Das Abbild wird von einem TFTP Server abgerufen.

ANMERKUNG: Die Option **-p** wird in der Remote-RACADM-Schnittstelle für den Unterbefehl fwupdate nicht unterstützt.

---

getssninfo

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **An DRAC 5 anmelden** haben.

In Tabelle A-11 wird der Unterbefehl **getssninfo** beschrieben.

Tabelle A-11. Unterbefehl getssninfo

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

Zusammenfassung

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

Beschreibung

Mit dem Befehl **getssninfo** erhält man eine Liste von mit dem DRAC verbundenen Benutzern. Die zusammenfassenden Informationen geben die folgende Auskunft:

- Benutzername
- IP-Adresse (wenn anwendbar)
- Sitzungstyp (Beispiel: seriell oder Telnet)
- Konsolen im Gebrauch (Beispiel: Virtueller Datenträger oder Virtueller KVM)

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

Eingabe

In Tabelle A-12 werden die Unterbefehlsoptionen für **getssninfo** beschrieben.

Tabelle A-12. getssninfo-Unterbefehl - Optionen

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

Beispiele

- `racadm getssninfo`

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

Tabelle A-13. Ausgabebeispiel für den Unterbefehl getssninfo

Benutzer	IP-Adresse	Typ	Konsolen
root	192.168.0.10	Telnet	Virtueller KVM

- `racadm getssninfo -A`

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

- `racadm getssninfo -A -u *`

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

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

---

getsysinfo

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **An DRAC 5 anmelden** haben.

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

Tabelle A-14. getsysinfo

Befehl	Definition
getsysinfo	Zeigt DRAC 5-Informationen, Systeminformationen und Watchdog-Statusinformationen an.

Zusammenfassung

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

Beschreibung

Mit dem Unterbefehl **getsysinfo** werden Informationen bezüglich RAC-, verwaltetes System- und Watchdog-Konfiguration angezeigt.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

Eingabe

In Tabelle A-15 werden die Unterbefehlsoptionen für **getsysinfo** beschrieben.

Tabelle A-15. getsysinfo-Unterbefehlsoptionen

Option	Beschreibung
-d	Anzeige von DRAC 5-Informationen.
-s	Zeigt Systeminformationen an
-w	Zeigt Watchdog-Informationen an.
-A	Unterdrückt das Drucken von Kopfzeilen und Beschriftungen.

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

Ausgabe

Mit dem Unterbefehl **getsysinfo** werden Informationen bezüglich RAC-, verwaltetes System- und Watchdog-Konfiguration angezeigt.

Beispielausgabe

```
RAC Information:
RAC Date/Time            = Thu Dec 8 20:01:33 2005
Firmware Version         = 1.0
Firmware Build           = 05.12.08
Last Firmware Update     = Thu Dec 8 08:09:36 2005

Hardware Version         = A00
Current IP Address       = 192.168.0.120
Current IP Gateway       = 192.168.0.1
Current IP Netmask       = 255.255.255.0
DHCP Enabled             = 0
MAC Address              = 00:14:22:18:cd:f9
Current DNS Server 1     = 0.0.0.0
Current DNS Server 2     = 0.0.0.0
DNS Servers from DHCP    = 0
Register DNS RAC Name    = 0
DNS RAC Name             = rac-48192
Current DNS Domain       =

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

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

Beispiele

- `racadm getsysinfo -A -s`

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

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

- `racadm getsysinfo -w -s`

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


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

Einschränkungen

Die Felder Hostname und BS-Name in der **getsysinfo**-Anzeige enthalten nur genaue Informationen, wenn Dell OpenManage auf dem verwalteten System installiert wird. Wenn OpenManage auf dem verwalteten System nicht installiert ist, können diese Felder leer oder fehlerhaft sein.

---

getractime

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **An DRAC 5 anmelden** haben.

In Tabelle A-16 wird der Unterbefehl **getractime** beschrieben.

Tabelle A-16. getractime

Unterbefehl	Definition
getractime	Zeigt die aktuelle Uhrzeit vom Fernzugriff-Controller 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 *jjjjmmttssmmss.mmmmmms* an. Dieses Format wird auch vom UNIX-Befehl **date** zurückgegeben.

Ausgabe

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

Beispielausgabe

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20051208201542.000000
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

ifconfig

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **Protokolle löschen** oder **DRAC 5 konfigurieren** haben.

In Tabelle A-17 wird der Unterbefehl **ifconfig** beschrieben.

Tabelle A-17. ifconfig

Unterbefehl	Definition
ifconfig	Zeigt den Inhalt der Netzschnittstellentabelle an.

Zusammenfassung

```
racadm ifconfig
```

---

netstat

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **Diagnosebefehle ausführen** haben.

In Tabelle A-18 wird der Unterbefehl **netstat** beschrieben.

Tabelle A-18. netstat

Unterbefehl	Definition
netstat	Anzeige der Routingtabelle und der aktuellen Verbindungen.

Zusammenfassung

```
racadm netstat
```

Unterstützte Schnittstellen

- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

ping

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **Diagnostische Befehle ausführen** oder **DRAC 5 konfigurieren** haben.

In Tabelle A-19 wird der Unterbefehl **ping** beschrieben.

Tabelle A-19. ping

Unterbefehl	Definition
ping	Prüft nach, ob die Ziel-IP-Adresse vom DRAC 5 mit dem aktuellen Routing-Tabelleninhalt erreichbar ist. Eine Ziel-IP-Adresse ist erforderlich. Ein ICMP-Echo-Paket wird zur Ziel-IP-Adresse gesendet, basierend auf dem Inhalt der aktuellen Routing-Tabelle.

Zusammenfassung

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

Unterstützte Schnittstellen

- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

setniccfg

ANMERKUNG: Zur Anwendung des Befehls **setniccfg** müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

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

Tabelle A-20. setniccfg

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

ANMERKUNG: Die Begriffe NIC und Ethernet-Verwaltungsanschluss können gegeneinander ausgetauscht werden.

Zusammenfassung

```
racadm setniccfg -d

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

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

Beschreibung

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

- Die Option **-d** aktiviert DHCP für den Ethernet-Verwaltungsanschluss (Standardeinstellung ist 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
  ```

- Die Option **-o** deaktiviert den Ethernet-Verwaltungsanschluss vollständig. <*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 angemessene Fehlermeldung angezeigt, wenn der Vorgang erfolglos ist. Wenn erfolgreich, wird eine Meldung angezeigt.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

getniccfg

ANMERKUNG: Zur Anwendung des Befehls **getniccfg** müssen Sie die Berechtigung **An DRAC 5 anmelden** haben.

In Tabelle A -21 werden die Unterbefehle **setniccfg** und **getniccfg** beschrieben.

Tabelle A-21. setniccfg / getniccfg

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

Zusammenfassung

```
racadm getniccfg
```

Beschreibung

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

Beispielausgabe

Mit dem Unterbefehl **getniccfg** wird eine entsprechende Fehlermeldung angezeigt, wenn der Vorgang nicht erfolgreich ist. Ansonsten wird die Ausgabe im folgenden Format angezeigt:

```
NIC Enabled     = 1

DHCP Enabled    = 1
```

```
IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

getsvctag

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **An DRAC 5 anmelden** haben.

In Tabelle A-22 wird der Unterbefehl **getsvctag** beschrieben.

Tabelle A-22. getsvctag

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

Zusammenfassung

```
racadm getsvctag
```

Beschreibung

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

Beispiel

Geben Sie getsvctag an der Befehlsaufforderung ein. Die Ausgabe lautet wie folgt:

```
Y76TP0G
```

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

racdump

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

In Tabelle A-23 wird der Unterbefehl **racdump** beschrieben.

Tabelle A-23. racdump

Unterbefehl	Definition

racdump	Zeigt Status- und allgemeine Informationen zum DRAC 5 und zum System an.

Zusammenfassung

```
racadm racdump
```

Beschreibung

Der Unterbefehl **racdump** ist ein einziger Befehl, mit dem ein Dump, der Status und allgemeine DRAC 5-Platineninformationen bezogen werden können.

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

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

Unterstützte Schnittstellen

- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

racreset

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

In Tabelle A-24 wird der Unterbefehl **racreset** beschrieben.

Tabelle A-24. racreset

Unterbefehl	Definition
racreset	Stellt den DRAC 5 neu ein.

HINWEIS: Wenn Sie einen racreset-Unterbefehl ausgeben, kann der DRAC bis zu eine Minute beanspruchen, bis er zu einem verwendbaren Zustand zurückkehrt.

Zusammenfassung

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

Beschreibung

Der Unterbefehl **racreset** gibt einen Reset zum DRAC 5 aus. Das Reset-Ereignis wird in das DRAC 5-Protokoll eingetragen.

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

HINWEIS: Das System muss nach einem Hardware-Reset des DRAC 5 neu gestartet werden, wie in Tabelle A-25 beschrieben.

In Tabelle A-25 werden die Unterbefehlsoptionen für **racreset** beschrieben.

Tabelle A-25. fracreset-Unterbefehlsoptionen

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

soft	Ein *Software*-Reset führt einen ordentlichen Neustart auf dem RAC aus.

Beispiele

- `racadm racreset`

  Beginnen Sie den DRAC 5 Software-Reset-Vorgang.

- `racadm racreset hard`

  Beginnen Sie den DRAC 5 Hardware-Reset-Vorgang.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

racresetcfg

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

In Tabelle A-26 wird der Unterbefehl **racresetcfg** beschrieben.

Tabelle A-26. racresetcfg

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

Zusammenfassung

```
racadm racresetcfg
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

Beschreibung

Der Befehl **racresetcfg** entfernt alle Eigenschaften-Einträge der Datenbank, die vom Benutzer konfiguriert wurden. Die Datenbank besitzt Standard-Eigenschaften für alle Einträge, die zur Wiederherstellung der ursprünglichen Standardeinstellungen der Karte verwendet werden. Nach dem Zurücksetzen der Datenbank-Eigenschaften wird der DRAC 5 automatisch zurückgesetzt.

HINWEIS: Mit diesem Befehl wird die aktuelle RAC-Konfiguration gelöscht und der RAC und die serielle Konfiguration werden auf die ursprünglichen Standardeinstellungen zurückgesetzt. Nach dem Reset sind Standardname und -kennwort **root** und **calvin**, und die IP-Adresse ist 192.168.0.120. Wenn Sie den Befehl **racresetcfg** von einem Netzwerk-Client (z. B. einem unterstützten WWW-Browser, telnet/ssh oder Remote-RACADM), ausgeben, müssen Sie die Standardeinstellungs-IP-Adresse verwenden.

ANMERKUNG: Mit diesem Unterbefehl wird auch die serielle Schnittstelle auf ihre Standard-Baudrate (57600) und COM-Anschluss zurückgesetzt. Die seriellen Einstellungen müssen u. U. über den BIOS-Setup-Bildschirm für den Server neu konfiguriert werden, um über den seriellen Anschluss auf den RAC zuzugreifen.

---

serveraction

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **Serversteuerungsbefehle ausführen** haben.

In Tabelle A-27 wird der Unterbefehl **serveraction** beschrieben.

Tabelle A-27. serveraction

Unterbefehl	Definition
serveraction	Führt einen Reset des verwalteten Systems oder einen Einschalten/Ausschalten-Zyklus durch.

Zusammenfassung

```
racadm serveraction <Maßnahme>
```

Beschreibung

Der Unterbefehl serveraction ermöglicht Benutzern, Stromverwaltungsvorgänge auf dem Hostrechner auszuführen. Tabelle A-28 beschreibt die **serveraction** Stromsteuerungsoptionen.

Tabelle A-28. serveraction-Unterbefehlsoptionen

Zeichenkette	Definition
<*Maßnahme***>**	Bestimmt die Maßnahme. Die Optionen für die Zeichenkette <*Maßnahme*> sind: • **powerdown** - Fährt das verwaltete System herunter. • **powerup** - Fährt das verwaltete System hoch. • **powercycle** - Leitet einen Ein-/Ausschaltvorgang auf dem verwalteten System ein. Diese Maßnahme ist dem Drücken des Netzschalters auf der Systemvorderseite ähnlich, um das System aus- und dann wieder einzuschalten. • **powerstatus** - Zeigt den aktuellen Stromstatus des Servers ("ON" oder "OFF") an • **hardreset** - Führt einen Reset (Neustart) auf dem verwalteten System aus.

Ausgabe

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

getraclog

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **An DRAC 5 anmelden** haben.

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

Tabelle A-29. getraclog

Befehl	Definition
getraclog -i	Zeigt die Anzahl der Einträge im DRAC 5-Protokoll an.
getraclog	Zeigt die DRAC 5 Protokoll-Einträge an.

Zusammenfassung

```
racadm getraclog-i

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

Beschreibung

Der Befehl **getraclog -i** zeigt die Anzahl der Einträge im DRAC 5-Protokoll an.

Im Folgenden werden Optionen für den Befehl **getraclog** zum Lesen von Einträgen aufgeführt:

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

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

Ausgabe

Die Standardausgabe-Anzeige enthält die Datensatznummer, Quelle, und Beschreibung. Der Zeitstempel beginnt um Mitternacht, dem 1. Januar, und nimmt so lange zu, bis das System startet. Nachdem das System gestartet wurde, wird der Zeitstempel des Systems vorgenommen.

Beispielausgabe

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

clrraclog

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

Zusammenfassung

```
racadm clrraclog
```

Beschreibung

mit dem **clrraclog**-Unterbefehl werden alle vorhandenen Aufzeichnungen vom RAC-Protokoll entfernt. Ein neuer Einzeldatensatz wird zur Aufzeichnung von Datum und Zeit des Löschens des Protokolls entfernt.

---

getsel

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **An DRAC 5 anmelden** haben.

In Tabelle A-30 wird der Unterbefehl **getsel** beschrieben.

Tabelle A-30. getsel

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

Zusammenfassung

```
racadm getsel-i

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

Beschreibung

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

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

-A - setzt die Ausgabe auf keine Kopfzeile oder Etiketten.

-c - Zeigt die maximale Anzahl der zurückzugebenden Einträge an.

-o - Zeigt die Ausgabe in einer einzelnen Zeile an.

-s - Gibt den für die Anzeige verwendeten Startdatensatz an

-E - Platziert die 16 Byte des reinen SEL an das Ende jeder Ausgabezeile als Sequenz von hexadezimalen Werten.

-R - Es werden nur die reinen Daten ausgegeben.

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

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

Ausgabe

Die Standardausgabe-Anzeige enthält Datensatznummer, Zeitstempel, Schweregrad, und Beschreibung.

Beispiel:

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

clrsel

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

Zusammenfassung

```
racadm clrsel
```

Beschreibung

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

- telnet/ssh/seriell-RACADM

---

gettracelog

ANMERKUNG: Zur Anwendung dieses Befehls müssen Sie die Berechtigung **An DRAC 5 anmelden** haben.

In Tabelle A-31 wird der Unterbefehl **gettracelog** beschrieben.

Tabelle A-31. gettracelog

Befehl	Definition
gettracelog -i	Zeigt die Anzahl der Einträge im DRAC 5-Ablaufverfolgungsprotokoll an.
gettracelog	Zeigt das DRAC 5-Ablaufverfolgungsprotokoll.

Zusammenfassung

```
racadm gettracelog-i

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

Beschreibung

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

-i - Zeigt die Anzahl von Einträgen im DRAC 5 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 Datensätzen zur Anzeige an

-s - gibt den anzuzeigenden Startdatensatz an

-A - Kopfzeilen oder Etiketten nicht anzeigen

Ausgabe

Die Standardausgabe-Anzeige enthält Datensatznummer, Zeitstempel, Schweregrad, und Beschreibung. Der Zeitstempel beginnt um Mitternacht, dem 1. Januar, und nimmt so lange zu, bis das System startet. Nachdem das System gestartet wurde, wird der Zeitstempel des Systems vorgenommen.

Beispiel:

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

sslcsrgen

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

In Tabelle A-32 wird der Unterbefehl **sslcsrgen** beschrieben.

Tabelle A-32. sslcsrgen

Unterbefehl	Beschreibung
sslcsrgen	Erstellt und lädt eine SSL Zertifikatssignierungsanforderung (CSR) vom RAC herunter.

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. Der CSR kann zum Erstellen eines kundenspezifischen SSL-Zertifikat verwendet werden, das für SSL-Transaktionen auf dem RAC verwendet werden kann.

Optionen

ANMERKUNG: Die Option **-f** wird für die seriell/telnet/ssh-Konsole nicht unterstützt.

In Tabelle A-33 werden die Unterbefehlsoptionen für **sslcsrgen** beschrieben.

Tabelle A-33. sslcsrgen-Unterbefehlsoptionen

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

ANMERKUNG: Wenn die Option **-f** nicht angeben wird, geht der Dateiname automatisch auf **sslcsr** in dem aktuellen Verzeichnis.

Wenn keine Optionen angegeben werden, wird ein 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 im Gange.

Einschränkungen

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

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

Beispiele

```
racadm sslcsrgen -s

oder

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

sslcertupload

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

In Tabelle A-34 wird der Unterbefehl **sslcertupload** beschrieben.

Tabelle A-34. sslcertupload

Unterbefehl	Beschreibung
sslcertupload	Lädt einen kundenspezifischen SSL-Server oder CA-Zertifikat vom Client zum RAC hoch.

Zusammenfassung

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

Optionen

In Tabelle A-35 werden die Unterbefehlsoptionen für **sslcertupload** beschrieben.

Tabelle A-35. sslcertupload-Unterbefehlsoptionen

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 0 zurück.

Einschränkungen

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

Beispiel

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

sslcertdownload

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

In Tabelle A-36 wird der Unterbefehl **sslcertdownload** beschrieben.

Tabelle A-36. sslcertdownload

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

Zusammenfassung

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

Optionen

In Tabelle A-37 werden die Unterbefehlsoptionen für **sslcertdownload** beschrieben.

Tabelle A-37. sslcertdownload-Unterbefehlsoptionen

Option	Beschreibung
-t	Gibt den Typ des herunterzuladenden Zertifikats an, entweder das Microsoft® Active Directory® Zertifikat oder das Server-Zertifikat. 1 = Server-Zertifikat 2 = Microsoft Active Directory-Zertifikat
-f	Gibt den Dateinamen des hochzuladenden Zertifikats an. Wenn die **-f** Option 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 0 zurück.

Einschränkungen

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

Beispiel

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

sslcertview

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

In Tabelle A-38 wird der Unterbefehl **sslcertview** beschrieben.

Tabelle A-38. sslcertview

Unterbefehl	Beschreibung
sslcertview	Zeigt den SSL Server oder das CA-Zertifikat an, der/das auf dem RAC besteht.

Zusammenfassung

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

Optionen

In Tabelle A-39 werden die Unterbefehlsoptionen für **sslcertview** beschrieben.

Tabelle A-39. sslcertview-Unterbefehlsoptionen

Option	Beschreibung
-t	Gibt den Typ des herunterzuladenden Zertifikats an, entweder das Microsoft Active Directory-Zertifikat oder das Server-Zertifikat. 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)          : DRAC5 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)          : DRAC5 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
DRAC5 default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
DRAC5 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

testemail

In Tabelle A-40 wird der Unterbefehl **testemail** beschrieben.

Tabelle A-40. Test-E-Mail-Konfiguration

Unterbefehl	Beschreibung
testemail	Prüft die Alarmfunktion der RAC-E-Mail.

Zusammenfassung

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

Beschreibung

Sendet eine Test-E-Mail vom RAC an ein vorgegebenes Ziel.

Stellen Sie vor der Durchführung des Test-E-Mail-Befehls sicher, dass der angegebene Index in der RACADM **cfgEmailAlert**-Gruppe aktiviert und ordnungsgemäß konfiguriert wird. Tabelle A-41 enthält eine Liste und zugehörige Befehle für die **cfgEmailAlert-**Gruppe.

Tabelle A-41. Test-E-Mail-Konfiguration

Maßnahme	Befehl
Aktivieren Sie die Warnung	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
Stellen Sie die Ziel-E-Mail-Adresse ein	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com
Stellen Sie die kundenspezifische Meldung ein, die zur Ziel-E-Mail-Adresse gesendet wird	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "Dies ist ein Test! "
Stellen Sie sicher, dass die SNMP-IP-Adresse korrekt konfiguriert wird	racadm config -g cfgRemoteHosts -o cfgRhostsSmptServerIpAddr -i 192.168.0.152
Die aktuellen E-Mail-Warnungseinstellungen ansehen	racadm getconfig -g cfgEmailAlert -i <*Index*> wo <*Index*> ist eine Zahl zwischen 1 und 4

Optionen

In Tabelle A-42 werden die Unterbefehlsoptionen für **testemail** beschrieben.

Tabelle A-42. Test-E-Mail-Unterbefehle

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

Ausgabe

Keine.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

testtrap

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

In Tabelle A-43 wird der Unterbefehl **testtrap** beschrieben.

Tabelle A-43. testtrap

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

Zusammenfassung

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

Beschreibung

Mit dem Unterbefehl **testtrap** wird die Trap-Warnungsfunktion des RAC-SNMP geprüft, indem ein Testtrap vom RAC an einen festgelegten Zieltrap-Hörer auf dem Netzwerk gesendet wird.

Bevor Sie den **testtrap**-Unterbefehl ausführen, stellen Sie sicher, dass der angegebene Index in der RACADM-**cfgIpmiPet**-Gruppe korrekt konfiguriert ist.

Tabelle A-41 enthält eine Liste und zugehörige Befehle für die **cfgIpmiPet**-Gruppe.

Tabelle A-44. CfgEmailAlert-Befehle

Maßnahme	Befehl
Aktivieren Sie die Warnung	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
Ziel-E-Mail IP-Adresse einstellen	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110
Aktuelle Testtrap-Einstellungen ansehen	racadm getconfig -g cfgIpmiPet -i <*Index*> wo <*Index*> ist eine Zahl zwischen 1 und 4

Eingabe

In Tabelle A-45 werden die Unterbefehlsoptionen für **testtrap** beschrieben.

Tabelle A-45. testtrap-Unterbefehlsoptionen

Option	Beschreibung
-i	Gibt den Index der Trap-Konfiguration an, die für den Test zu verwenden ist. Gültige Werte sind zwischen 1 und 4.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

vmdisconnect

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **Zugriff auf Virtueller Datenträger** haben.

Tabelle A-46 beschreibt den **vmdisconnect**-Unterbefehl.

Tabelle A-46. vmdisconnect

Unterbefehl	Beschreibung
vmdisconnect	Schließt alle offenen RAC virtueller Datenträger-Verbindungen von Remote Clients.

Zusammenfassung

```
racadm vmdisconnect
```

Beschreibung

Mit dem **vmdisconnect**-Unterbefehl kann ein Benutzer die virtueller Datenträger-Sitzung eines anderen Benutzers trennen. Wenn unterbrochen, spiegelt die Internet-basierte Benutzeroberfläche den korrekten Verbindungsstatus wider. Das ist nur durch den Gebrauch von lokalem oder Remote-racadm verfügbar.

Mit dem Unterbefehl **vmdisconnect** wird es einem RAC-Benutzer ermöglicht, alle aktiven Sitzungen des virtuellen Datenträgers zu trennen. Die aktiven Sitzungen des virtuellen Datenträgers können auf der Internet-basierten RAC-Schnittstelle oder durch Verwendung des racadm-Unterbefehls **getsysinfo** angezeigt werden.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

---

vmkey

ANMERKUNG: Um diesen Befehl zu verwenden, müssen Sie die Berechtigung **Zugriff auf Virtueller Datenträger** haben.

Tabelle A-47 beschreibt den **vmkey**-Unterbefehl.

Tabelle A-47. vmkey

Unterbefehl	Beschreibung
vmkey	Führt schlüsselbezogene Virtueller Datenträger-Vorgänge aus.

Zusammenfassung

```
racadm vmkey <Maßnahme>
```

Wenn `<Maßnahme>` als `Zurücksetzen` konfiguriert wird, wird der virtuelle Flash-Speicher auf die Standardgröße von 16 MB zurückgesetzt.

Beschreibung

Wenn ein kundenspezifisches Virtueller Datenträger Schlüssel-Image zum RAC hochgeladen wird, wird die Schlüsselgröße die Bildgröße. Der Vmkey-Subbefehl kann verwendet werden, um den Schlüssel auf seine ursprüngliche Standardgröße zurückzustellen, d. h. 16 MB auf dem DRAC 5.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- telnet/ssh/seriell-RACADM

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5 Eigenschaften-Datenbankgruppe und Objektdefinitionen

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Die DRAC 5-Eigenschaftendatenbank enthält die Konfigurationsinformationen für den DRAC 5. 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 Gruppe und Objekt-ID mit dem Dienstprogramm racadm, um den DRAC 5 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 Anzeigenparameter, um Informationen über die Besonderheiten des abgefragten DRAC 5 zu erhalten.

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

idRacProductInfo (Nur-Lesen)

Zulässige Werte

Zeichenkette mit bis zu 63 ASCII-Zeichen.

Standardeinstellung

"Dell Remote Access Controller 5"

Beschreibung

Verwendet einen Text-String, um das Produkt zu identifizieren.

idRacDescriptionInfo (Nur-Lesen)

Zulässige Werte

Zeichenkette mit bis zu 255 ASCII-Zeichen

Standardeinstellung

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

Beschreibung

Eine Textbeschreibung des RAC-Typs.

idRacVersionInfo (Nur-Lesen)

Zulässige Werte

Zeichenkette mit bis zu 63 ASCII-Zeichen.

Standardeinstellung

"1.0"

Beschreibung

Eine Zeichenkette, die die aktuelle Produktfirmware-Version enthält.

idRacBuildInfo (Nur-Lesen)

Zulässige Werte

Zeichenkette mit bis zu 16 ASCII-Zeichen.

Standardeinstellung

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

Beschreibung

Eine Zeichenkette mit der aktuellen Produkt-Build-Version.

idRacName (Nur-Lesen)

Zulässige Werte

Zeichenkette mit bis zu 15 ASCII-Zeichen

Standardeinstellung

DRAC 5

Beschreibung

Ein vom Benutzer vergebener Name zur Identifizierung dieses Controllers.

idRacType (Nur-Lesen)

Standardeinstellung

6

Beschreibung

Identifiziert den Remote Access Controller-Typ als den DRAC 5.

---

cfgLanNetworking

Diese Gruppe enthält Parameter, um den DRAC 5-NIC zu konfigurieren.

Es ist eine Instanz der Gruppe zulässig. Für alle Objekte in dieser Gruppe ist ein Reset des DRAC 5-NIC erforderlich, der einen kurzen Verlust in der Konnektivität verursachen kann. Objekte, die die DRAC 5-NIC-IP-Adresseneinstellungen ändern, aktiven Benutzersitzungen, schließen alle aktiven Benutzersitzungen und erfordern, dass Benutzer mit den aktualisierten IP-Adresseneinstellungen wiederverbinden.

cfgDNSDomainNameFromDHCP (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

1

Beschreibung

Bestimmt, dass der RAC DNS-Domänenname von dem Netzwerk-DHCP-Server zugeteilt werden sollte.

cfgDNSDomainName (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette mit bis zu 254 ASCII-Zeichen Mindestens ein Zeichen muss ein Buchstabe sein. Zeichen müssen alphanumerisch, '-' oder '.' sein.

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

Standardeinstellung

""

Beschreibung

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

cfgDNSRacName (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

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

ANMERKUNG: Manche DNS-Server registrieren nur Namen bis zu 31 Zeichen Länge.

Standardeinstellung

rac-*Service-Tag-Nummer*

Beschreibung

Zeigt den RAC-Namen an, das heißt, die rac-*Service-Tag-Nummer*(standardmäßig). Dieser Parameter ist nur gültig, wenn **cfgDNSRegisterRac** auf 1 (WAHR) eingestellt ist.

cfgDNSRegisterRac (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Registriert den DRAC 5-Namen auf dem DNS-Server.

cfgDNSServersFromDHCP (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Gibt an, dass die DNS Server-IP-Adressen vom DHCP Server auf dem Netzwerk zugeteilt werden sollten.

cfgDNSServer1 (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

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

Beschreibung

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

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

cfgDNSServer2 (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

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 (FALSCH) eingestellt ist.

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

cfgNicEnable (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert den RAC Netzwerkschnittstellen-Controller. Wenn die NIC deaktiviert wird, sind die Remote-Netzwerkschnittstellen zum RAC nicht mehr zugänglich, und der RAC ist nur durch die serielle oder lokale RACADM-Schnittstelle verfügbar.

cfgNicIpAddress (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben. Dieser Parameter kann nur konfiguriert werden, wenn der Parameter **cfgNicUseDhcp** auf 0 (FALSCH) eingestellt ist.

Zulässige Werte

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

Standardeinstellung

192.168.0.120

Beschreibung

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

cfgNicNetmask (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben. Dieser Parameter kann nur konfiguriert werden, wenn der Parameter **cfgNicUseDhcp** auf 0 (FALSCH) 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 Anweisung der RAC-IP-Adresse verwendete Subnetzmaske. Diese Eigenschaft ist nur gültig, wenn **cfgNicUseDhcp** auf **0** (FALSCH) eingestellt ist.

cfgNicGateway (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben. Dieser Parameter kann nur konfiguriert werden, wenn der Parameter **cfgNicUseDhcp** auf 0 (FALSCH) 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** (FALSCH) eingestellt ist.

cfgNicUseDhcp (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Gibt an, ob DHCP verwendet wird, um die RAC-IP-Adresse zuzuweisen. Wenn diese Eigenschaft auf 1 (WAHR) eingestellt wird, dann werden RAC-IP-Adresse, -Subnetzmaske und -Gateway vom DHCP Server auf dem Netzwerk zugeteilt. Wenn diese Eigenschaft auf **0** (FALSCH) gesetzt wird, werden statische IP-Adresse, Subnetzmaske und Gateway von den Eigenschaften **cfgNicIpAddress**, **cfgNicNetmask** und **cfgNicGateway** zugewiesen.

ANMERKUNG: Wenn Sie Ihr System im Remote-Zugriff aktualisieren, verwenden Sie den **setniccfg** Befehl.

cfgNicSelection (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (geteilt)

1 (Freigegeben für Failover)

2 (Dediziert)

Standardeinstellung

2

Beschreibung

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

Tabelle B-1. cfgNicSelection Unterstützte Modi

Modus	Beschreibung
Freigegeben	Wird verwendet, wenn der integrierte Host-Server-NIC mit dem RAC auf dem Host-Server geteilt wird. Dieser Modus ermöglicht, dass Konfigurationen zur allgemeinen Zugänglichkeit dieselbe IP-Adresse auf dem Host-Server und dem RAC auf dem Netzwerk verwenden.
Freigegeben für Failover	Aktiviert Teaming-Fähigkeiten zwischen integrierten Netzwerkschnittstellen-Controllern des Host-Servers.
Dediziert	Legt fest, dass die RAC-NIC als dedizierte NIC für Remote-Zugänglichkeit verwendet wird.

cfgNicMacAddress (Nur-Lesen)

Zulässige Werte

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

Standardeinstellung

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

Beschreibung

The RAC-NIC MAC-Adresse.

cfgNicVLanEnable (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die VLAN-Fähigkeiten von RAC/BMC.

cfgNicVLanId (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 – 4094

Standardeinstellung

0

Beschreibung

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

cfgNicVLanPriority (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 – 7

Standardeinstellung

0

Beschreibung

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

cfgRemoteHosts

Diese Gruppe enthält Eigenschaften, die die Konfiguration von verschiedenen entfernten Komponenten erlauben, z. B. den SMTP Server für E-Mail-Warnungen und TFTP-Server-IP-Adressen für Firmware-Updates.

cfgRhostsSmtpServerIpAddr (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Eine Zeichenkette, die eine gültige SMTP-Server-IP-Adresse darstellt. Beispiel: `192.168.0.55`.

Standardeinstellung

0.0.0.0

Beschreibung

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

cfgRhostsFwUpdateTftpEnable (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert das RAC-Firmware-Update von einem Netzwerk-TFTP Server.

cfgRhostsFwUpdateIpAddr (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Eine Zeichenkette, die eine gültige TFTP-Server-IP-Adresse darstellt. Beispiel: `192.168.0.61`.

Standardeinstellung

0.0.0.0

Beschreibung

Gibt die IP-Adresse für den Netzwerk-TFTP-Server an, die für RAC TFTP Firmware-Aktualisierungsvorgänge verwendet wird.

cfgRhostsFwUpdatePath (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

""

Beschreibung

Gibt den TFTP-Pfad zum Speicherort der RAC Firmware-Bilddatei auf dem TFTP-Server an. Der TFTP-Pfad ist relativ zum TFTP-Stamm-Pfad auf dem TFTP Server.

ANMERKUNG: Der Server kann weiterhin erfordern, dass das Laufwerk angegeben wird (zum Beispiel **C**).

---

cfgUserAdmin

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

Bis zu 16 Beispiele der Benutzergruppe sind erlaubt. Jedes Beispiel vertritt die Konfiguration für einen einzelnen Benutzer.

cfgUserAdminIpmiLanPrivilege (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft zu modifizieren, müssen Sie die Berechtigung **Benutzer konfigurieren** haben.

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

15 (Kein Zugang)

Standardeinstellung

4 (Benutzer 2)

15 (Alle anderen)

Beschreibung

Die maximale Berechtigung auf dem IPMI LAN-Kanal.

cfgUserAdminIpmiSerialPrivilege (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft zu modifizieren, müssen Sie die Berechtigung **Benutzer konfigurieren** haben.

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

15 (Kein Zugang)

Standardeinstellung

4 (Benutzer 2)

15 (Alle anderen)

Beschreibung

Die maximale Berechtigung auf dem seriellen IPMI-Kanal.

cfgUserAdminPrivilege (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft zu modifizieren, müssen Sie die Berechtigung **Benutzer konfigurieren** haben.

Zulässige Werte

0x0000000 bis 0x00001ff und 0x0

Standardeinstellung

0x0000000

Beschreibung

Diese Eigenschaft bestimmt die für den Benutzer erlaubten rollenbasierten Autoritäts-Berechtigungen. Der Wert wird als Bitmask dargestellt, was jede Kombination von Berechtigungswerten zulässt. Tabelle B-2 beschreibt die erlaubten Benutzerberechtigungs-Bitmasken.

Tabelle B-2. Bit-Masken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
Bei DRAC 5 anmelden	0x0000001
DRAC 5 konfigurieren	0x0000002
Benutzer konfigurieren	0x0000004
Protokolle löschen	0x0000008
Server-Steuerungsbefehle ausführen	0x0000010
Auf die Konsolenumleitung zugreifen	0x0000020
Auf den virtuellen Datenträger zugreifen	0x0000040
Testwarnungen	0x0000080
Debug-Befehle ausführen	0x0000100

Beispiele

Tabelle B-3 enthält Beispielsberechtigungs-Bitmasken für Benutzer mit einer oder mehr Berechtigungen.

Tabelle B-3. Beispiel-Bitmasken für Benutzerberechtigungen

Benutzerberechtigung(en)	Berechtigungs-Bitmaske
Dem Benutzer ist nicht gestattet, auf den RAC zuzugreifen.	0x00000000
Der Benutzer kann sich nur am RAC anmelden und RAC- und Serverkonfigurationsinformationen ansehen.	0x00000001
Der Benutzer kann sich am RAC anmelden und die Konfiguration ändern.	0x00000001 + 0x00000002 = 0x00000003
Der Benutzer kann sich am RAC anmelden, auf virtuelle Datenträger und auf die Konsolenumleitung zugreifen.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft zu modifizieren, müssen Sie die Berechtigung **Benutzer konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 16.

Standardeinstellung

""

Beschreibung

Der Name des Benutzers dieses Indexes. Der Benutzer-Index 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 Zeichenkette darf keine(n) "/" (Vorwärtsschrägstrich, "\" (umgekehrten Schrägstrich), "." (Punkt), "@" ("Klammeraffen") oder Anführungszeichen enthalten.

ANMERKUNG: Dieser Eigenschaft-Wert MUSS sich eindeutig von anderen Benutzerbeispielen unterscheiden.

cfgUserAdminPassword (Nur Schreiben)

ANMERKUNG: Um diese Eigenschaft zu modifizieren, müssen Sie die Berechtigung **Benutzer konfigurieren** haben.

Zulässige Werte

Eine Zeichenkette mit bis zu 20 ASCII-Zeichen

Standardeinstellung

""

Beschreibung

Das Kennwort für diesen Benutzer. Die Benutzer-Kennwörter werden verschlüsselt und sind nicht sichtbar bzw. können nicht angezeigt werden, nachdem diese Eigenschaft geschrieben wurde.

cfgUserAdminEnable

ANMERKUNG: Um diese Eigenschaft zu modifizieren, müssen Sie die Berechtigung **Benutzer konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert einen einzelnen Benutzer.

cfgUserAdminSolEnable

ANMERKUNG: Um diese Eigenschaft zu modifizieren, müssen Sie die Berechtigung **Benutzer konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert Seriell über LAN (SOL) -Benutzerzugang.

---

cfgEmailAlert

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

In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben. Bis zu vier Beispiele dieser Gruppe sind erlaubt.

cfgEmailAlertIndex (Nur-Lesen)

Zulässige Werte

1–4

Standardeinstellung

Dieser Parameter wird beruhend auf vorhandenen Beispielen bestückt.

Beschreibung

Der eindeutige Index eines Warnungsbeispiels.

cfgEmailAlertEnable (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Gibt die Ziel-E-Mail-Adresse für E-Mail-Warnungen an. Beispiel: `user1@company.com`.

cfgEmailAlertAddress (Nur-Lesen)

Zulässige Werte

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

Standardeinstellung

""

Beschreibung

Die E-Mail-Adresse der Warnungsquelle.

cfgEmailAlertCustomMsg (Nur-Lesen)

Zulässige Werte

Zeichenkette. Maximale Länge = 32.

Standardeinstellung

""

Beschreibung

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

---

cfgSessionManagement

Diese Gruppe enthält Parameter zur Konfiguration der Anzahl von Sitzungen, die eine Verbindung zum DRAC 5 herstellen können.

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

cfgSsnMgtConsRedirMaxSessions (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 – 2

Standardeinstellung

2

Beschreibung

Gibt die maximale Anzahl von auf dem RAC erlaubten Konsolenumleitungssitzungen an.

cfgSsnMgtRacadmTimeout (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

10 –1920

Standardeinstellung

30

Beschreibung

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

cfgSsnMgtWebserverTimeout (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

60 – 1920

Standardeinstellung

300

Beschreibung

Definiert das Webserver-Zeitlimit. Diese Eigenschaft stellt die Zeit in Sekunden ein, die eine Verbindung im Leerlauf verbleiben kann (es gibt keine Benutzereingabe). Die Sitzung wird annulliert, wenn die durch diese Eigenschaft eingestellte Frist erreicht wird. Änderungen an dieser Einstellung betreffen die aktuelle Sitzung nicht (Sie müssen sich ab- und wieder anmelden, um die neuen Einstellungen wirksam zu machen).

Eine abgelaufene Webserver-Sitzung meldet die aktuelle Sitzung ab.

cfgSsnMgtSshIdleTimeout (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (Kein Zeitlimit)

60 – 1920

Standardeinstellung

300

Beschreibung

Bestimmt das Zeitlimit für den Secure Shell-Leerlauf. Diese Eigenschaft stellt die Zeit in Sekunden ein, die eine Verbindung im Leerlauf verbleiben kann (es gibt keine Benutzereingabe). Die Sitzung wird annulliert, wenn die durch diese Eigenschaft eingestellte Frist erreicht wird. Änderungen an dieser Einstellung betreffen die aktuelle Sitzung nicht (Sie müssen sich ab- und wieder anmelden, um die neuen Einstellungen wirksam zu machen).

Eine ungültige 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 erscheint, wechselt das System zu der Shell zurück, die die Secure Shell-Sitzung erstellt hatte.

cfgSsnMgtTelnetTimeout (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (Kein Zeitlimit)

60 – 1920

Standardeinstellung

0

Beschreibung

Definiert das Telnet Leerlauf-Zeitlimit. Diese Eigenschaft stellt die Zeit in Sekunden ein, die eine Verbindung im Leerlauf verbleiben kann (es gibt keine Benutzereingabe). Die Sitzung wird annulliert, wenn die durch diese Eigenschaft eingestellte Frist erreicht wird. Änderungen an dieser Einstellung betreffen die aktuelle Sitzung nicht (Sie müssen sich ab- und wieder anmelden, um die neuen Einstellungen wirksam zu machen).

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 hatte.

---

cfgSerial

Diese Gruppe enthält Konfigurationsparameter für die serielle DRAC 5-Schnittstelle.

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

cfgSerialBaudRate (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

9600, 28800, 57600, 115200

Standardeinstellung

57600

Beschreibung

Stellt die Baudrate für die serielle DRAC 5-Schnittstelle ein.

cfgSerialConsoleEnable (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die serielle RAC-Schnittstelle.

cfgSerialConsoleQuitKey (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

ZEICHENKETTE

MaxLen = 4

Standardeinstellung

^ \ (<Strg><\>)

ANMERKUNG: "^" ist die <Strg>-Taste.

Beschreibung

Diese Taste oder Tastenkombination beendet die Textkonsolenumleitung, wenn der Befehl **connect com2** verwendet wird. Der **cfgSerialConsoleQuitKey-**Wert kann wie folgt angezeigt werden:

- Dezimaler Wert - Beispiel: "95"
- Hexadezimaler Wert - Beispiel: "0x12"
- Oktalwert - Beispiel: "007"
- ASCII-Wert - Beispiel: "^a"

ASCII-Werte können anhand der folgenden Escape-Tasten-Codes dargestellt werden:

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

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

cfgSerialConsoleIdleTimeout (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 = kein Zeitlimit

60 – 1920

Standardeinstellung

300

Beschreibung

Die maximale Anzahl von Sekunden, bis eine inaktive serielle Sitzung getrennt wird.

cfgSerialConsoleNoAuth (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (aktiviert serielle Anmeldungsauthentifizierung)

1 (deaktiviert serielle Anmeldungsauthentifizierung)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die serielle RAC-Anmeldungsauthentifizierung.

cfgSerialConsoleCommand (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Beschreibung

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

Standardeinstellung

""

Beispiel

"connect com2"

cfgSerialHistorySize (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 – 8192

Standardeinstellung

8192

Beschreibung

Gibt die maximale Größe des seriellen Verlaufspuffers an.

cfgSerialSshEnable (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Secure Shell (SSH)-Schnittstelle auf dem DRAC 5.

cfgSerialTelnetEnable (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die telnet-Konsolenschnittstelle auf dem RAC.

cfgSerialCom2RedirEnable (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Standardeinstellung

1

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Beschreibung

Aktiviert oder deaktiviert die Konsole für COM 2-Schnittstellenumleitung.

---

cfgNetTuning

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

HINWEIS: Bei der Änderung von Eigenschaften in dieser Gruppe muss mit äußerster Vorsicht vorgegangen werden. Eine unsachgemäße Modifizierung der Eigenschaften in dieser Gruppe kann dazu führen, dass Ihre RAC-NIC inoperabel wird.

cfgNetTuningNicAutoneg (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (Aktiviert)

0 (Deaktiviert)

Standardeinstellung

1

Beschreibung

Aktiviert Autoverhandlung der physischen Verbindungstaktrate und -Duplex. Wenn aktiviert, wird Autoverhandlung Vorrang vor Werten haben, die in den Objekten **cfgNetTuningNic100MB** und **cfgNetTuningNicFullDuplex** eingestellt sind.

cfgNetTuningNic100MB (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (10 MBit)

1 (100 MBit)

Standardeinstellung

1

Beschreibung

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

cfgNetTuningNicFullDuplex (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (Halb-Duplex)

1 (Voll-Duplex)

Standardeinstellung

1

Beschreibung

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

cfgNetTuningNicMtu (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

576 – 1500

Standardeinstellung

1500

Beschreibung

Die Größe der maximalen Übertragungseinheit in Bytes, die vom DRAC 5-NIC verwendet wird.

cfgNetTuningTcpSrttDflt (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

6 – 384

Standardeinstellung

6

Beschreibung

Der geglättete Standardbasiswert der Umlaufzeitüberschreitung für die TCP-Rückübertragungsdauer in Einheiten zu 0,5 Sekunden. (Geben Sie hexadezimale Werte ein.)

---

cfgOobSnmp

Die Gruppe enthält Parameter zur Konfiguration des SNMP-Agenten und der Trap-Fähigkeiten des DRAC 5.

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

cfgOobSnmpAgentCommunity (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 31.

Standardeinstellung

public

Beschreibung

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

cfgOobSnmpAgentEnable (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert den SNMP-Agenten im RAC.

---

cfgRacTuning

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

cfgRacTuneHttpPort (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

10 – 65535

Standardeinstellung

80

Beschreibung

Gibt die Schnittstellennummer an, die für die HTTP-Netzwerkkommunikation mit dem RAC zu verwenden ist.

cfgRacTuneHttpsPort (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

10 – 65535

Standardeinstellung

443

Beschreibung

Gibt die Schnittstellennummer an, die für die HTTPS-Netzwerkkommunikation mit dem RAC zu verwenden ist.

cfgRacTuneIpRangeEnable

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

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

cfgRacTuneIpRangeAddr

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette, formatierte IP-Adresse. Beispiel: `192.168.0.44`.

Standardeinstellung

`192.168.1.1`

Beschreibung

Bestimmt das annehmbare IP-Adressen-Bitmuster in Positionen, die durch die Einsen (1) in der Bereichsmaskeneigenschaft (**cfgRacTuneIpRangeMask**) bestimmt werden.

cfgRacTuneIpRangeMask

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Normale IP-Maskenwerte mit linksbündigen Bits

Standardeinstellung

`255.255.255.0`

Beschreibung

Zeichenkette, formatierte IP-Adresse. Beispiel: `255.255.255.0`.

cfgRacTuneIpBlkEnable

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

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

cfgRacTuneIpBlkFailcount

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

2 – 16

Standardeinstellung

5

Beschreibung

Die maximale Anzahl an Anmeldungsfehlern im Fenster, bevor die Anmeldungsversuche von dieser IP-Adresse zurückgewiesen werden.

cfgRacTuneIpBlkFailWindow

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

2 – 65535

Standardeinstellung

60

Beschreibung

Definiert die Zeitspanne in Sekunden, während der die fehlerhaften Versuche gezählt werden. Wenn die Fehlversuche diese Grenze erreichen, werden die Misserfolge von der Zählung ausgelassen.

cfgRacTuneIpBlkPenaltyTime

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

2 – 65535

Standardeinstellung

300

Beschreibung

Definiert die Zeitspanne in Sekunden, in der Sitzungsanforderungen von einer IP-Adresse mit übermäßigen Fehlern zurückgewiesen werden.

cfgRacTuneSshPort (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 – 65535

Standardeinstellung

22

Beschreibung

Gibt die für die RAC SSH-Schnittstelle verwendete Schnittstellennummer an.

cfgRacTuneTelnetPort (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 – 65535

Standardeinstellung

23

Beschreibung

Gibt die für die RAC Telnet-Schnittstelle verwendete Schnittstellennummer an.

cfgRacTuneRemoteRacadmEnable (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

1

Beschreibung

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

cfgRacTuneConRedirEncryptEnable (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Chiffriert das Video in einer Konsolenumleitungssitzung.

cfgRacTuneConRedirPort (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 – 65535

Standardeinstellung

5901

Beschreibung

Gibt die Schnittstelle an, die für Tastatur- und Maus-Aktivitäten während der Konsolenumleitungstätigkeit mit dem RAC zu verwenden ist.

ANMERKUNG: Dieses Objekt erfordert einen DRAC 5-Reset, bevor es aktiviert wird.

cfgRacTuneConRedirVideoPort (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 – 65535

Standardeinstellung

5901

Beschreibung

Gibt die Schnittstelle an, die für den Videoverkehr während der Konsolenumleitungstätigkeit mit dem RAC zu verwenden ist.

ANMERKUNG: Dieses Objekt erfordert einen DRAC 5-Reset, bevor es aktiviert wird.

cfgRacTuneAsrEnable (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Absturzbildschirm-Abspeicherungsfunktion des RAC.

ANMERKUNG: Dieses Objekt erfordert einen DRAC 5-Reset, bevor es aktiviert wird.

cfgRacTuneDaylightOffset (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 – 60

Standardeinstellung

0

Beschreibung

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

cfgRacTuneTimezoneOffset (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

-720 – 780

Standardeinstellung

0

Beschreibung

Gibt den Zeitzonenausgleich (in Minuten) von GMT/UTC für die Einstellung der RAC-Zeit an. Einige allgemeine Zeitzonenausgleiche für Zeitzonen in den Vereinigten Staaten folgen:

-480 (PST - Pacific Standard Time)

-420 (MST - Mountain Standard Time)

-360 (CST - Central Standard Time)

-300 (EST - Eastern Standard Time)

cfgRacTuneWebserverEnable (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert und deaktiviert den RAC-Webserver. Wenn diese Eigenschaft deaktiviert wird, ist der RAC bei Verwendung von Client-Webbrowsern oder Remote-RACADM nicht zugänglich. Diese Eigenschaft hat keine Wirkung auf die telnet/ssh/seriell- oder lokalen RACADM-Schnittstellen.

cfgRacTuneLocalServerVideo (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (Wahr)

0 (Deaktivieren)

Standardeinstellung

1

Beschreibung

Aktiviert (schaltet EIN) oder deaktiviert (schaltet AUS) den lokalen Server-Video.

---

ifcRacManagedNodeOs

Diese Gruppe enthält Eigenschaften, die das Verwaltete Server-Betriebssystem definieren.

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

ifcRacMnOsHostname (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

""

Beschreibung

Der Host-Name des verwalteten Systems.

ifcRacMnOsOsName (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

""

Beschreibung

Der Betriebssystemname des verwalteten Systems.

---

cfgRacSecurity

Diese Gruppe wird verwendet, um Einstellungen bezüglich der Funktion RAC SSL-Zertifikatssignierungsanforderung (CSR) zu konfigurieren. Die Eigenschaften in dieser Gruppe MÜSSEN vor dem Erzeugen eines CSR vom RAC konfiguriert werden.

Unter dem RACADM **sslcsrgen**-Unterbefehl finden Sie weitere Informationen über das Erstellen von Zertifikatssignierungsanforderungen.

cfgSecCsrCommonName (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Allgemeinen Namen (CN) an.

cfgSecCsrOrganizationName (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Organisationsnamen (O) an.

cfgSecCsrOrganizationUnit (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt die CSR-Organisationseinheit (OU) an.

cfgSecCsrLocalityName (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Ort (L) an.

cfgSecCsrStateName (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Zustandsnamen (S) an.

cfgSecCsrCountryCode (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 2.

Standardeinstellung

""

Beschreibung

Gibt die CSR-Landescode (CC) an

cfgSecCsrEmailAddr (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt die CSR E-Mail-Adresse an.

cfgSecCsrKeySize (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

512

1024

2048

Standardeinstellung

1024

Beschreibung

Gibt die asymmetrische SSL-Schlüsselgröße für den CSR an.

cfgRacVirtual

Diese Gruppe enthält Parameter, um die Funktion DRAC 5 virtueller Datenträger zu konfigurieren. Es ist eine Instanz der Gruppe zulässig. In den folgenden Unterabschnitten werden die Objekte in dieser Gruppe beschrieben.

cfgVirMediaAttached (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Dieses Objekt wird verwendet, um die virtuellen Geräte über den USB-Bus mit dem System zu verbinden. Wenn die Geräte angeschlossen sind, erkennt der Server gültige, am System angeschlossene USB-Großspeichergeräte. Dies entspricht dem Anschließen eines lokalen USB-CD-ROM/Diskettenlaufwerks am USB-Anschluss des Systems. Wenn die Geräte angeschlossen sind, können Sie dann im Remote-Zugriff über die Internet-basierte DRAC5-Schnittstelle oder die CLI eine Verbindung zu den virtuellen Geräten herstellen. Durch die Einstellung dieses Objekts auf **0** werden die Geräte veranlasst, sich vom USB-Bus zu trennen.

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

cfgVirAtapiSrvPort (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **Zugriff auf Virtueller Datenträger** haben.

Zulässige Werte

1 – 65535

Standardeinstellung

3669

Beschreibung

Gibt die für chiffrierte Verbindungen des virtuellen Datenträgers mit dem RAC verwendete Schnittstellennummer an.

cfgVirAtapiSrvPortSsl (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Jede unbenutzte Schnittstelle zwischen 0 und 65535 dezimal.

Standardeinstellung

3669

Beschreibung

Stellt die für SSL-Verbindungen des virtuellen Datenträgers verwendete Schnittstelle ein.

cfgVirMediaKeyEnable (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert das Hauptmerkmal des virtuellen Datenträgers des RAC.

cfgVirMediaBootOnce (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (Aktiviert)

0 (Deaktiviert)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Einmal-Start-Funktion des virtuellen Datenträgers des RAC. Wenn diese Eigenschaft aktiviert wird, versucht diese Funktion, wenn der Host-Server neugestartet wird, von den virtuellen Datenträgergeräten zu starten - wenn die entsprechenden Datenträger im Gerät installiert sind.

cfgFloppyEmulation (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (Wahr)

0 (Falsch)

Standardeinstellung

1

Beschreibung

When set to 0, the Virtual Floppy drive is recognized as a removable disk by Windows operating systems. Windows-Betriebssysteme werden den Laufwerksbuchstaben C: oder höher während der Aufzählung zuweisen. Wenn auf 1 eingestellt, wird das virtuelle Diskettenlaufwerk als ein Diskettenlaufwerk

von Windows-Betriebssystemen erkannt. Windows-Betriebssysteme werden die Laufwerksbuchstaben A: oder B: zuweisen.

---

cfgActiveDirectory

Diese Gruppe enthält Parameter, um die Funktion DRAC 5 Active Directory zu konfigurieren.

cfgADRacDomain (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Jeder druckfähige Text-String ohne unbedruckten Seitenbereich. Länge wird auf 254 Zeichen beschränkt.

Standardeinstellung

""

Beschreibung

Active Directory-Domäne, in der sich der DRAC befindet

cfgADRacName (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Jeder druckfähige Text-String ohne unbedruckten Seitenbereich. Länge wird auf 254 Zeichen beschränkt.

Standardeinstellung

""

Beschreibung

Name von DRAC, wie im Active Directory-Wald registriert.

cfgADEnable (Lesen / Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Active Directory-Benutzerauthentifizierung auf dem RAC. Wenn diese Eigenschaft deaktiviert wird, wird statt dessen lokale RAC-Authentifizierung für Benutzeranmeldungen verwendet.

cfgADAuthTimeout(Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

15 – 300

Standardeinstellung

120

Beschreibung

Gibt die Anzahl von Sekunden an, die auf die Ausführung von Authentifizierungsanforderungen von Active Directory gewartet wird, bevor das Zeitlimit erreicht wird.

cfgADRootDomain (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Jeder druckfähige Text-String ohne unbedruckten Seitenbereich. Länge wird auf 254 Zeichen beschränkt.

Standardeinstellung

""

Beschreibung

Root-Domäne des Domänen-Waldes.

cfgFloppyEmulation (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 = Aktiviert Erweitertes Schema mit Active Directory.

2 = aktiviert Standardschema mit Active Directory.

Standardeinstellung

1 = Erweitertes Schema

Beschreibung

Bestimmt den Schema-Typ, der mit Active Directory verwendet wird.

cfgStandardSchema

Diese Gruppe enthält Parameter, um die Standard-Schemaeinstellungen zu konfigurieren.

cfgSSADRoleGroupIndex (Nur-Lesen)

Zulässige Werte

Ganze Zahl von 1 bis 5.

Beschreibung

Index der Rollengruppe, wie im Active Directory registriert.

cfgSSADRoleGroupName (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Jeder druckfähige Text-String ohne unbedruckten Seitenbereich. Länge wird auf 254 Zeichen beschränkt.

Standardeinstellung

(Vordruck)

Beschreibung

Name der Rollengruppe, wie im Active Directory-Wald registriert.

cfgSSADRoleGroupDomain (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Jeder druckfähige Text-String ohne unbedruckten Seitenbereich. Länge wird auf 254 Zeichen beschränkt.

Standardeinstellung

(Vordruck)

Beschreibung

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

cfgSSADRoleGroupPrivilege (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0x00000000 bis **0x000001ff**

Standardeinstellung

(Vordruck)

Beschreibung

Verwenden Sie die Zahlen der Bit-Maske in der Tabelle B-4, um rollenbasierte Authoritätsberechtigungen für eine Rollengruppe einzustellen.

Tabelle B-4. Bit-Masken für **Berechtigungen der Rollengruppe**

Berechtigung der Rollengruppe	Bit-Maske
Bei DRAC 5 anmelden	0x00000001
DRAC 5 konfigurieren	0x00000002
Benutzer konfigurieren	0x00000004
Protokolle löschen	0x00000008
Server-Steuerungsbefehle ausführen	0x00000010
Auf die Konsolenumleitung zugreifen	0x00000020
Auf den virtuellen Datenträger zugreifen	0x00000040
Testwarnungen	0x00000080
Debug-Befehle ausführen	0x00000100

---

cfgIpmiSerial

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

cfgIpmiSerialConnectionMode (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (Terminal)

1 (Grundlegend)

Standardeinstellung

1

Beschreibung

Wenn die DRAC 5-Eigenschaft **cfgSerialConsoleEnable** auf 0 (deaktiviert) gesetzt wird, wird der serielle DRAC 5-Anschluss zum seriellen IPMI-Anschluss. Diese Eigenschaft bestimmt den definierten IPMI- Modus des seriellen Anschlusses.

Im grundlegenden Modus verwendet die Schnittstelle Binärdaten mit der Absicht des Kommunizierens mit einem Anwenderprogramm auf dem seriellen Client. Im Terminalmodus nimmt die Schnittstelle an, dass ein stummer ASCII-Terminal angeschlossen ist und lässt die Eingabe sehr einfacher Befehle zu.

cfgIpmiSerialBaudRate (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

9600, 19200, 57600, 115200

Standardeinstellung

57600

Beschreibung

Gibt die Baudrate für eine serielle Verbindung über IPMI an.

cfgIpmiSerialChanPrivLimit (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

Gibt die maximale auf dem seriellen IPMI-Kanal erlaubte Berechtigungsstufe an.

cfgIpmiSerialFlowControl (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (Keine)

1 (CTS/RTS)

2 (XON/XOFF)

Standardeinstellung

1

Beschreibung

Gibt die Ablaufsteuerung für den seriellen IPMI-Anschluss an.

cfgIpmiSerialHandshakeControl (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

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

cfgIpmiSerialLineEdit (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

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

cfgIpmiSerialEchoControl (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Echo-Steuerung auf der seriellen IPMI-Schnittstelle.

cfgIpmiSerialDeleteControl (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

0

Beschreibung

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

cfgIpmiSerialNewLineSequence (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (Keine)

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

Standardeinstellung

1

Beschreibung

Legt die Neue Zeilen-Abfolgespezifizierung für die serielle IPMI-Schnittstelle fest.

cfgIpmiSerialInputNewLineSequence (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (<ENTER>)

1 (NULL)

Standardeinstellung

1

Beschreibung

Legt die Neue Zeileneingabe-Abfolgespezifizierung für die serielle IPMI-Schnittstelle fest.

---

cfgIpmiSol

Diese Gruppe wird zum Konfigurieren der Seriellen-über-LAN-Fähigkeiten des Systems verwendet.

cfgIpmiSolEnable (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert Seriell über LAN (SOL).

cfgIpmiSolBaudRate (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

9600, 19200, 57600, 115200

Standardeinstellung

57600

Beschreibung

Die Baudrate für die serielle Kommunikation über LAN.

cfgIpmiSolMinPrivilege (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

Gibt die für den Zugang für seriell-über-LAN erforderliche Mindestberechtigungsstufe an.

cfgIpmiSolAccumulateInterval (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 - 255.

Standardeinstellung

10

Beschreibung

Gibt die typische Zeitdauer an, die der BMC vor dem Übertragen eines teilweisen SOL Zeichen-Datenpakets wartet. Dieser Wert besteht aus 1-basierten 5 ms-Stufen.

cfgIpmiSolSendThreshold (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 – 255

Standardeinstellung

255

Beschreibung

Der SOL Schwellengrenzwert.

---

cfgIpmiLan

Diese Gruppe wird zum Konfigurieren der IPMI über LAN-Fähigkeiten des Systems verwendet.

cfgIpmiLanEnable (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die IPMI über LAN-Schnittstelle.

cfgIpmiLanPrivLimit (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

0

Beschreibung

Gibt die maximal zulässige Berechtigungsstufe für IPMI über LAN-Zugang an.

cfgIpmiLanAlertEnable (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die globale E-Mail-Warnung. Diese Eigenschaft überschreibt alle einzelnen E-Mail-Alarm-Aktivierungs/Deaktivierungseigenschaften.

cfgIpmiEncryptionKey (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** sowie Administratorrechte haben.

Zulässige Werte

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

Standardeinstellung

"00000000000000000000"

Beschreibung

IPMI-Verschlüsselungstaste.

cfgIpmiPetCommunityName (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Eine Zeichenkette bis zu 18 Zeichen.

Standardeinstellung

"public"

Beschreibung

Der SNMP-Community-Name für Traps.

---

cfgIpmiPef

Diese Gruppe wird zum Konfigurieren der auf dem verwalteten Server verfügbaren Plattformereignisfilter verwendet.

Die Ereignisfilter können zur Kontrolle von Regeln verwendet werden, die ausgelöst werden, wenn kritische Ereignisse auf dem verwalteten System auftreten.

cfgIpmiPefName (Nur-Lesen)

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

Der Name des Index-Filters.

Beschreibung

Gibt den Namen des Plattformereignisfilters an.

cfgIpmiPefIndex (Nur-Lesen)

Zulässige Werte

1 – 17

Standardeinstellung

Der Indexwert eines Plattformereignisfilterobjekts.

Beschreibung

Gibt den Index eines spezifischen Plattformereignisfilters an.

cfgIpmiPefAction (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (Keine)

1 (Herunterfahren)

2 (Reset)

3 (Aus-/Einschaltzyklus)

Standardeinstellung

0

Beschreibung

Bestimmt die Maßnahme, die auf dem verwalteten System ausgeführt wird, wenn die Warnung ausgelöst wird.

cfgIpmiPefEnable (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert einen spezifischen Plattformereignisfilter.

---

cfgIpmiPet

Diese Gruppe wird verwendet, um Plattform-Ereignis-Traps auf dem verwalteten System zu konfigurieren.

cfgIpmiPetIndex (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

1 – 4

Standardeinstellung

Der entsprechende Indexwert.

Beschreibung

Eindeutiger Bezeichner für den Index, der dem Trap entspricht.

cfgIpmiPetAlertDestIpAddr (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

Eine gültige IP-Adresse darstellende Zeichenkette. 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 erhält einen SNMP-Trap, wenn ein Ereignis auf dem verwalteten System ausgelöst wird.

cfgIpmiPetAlertEnable (Lesen/Schreiben)

ANMERKUNG: Zur Änderung dieser Eigenschaft müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert einen spezifischen Trap.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Unterstützte RACADM-Schnittstellen

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Die folgende Tabelle enthält eine Übersicht über die RACADM-Unterbefehle und ihren entsprechenden Schnittstelle-Support.

Tabelle C-1. RACADM-Unterbefehl Schnittstellen-Support

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

✓ = Unterstützt; ✗ =Nicht unterstützt

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Browser-Vorinstallation

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Wenn Sie Linux ausführen und sich auf Ihrer Verwaltungsstation ein schreibgeschütztes Dateisystem befindet, kann auf einem Client-System ein Browser installiert werden, ohne dass eine Verbindung zu einem DRAC 5 erforderlich ist. Durch Verwenden des systemeigenen Plugin-Installationspakets kann der Browser während der Client-Setup-Phase manuell installiert werden.

HINWEIS: In einer schreibgeschützten Client-Umgebung wird das installierte VM-Plugin betriebsunfähig, wenn die DRAC 5-Firmware auf eine neuere Version des Plugin aktualisiert wird. Dies ist der Fall, weil früheren Plugin-Funktionen nicht erlaubt wird, zu funktionieren, wenn die Firmware eine neuere Plugin-Version enthält. In diesem Fall wird der Client dazu aufgefordert, eine Plugin-Installation vorzunehmen. Da das Dateisystem schreibgeschützt ist, wird die Installation fehlschlagen, und die Plugin-Funktionen werden nicht verfügbar sein.

Plugin-Installationspaket erhalten

Um das Plugin-Installationspaket zu erhalten, führen Sie Folgendes aus:

1. Melden Sie sich bei einem vorhandenen DRAC5 an
2. Ändern Sie den URL in der Adresszeile des Browsers von:

   ```
   https://<RAC_IP>/cgi-bin/webcgi/main
   ```

   zu:

   ```
   https://<RAC_IP>/plugins/ # Achten Sie darauf, auch den Trailing Slash zu verwenden.
   ```

3. Beachten Sie die beiden Unterverzeichnisse vm und vkvm. Wechseln Sie zum entsprechenden Unterverzeichnis, klicken Sie mit der rechten Maustaste auf die Datei rac5XXX.xpi, und wählen Sie **Link-Ziel speichern als...** aus.
4. Wählen Sie einen Speicherort für die Datei des Plugin-Installationspakets aus.

Plugin-Installation

So installieren Sie das Plugin-Installationspaket:

1. Kopieren Sie das Installationspaket zur systemeigenen Dateisystemfreigabe des Clients, auf die der Client Zugriff hat.
2. Öffnen Sie auf dem Client-System eine Browser-Instanz.
3. Geben Sie in der Browser-Adresszeile den Dateipfad zum Plugin-Installationspaket ein. Beispiel:

   Datei:///tmp/rac5vm.xpi

4. Der Browser führt den Benutzer durch die Plugin-Installation.

Wenn der Browser einmal installiert ist, fordert er diese Plugin-Installation nicht mehr an, solange die Ziel-DRAC5-Firmware keine neuere Version des Plugins enthält.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5 Übersicht

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Der Dell™ Remote Access Controller 5 (DRAC 5) ist eine Systems Management-Hardware- und Software-Lösung für Remote-Verwaltungsfähigkeiten, Wiederherstellung eines abgestürzten Systems und Stromsteuerungsfunktionen für Dell PowerEdge™-Systeme.

Da der DRAC 5 (falls installiert) mit dem Baseboard Management-Controller (BMC) des Systems kommuniziert, kann er dahingehend konfiguriert werden, Ihnen E-Mail-Warnungen für Warnungen oder Fehler bezüglich Stromspannungen, Temperaturen, Eingriffen und Lüftertaktraten zu schicken. Der DRAC 5 protokolliert auch Ereignis-Daten und den neuesten Absturzbildschirm (nur für Systeme, die das Microsoft® Windows® Betriebssystem ausführen), um Ihnen zu helfen, die wahrscheinliche Ursache eines Systemausfalls zu diagnostizieren.

Der DRAC 5 hat seinen eigenen Mikroprozessor und Speicher und wird durch das System angetrieben, in dem es installiert wird. Der DRAC 5 kann auf Ihrem System vorinstalliert sein oder getrennt in einem Einbausatz vorhanden sein.

Um mit dem DRAC 5 zu beginnen, lesen Sie "Installation und Setup des DRAC 5".

Was gibt es Neues bei DRAC 5 in dieser Ausgabe?

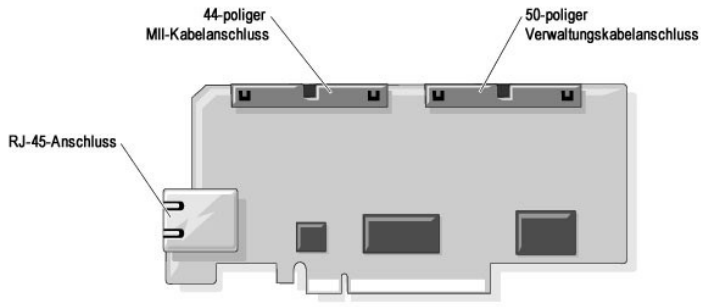
Für diese Ausgabe unterstützt DRAC 5 Firmware-Version 1.20 Folgendes:

- Standardschema mit Microsoft Active Directory® - Bietet Standardobjekte von Active Directory zur Verwendung in der Verwaltung von DRAC 5-Benutzern und -Benutzerberechtigungen. Siehe "Standardschema-Übersicht von Active Directory".
- Einzelner Wald, mehrfacher Struktur-Support für Active Directory - Bietet Support für die Benutzerauthentifizierung über mehrere Strukturen in einem einzelnen Wald in Microsoft Active Directory. Siehe "DRAC 5 mit Active Directory verwenden: Häufig gestellte Fragen".
- Lokales Video deaktivieren - Bietet die Fähigkeit, den Videoausgang zu einem lokalen Monitor eines Servers ein- und auszuschalten, was bei der Verwaltung von Remote-Systemen nützlich ist.Siehe "Lokales Video deaktivieren oder aktivieren".
- Zuweisung des Laufwerksbuchstabens im virtuellen Datenträger - Bietet neue Funktionalität für virtuelle Diskettenlaufwerke. Ein virtuelles Diskettenlaufwerk wird als Laufwerksbuchstabe A: oder B: von Windows-Betriebssystemen erkannt und wird eher als ein Diskettenlaufwerk als ein wechselbares Festplattenlaufwerk gezählt, das den Laufwerksbuchstaben C: oder höher annimmt. Siehe "cfgFloppyEmulation (Lesen/Schreiben)".

DRAC 5 Hardwarefunktionen

Abbildung 1-1 zeigt die DRAC 5 Hardware.

Abbildung 1-1. DRAC 5 Hardwarefunktionen



Hardwarespezifikationen

Stromanforderungen

Tabelle 1-1 enthält die Stromanforderungen für den DRAC 5.

Tabelle 1-1. DRAC 5-Stromanforderungen

Systemstrom
1.2 auf +3.3 V AUX (Maximum)
550 mA auf +3.3 V hauptsächlich (Maximum)
0 mA +5V hauptsächlich (Maximum)

Stecker

ANMERKUNG: Installationsanleitungen für die DRAC 5-Hardware erhalten Sie im Dokument *Remote-Zugriffskarte installieren* oder dem *Installations- und Fehlerbehebungshandbuch*, das Ihrem System beiliegt.

DRAC 5 umfasst eine integrierte 10/100 MBit/s RJ-45 NIC, ein 50-poliges Verwaltungskabel sowie ein 44-poliges MII-Kabel. Siehe Abbildung 1-1 für die DRAC 5 Kabelanschlüsse.

Das 50-polige Managementkabel ist die Hauptschnittstelle zum DRAC, die Konnektivität zu USB, Seriell, Video, und einem zwischenintegrierten Schaltkreis (I2C)-Bus enthält. Das 44-polige MII-Kabel verbindet die DRAC-NIC mit der Hauptplatine des Systems. Der RJ-45 Anschluss verbindet die DRAC-NIC mit einem bandexternen Anschluss, wenn der DRAC 5 im **Dedizierten NIC**-Modus konfiguriert wird.

Sie können mittels des Management- und des MII-Kabels Ihren DRAC in drei getrennten Modi konfigurieren, abhängig von Ihren Bedürfnissen. "DRAC-Modi" in "RACADM Befehlszeilenoberfläche verwenden" enthält weitere Informationen.

DRAC 5-Schnittstellen

Tabelle 1-2 kennzeichnet die vom DRAC 5 verwendeten Schnittstellen, die auf eine Server-Verbindung hören. Tabelle 1-3 kennzeichnet die Schnittstellen, die der DRAC 5 als Client verwendet. Diese Informationen sind erforderlich, wenn Firewalls für den Remote-Zugriff auf einen DRAC 5 geöffnet werden.

Tabelle 1-2. DRAC 5 Server Hörschnittstellen

Schnittstellennummer	Funktion
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
161	SNMP Agent
443*	HTTPS
623	RMCP/RMCP +
3668*	Virtueller Datenträger-Server
3669*	Virtueller Datenträger Secure Service
5900*	Konsolenumleitungstastatur/Maus
5901*	Konsolenumleitungsvideo
* Konfigurierbare Schnittstelle	

Tabelle 1-3. DRAC 5 Client-Schnittstellen

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

Unterstützte Remote-Zugriffsverbindungen

Tabelle 1-4 führt die Verbindungsfunktionen auf.

Tabelle 1-4. Unterstützte Remote-Zugriffsverbindungen

Verbindung	Funktionen
DRAC 5-NIC	• 10/100 Mbps Ethernet • DHCP-Unterstützung • SNMP-Traps und E-Mail-Ereignis-Benachrichtigung • Dediziertes Netzwerk-Interface für das DRAC 5 webbasierte Interface • Support für telnet/ssh-Konsolen- und RACADM CLI-Befehle einschließlich Systemstart-,Reset-, Hochfahren-, und Herunterfahren-Befehle
Serielle Schnittstelle	• Support für die serielle Konsolen- und RACADM CLI-Befehle einschließlich Systemstart-, Reset-, Hochfahren-, und Herunterfahren-Befehle • Unterstützung für die Text-Only-Konsolenumleitung zu einem VT-100-Terminal oder Terminal-Emulator

DRAC 5 Sicherheitsfunktionen

Der DRAC 5 bietet die folgenden Sicherheitsfunktionen:

- Benutzerauthentifizierung durch Microsoft Active Directory optional) oder durch Hardware-gespeicherte Benutzer-ID und Kennwörter
- Rollenbasierte Autorität, die einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren
- Benutzer-ID und Kennwort-Konfiguration über die webbasierte Schnittstelle oder Racadm-CLI
- RACADM CLI- und webbasierter Schnittstellen-Vorgang, der SSL 128-Bit-Verschlüsselung und SSL 40-Bit-Verschlüsselung (für Länder, wo 128 Bit nicht annehmbar ist) unterstützt

  ANMERKUNG: Telnet unterstützt SSL-Verschlüsselung nicht.

- Sitzungszeitlimit-Konfiguration (in Sekunden) über die webbasierte Schnittstelle oder RACADM CLI
- Konfigurierbare IP-Schnittstellen (wo anwendbar)
- Secure Shell (SSH), die eine verschlüsselte Transportschicht für höhere Sicherheit verwendet.
- Anmeldungsmisserfolg-Beschränkung pro IP-Adresse, mit Anmeldungsblockierung der IP-Adresse, wenn die Grenze überschritten wird.
- Beschränkter IP-Adressenbereich für Clients, die an den DRAC 5 angeschlossen werden

Unterstützte Plattformen

Der DRAC 5 unterstützt die folgenden PowerEdge-Systeme:

- 1900
- 1950
- 2900
- 2950
- 2970
- 6950

Das *Dell PowerEdge Kompatibilitätshandbuch* auf der Dell Support-Website unter **support.dell.com** enthält die neuesten unterstützten Plattformen.

Unterstützte Betriebssysteme

Tabelle 1-5 führt die Betriebssysteme auf, die den DRAC 5 unterstützen.

Das *Dell OpenManage™ Server Administrator-Kompatibilitätshandbuch* auf der Dell Support-Website unter **support.dell.com** enthält die neuesten Informationen.

Tabelle 1-5. Unterstützte Betriebssysteme

Betriebssystem-Familie	Betriebssystem
Microsoft Windows	Windows 2000 Advanced Server mit Service Pack 4 (SP4) Windows 2000 Server mit SP4.

	Windows Server 2003 R2 Standard und Enterprise Editionen mit SP2 (32 Bit). Windows Server 2003 Web Edition mit SP2 (32 Bit). Windows Server 2003 R2 Standard- und Enterprise-Editionen mit SP2 (x86_64). Windows Server 2003 Standard- und Enterprise X64-Editionen mit SP1 und SP2. Windows-Speicher-Server 2003 R2 Workgroup, Standard- und Enterprise x64-Editionen (x86_64). Windows Vereinigter Datenspeicher-Server-2003 - goldene Standard- und Enterprise X64-Editionen (x86_64). Windows Vista™. **ANMERKUNG:** Wenn Sie Windows Server 2003 mit dem Service Pack 1 installieren, seien Sie sich bewusst, dass die Sicherheitseinstellungen von DCOM geändert werden. Weitere Informationen finden Sie im Artikel 903220 auf der Microsoft Support-Website unter **support.microsoft.com/kb/903220**.
Red Hat® Linux	Enterprise Linux Linux WS, ES und AS (Version 3) (x86 und x86_64). Enterprise Linux WS, ES und AS (Version 4) (ia32 und x86_64). Enterprise Linux WS, ES und AS (Version 4) (x86 und x86_64). Enterprise Linux 5 (x86 und x86-64). **ANMERKUNG:** Wenn Sie DRAC 5 mit Red Hat Enterprise Linux (Version 5)-Systemen verwenden, wird der Support auf einen verwalteten Knoten und racadm CLI beschränkt; verwaltete Konsole (webbasierte Schnittstelle) wird nicht unterstützt.
SUSE® Linux	Enterprise Server 9 mit Update 2 und Update 3 (x86_64). Enterprise Server 10 (Gold) (x86_64).

Unterstützte Internetbrowser

HINWEIS: Konsolenumleitung und Virtueller Datenträger unterstützen nur 32-Bit Internetbrowser. Das Verwenden von 64-Bit-Internetbrowsern kann unerwartete Ergebnisse oder Betriebsfehler hervorrufen.

Tabelle 1-6 führt die Internetbrowser auf, die den DRAC 5 unterstützen.

Das *Dell OpenManage™ Server Administrator-Kompatibilitätshandbuch* auf der Dell Support-Website unter **support.dell.com** enthält die neuesten Informationen.

Tabelle 1-6. Unterstützte Internetbrowser

Betriebssystem	Unterstützter Internetbrowser
Windows	Internet Explorer 6.0 (32 Bit) mit Service Pack 2 (SP2) für Windows XP und nur Windows 2003 R2 SP2. Internet Explorer 7.0 für Windows Vista, Windows XP und nur Windows 2003 R2 SP2 nur. Lokalisierte Versionen der DRAC 5 webbasierten Schnittstelle finden Sie unter: 1. Öffnen Sie die Windows-**Systemsteuerung**. 2. Doppelklicken Sie auf das Symbol **Regionale Optionen**. 3. Wählen Sie das gewünschte Gebietsschema aus dem Drop-Down-Menü **Ihr Gebietsschema (Standort)** aus. **HINWEIS:** Wenn Sie den Virtueller Datenträger-Client ausführen, müssen Sie Internet Explorer 6.0 mit Service Pack 1 oder später verwenden.
Linux	Mozilla Firefox 1.5 (32-Bit) nur auf SUSE Linux (Version 10). Nur Mozilla Firefox 2.0 (32-Bit).

Whitelist-Funktion in Mozilla Firefox deaktivieren

Firefox enthält eine "Whitelist"-Funktion, die zusätzliche Sicherheit bietet. Wenn die Whitelist-Funktion aktiviert ist, erfordert der Browser Benutzerberechtigung, um für jede einzelne Site, die das Plugin hostet, Plugins installieren zu können. Dieses Verfahren erfordert, dass für jeden einzelnen RAC IP/DNSname ein Plugin installiert wird, auch wenn die Plugin-Versionen identisch sind.

Um die Whitelist-Funktion zu deaktivieren und sich wiederholende, unnötige Plugin-Installationen zu vermeiden, führen Sie folgende Schritte aus:

1. Öffnen Sie ein Internetbrowser-Fenster in Firefox.

2. Geben Sie im Adressfeld Folgendes ein, und drücken Sie auf <Eingabe>:

   ```
   about:config
   ```

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

   Die Werte für **Einstellungsname**, **Status**, **Typ** und **Wert** ändern Sie 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.

Funktionen

Der DRAC 5 enthält die folgenden Funktionen:

- Dynamische Domänenname-System (DNS) -Registrierung
- Remote-Systemverwaltung und -Überwachung mittels Internet-basierter Benutzeroberfläche, serieller Verbindung, Remote-RACADM oder Telnet-Verbindung.
- Support für Active Directory-Authentifizierung - Fasst alle DRAC 5-Benutzer-IDs und -Kennwörter in Active Directory zusammen, das Standardschema und Erweitertes Schema verwendet.
- Konsolenumleitung - Enthält Remote-Systemtastatur-, Video- und Maus-Funktionen.
- Virtueller Datenträger - Ermöglicht einem verwalteten Systen, auf ein Datenträgerlaufwerk auf der Verwaltungsstation zuzugreifen.
- Zugriff auf Systemereignisprotokolle - Bietet Zugang zum Systemereignisprotokoll (SEL), DRAC 5-Protokoll und Bildschirm letzter Absturz des abgestürzten oder nicht reagierenden Systems, unabhängig vom Betriebssystem-Zustand.
- Dell OpenManage™Software-Integration - Ermöglicht, die webbasierte DRAC 5 Schnittstelle vom Dell OpenManage Server Administrator oder IT Assistent zu starten.
- RAC-Warnung - Warnt Sie vor potenziellen Problemen mit verwalteten Knoten mittels E-Mail-Benachrichtigung oder eines SNMP-Traps, mit den NIC-Einstellungen **Dediziert**, **Freigegeben für Failover**, oder **Freigegeben**.
- Lokale und Remote-Konfiguration - Lokale und Remote-Konfiguration mittels des RACADM Befehlszeilendienstprogramms.
- Remote-Stromverwaltung - Enthält Remote Stromverwaltungsfunktionen von einer Verwaltungskonsole aus, wie Herunterfahren und Reset.
- IPMI-Support.
- Secure Sockets Layer (SSL) -Verschlüsselung - Bietet sichere Remote-Systemverwaltung über die webbasierte Schnittstelle.
- Kennwort-Stufe-Sicherheitsmanagement - Verhindert unberechtigten Zugriff auf ein Remote-System.
- Rollenbasierte Autorität- Enthält zuweisbare Berechtigungen für verschiedene Systems Management-Tasks.

Weitere nützliche Dokumente

Zusätzlich zu diesem *Benutzerhandbuch* bieten die folgenden Dokumente zusätzliche Informationen über das Setup und Betrieb des DRAC 5 in Ihrem System:

- DRAC 5-Online-Hilfe bietet Informationen über das Verwenden des webbasierten Interface.
- Im *Dell OpenManage™ IT Assistant-Benutzerhandbuch* und im *Dell OpenManage IT Assistant Referenzhandbuch* finden Sie Informationen über den IT Assistant.
- Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen über die Installation und Verwendung von Server Administrator.
- Im *Dell OpenManage Baseboard-Verwaltungs-Controller Dienstprogramm-Benutzerhandbuch* finden Sie Informationen über die Konfiguration des Baseboard-Verwaltungs-Controllers (BMC), die Konfiguration des verwalteten Systems mittels des BMC-Verwaltungsdienstprogramms sowie weitere BMC-Informationen.
- Das *Dell Update Packages Benutzerhandbuch* enthält Informationen über Besorgung und Anwendung von Dell Update-Paketen als ein Teil Ihrer Systemaktualisierungsstrategie.

Die folgenden System-Dokumente sind außerdem erhältlich, um mehr Informationen über das System zu bieten, in dem Ihr DRAC 5 installiert wird:

- Das *Produktinformationshandbuch* enthält wichtige Sicherheits- und Durchführungsinformationen. Garantie-Informationen können innerhalb dieses Dokumentes oder als ein getrenntes Dokument beigelegt sein.
- Das *Rackinstallationshandbuch* und die *Rackinstallationsanleitungen*, die in Ihrer Racklösung enthalten sind, beschreiben, wie man Ihr System in ein Rack einbaut.
- Das *Handbuch zum Einstieg* enthält eine Übersicht über die Systemfunktionen, Einrichtung des Systems und technische Daten.
- *Hardwarebenutzerhandbuch* gibt Auskunft über die Systemfunktionen und beschreibt die Fehlerbehebung am System sowie die Installation oder den Austausch von Systemkomponenten.
- Die Dokumentation zur Systems Management Software beschreibt die Funktionen, Anforderungen, Installation und grundlegenden Betrieb der Software.
- Die Betriebssystem-Dokumentation beschreibt wie man (falls erforderlich) die Betriebssystem-Software installiert, konfiguriert und verwendet.

- Die Dokumentation für Komponenten, die Sie getrennt gekauft haben, bietet Informationen, um diese Optionen zu konfigurieren und installieren.
- Aktualisierungen sind manchmal im System enthalten, um Änderungen am System, an der Software, und/oder Dokumentation zu beschreiben.

  ANMERKUNG: Lesen Sie immer die Aktualisierungen zuerst, weil sie oft Informationen in anderen Dokumenten ersetzen.

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Bereitstellung des Betriebssystems mittels VM-CLI

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Das Dienstprogramm Virtueller Datenträger-Befehlszeilenoberfläche (VM-CLI) ist eine Befehlszeilenoberfläche, die die Funktionen des Virtuellen Datenträgers von der Verwaltungsstation zum DRAC 5 im Remote-System bereitstellt. Mit VM-CLI und Scriptmethoden können Sie Ihr Betriebssystem auf mehreren Remote-Systemen in Ihrem Netzwerk einsetzen.

Dieser Abschnitt gibt Auskunft über die Integrierung des VM-CLI Dienstprogramms in Ihr Betriebsnetz.

Bevor Sie Beginnen

Vor dem Einsatz des VM-CLI Dienstprogramms stellen Sie sicher, dass die gewünschten Remote-Systeme und das Betriebsnetz den in den folgenden Abschnitten aufgeführten Anforderungen entsprechen.

Remote-System-Anforderungen

- Die DRAC 5-Karte wird in jedem Remote-System installiert
- Das virtuelle Gerät in jedem Remote System ist das erste Gerät in der BIOS-Startreihenfolge.

Dell benutzerdefinierte Werksintegration

Wenn Sie Ihr System mit Dell Custom Factory Integration (CFI) -Optionen bei Dell bestellen, kann Dell Ihr System mit einer DRAC 5-Karte vorkonfigurieren, die einen DDNS-Namen und ein vorkonfiguriertes System-BIOS enthält, das für den Virtuellen Datenträger aktiviert ist. Mit dieser Konfiguration ist Ihr System bereit, von seinen Virtueller Datenträger-Geräten zu starten, wenn es in Ihr Betriebsnetz installiert wird.

Weitere Informationen sind auf der Dell-Website unter **www.dell.com** erhältlich.

Netzwerk-Anforderungen

Eine Netzwerkfreigabe muss die folgenden Komponenten enthalten:

- Betriebssystemdateien
- Erforderliche Treiber
- Betriebssystem-Startbilddatei(en)

Die Abbilddatei muss ein Diskettenabbild oder CD/DVD ISO-Abbild mit einem industriestandardmäßigen, startfähigen Format sein.

Startfähige Abbilddatei erstellen

Bevor Sie die Abbilddatei den Remote-Systemen bereitstellen, stellen Sie sicher, dass ein unterstütztes System von der Datei starten kann. Um die Abbilddatei zu prüfen, übertragen Sie sie auf ein Testsystem mit der DRAC 5 Internetbenutzeroberfläche und dann starten Sie das System neu.

Die folgenden Abschnitte enthalten spezifische Informationen über das Erstellen von Abbilddateien für Linux- und Windows-Systeme.

Erstellen einer Abbilddatei für Linux-Systeme

Verwenden Sie das Datenvervielfältigungs-Dienstprogramm, um eine startfähige Abbilddatei für das Linux-System zu erstellen.

Um das Dienstprogramm auszuführen, öffnen Sie eine Befehls-Eingabeaufforderung und geben Sie Folgendes ein:

```
dd if=<Eingabegerät> of=<Ausgabedatei>
```

Beispiel:

```
dd if=/dev/fd0 of=myfloppy.img
```

Abbilddatei für Windows-Systeme erstellen

Wenn Sie ein Datenvervielfältigungs-Dienstprogramm für Windows-Abbilddateien wählen, wählen Sie ein Dienstprogramm, das die Abbilddatei und die CD/DVD-Startsektoren kopiert.

Vorbereitung auf die Bereitstellung

Remote-Systeme konfigurieren

1. Erstellen Sie eine Netzwerkfreigabe, auf die über die Verwaltungsstation zugegriffen werden kann.

2. Kopieren Sie die Betriebssystem-Dateien zur Netzwerkfreigabe.

3. Wenn Sie eine startfähige, vorkonfigurierte Bereitstellungs-Abbilddatei zur Bereitstellung des Betriebssystems zu den Remote-Systemen haben, können Sie diesen Schritt überspringen.

   Wenn Sie keine startfähige, vorkonfigurierte Bereitstellungs-Abbilddatei haben, erstellen Sie die Datei. Schließen Sie alle für die Betriebssystem-Bereitstellungsverfahren verwendeten Programme und/oder Skripte ein

   Um zum Beispiel das Microsoft® Windows® Betriebssystem bereitzustellen, kann die Abbilddatei Programme enthalten, die den von Microsoft Systems Management Server (SMS) verwendeten Bereitstellungsmethoden ähnlich sind.

   Wenn Sie die Abbilddatei erstellen, führen Sie folgendes aus:

   - Befolgen Sie die netzwerkbasierten Standardinstallationsverfahren
   - Kennzeichnen Sie das Bereitstellungsimage als "read only", um sicherzustellen, dass jedes Zielsystem startet und dasselbe Bereitstellungsverfahren ausführt

4. Führen Sie eins der folgenden Verfahren aus:

   - Integrieren Sie RACADM und die Befehlszeilenoberfläche des Virtuellen Datenträgers (VM-CLI) in Ihre vorhandene Betriebssystem-Bereitstellungsanwendung. Verwenden Sie das Beispiel-Bereitstellungsskript als Anleitung, wenn Sie die DRAC 5-Dienstprogramme in Ihre vorhandene Betriebssystem-Bereitstellungsanwendung integrieren.
   - Verwenden Sie das vorhandene **vmdeploy**-Skript, um Ihr Betriebssystem bereitzustellen.

Betriebssystem bereitstellen

Verwenden Sie das im Dienstprogramm enthaltene VM-CLI-Dienstprogramm und **vmdeploy** Skript, um das Betriebssystem zu Ihren Remote Systemen bereitzustellen.

Bevor Sie beginnen, sehen Sie sich das **vmdeploy**-Beispiel-Script an, das mit dem VM-CLI-Dienstprogramm enthalten ist. Das Skript enthält ausführliche Voraussetzungen für die Bereitstellung des Betriebssystems zu Remote-Systemen in Ihrem Netzwerk.

Das folgende Verfahren enthält eine hochstufige Übersicht zur Bereitstellung des Betriebssystems auf Remote-Zielsystemen.

1. Identifizieren Sie die Remote-Systeme, die bereitgestellt werden.

2. Notieren Sie die DRAC 5-Namen und IP-Adressen der Remote-Zielsysteme.

3. Führen Sie das folgende Verfahren für jedes Remote-Zielsystem aus:
   a. Konfigurieren Sie ein VM-CLI-Verfahren, das die folgenden Parameter für das Remote-Zielsystem einbezieht:
      - DRAC 5 IP-Adresse oder DDNS-Name
      - Startfähiger Bereitstellung-Abbilddateiname
      - DRAC 5-Benutzername
      - DRAC 5-Benutzerkennwort
   b. Setzen Sie die Ziel-DRAC 5-Option **Einmaliger Start** mittels RACADM.
   c. Starten Sie das DRAC 5 System neu mit RACADM.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5 SM-CLP Befehlszeilenoberfläche verwenden

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Dieser Abschnitt gibt Auskunft über das Server-Management Workgroup (SMWG) Server-Verwaltungsbefehlszeilenprotokoll (SM-CLP), das im DRAC 5 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 über diese Angaben finden Sie auf der Website zur Distributed Management Task Force (DMTF) unter **www.dmtf.org**.

Das DRAC 5 SM-CLP ist ein Protokoll, das nach DMTF und SMWG mit ihren Normen für Systems Management CLI-Umsetzungen gestaltet ist. 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.

DRAC 5 SM-CLP-Support

DRAC 5 ist das erste RAC-Produkt, das Support für das auf dem SM-CLP-Standard basierende Befehlszeilenprotokoll bietet. Der Host für den SM-CLP ist die DRAC 5 Controller-Firmware und Telnet, SSH, und seriellbasierte Schnittstellen werden unterstützt. Die DRAC 5 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 DRAC 5 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.

Tabelle 11-1 enthält eine Liste der unterstützten CLI-Verben.

Tabelle 11-1. Unterstützte CLI-Verben

Verb	Definition
cd	Wechselt durch die MAP mittels der Shell.
delete	Löscht ein Objekt-Beispiel.
help	Zeigt die Hilfe für ein spezifisches Ziel an.
reset	Setzt das Ziel zurück.
show	Zeigt die Zieleigenschaften, Verben, und Unterziele an.
start	Schaltet ein Ziel ein.
stop	Fährt ein Ziel herunter.
exit	Beendet SM-CLP Shell-Sitzung.
version	Zeigt die Versionsattribute eines Ziels an.

SM-CLP-Verwaltungsvorgänge und Ziele

SM-CLP fördert das Konzept von Verben und Zielen, zur Bereitstellung von Systems Management-Fähigkeiten durch den CLI. Das Verb zeigt den auszuführenden Vorgang an und das Ziel bestimmt die Entität (oder Objekt), die den Vorgang ausführt.

Es folgt ein Beispiel der SM-CLP Befehlszeilensyntax.

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

Während einer typischen SM-CLP Sitzung kann der Benutzer Vorgänge mittels der in Tabelle 11-1 aufgeführten Verben ausführen.

Verwaltungsvorgänge

Der DRAC 5 SM-CLP ermöglicht Benutzern die Verwaltung der folgenden Punkte:

- Server-Stromverwaltung - Einschalten, herunterfahren oder das System neu starten
- Systemereignisprotokoll (SEL) -Verwaltung - Anzeige oder Löschen der SEL-Datensätze

Ziele

Tabelle 11-2 enthält eine Liste von durch den SM-CLP gebotenen Zielen, die diese Vorgänge unterstützen.

Tabelle 11-2. SM-CLP-Ziele

Ziel	Definition
/system1	Das verwaltete System-Ziel.
/system1/logs1	Das Protokollsammlungsziel
/system1/logs1/log1	Das Systemereignisprotokoll (SEL) -Ziel auf dem verwalteten System.
/system1/logs1/log1/record1	Ein einzelnes SEL-Datensatzbeispiel auf dem verwalteten System.

Optionen

Tabelle 11-3 führt die unterstützten SM-CLP-Optionen auf.

Tabelle 11-3. Unterstützte SM-CLP-Optionen

SM-CLP-Option	Beschreibung
-all	Beauftragt das Verb, alle möglichen Funktionen auszuführen.
-display	Zeigt die benutzerdefinierten Daten an.
-examine	Beauftragt den Befehlsprozessor, die Befehl-Syntax zu validieren, ohne den Befehl auszuführen.
-help	Zeigt Hilfe zu den Befehlsverben an.
-version	Zeigt die Befehlsverb-Version an.

SM-CLP-Ausgabeformat

Der DRAC 5 unterstützt gegenwärtig textbasierte Ausgaben, wie in den SM-CLP-Spezifikationen beschrieben.

DRAC 5 SM-CLP, Beispiele

Die folgenden Absätze enthalten Beispiele zur Verwendung des SM-CLP für die folgenden Vorgänge:

- Server-Stromverwaltung
- SEL-Management
- MAP-Ziel-Navigierung
- Anzeigesystemeigenschaften

Server-Stromverwaltung

Tabelle 11-4 enthält Beispiele für die Verwendung von SM-CLP zur Ausführung von Stromverwaltungsvorgängen auf einem verwalteten System.

Tabelle 11-4. Server-Stromverwaltungsvorgänge

Vorgang	Syntax

Anmeldung am RAC über die telnet/SSH-Schnittstelle	`>ssh 192.168.0.120`
	`>login: root`
	`>password:`

SM-CLP Verwaltungs-Shell	`-`
	`>smclp`
	`DRAC5 SM-CLP System Management Shell, version 1.0`
	`Copyright (c) 2004-2006 Dell, Inc.`
	`All Rights Reserved`
	`->`

Server herunterfahren	`-`
	`->stop /system1`
	`system1 has been stopped successfully`

Server von einem ausgeschalteten Zustand hochfahren	-

	->start /system1 system1 has been started successfully
Server neu starten	->reset /system1 system1 has been reset successfully

SEL-Management

Tabelle 11-5 enthält Beispiele für die Verwendung von SM-CLP, um SEL-verwandte Vorgänge auf dem verwalteten System auszuführen.

Tabelle 11-5. SEL-Verwaltungsvorgänge

Vorgang	Syntax
SEL ansehen	->show /system1/logs1/log1 /system1/logs1/log1 Targets: Record1 Record2 Record3 Record4 Record5 Properties: InstanceID = IPMI:BMC1 SEL Log MaxNumberOfRecords = 512 CurrentNumberOfRecords = 5 Name = IPMI SEL EnabledState = 2 OperationalState = 2 HealthState = 2 Caption = IPMI SEL Description = IPMI SEL ElementName = IPMI SEL Commands: cd show help exit version
SEL-Datensatz ansehen	->show /system1/logs1/log1/record4 /system1/logs1/log1/record4 Properties: LogCreationClassName = CIM_RecordLog CreationClassName = CIM_LogRecord LogName = IPMI SEL RecordID = 1 MessageTimeStamp = 20050620100512.000000-000 Description = FAN 7 RPM: fan sensor, detected a failure ElementName = IPMI SEL Record Commands: cd show help exit version
SEL löschen	->delete /system1/logs1/log1/record* All records deleted successfully

MAP Ziel-Navigation

Tabelle 11-6 enthält Beispiele für die Verwendung des Verbs **cd**, um innerhalb der MAP zu navigieren. In allen Beispielen wird angenommen, dass das ausgängliche Standardziel '/' ist.

Tabelle 11-6. Map-Zielnavigationsvorgänge

Vorgang	Syntax
Zum System-Ziel wechseln und einen Neustart durchführen	->cd system1 ->reset **ANMERKUNG:** Das aktuelle Standardeinstellungsziel ist '/'.
Wechseln Sie zum SEL-Ziel und zeigen Sie die Protokolldatensätze an	->cd system1

	->cd logs1/log1 ->show
	->cd system1/logs1/log1 ->show
Aktuelles Ziel anzeigen	->cd.
Eine Stufe höher gehen	->cd..
Shell beenden	->exit

Systemeigenschaften

Tabelle 11-7 führt die System-Eigenschaften auf, die angezeigt werden, wenn der Benutzer folgendes eingibt:

```
show /system1
```

Diese Eigenschaften werden aus dem Grundsystemprofil abgeleitet, das von der Normengruppe bereitgestellt wird und auf der **CIM_ComputerSystem-**Klasse laut Definition durch das CIM-Schema beruht.

Weitere Informationen erhalten Sie über die DMTF CIM-Schema-Definitionen.

Tabelle 11-7. Systemeigenschaften

Objekt	Eigenschaft	Beschreibung
CIM_Computersystem	Name	Eindeutiger Bezeichner eines System-Beispiels, der in der Unternehmensumgebung besteht. MaxLen = 256
	ElementName	Benutzerfreundlicher Name für das System. MaxLen = 64
	NameFormat	Identifiziert die Methode, mit der der Name erstellt wird. Werte: Andere, IP, Wählen, HID, NWA, HWA, X25, ISDN, IPX, DCC, ICD, E.164, SNA, OID/OSI, WWN, NAA
	Dedicated	Aufzählung, die anzeigt, ob das System ein Spezialsystem oder ein Allgemeinzwecksystem ist. Werte: 0=Nicht Reserviert 1=Unbekannt 2=Andere 3=Speicher 4=Router 5=Switch 6=Layer 3 Schalter 7=CentralOffice Switch 8=Hub 9=Zugang-Server 10=Firewall 11=Print 12=E/A 13=Web-Caching 14=Management 15=Server blockieren 16=Dateiserver 17=Mobiles Benutzergerät, 18=Verstärker 19=Bridge/Extender

		20=Gateway 21=Speicher-Virtualizer 22=Datenträger-Bibliothek 23=Extender-Knoten 24=NAS-Kopf 25=Eigenständiges NAS 26=USV 27=IP-Telefon 28=Management-Controller 29=Chassis-Manager
	ResetCapability	Definiert die Reset-Methoden, die auf dem System verfügbar sind Werte: 1=Andere 2=Unbekannt 3=Deaktiviert 4=Aktiviert 5=Nicht umgesetzt
	CreationClassName	Die Superklasse, von der dieses Beispiel abgeleitet wurde.
	EnabledState	Zeigt die aktivierten/deaktivierten Zustände des Systems an. Werte: 0=Unbekannt 1=Andere 2=Aktiviert 3=Deaktiviert 4=Herunterfahren 5=Nicht anwendbar 6=Aktiviert, aber Offline 7=In Test 8=Verzögert 9=Stilllegen 10=Start
	EnabledDefault	Zeigt die Standardstartkonfiguration für den aktivierten Zustand des Systems an. Standardmäßig ist das System "Aktiviert" (Wert=2). Werte: 2=Aktiviert 3=Deaktiviert 4=Nicht anwendbar 5=Aktiviert, aber Offline 6=Keine Standardeinstellung
	RequestedState	Zeigt den letzten angeforderten oder gewünschten Zustand für das System an. Werte: 2=Aktiviert 3=Deaktiviert 4=Herunterfahren 5=Keine Änderung

		6=Offline 7=Test 8=Verzögert 9=Stilllegen 10=Neustart 11=Zurücksetzen 12=Nicht anwendbar
	HealthState	Zeigt den aktuellen Funktionszustand des Systems an. Werte: 0=Unbekannt 5=OK 10=Herabgesetzt/Warnung 15=Minder schwerer Fehler 20=Schwerwiegender Fehler 30=Kritischer Fehler 35=Nicht behebbarer Fehler
	OperationalStatus	Zeigt den aktuellen Status des Systems an. Werte: 0=Unbekannt 1=Andere 2=OK 3=Herabgesetzt 4=Gestresst 5=Vorhergesagter Fehler 6=Fehler 7=Nicht behebbarer Fehler 8=Start 9=Stopp 10=Angehalten 11=In Betrieb 12=Kein Kontakt 13=Kommunikation verloren 14=Abgebrochen 15=Ruhezustand 16=Supporteinheit fehlerhaft 17=Abgeschlossen 18=Strom-Modus
	Description	Eine textbasierte Beschreibung des Systems.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Fehlerbehebung

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

---

Störungen beim DRAC 5 beheben

Die folgenden Tabellen enthalten Hilfe zur Fehlerbehebung an DRAC 5 und RACADM:

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5 installieren und einrichten

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Dieser Abschnitt enthält Informationen über Installation und Setup der DRAC 5-Hardware und -Software.

Bevor Sie Beginnen

Sammeln Sie die folgenden Artikel aus dem Lieferumfang des Systems, bevor Sie die RAC 5-Software installieren und konfigurieren:

- DRAC 5-Hardware (zurzeit installiert oder im optionalen Einbausatz)
- DRAC 5 Installationsverfahren (in diesem Kapitel)
- CD *Dell PowerEdge Installation und Server-Management*
- CD *Dell Systems Management Consoles*
- CD *Dell PowerEdge Service and Diagnostic Utilities*
- CD *Dell PowerEdge Documentation*

DRAC 5-Hardware installieren

ANMERKUNG: Die DRAC 5-Verbindung emuliert eine USB-Tastaturverbindung. Infolgedessen wird das System wenn Sie es neu starten nicht benachrichtigen, wenn Ihre Tastatur nicht angeschlossen ist.

Der DRAC 5 kann auf Ihrem System vorinstalliert, oder getrennt in einem Einbausatz erhältlich sein. Zum Starten des auf dem System installierten DRAC 5 siehe "Software-Installation und Konfigurationsübersicht".

Wenn kein DRAC 5 auf Ihrem System installiert ist, siehe die im DRAC 5-Einbausatz enthaltene Anleitung *Remote-Zugriffskarte installieren* bzw. das *Installations- und Fehlerbehebungshandbuch* für Hardwareinstallationsanleitungen für Ihre Plattform.

ANMERKUNG: Das mit dem System ausgelieferte *Installations-und Fehlerbehebungshandbuch* enthält Informationen über den Ausbau des DRAC 5. Prüfen Sie außerdem alle Microsoft® Active Directory® RAC-Eigenschaften, die mit dem entfernten DRAC 5 verbunden sind, um ordnungsgemäße Sicherheit zu gewährleisten, wenn Sie erweitertes Schema verwenden.

Das System für die Verwendung eines DRAC 5 konfigurieren

Zum Konfigurieren des Systems für die Verwendung eines DRAC 5 verwenden Sie das Dell™ Remote-Zugriffkonfigurationsdienstprogramm (früher bekannt als das BMC Setup-Modul).

Um das Dell Remote-Zugriffskonfigurationsdienstprogramm auszuführen, führen Sie die folgenden Schritte aus:

1. Schalten Sie Ihr System ein oder starten Sie es erneut.
2. Drücken Sie <Strg><E>, wenn während des POST dazu aufgefordert wird

   Wenn das Betriebssystem zu laden beginn, bevor Sie <Strg><E> drücken, lassen Sie das System den Startvorgang beenden, dann starten Sie das System neu und versuchen es erneut.
3. Konfigurieren Sie die NIC.
   a. Mit der Abwärts-Pfeiltaste die **NIC-Auswahl** hervorheben.

b. Wählen Sie mit den Rechts- und Links-Pfeiltasten eine der folgenden NIC-Auswahlen:

- **Dediziert** - Diese Option auswählen, um das Remote-Zugriffsgerät zu aktivieren und die auf dem Remote Access Controller (RAC) verfügbare dedizierte Netzschnittstelle zu verwenden. Diese Schnittstelle ist nicht für das Host-Betriebssystem freigegeben und leitet den Verwaltungsverkehr zu einem getrennten physischen Netzwerk, wodurch es vom Anwendungsverkehr getrennt gehalten werden kann. Diese Option ist nur verfügbar, wenn eine DRAC-Karte im System installiert ist.
- **Freigegeben** - Diese Option auswählen, um die Netzschnittstelle an das Host-Betriebssystem freizugeben. Die Remote-Zugriffsgerätenetzschnittstelle ist völlig funktionell, wenn das Host-Betriebssystem für das NIC-Teaming konfiguriert wird. Das Remote-Zugriffsgerät erhält Daten über NIC 1 und NIC 2, aber überträgt Daten nur über NIC 1. Wenn NIC 1 ausfällt, ist das Remote-Zugriffsgerät nicht zugänglich.
- **Failover** - Diese Option auswählen, um die Netzschnittstelle an das Host-Betriebssystem freizugeben. Die Remote-Zugriffsgerätenetzschnittstelle ist völlig funktionell, wenn das Host-Betriebssystem für das NIC-Teaming konfiguriert wird. Das Remote-Zugriffsgerät erhält Daten über NIC 1 und NIC 2, aber überträgt Daten nur über NIC 1. Wenn NIC 1 ausfällt, schaltet das Remote-Zugriffsgerät für die gesamte Datenübertragung auf die NIC 2 um. Das Remote-Zugriffsgerät verwendet NIC 2 weiterhin für die Datenübertragung. Wenn NIC 2 versagt, schaltet das Remote-Zugriffsgerät die gesamte Datenübertragung zurück auf die NIC 1.

4. Netzwerk-Controller LAN-Parameter zur Verwendung von DHCP oder einer statischen IP-Adressenquelle konfigurieren.
   a. Mit der Abwärts-Pfeiltaste **LAN-Parameter** auswählen, und <Eingabe> drücken.
   b. **IP-Adressenquelle** mit den Aufwärts- und Abwärts-Pfeiltasten wählen.
   c. Mit der Rechts- und Links-Pfeiltaste **DHCP** oder **Statisch** wählen.
   d. Wenn Sie **Statisch** gewählt haben, konfigurieren Sie die **Ethernet-IP-Adresse**, **Subnetzmaske** und **Standard-Gateway-**Einstellungen.
   e. Drücken Sie <Esc>.
5. Drücken Sie <Esc>.
6. **Änderungen speichern und Beenden** wählen.

   Das System startet automatisch neu.

ANMERKUNG: Beim Anzeigen der Internet-Benutzeroberfläche auf einem Dell PowerEdge 1900-System, das mit einem NIC konfiguriert ist, zeigt die NIC-Konfigurationsseite zwei NICs an (NIC1 und NIC2). Dieses Verhalten ist normal. Das PowerEdge 1900-System (und andere PowerEdge-Systeme, die mit einem einzelnen LAN auf der Hauptplatine konfiguriert sind) können anhand von NIC-Teaming konfiguriert werden. Die Modi Freigegeben und Team arbeiten auf diesen Systemen unabhängig voneinander.

Das *Dell OpenManage Baseboard-Verwaltungs-Controller Dienstprogramm-Benutzerhandbuch* enthält weitere Informationen über das Dell Remote-Zugriffskonfigurationsdienstprogramm.

Software-Installation und Konfigurationsübersicht

Dieser Abschnitt bietet eine Übersicht auf höchster Ebene des DRAC 5 Softwareinstallations und Konfigurationsverfahrens. DRAC 5 mit der webbasierten Schnittstelle, RACADM-CLI oder Seriell/Telnet/SSH-Konsole konfigurieren.

Um weitere Informationen über die DRAC 5-Software-Komponenten zu erhalten, lesen Sie "Software auf dem verwalteten System installieren".

DRAC 5-Software installieren

Zum Installieren der DRAC 5-Software führen Sie die folgenden Schritte in der vorgegebenen Reihenfolge aus:

1. Installieren Sie die Software auf dem verwalteten System. Siehe "Software auf dem verwalteten System installieren".
2. Installieren Sie die Software auf der Verwaltungsstation. Siehe "Software auf der Verwaltungsstation installieren".

DRAC 5 konfigurieren

Zum Konfigurieren des DRAC 5 führen Sie die folgenden Schritte in der vorgegebenen Reihenfolge aus:

1. Wählen Sie eins der folgenden Konfigurationshilfsprogramme aus:
   - Webbasiertes Interface
   - RACADM-CLI
   - Seriell/Telnet/SSH-Konsole

HINWEIS: Die Verwendung von mehr als einem DRAC 5-Konfigurationshilfsprogramm zur gleichen Zeit kann zu unerwarteten Ergebnissen führen.

2. Konfigurieren Sie die DRAC 5-Netzwerk-Einstellungen. Siehe "DRAC 5-Netzwerk-Einstellungen konfigurieren".
3. Fügen Sie DRAC 5-Benutzer hinzu und konfigurieren Sie diese. Siehe "DRAC 5-Benutzer hinzufügen und konfigurieren".

4. Konfigurieren Sie den Internetbrowser, um auf die webbasierte Schnittstelle zuzugreifen. Siehe "Einen unterstützten Internetbrowser konfigurieren".

5. Deaktivieren Sie die Windows® -Option Automatischer Neustart. Siehe "Windows-Option automatischer Neustart deaktivieren".

6. Aktualisieren Sie die DRAC 5-Firmware. Siehe "DRAC 5-Firmware aktualisieren".

7. Greifen Sie auf den DRAC 5 über ein Netzwerk zu. Siehe "Über ein Netzwerk auf DRAC 5 zugreifen".

Software auf dem verwalteten System installieren

Software auf dem verwalteten System installieren ist optional. Ohne Managed System Software kann der RACADM nicht mehr lokal verwendet werden und der RAC kann den Bildschirm letzter Absturz nicht erfassen.

Um die Managed System Software zu installieren, installieren Sie die Software auf dem Managed System mittels der CD *Dell PowerEdge Installation and Server Management*. Anleitungen zur Installation dieser Software sind im *Schnellinstallationshandbuch* enthalten.

Managed System Software installiert Ihre Auswahlen von der entsprechenden Version von Server Administrator auf dem Managed System.

ANMERKUNG: Installieren Sie die DRAC 5 Management Station Software und die DRAC 5 Managed System Software nicht auf demselben System.

Wenn Server Administrator nicht auf dem Managed System installiert wird, können Sie den Bildschirm Letzter Absturz des Systems nicht ansehen oder die Funktion **Autom. Wiederherstellung** verwenden.

Weitere Informationen über den Bildschirm Letzter Absturz erhalten Sie unter "Den Bildschirm Letzter Absturz anzeigen".

Das verwaltete System konfigurieren, um den Bildschirm Letzter Absturz zu erfassen

Bevor der DRAC 5 den Bildschirm Letzter Absturz erfassen kann, müssen Sie das verwaltete System mit den folgenden Voraussetzungen konfigurieren.

1. Die Managed System Software installieren. Weitere Informationen über das Installieren der Managed System Software erhalten Sie im *Server Administrator-Benutzerhandbuch*.

2. Führen Sie ein unterstütztes Microsoft® Windows® Betriebssystem aus, wobei die Windows-Funktion "automatischer Neustart" in den **Windows-Start und Wiederherstellungs-Einstellungen** abgewählt ist.

3. Aktivieren Sie den Bildschirm Letzter Absturz (standardmäßig deaktiviert).

   Zur Verwendung von lokalem RACADM öffnen Sie eine Eingabeaufforderung und geben Sie die folgenden Befehle ein:

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

4. Aktivieren Sie den Zeitgeber für Autom. Wiederherstellung und setzen Sie die **Autom. Wiederherstellung**smaßnahme auf **Reset**, **Herunterfahren** oder **Aus- und Einschaltzyklus**. Zum Konfigurieren des Zeitgebers für **Autom. Wiederherstellung** müssen Sie Server Administrator oder IT-Assistant verwenden.

   Informationen über die Konfiguration des Zeitgebers für **Autom. Wiederherstellung** enthält das *Server Administrator-Benutzerhandbuch*. Um sicherzustellen, dass der Bildschirm Letzter Absturz erfasst werden kann, muss der Zeitgeber für **Autom. Wiederherstellung** auf mindestens 60 Sekunden eingestellt werden. Die Standardeinstellung ist 480 Sekunden.

   Der Bildschirm Letzter Absturz ist nicht verfügbar, wenn **Autom. Wiederherstellung**smaßnahme auf **Herunterfahren** oder **Aus- und Einschalten** gesetzt ist, wenn das Managed System ausgeschaltet wird.

Die Windows-Option Automatischer Neustart deaktivieren

Um sicherzustellen, dass die webbasierte DRAC 5 Schnittstellen-Funktion Bildschirm Letzter Absturz korrekt arbeitet, deaktivieren Sie die Option **Automatischer Neustart** auf Managed Systemen, die die Betriebssysteme Microsoft Windows Server 2003 und Windows 2000 ausführen.

Die Option Automatischer Neustart in Windows Server 2003 deaktivieren

1. Öffnen Sie die Windows-**Systemsteuerung** und doppelklicken Sie auf das **System**-Symbol.

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

3. Unter **Autostart und Wiederherstellung** klicken Sie auf **Einstellungen**.

4. Wählen Sie das Kontrollkästchen **Automatischer Neustart** ab.

5. Klicken Sie zweimal auf **OK.**

Die Option Automatischer Neustart in Windows Server 2000 deaktivieren

1. Öffnen Sie die Windows-**Systemsteuerung** und doppelklicken Sie auf das **System-**Symbol.
2. Klicken Sie auf das Register **Erweitert**.
3. Klicken Sie auf die Schaltfläche **Autostart und Wiederherstellung...**.
4. Wählen Sie das Kontrollkästchen **Automatischer Neustart** ab.

Software auf der Verwaltungsstation installieren

Ihr System enthält den Dell OpenManage Systemverwaltungssoftware-Einbausatz. Dieser Einbausatz umfasst, ist jedoch nicht auf die folgenden Komponenten beschränkt:

- CD *Dell PowerEdge Installation und Server-Management* - Eine startfähige CD mit den Hilfsprogrammen, die zum Konfigurieren des Systems und Installieren des Betriebssystems erforderlich sind. Diese CD enthält die neuesten Systems Management Software-Produkte, einschließlich Dell OpenManage Server Administrator Diagnostics, Storage-Management und Fernzugangsdienste.
- CD *Dell Systems Management Consoles* - Enthält die neuesten Dell Systems Management Console-Produkte einschließlich Dell OpenManage IT Assistant.
- CD *Dell PowerEdge Service and Diagnostic Utilities* - Enthält die Hilfsprogramme, die zum Konfigurieren des Systems erforderlich sind und Firmware, Diagnose und Dell-optimierte Treiber für das System.
- CD *Dell PowerEdge Dokumentation*- Hilft Ihnen, auf dem neuesten Stand zu bleiben, mit Dokumentation für Systeme, Systems Management Software-Produkte, Peripheriegeräte und RAID-Controller.

Informationen über die Installation der Server Administrator-Software enthält das *Server Administrator-Benutzerhandbuch*.

Red Hat Enterprise Linux (Version 4)-Verwaltungsstation konfigurieren

Der Dell Digital-KVM Viewer erfordert zusätzliche Konfiguration, um auf einer Red Hat Enterprise Linux (Version 4)-Verwaltungsstation auszuführen. Wenn Sie das Red Hat Enterprise Linux (Version 4) Betriebssystem auf Ihrer Verwaltungsstation installieren, führen Sie die folgenden Verfahren aus:

- Wenn dazu aufgefordert wird, Pakete hinzuzufügen oder zu entfernen, installieren Sie die optionale **Legacy-Software-Entwicklungs**software. Dieses Software-Paket enthält die Software-Komponenten, die zum Ausführen des Dell Digital-KVM-Viewers auf der Verwaltungsstation erforderlich sind.
- Um sicherzustellen, dass der Dell KVM Digitalzuschauer ordnungsgemäß funktioniert, öffnen Sie die folgenden Schnittstellen auf Ihrer Firewall:
  - Tastatur- und Maus-Port (Standard: Port 5900)
  - Video-Port (Standard: Port 5901)

RACADM auf einer Linux-Verwaltungsstation installieren und entfernen

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

ANMERKUNG: Wenn Sie **Setup** auf der CD *Systems Management Consoles* ausführen, wird das RACADM-Dienstprogramm für alle unterstützten Betriebssysteme auf der Verwaltungsstation installiert.

RACADM installieren

1. Melden Sie sich als 'root' an dem System an, auf dem Sie die Verwaltungsstation-Komponenten installieren wollen.
2. Laden Sie gegebenenfalls die CD *Dell Systems Management Consoles* mit dem folgenden oder einem ähnlichen Befehl:

   ```
   mount /media/cdrom
   ```

3. Wechseln Sie zum Verzeichnis **/linux/rac** und führen Sie den folgenden Befehl aus:

   ```
   rpm -ivh *.rpm
   ```

Für Hilfe mit dem RACADM-Befehl geben Sie nach der Eingabe der vorherigen Befehle **racadm help** ein. Weitere Informationen über RACADM finden Sie in "RACADM-Befehlszeilenoberfläche verwenden".

RACADM deinstallieren

Um RACADM zu deinstallieren, öffnen Sie eine Eingabeaufforderung und geben Sie folgendes ein:

```
rpm -e <racadm_Paket_Name>
```

wobei *<racadm_Paket_Name>* das rpm-Paket ist, das zum Installieren der RAC-Software verwendet wurde.

Wenn zum Beispiel der rpm Paket-Name **srvadmin-racadm5** ist, dann geben Sie ein:

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

Einen unterstützten Internetbrowser konfigurieren

Die folgenden Abschnitte enthalten Anleitungen zur Konfiguration von unterstützten Internetbrowsern. Eine Liste von unterstützten Internetbrowsern erhalten Sie unter "Unterstützte Internetbrowser".

Den Internetbrowser zum Anschluss an die webbasierte Schnittstelle konfigurieren

Wenn Sie die Verbindung an die webbasierte DRAC 5-Schnittstelle von einer Verwaltungsstation erstellen, die über einen Proxyserver an das Internet angeschlossen ist, muss der Internetbrowser darauf eingestellt werden, von diesem Server auf das Internet zuzugreifen.

Zum Konfigurieren des Internet Explorer Internetbrowsers zum Zugriff auf einen Proxyserver führen Sie die folgenden Schritte aus:

1. Öffnen Sie ein Internetbrowser-Fenster.
2. Klicken Sie auf **Hilfsprogramme** und dann auf **Internetoptionen**.
3. Vom Fenster **Internetoptionen**, klicken Sie auf das Register **Verbindungen**.
4. Unter den **Lokales Netzwerk (LAN) -Einstellungen** klicken Sie auf **LAN-Einstellungen**.
5. Wenn das Kästchen **Verwenden Sie einen Proxyserver** ausgewählt wird, wählen Sie das Kästchen **Umgehen Sie Proxyserver für lokale Adressen**.
6. Klicken Sie zweimal auf **OK.**

Liste vertrauenswürdiger Domänen

Wenn Sie über den Internet-Browser auf die DRAC 5-webbasierte Schnittstelle zugreifen, werden Sie dazu aufgefordert, die DRAC 5-IP-Adresse zur Liste vertrauenswürdiger Domänen hinzuzufügen, wenn die IP-Adresse auf der Liste fehlt. Wenn Sie diesen Vorgang ausgeführt haben, klicken Sie auf Aktualisieren oder starten Sie den Internet-Browser neu, um eine neue Verbindung zur DRAC 5-webbasierten Schnittstelle herzustellen.

32-Bit- und 64-Bit-Internetbrowser

Die DRAC 5-webbasierte Schnittstelle wird auf 64-Bit-Internetbrowsern nicht unterstützt. Wenn Sie einen 64-Bit-Browser öffnen, auf die Konsolenumleitungsseite zugreifen und versuchen, das Plugin zu installieren, schlägt das Installationsverfahren fehl. Wenn dieser Fehler nicht bestätigt wurde und Sie dieses Verfahren wiederholen, wird die Konsolenumleitungsseite geladen, obwohl die Plugin-Installation während Ihres ersten Versuchs fehlschlägt. Dieses Problem tritt auf, weil der Internet-Browser die Plugin-Informationen im Profilverzeichnis speichert, obwohl das Plugin-Installationsverfahren fehlgeschlagen ist. Um dieses Problem zu lösen, installieren Sie einen unterstützten 32-Bit-Internetbrowser, führen ihn aus und melden sich bei DRAC 5 an.

Lokalisierte Versionen des webbasierten Interface anzeigen

Windows

Die webbasierte DRAC 5-Schnittstelle wird auf den folgenden Windows Betriebssystemsprachen unterstützt:

- Englisch
- Französisch
- Deutsch
- Spanisch
- Japanisch
- Vereinfachtes Chinesisch

Um eine lokalisierte Version der webbasierten DRAC 5-Schnittstelle in Internet Explorer anzusehen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf das **Hilfsprogramme-**Menü und wählen Sie **Internetoptionen**.
2. Im Fenster **Internetoptionen** klicken Sie auf **Sprachen**.
3. Im **Fenster Spracheinstellung** klicken Sie auf **Hinzufügen**.
4. Im Fenster **Sprache hinzufügen** wählen Sie eine unterstützte Sprache.

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

Linux

Wenn Sie die Konsolenumleitung auf einem Red Hat Enterprise Linux-Client (Version 4) mit einer GUI für vereinfachtes Chinesisch ausführen, erscheint das Anzeigemenü und der Titel eventuell in willkürlichen Zeichen. Dieses Problem wird durch eine falsche Verschlüsselung im Red Hat Enterprise Linux-Betriebssystem für vereinfachtes Chinesisch (Version 4) verursacht. Um dieses Problem zu lösen, modifizieren Sie die aktuellen Verschlüsselungseinstellungen, indem Sie folgende Schritte ausführen:

1. Öffnen Sie einen Befehls-Terminal.
2. Geben Sie "locale" ein, und drücken Sie auf <Eingabe>. Die folgende Ausgabe erscheint.

   ```
   LANG=zh_CN.UTF-8
   LC_CTYPE="zh_CN.UTF-8"
   LC_NUMERIC="zh_CN.UTF-8"
   LC_TIME="zh_CN.UTF-8"
   LC_COLLATE="zh_CN.UTF-8"
   LC_MONETARY="zh_CN.UTF-8"
   LC_MESSAGES="zh_CN.UTF-8"
   LC_PAPER="zh_CN.UTF-8"
   LC_NAME="zh_CN.UTF-8"
   LC_ADDRESS="zh_CN.UTF-8"
   LC_TELEPHONE="zh_CN.UTF-8"
   LC_MEASUREMENT="zh_CN.UTF-8"
   LC_IDENTIFICATION="zh_CN.UTF-8"
   LC_ALL=
   ```
3. Wenn die Werte "zh_CN.UTF-8" einschließen, sind keine Änderungen erforderlich. Wenn die Werte "zh_CN.UTF-8" nicht einschließen, fahren Sie mit Schritt 4 fort.
4. Wechseln Sie zur Datei /etc/sysconfig/i18n.
5. Wenden Sie in der Datei folgende Änderungen an:

   Aktueller Eintrag:

   ```
   LANG="zh_CN.GB18030"
   SUPPORTED="zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
   ```

   Aktualisierter Eintrag:

   ```
   LANG="zh_CN.UTF-8"
   SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
   ```
6. Melden Sie sich beim Betriebssystem ab und dann wieder an.
7. Starten Sie DRAC 5 neu.

Wenn Sie von irgendeiner anderen Sprache zu vereinfachtem Chinesisch wechseln, ist sicherzustellen, dass die Korrektur noch gültig ist. Ist dies nicht der Fall, wiederholen Sie dieses Verfahren.

DRAC 5-Eigenschaften konfigurieren

Konfigurieren Sie die DRAC 5-Eigenschaften (Netzwerk, Benutzer, Warnungen usw.) mittels der webbasierten Schnittstelle oder des RACADM.

Weitere Informationen über die Verwendung der webbasierten Schnittstelle finden Sie unter "Zugriff auf die webbasierte Schnittstelle". Weitere Informationen über die Verwendung von RACADM in einer seriellen oder Telnet-Verbindung finden Sie unter "RACADM Befehlszeilenoberfläche verwenden".

DRAC 5-Netzwerk-Einstellungen konfigurieren

HINWEIS: Durch Änderungen an der DRAC 5 Netzwerk-Einstellungen kann die aktuelle Netzwerkverbindung getrennt werden.

DRAC 5-Netzwerkeinstellungen mit Hilfe eines der folgenden Hilfsprogramme konfigurieren:

- Webbasierte Schnittstelle - siehe "DRAC 5 NIC konfigurieren"
- RACADM CLI - siehe "cfgLanNetworking"
- Dell Remote-Zugriffskonfigurationsdienstprogramm - siehe "System zur Verwendung eines DRAC 5 konfigurieren"

ANMERKUNG: Wird der DRAC 5 in einer Linux-Umgebung eingesetzt, siehe "RACADM installieren".

DRAC 5-Benutzer hinzufügen und konfigurieren

Verwenden Sie eins der folgenden Hilfsprogramme, um DRAC 5-Benutzer hinzuzufügen und zu konfigurieren:

- Webbasiertes Interface - Siehe "DRAC 5-Benutzer hinzufügen und konfigurieren".
- Racadm-CLI - siehe "cfgUserAdmin".

DRAC 5-Firmware aktualisieren

Verwenden Sie eine der folgenden Methoden, um Ihre DRAC 5-Firmware zu aktualisieren.

- Webbasierte Schnittstelle - siehe "DRAC 5-Firmware mit der webbasierten Schnittstelle aktualisieren".
- RACADM CLI - siehe "fwupdate".
- Dell Update Packages - siehe *Dell Update Packages Handbuch* für Informationen über den Erwerb und die Verwendung von Dell Update-Paketen als Teil der Systemaktualisierungsstrategie

Bevor Sie Beginnen

Bevor Sie Ihre DRAC 5-Firmware anhand von lokalem RACADM oder Dell Update Packages aktualisieren, führen Sie die folgenden Verfahren aus. Andernfalls schlägt der Firmware-Aktualisierungsvorgang eventuell fehl.

1. Installieren und aktivieren Sie die entsprechende IPMI und die entsprechenden Treiber des verwalteten Knotens.
2. Wenn Ihr System das Windows-Betriebssystem ausführt, aktivieren und starten Sie die **Windows Management Instrumentation**-Dienste (WMI).
3. Wenn Ihr System SUSE Linux Enterprise Server (Version 10) für Intel EM64T ausführt, starten Sie den **Raw**-Dienst.
4. Stellen Sie sicher, dass der RAC-Virtual Flash entladen ist oder vom Betriebssystem bzw. einer anderen Anwendung oder einem anderen Benutzer nicht verwendet wird.
5. Trennen Sie die Verbindung zum virtuellen Datenträger, und entladen Sie ihn.
6. Stellen Sie sicher, dass USB aktiviert ist.

DRAC 5-Firmware herunterladen

Zum Aktualisieren der DRAC 5-Firmware laden Sie die neueste Firmware von der Dell Support-Website unter **support.dell.com** und speichern Sie die Datei zu Ihrem lokalen System.

Die folgenden Software-Komponenten sind in Ihrem DRAC 5-Firmwarepaket enthalten:

- Kompilierte DRAC 5-Firmwarecodes und -Daten
- Vergrößerungs-ROM-Image
- Webbasiertes Interface, JPEG und andere Benutzeroberflächen-Datendateien
- Standardeinstellungskonfigurationsdateien

Verwenden Sie die Seite **Firmware-Aktualisierung**, um die DRAC 5-Firmware zur spätesten Revision zu aktualisieren. Wenn Sie die Firmware-Aktualisierung ausführen, behält die Aktualisierung die aktuellen DRAC 5-Einstellungen bei.

DRAC 5-Firmware mittels der webbasierten Schnittstelle aktualisieren

1. Öffnen Sie die webbasierte Schnittstelle und melden Sie sich am Remote-System an.

   Siehe "Zugriff auf die webbasierte Schnittstelle".

2. In der **System**struktur klicken Sie auf **Remote-Zugriff** und dann auf das **Aktualisierung**-Register.

3. Geben Sie auf der Seite **Firmware-Update** in das Feld **Firmware-Image** den Pfad zu dem Firmware-Image ein, das Sie von **support.dell.com** heruntergeladen haben oder klicken Sie auf **Durchsuchen**, um zum Image zu wechseln.

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

   Beispiel:

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

   Der Name des Standardfirmware-Image ist **firmimg.d5**.

4. Klicken Sie auf **Aktualisieren**.

   Die Aktualisierung kann mehrere Minuten in Anspruch nehmen. Wenn abgeschlossen, erscheint ein Dialogfeld.

5. Klicken Sie auf **OK,** um die Sitzung zu schließen und sich automatisch abzumelden.

6. Nach dem DRAC 5-Reset klicken Sie auf **Anmelden**, um sich am DRAC 5 anzumelden.

Browser-Cache löschen

Nach dem Firmware-Upgrade löschen Sie den Internetbrowser-Cache.

Die Online-Hilfe Ihres Internetbrowsers enthält weitere Informationen.

Über ein Netzwerk auf DRAC 5 zugreifen

Nachdem Sie den DRAC 5 konfiguriert haben, können Sie im Remote-Zugriff mittels einer der folgenden Schnittstellen auf das Managed System zugreifen:

- Webbasiertes Interface
- RACADM
- Telnet-Konsole
- SSH
- IPMI

Tabelle 2-1 beschreibt jede DRAC 5-Schnittstelle.

Tabelle 2-1. DRAC 5-Interfaces

Interface	Beschreibung
Webbasiertes Interface	Enthält Remote-Zugriff zum DRAC 5 über eine graphische Benutzeroberfläche. Die webbasierte Schnittstelle ist in die DRAC 5-Firmware integriert und der Zugriff darauf erfolgt von einem unterstützten Internetbrowser über die NIC-Schnittstelle auf der Verwaltungsstation. Eine Liste von unterstützten Internetbrowsern erhalten Sie unter "Unterstützte Internetbrowser".
RACADM	Bietet Remote-Zugriff zum DRAC 5 mittels einer Befehlszeilenoberfläche. RACADM verwendet die IP-Adresse des Managed Systems, um RACADM-Befehle (RACADM Remote-Fähigkeitsoption [-r]) auszuführen. **ANMERKUNG:** Die racadm-Remote-Fähigkeit wird nur auf Verwaltungsstationen unterstützt. Weitere Informationen finden Sie in "Unterstützte Internetbrowser". **ANMERKUNG:** Wenn Sie die racadm-Remote-Fähigkeit verwenden, müssen Sie Schreiberlaubnis auf den Orndern haben, auf denen Sie die **racadm**-Unterbefehle verwenden, die Dateivorgänge einbeziehen; zum Beispiel: `racadm getconfig -f <Dateiname>`

	oder `racadm sslcertupload -t 1 -f c:\cert\cert.txt-Unterbefehle`
Telnet-Konsole	Gewährt Zugang durch den DRAC 5 zu den Server RAC-Anschluss- und Hardware-Managementschnittstellen über die DRAC 5 NIC und enthält Support für serielle und RACADM-Befehle einschließlich **powerdown**, **powerup**, **powercycle** und **hardreset**. **ANMERKUNG:** Telnet ist ein ungesichertes Protokoll, das alle Daten - einschließlich Kennwörter - im Klartext übersendet. Wenn Sie vertrauliche Informationen übersenden, verwenden Sie die SSH-Schnittstelle.
SSH-Schnittstelle	Bietet dieselben Fähigkeiten wie die Telnet-Konsole, die eine verschlüsselte Transportschicht für die höhere Sicherheit verwendet.
IPMI-Schnittstelle	Gibt Zugang über den DRAC 5 zu den grundlegenden Verwaltungsfunktionen des Remote-Systems. Die Schnittstelle umfasst IPMI über LAN, IPMI über Seriell und Seriell über LAN. Weitere Informationen finden Sie im *Dell OpenManage Baseboard Verwaltungs-Controllerbenutzerhandbuch*.

ANMERKUNG: Der DRAC 5 Standardbenutzername ist `root` und das Standardkennwort ist `calvin`.

Sie können auf das webbasierte DRAC 5-Interface mittels eines unterstützten Internetbrowsers über die DRAC 5-NIC oder über den Server Administrator oder IT Assistant zugreifen.

"Unterstützte Internetbrowser" enthält eine Liste der unterstützten Internetbrowser.

Zum Zugriff auf den DRAC 5 mit einem unterstützten Internetbrowser siehe "Zugriff auf die webbasierte Schnittstelle".

Zum Zugriff auf die DRAC 5 Fernzugriff-Schnittstelle mittels Server Administrator starten Sie den Server Administrator. Von der System-Struktur im linken Fensterbereich der Server Administrator-Einstiegsseite klicken Sie auf **System**→ **Hauptsystemgehäuse**→ **Remote Access Controller**. Weitere Informationen finden Sie in dem Server Administrator-Benutzerhandbuch.

Für Informationen über den Zugriff auf den DRAC 5 mittels RACADM siehe "RACADM Befehlszeilenoberfläche verwenden".

IPMI konfigurieren

Dieser Abschnitt enthält Informationen über das Konfigurieren und Verwenden der DRAC 5 IPMI-Schnittstelle. Die Schnittstelle enthält folgendes:

- IPMI über LAN
- IPMI über seriell
- Seriell über LAN

Der DRAC5 ist völlig IPMI 2.0-konform. Sie können den DRAC IPMI mittels Ihres Browsers, eines offenen Quelldienstprogramms wie *ipmitool*; mittels Dell OpenManage IPMI-Shell, **ipmish**, oder RACADM konfigurieren.

Für weitere Informationen über die Anwendung der IPMI-Shell, ipmish, siehe das *Dell OpenManage™ BMC Benutzerhandbuch* auf der Dell Support-Website unter **support.dell.com**.

Weitere Informationen über die Anwendung von RACADM finden Sie in "RACADM verwenden".

IPMI mittels der webbasierten Schnittstelle konfigurieren

1. Melden Sie sich über einen unterstützten Internetbrowser am Remote-System an. Siehe "Zugriff auf die webbasierte Schnittstelle".
2. IPMI über LAN konfigurieren.
   a. In der **System-**Struktur klicken Sie auf **Remote-Zugang**.
   b. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**.
   c. Auf der Seite **Netzwerkkonfiguration** unter **IPMI LAN Einstellungen** wählen Sie **IPMI über LAN aktivieren** und klicken Sie auf **Änderungen anwenden**.
   d. IPMI LAN-Kanalberechtigungen aktualisieren, falls erfordert.

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

   Unter **IPMI LAN-Einstellungen** auf das Dropdown-Menü **Beschränkung der Channel-Berechtigungsebene** klicken, **Administrator**, **Operator**, oder **Benutzer** wählen und auf **Änderungen anwenden** klicken.

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

   ANMERKUNG: Der DRAC 5 IPMI unterstützt das RMCP+-Protokoll.

   Unter **IPMI LAN-Einstellungen** im Feld **Verschlüsselungsschlüssel** den Verschlüsselungsschlüssel eingeben und auf **Änderungen anwenden** klicken.

   ANMERKUNG: Der Verschlüsselungsschlüssel muss aus einer geraden Anzahl hexadezimaler Zeichen mit maximal 40 Zeichen bestehen.

3. IPMI-Seriell über LAN (SOL) konfigurieren.

   a. In der **System-**Struktur klicken Sie auf **Remote-Zugang**.

   b. Im Register **Konfiguration** auf **Seriell über LAN** klicken.

   c. Auf der Seite **Seriell über LAN-Konfiguration** wählen Sie **Seriell über LAN aktivieren**.

   d. Aktualisieren Sie die IPMI SOL-Baudrate.

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

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

   f. **Erforderliche Mindestberechtigung** aktualisieren**.** Diese Eigenschaft definiert die Mindest-Benutzerberechtigung, die zur Verwendung der Funktion **Seriell über LAN** erforderlich ist.

   Klicken Sie auf das Dropdown-Menü **Beschränkung der Channel-Berechtigungsebene,** wählen Sie **Benutzer**, **Operator** oder **Administrator**.

   g. Klicken Sie auf **Änderungen anwenden**.

4. IPMI seriell konfigurieren.

   a. Im **Konfiguration-**Register auf **Serie** klicken.

   b. Im Menü **Serielle Konfiguration** ändern Sie den seriellen IPMI-Verbindungsmodus zu der entsprechenden Einstellung.

   Unter **IPMI Seriell** klicken Sie auf das Dropdown-Menü **Verbindungsmoduseinstellung** und wählen Sie den entsprechenden Modus aus.

   c. Stellen Sie die serielle IPMI-Baudrate ein.

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

   d. Stellen Sie die Beschränkung der Channel-Berechtigungsebene ein.

   Klicken Sie auf das Dropdown-Menü **Beschränkung der Channel-Berechtigungsebene,** wählen Sie **Administrator**, **Operator** oder **Benutzer**.

   e. Klicken Sie auf **Änderungen anwenden**.

   f. Stellen Sie sicher, dass der serielle MUX richtig im BIOS-Installationsprogramm des Managed Systems eingestellt ist.

      - Starten Sie das System neu.
      - Während des POST drücken Sie <F2>, um das BIOS-Installationsprogramm zu beginnen.
      - Wechseln Sie zu **Serial Communication (Serielle Kommunikation)**.
      - Im Menü **Serial Connection (Serielle Verbindung)** stellen Sie sicher, dass **External Serial Connector (Externer Seriell-Anschluss)** auf **Remote Access Device (Remote-Zugriffsgerät)** gesetzt ist.
      - BIOS-Setupprogramm speichern und beenden.
      - Starten Sie das System neu.

Wenn IPMI-seriell im Terminalmodus ist, können Sie die folgenden zusätzlichen Einstellungen konfigurieren:

- Löschsteuerung
- Echo-Steuerung
- Zeilenbearbeitung
- Neue Zeilen-Folgen
- Neue Zeilen-Folgen eingeben

Weitere Informationen über diese Eigenschaften finden Sie in der IPMI 2.0-Spezifikation.

IPMI mittels RACADM CLI konfigurieren

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

2. IPMI über LAN konfigurieren.

   Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie <Eingabe>:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
   ```

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

   a. IPMI-Kanalberechtigungen aktualisieren.

An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <Stufe>
```

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 den IPMI LAN-Kanalverschlüsselungsschlüssel ein, falls erforderlich.

ANMERKUNG: Der DRAC 5 IPMI unterstützt das RMCP+-Protokoll. Die IPMI 2.0-Spezifikationen enthalten weitere Informationen.

An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <Schlüssel>
```

wobei *<Schlüssel>* ein 20-Zeichen Verschlüsselungsschlüssel in einem gültigen Hexadezimal-Format ist.

3. IPMI-Seriell über LAN (SOL) konfigurieren.

An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a. Die IPMI SOL Mindestberechtigungsebene aktualisieren.

Die IPMI SOL-Mindestberechtigungsebene bestimmt die Mindestberechtigung, die zur Aktivierung von IPMI SOL erforderlich ist. Weitere Informationen enthält die IPMI 2.0 Spezifikation.

An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <Stufe>
```

wobei <*Stufe*> eine der folgenden ist:

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

Um zum Beispiel die IPMI-Berechtigungen für 2 (Benutzer) zu konfigurieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

b. Aktualisieren Sie die IPMI SOL-Baudrate.

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

An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <Baud_Rate>
```

wobei <*Baud_Rate*> 9600, 19200, 57600 oder 115200 Bits pro Sekunde ist.

Beispiel:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. SOL aktivieren.

ANMERKUNG: SOL kann für jeden einzelnen Benutzer aktiviert oder deaktiviert werden.

An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <ID> 2
```

wobei <*ID*> die eindeutige ID des Benutzers ist.

4. IPMI seriell konfigurieren.

a. IPMI serieller Verbindungsmodus zur entsprechenden Einstellung ändern.

An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

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

b. Stellen Sie die serielle IPMI-Baudrate ein.

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <Baud_Rate>
```

wobei <*Baud_Rate*> 9600, 19200, 57600 oder 115200 Bits pro Sekunde ist.

Beispiel:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600
```

c. Aktivieren Sie die serielle IPMI Hardware-Ablaufsteuerung.

An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

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

d. Stellen Sie die serielle IPMI Kanalmindestberechtigungsstufe ein.

An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <Stufe>
```

wobei <*Stufe*> eine der folgenden ist:

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

Zum Beispiel: um die seriellen IPMI-Kanalberechtigungen auf 2 (Benutzer) einzustellen, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

e. Stellen Sie sicher, dass der serielle MUX ordnungsgemäß im BIOS-Installationsprogramm eingestellt ist.

- Starten Sie das System neu.
- Während des POST drücken Sie <F2>, um das BIOS-Installationsprogramm zu beginnen.
- Wechseln Sie zu **Serial Communication (Serielle Kommunikation)**.
- Im Menü **Serial Connection (Serielle Verbindung)** stellen Sie sicher, dass **External Serial Connector (Externer Seriell-Anschluss)** auf **Remote Access Device (Remote-Zugriffsgerät)** gesetzt ist.
- BIOS-Setupprogramm speichern und beenden.
- Starten Sie das System neu.

Die IPMI- Konfiguration ist abgeschlossen.

Wenn IPMI seriell im Terminalmodus ist, können Sie die folgenden zusätzlichen Einstellungen mittels der Befehle **racadm config cfgIpmiSerial** konfigurieren:

- Löschsteuerung
- Echo-Steuerung
- Zeilenbearbeitung
- Neue Zeilen-Folgen
- Neue Zeilen-Folgen eingeben

Weitere Informationen über diese Eigenschaften finden Sie in der IPMI 2.0-Spezifikation.

Plattformereignisse konfigurieren

Plattformereigniskonfiguration enthält einen Mechanismus, um das Remote-Zugriffsgerät dahingehend zu konfigurieren, dass ausgewählte Maßnahmen an bestimmten Ereignis-Meldungen ausgeführt werden. Diese Maßnahmen umfassen Neustart, Aus-/Einschalten, Herunterfahren und das Auslösen einer Warnung (Plattformereignis-Trap [PET] und/oder E-Mail).

Die filtrierbaren Plattformereignisse umfassen die folgenden:

- Lüftersondenfehler
- Batteriesondenwarnung
- Batteriesondenfehler

- Diskreter Spannungssondenfehler
- Temperatursondenwarnung
- Temperatursondenfehler
- Gehäuseeingriff festgestellt
- Redundanz herabgesetzt
- Redundanz verloren
- Prozessorwarnung
- Prozessorfehler
- Prozessor nicht vorhanden
- PS/VRM/D2D-Warnung
- PS/VRM/D2D-Fehler
- Netzteil nicht vorhanden
- Hardwareprotokollfehler
- Automatische Systemwiederherstellung

Wenn ein Plattform-Ereignis eintritt (Beispiel: ein Lüftersondenfehler), wird ein Systemereignis erstellt und im Systemereignisprotokoll (SEL) registriert. Wenn dieses Ereignis einem Plattformereignisfilter (PEF) in der Plattformereignisfilterliste in der webbasierten Schnittstelle entspricht und Sie diesen Filter auf die Erstellung einer Warnung (PET oder E-Mail) konfiguriert haben, dann wird eine PET- oder E-Mail-Warnung an ein oder mehrere konfigurierte Ziele gesendet.

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

Plattformereignisfilter (PEF) konfigurieren

Konfigurieren Sie Ihre Plattformereignisfilter, bevor Sie die Plattformereignis-Traps oder E-Mail-Warnungseinstellungen konfigurieren.

PEF mittels der Internetbenutzeroberfläche konfigurieren

1. Melden Sie sich über einen unterstützten Internetbrowser am Remote-System an. Siehe "Zugriff auf die webbasierte Schnittstelle".
2. Klicken Sie auf das Register **Warnungsverwaltung** und dann auf **Plattformereignisse**.
3. Globale Warnungen aktivieren.
   a. Klicken Sie auf **Warnungsverwaltung** und wählen Sie **Plattformereignisse**.
   b. Wählen Sie das Kontrollkästchen **Plattformereignisfilterwarnung**.
4. Unter **Plattformereignisfilterkonfiguration** wählen Sie das Kontrollkästchen **Plattformereignisfilterwarnungen aktivieren** und klicken Sie dann auf **Änderungen anwenden**.
5. Unter **Plattformereignisfilterliste** auf den Filter doppelklicken, den Sie konfigurieren wollen.
6. Auf der Seite **Plattformereignisse festlegen** die entsprechenden Auswahlen vornehmen und dann auf **Änderungen anwenden** klicken.

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

PEF mittels RACADM CLI konfigurieren

1. PEF aktivieren.

   Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie <Eingabe>:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
   ```

   wobei 1 und 1 der PEF-Index und die Auswahloption aktivieren/deaktivieren sind.

   Der PEF-Index kann ein Wert von 1 bis 17 sein. Die Auswahl aktivieren/deaktivieren kann auf 1 (Aktiviert) oder 0 (Deaktiviert) eingestellt werden.

   Beispiel: Um PEF mit dem Index 5 zu aktivieren, geben Sie den folgenden Befehl ein:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
   ```

2. PEF-Maßnahmen konfigurieren.

   An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 *<Maßnahme>*

wobei <*action*> Wertbits wie folgt sind:

- <*Maßnahme*> Wertbit 0 - 1 = Warnungsmaßnahme aktivieren, 0 = Warnung deaktivieren
- <*Maßnahme*> Wertbit 1 - 1 = ausschalten; 0 = nicht ausschalten
- <*Maßnahme*> Wertbit 2 - 1 = Neustart; 0 = kein Neustart
- <*Maßnahme*> Wertbit 3 - 1 = Aus-/Einschalten; 0 = kein Aus-/Einschalten

Beispiel: um PEF zu aktivieren, um das System neu zu starten, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 2
```

wobei 1 der PEF-Index, und 2 die PEF-Maßnahme für den Neustart ist.

PET konfigurieren

PET mittels der Internetbenutzeroberfläche konfigurieren

1. Melden Sie sich über einen unterstützten Internetbrowser am Remote-System an. Siehe "Zugriff auf die webbasierte Schnittstelle".
2. Stellen Sie sicher, dass Sie die Verfahren in "PEF über die Internetbenutzeroberfläche konfigurieren" ausführen.
3. Konfigurieren Sie Ihre PET-Regel.
   a. Im Register **Warnungsverwaltung** auf **Traps-Einstellungen** klicken.
   b. Unter **Ziel-Konfigurationseinstellungen** das Feld **Community-Zeichenkette** mit den entsprechenden Informationen konfigurieren und dann auf **Änderungen anwenden** klicken.
4. Konfigurieren Sie Ihre PET-IP-Adresse
   a. In der Spalte **Zielnummer** klicken Sie auf eine Zielnummer.
   b. Stellen Sie sicher, dass das Kontrollkästchen **Ziel aktivieren** ausgewählt ist.
   c. Geben Sie eine gültige PET-Ziel-IP-Adresse in das **Ziel-IP-Adresse** Feld ein.
   d. Klicken Sie auf **Änderungen anwenden**.
   e. Klicken Sie auf **Test-Trap senden**, um die konfigurierte Warnung (wenn gewünscht) zu prüfen.

   ANMERKUNG: Ihr Benutzerkonto muss die Berechtigung **Testwarnungen** haben, um dieses Verfahren auszuführen. Siehe Tabelle 4-8.

   f. Wiederholen Sie Schritt a bis Schritt e für alle verbleibenden Zielnummern.

PET mit RACADM- CLI konfigurieren

1. Aktivieren Sie die globalen Warnungen.

   Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie <Eingabe>:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. PET aktivieren.

   An der Eingabeaufforderung geben Sie die folgenden Befehle ein und drücken Sie nach jedem Befehl <Eingabe>:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
   ```

   wobei 1 und 1 der PET-Index und die Aktivieren/Deaktivieren-Auswahl sind.

   Der PET-Zielindex kann ein Wert von 1 bis 4 sein. Die Auswahl aktivieren/deaktivieren kann auf 1 (Aktiviert) oder 0 (Deaktiviert) eingestellt werden.

   Beispiel: um PET mit dem Index 4 zu aktivieren, geben Sie den folgenden Befehl ein:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 0
   ```

3. Konfigurieren Sie Ihre PET-Regel.

   An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

`racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <IP_Adresse>`

wobei 1 der PET-Zielindex und <*IP_Adresse*> die Ziel-IP-Adresse des Systems ist, das die Plattformereigniswarnungen erhält.

4. Community-Namenzeichenkette konfigurieren.

   An der Eingabeaufforderung geben Sie Folgendes ein:

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

E-Mail-Warnungen konfigurieren

E-Mail-Warnungen mittels der Internetbenutzeroberfläche konfigurieren

1. Melden Sie sich über einen unterstützten Internetbrowser am Remote-System an. Siehe "Zugriff auf die webbasierte Schnittstelle".
2. Stellen Sie sicher, dass Sie die Verfahren in "PEF über die Internetbenutzeroberfläche konfigurieren" ausführen.
3. Konfigurieren Sie Ihre E-Mail-Warnungseinstellungen.
   a. Im Register **Warnungsverwaltung** auf **E-Mail-Warnungseinstellungen** klicken.
   b. Unter **SMTP (E-Mail) Server-Adresseinstellungen** konfigurieren Sie das Feld **SMTP (E-Mail) Server-IP-Adresse** mit den entsprechenden Informationen und klicken Sie dann auf **Änderungen anwenden**.
4. Konfigurieren Sie Ihr E-Mail-Warnungsziel.
   a. In der Spalte **E-Mail-Warnungsnummer** klicken Sie auf eine E-Mail-Warnungsnummer.
   b. Stellen Sie sicher, dass das Kontrollkästchen **E-Mail-Warnung aktivieren** ausgewählt ist.
   c. Geben Sie eine gültige E-Mail-Adresse in das Feld **Ziel-E-Mail-Adresse** ein.
   d. Geben Sie eine Beschreibung in das Feld **E-Mail-Beschreibung** ein (falls erforderlich).
   e. Klicken Sie auf **Änderungen anwenden**.
   f. Klicken Sie auf **Test-E-Mail senden**, um die konfigurierte E-Mail-Warnung zu überprüfen (wenn gewünscht).

   ANMERKUNG: Ihr Benutzerkonto muss die Berechtigung **Testwarnungen** haben, um dieses Verfahren auszuführen. Siehe Tabelle 4-8.

   g. Wiederholen Sie Schritt a bis Schritt e für alle restlichen E-Mail-Warnungseinstellungen.
5. Globale Warnungen aktivieren.
   a. Klicken Sie auf **Warnungsverwaltung** und wählen Sie **Plattformereignisse**.
   b. Wählen Sie das Kontrollkästchen **Plattformereignisfilterwarnung**.

E-Mail-Warnungen mittels RACADM-CLI konfigurieren

1. Aktivieren Sie die globalen Warnungen.

   Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie <Eingabe>:

   `racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1`

2. E-Mail-Warnungen aktivieren.

   An der Eingabeaufforderung geben Sie die folgenden Befehle ein und drücken Sie nach jedem Befehl <Eingabe>:

   `racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1`

   wobei 1 und 1 der E-Mail-Zielindex und die Aktivieren/Deaktivieren-Auswahl sind.

   Der E-Mail-Ziel-Index kann ein Wert von 1 bis 4 sein. Die Auswahl aktivieren/deaktivieren kann auf 1 (Aktiviert) oder 0 (Deaktiviert) eingestellt werden.

   Beispiel: Um E-Mail mit dem Index 4 zu aktivieren, tippen Sie den folgenden Befehl:

   `racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1`

3. Konfigurieren Sie Ihre E-Mail-Einstellungen.

An der Eingabeaufforderung geben Sie folgenden Befehl ein und drücken Sie <Eingabe>:

`racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <E-Mail_Adresse>`

wobei `1` der E-Mail-Ziel-Index und <*E-Mail_Adresse*> die Ziel-E-Mail-Adresse ist, die die Plattform-Ereignis-Warnungen erhält.

Zum Konfigurieren einer kundenspezifischen Meldung geben Sie den folgenden Befehl an der Eingabeaufforderung ein und drücken Sie <Eingabe>:

`racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <benutzerdefinierte_Meldung>`

wobei `1` der E-Mail-Ziel-Index und <*benutzerdefinierte_Meldung*> die kundenspezifische Meldung ist.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5-Befehlszeilenkonsole konfigurieren und verwenden

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Dieser Abschnitt enthält Informationen über die DRAC 5-Befehlszeilenkonsole (oder *seriell/telnet/ssh-Konsole*) -Funktionen, und erklärt, wie man das System einrichtet, so dass Sie Systemmanagementmaßnahmen über die Konsole ausführen können.

Funktionen der Befehlszeilenkonsole

DRAC 5 unterstützt die folgenden seriellen und Telnet Konsolen-Funktionen:

- Eine serielle Clientverbindung und bis zu vier gleichzeitige Telnet-Clientverbindungen
- Bis zu vier gleichzeitige SSH-Clientverbindungen
- Zugriff auf die Konsolen des verwalteten Systems über die serielle Schnittstelle des Systems und durch die DRAC 5-NIC
- Konsolenbefehle, mit denen Sie den DRAC 5 hochfahren, herunterfahren, aus- und einschalten, zurückstellen, konfigurieren oder seine Protokolle ansehen können.
- Unterstützt den **RACADM**-Befehl, was für das Scripting von Nutzen ist
- Befehlszeilenbearbeitung und Protokoll
- Der serielle Befehl **connect com2** um mit der Textkonsole des verwalteten Systems, die über eine serielle Schnittstelle ausgegeben wird (einschließlich BIOS und Betriebssystem), in Verbindung zu stehen, sie anzuzeigen und mit ihr zu interagieren.

  ANMERKUNG: Wenn Sie Linux auf dem verwalteten System ausführen, enthält der serielle Befehl **connect com2** eine wahre Linux Konsolenstromschnittstelle.

- Sitzungszeitüberschreitungssteuerung auf allen Konsole-Schnittstellen

---

Das verwaltete System aktivieren und konfigurieren, um eine serielle oder Telnet-Konsole zu verwenden

Die folgenden Abschnitte enthalten Informationen darüber, wie man eine seriell/telnet/ssh-Konsole auf dem verwalteten System aktiviert und konfiguriert.

Den seriellen Befehl connect com2 verwenden

Wenn der serielle Befehl **connect com2** verwendet wird, müssen folgende Punkte sachgemäß konfiguriert werden:

- Die Einstellung **Serial Communication (Serielle Datenübertragung)**→ **Serial Port (Serielle Schnittstelle)** im **BIOS-Setup**-Programm.
- Die DRAC-Konfigurationseinstellungen.

Wenn eine Telnet-Sitzung zum DRAC 5 aufgebaut wird und diese Einstellungen falsch sind, kann **connect com2** einen leeren Bildschirm anzeigen.

BIOS-Installationsprogramm für eine serielle Verbindung auf dem verwalteten System konfigurieren

Führen Sie die folgenden Schritte aus, um das **BIOS-Setup**-Programm dahingehend zu konfigurieren, dass es die Ausgabe zu einem seriellen Anschluss umleitet.

ANMERKUNG: Das **System-Setup**-Programm muss in Verbindung mit dem Befehl **connect com2** konfiguriert werden.

1. Schalten Sie Ihr System ein oder starten Sie es erneut.
2. Drücken Sie sofort auf <F2>, nachdem Sie die folgende Meldung sehen:

```
<F2> = System Setup

(<F2> = System-Setup)
```

3. Rollen Sie abwärts und wählen Sie **Serial Communication (Serielle Kommunikation)** durch Drücken von <Eingabe>.

4. Auf dem Bildschirm **Serial Communication (Serielle Kommunikation)** die folgenden Einstellungen vornehmen:

   External Serial Connector — Remote Access Device (Externer Serieller Anschluss - Remote-Zugriffsgerät)

   Redirection After Boot — Disabled (Umleitung nach Start - Deaktiviert)

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

Serielle Remote-Zugriffschnittstelle verwenden

Wenn eine serielle Verbindung mit dem RAC-Gerät aufgebaut wird, sind die folgenden Schnittstellen verfügbar:

- Serielle IPMI-Schnittstelle
- Serielle RAC-Schnittstelle

Serielle IPMI-Schnittstelle

In der seriellen IPMI-Schnittstelle sind die folgenden Modi verfügbar:

- **IPMI-Terminalmodus** - Unterstützt ASCII-Befehle, die von einem seriellen Terminal gesendet werden. Der Befehlssatz ist auf eine beschränkte Anzahl von Befehlen (einschließlich der Stromsteuerung) begrenzt und unterstützt Roh-IPMI-Befehle, die als Hexadezimal-ASCII-Zeichen eingegeben werden.
- **IPMI grundlegender Modus** - Unterstützt eine binäre Schnittstelle für den Programmzugang, wie die IPMI-Shell (IPMISH), die mit dem Baseboard Verwaltungsdienstprogramm (BMU) enthalten ist.

Um den IPMI-Modus mit RACADM zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Deaktivieren Sie die serielle RAC-Schnittstelle.

   An der Eingabeaufforderung geben Sie folgendes ein:

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

2. Aktivieren Sie den entsprechenden IPMI-Modus.

   Beispiel: Geben Sie an der Eingabeaufforderung folgendes ein:

   ```
   racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 oder 1>
   ```

Weitere Informationen finden Sie in "**DRAC 5 Definitionen für Eigenschaft-Datenbank-Gruppen und Objekte**".

Serielle RAC-Schnittstelle

RAC unterstützt auch eine serielle Konsolenschnittstelle (oder *serielle RAC-Konsole*), die einen RAC-CLI enthält, der nicht durch IPMI definiert wird. Wenn Ihr System eine RAC-Karte mit aktivierter **Serieller Konsole** enthält, überschreibt die RAC-Karte die seriellen IPMI-Einstellungen und zeigt die serielle RAC CLI-Schnittstelle an.

Zum Aktivieren der seriellen RAC-Terminalschnittstelle setzen Sie die Eigenschaft **cfgSerialConsoleEnable** auf **1** (WAHR).

Beispiel:

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

Siehe "cfgSerialConsoleEnable (Lesen/Schreiben)" für weitere Informationen.

Tabelle 3-1 enthält die seriellen Schnittstelleneinstellungen.

Tabelle 3-1. Serielle Schnittstellen-Einstellungen

IPMI-Modus	Serielle RAC-Konsole	Interface
Grundlegend	Deaktiviert	Grundlegender Modus
Grundlegend	Aktiviert	RAC CLI
Terminal	Deaktiviert	IPMI-Terminalmodus
Terminal	Aktiviert	RAC CLI

Linux für die serielle Konsolenumleitung während des Starts konfigurieren

Die folgenden Schritte sind spezifisch für den Linux GRand Unified Bootloader (GRUB). Ähnliche Änderungen würden notwendig sein, um einen anderen Bootloader zu verwenden.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters müssen Sie das Fenster oder die Anwendung, die die umgeleitete Konsole anzeigt, auf 25 Reihen x 80 Spalten einstellen, um die ordnungsgemäße Textanzeige sicherzustellen, sonst können einige Textbildschirme durcheinander gebracht werden.

Die Datei **/etc/grub.conf** muss wie folgt bearbeitet werden:

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

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

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

   ```
   kernel ............. console=ttyS1,57600
   ```

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

Tabelle 3-2 enthält ein Beispiel einer **/etc/grub.conf-**Datei, die die in diesem Verfahren beschriebenen Änderungen zeigt.

Tabelle 3-2. Beispieldatei: /etc/grub.conf

```
# grub.conf generated by anaconda
# (grub.conf durch anaconda erstellt)
#
# Note that you do not have to rerun grub after making changes
# to this file
# (Beachten Sie, dass grub nicht erneut ausgeführt werden muss, nachdem Änderungen
# an dieser Datei vorgenommen wurden)
# NOTICE:  You do not have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /, e.g.
# (HINWEIS:  Sie haben keine /-Startpartition.  Dies bedeutet, dass
#          alle Kernel und initrd-Pfade mit / in Beziehung stehen, z. B.)
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=/dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

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

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0 console=ttyS1,57600
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

Wenn Sie die Datei **/etc/grub.conf** bearbeiten, verwenden Sie die folgenden Richtlinien:

1. Deaktivieren Sie die GRUB-Grafikschnittstelle und verwenden Sie die textbasierte Schnittstelle; ansonsten wird der GRUB-Bildschirm nicht in der RAC-Konsolenumleitung angezeigt. Zum Deaktivieren der Grafikschnittstelle kommentieren Sie die Zeile aus, die mit splashimage beginnt.

2. Zum Starten mehrerer GRUB-Optionen, um Konsolensitzungen über die serielle RAC-Verbindung zu beginnen, fügen Sie allen Optionen die folgende Zeile hinzu:

   ```
   console=ttyS1,57600
   ```

   Tabelle 3-2 zeigt, dass console=ttyS1,57600 nur zur ersten Option hinzugefügt wurde.

Anmeldung zur Konsole nach dem Start aktivieren

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

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

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

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

Tabelle 3-3. Beispieldatei: /etc/innitab

```
#
# inittab  This file describes how the INIT process should set up
#          the system in a certain run-level.
# (inittab    Diese Datei beschreibt, wie der INIT-Vorgang
#             das System in einer bestimmten Ausführungsstufe einrichten sollte.)
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
# (Autor:   Miquel van Smoorenburg
#          Geändert für RHS Linux von Marc Ewing und Donnie Barnes)
#
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have
#       networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
# (Standardausführungsstufe. Die von RHS verwendeten Runlevel sind:
#   0 - halt (initdefault NICHT auf diese Einstellung setzen)
#   1 - Einfacher Benutzermodus
#   2 - Mehrfachbenutzer, ohne NFS (Dasselbe wie 3, wenn
#       nicht vernetzt ist)
#   3 - Voller Mehrfachbenutzermodus
#   4 - unbenutzt
#   5 - X11
#   6 - neustarten (initdefault NICHT auf diese Einstellung setzen))

#
id:3:initdefault:

# System initialization.
# (Systeminitialisierung.)
si::sysinit:/etc/rc.d/rc.sysinit
```

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

```
# Things to run in every runlevel.
# (In jeder Ausführungsstufe auszuführende Dateien.)
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
# (Trap Strg-Alt-Entf)
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
#
# (Wenn die UPS einen Stromausfall anzeigt, ist anzunehmen, dass noch ein paar
# Minuten von Strom verbleiben. Planen Sie ein Herunterfahren innerhalb der nächsten zwei Minuten.
# Dies setzt selbstverständlich voraus, dass der Strom eingeschaltet ist und Ihre
# UPS angeschlossen ist und ordnungsgemäß funktioniert.)
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
# (Wenn die Stromversorgung vor dem Herunterfahren wieder hergestellt wurde, brechen Sie ab.)
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
# Run gettys in standard runlevels
# (gettys in Standardausführungsstufen ausführen)
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
#
# (xdm in Ausführungsstufe 5 ausführen
# xdm ist jetzt ein separater Dienst)
x:5:respawn:/etc/X11/prefdm -nodaemon
```

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

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

```
ttyS1
```

Tabelle 3-4 zeigt eine Beispieldatei mit der neuen Zeile.

Tabelle 3-4. Beispieldatei: /etc/securetty

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

DRAC 5 Seriell/Telnet/SSH-Konsole aktivieren

Die seriell/telnet/ssh-Konsole kann lokal oder im Remote-Zugriff aktiviert werden.

Seriell/Telnet/SSH-Konsole lokal aktivieren

ANMERKUNG: Sie (der aktuelle Benutzer) müssen die Berechtigung **DRAC 5 konfigurieren** haben, um die Schritte in diesem Abschnitt auszuführen.

Um die seriell/telnet/ssh-Konsole vom verwalteten System zu aktivieren, geben Sie die folgenden lokalen RACADM-Befehle von einer Eingabeaufforderung aus ein:

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

racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

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

Für ausführliche Informationen über die Verwendung der Befehle **RACADM**, **serial/telnet/ssh** und **RACADM** siehe "RACADM-Befehlszeilenoberfläche verwenden".

Seriell/Telnet/SSH-Konsole im Remote-Zugriff aktivieren

Um die seriell/telnet/ssh-Konsole im Remote-Zugriff zu aktivieren, geben Sie die folgenden Remote-**RACADM**-Befehle von einer Befehlseingabeaufforderung aus ein:

```
racadm -u <Benutzername> -p <Kennwort> -r <DRAC 5-IP-Adresse> config -g cfgSerial cfgSerialConsoleEnable 1

racadm -u <Benutzername> -p <Kennwort> -r <DRAC 5-IP-Adresse> config -g cfgSerial cfgSerialTelnetEnable 1

racadm -u <Benutzername> -p <Kennwort> -r <DRAC 5-IP-Adresse> config -g cfgSerial cfgSerialSshEnable 1
```

RACADM-Befehl zum Konfigurieren der Einstellungen für die serielle und Telnet-Konsole verwenden

Dieser Unterabschnitt enthält die Schritte zum Festlegen der Standardkonfigurationseinstellungen für die seriell/telnet/ssh-Konsolenumleitung.

Um die Einstellungen zu konfigurieren, geben Sie den RACADM-Befehl **config** mit der entsprechenden Gruppe, Eigenschaft und Eigenschaft-Wert(en) für die Einstellung ein, die Sie konfigurieren wollen.

Sie können RACADM-Befehle lokal oder im Remote-Zugriff eingeben. Wenn Sie RACADM-Befehle im Remote-Zugriff verwenden, müssen Sie Benutzernamen, Kennwort und die verwaltete System-DRAC 5 IP-Adresse mit eingeben.

Eine vollständige Liste von verfügbaren seriell/telnet/ssh- und RACADM CLI-Befehlen, finden Sie in "RACADM-Befehlszeilenoberfläche verwenden".

RACADM lokal verwenden

Zur lokalen Eingabe von RACADM-Befehlen geben Sie den folgenden Befehl von einer Eingabeaufforderung auf dem verwalteten System ein:

```
racadm config -g <Gruppe> -o <Eigenschaft> <Wert>
```

Um eine Liste von Eigenschaften anzusehen, geben Sie den folgenden Befehl von einer Eingabeaufforderung auf dem verwalteten System ein:

```
radadm getconfig -g <Gruppe>
```

RACADM im Remote-Zugriff verwenden

Um RACADM-Befehle im Remote-Zugriff zu verwenden, geben Sie den folgenden Befehl von einer Eingabeaufforderung auf einer Verwaltungsstation aus ein:

```
racadm -u <Benutzername> -p <Kennwort> -r <DRAC 5-IP-Adresse> config -g <Gruppe> -o <Eigenschaft> <Wert>
```

Stellen Sie sicher, dass Ihr Webserver mit einer DRAC 5-Karte konfiguriert ist, bevor Sie RACADM im Remote-Zugriff verwenden. Ansonsten überschreitet der RACADM das Zeitlimit und die folgende Meldung wird angezeigt:

```
Unable to connect to RAC at specified IP address.

(Kein Anschluss an RAC an der angegebenen IP-Adresse.)
```

Zum Aktivieren des Webservers mittels Secure Shell (SSH), Telnet oder lokalem RACADM geben Sie den folgenden Befehl von einer Eingabeaufforderung auf einer Verwaltungsstation ein:

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

Konfigurationseinstellungen anzeigen

Tabelle 3-5 enthält die Maßnahmen und zugehörigen Befehle für die Anzeige der Konfigurationseinstellungen. Um die Befehle auszuführen, öffnen Sie eine Eingabeaufforderung auf dem verwalteten System, geben Sie den Befehl ein und drücken Sie <Eingabe>.

Tabelle 3-5. Konfigurationseinstellungen anzeigen

Maßnahme	Befehl
Verfügbare Gruppen auflisten.	racadm getconfig -h
Aktuelle Einstellungen für eine besondere Gruppe anzeigen.	racadm getconfig -g *<Gruppe>* Beispiel: Um eine Liste von allen **cfgSerial-**Gruppeneinstellungen anzuzeigen, geben Sie den folgenden Befehl ein: racadm getconfig -g cfgSerial
Zeigen Sie die aktuellen Einstellungen für eine besondere Gruppe im Remote-Zugriff an.	racadm -u *<Benutzer>* -p *<Kennwort>* -r *<DRAC 5-IP-Adresse>* getconfig -g cfgSerial Beispiel: Für eine Liste aller Einstellungen für die **cfgSerial**-Gruppe im Remote-Zugriff geben Sie folgendes ein: racadm -u root -p calvin -r 192.168.0.1 getconfig -g cfgSerial

Die Telnet-Schnittstellennummer konfigurieren

Geben Sie den folgenden Befehl ein, um die Telnet-Schnittstellennummer auf dem DRAC 5 zu ändern.

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <neue Schnittstellennummer>
```

Secure Shell (SSH) verwenden

Es ist wichtig, dass Geräte und Geräteverwaltung des Systems sicher sind. Integrierte angeschlossene Geräte sind der Kern von vielen Geschäftsprozessen. Wenn diese Geräte gefährdet werden, kann das Geschäft des Kunden gefährdet sein, was neue Sicherheitsanforderungen für die Befehlszeilenoberflächen- (CLI) Geräteverwaltungssoftware erfordert.

Secure Shell (SSH) ist eine Befehlszeilensitzung, die dieselben Fähigkeiten wie eine Sitzung von Telnet umfasst, jedoch mit verbesserter Sicherheit. Der DRAC 5 unterstützt SSH Version 2 mit Kennwortauthentifizierung. SSH wird auf dem DRAC 5 aktiviert, wenn Sie Ihre DRAC 5-Firmware installieren oder aktualisieren.

Sie können entweder PuTTY oder OpenSSH auf der Verwaltungsstation verwenden, um mit dem DRAC 5 des verwalteten Systems zu verbinden. Wenn ein Fehler während des Anmeldungsverfahrens auftritt, gibt der Secure Shell-Client eine Fehlermeldung aus. Der Meldungstext ist vom Client abhängig und wird nicht vom DRAC 5 gesteuert.

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

Nur vier SSH-Sitzungen werden jeweils zu einer vorgegebenen Zeit unterstützt. Das Sitzungszeitlimit wird gesteuert durch die Eigenschaft `cfgSsnMgtSshIdleTimeout`, wie in "DRAC 5 Eigenschaften-Datenbankgruppe und Objektdefinitionen" beschrieben.

Sie können den SSH auf dem DRAC 5 mit dem folgenden Befehl aktivieren:

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

Sie können die SSH-Schnittstelle mit dem folgenden Befehl ändern:

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

Für weitere Informationen über die Eigenschaften `cfgSerialSshEnable` und `cfgRacTuneSshPort` siehe "DRAC 5 Eigenschaften-Datenbankgruppe und Objektdefinitionen".

Die DRAC 5 SSH-Umsetzung unterstützt mehrfache Verschlüsselungs-Schemata, siehe Tabelle 3-6.

Tabelle 3-6. Verschlüsselungs-Schemata

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

ANMERKUNG: SSHv1 wird nicht unterstützt.

Zusätzliche DRAC 5-Sicherheitsoptionen aktivieren

Um unberechtigten Zugriff zu Ihrem Remote-System zu verhindern, enthält der DRAC 5 die folgenden Funktionen:

- IP-Adressenfilter (IPRange) - Definiert einen spezifischen Bereich von IP-Adressen, die auf den DRAC 5 zugreifen können.
- IP-Adressenblockieren - Beschränkt die Anzahl von fehlgeschlagenen Anmeldungsversuchen von einer spezifischen IP-Adresse

Diese Funktionen sind in der DRAC 5 Standardkonfiguration deaktiviert. Verwenden Sie den folgenden Unterbefehl oder die webbasierte Schnittstelle, um diese Funktionen zu aktivieren.

```
racadm config -g cfgRacTuning -o <Objekt_Name> <Wert>
```

Verwenden Sie darüber hinaus diese Funktionen in Verbindung mit den entsprechenden Sitzungszeitüberschreitungswerten und einem festgelegten Sicherheitsplan für Ihr Netzwerk.

Die folgenden Unterabschnitte enthalten zusätzliche Informationen über diese Funktionen.

IP-Filter (IpRange)

Die IP-Adressenfiltrierung (oder *IP-Bereichüberprüfung*) gestattet DRAC 5-Zugriff nur von Clients oder Verwaltungsstationen, deren IP-Adressen innerhalb eines benutzerspezifischen Bereiches liegen. Alle anderen Anmeldungen werden abgelehnt.

Die IP-Entstörung vergleicht die IP-Adresse einer eingehenden Anmeldung mit dem IP-Adressenbereich, der in den folgenden **cfgRacTuning**-Eigenschaften angegeben wird:

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

Die Eigenschaft **cfgRacTuneIpRangeMask** wird sowohl auf die eingehende IP-Adresse als auch auf die **cfgRacTuneIpRangeAddr**-Eigenschaften angewendet. Wenn die Ergebnisse von beiden Eigenschaften identisch sind, wird der eingehenden Anmeldeanforderung der Zugriff auf den DRAC 5 gestattet. Anmeldungen von IP-Adressen außerhalb dieses Bereiches 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.

Siehe "DRAC 5 Eigenschaften-Datenbankgruppe und Objektdefinitionen" für eine vollständige Liste der **cfgRacTune**-Eigenschaften.

Tabelle 3-7. IP-Adressenfiltrierung (IpRange) -Eigenschaften

Eigenschaft	Beschreibung
cfgRacTuneIpRangeEnable	Aktiviert die IP-Bereichsüberprüfungsfunktion.
cfgRacTuneIpRangeAddr	Bestimmt das akzeptable IP-Adressen-Bitmuster, abhängig von den Einsen (1) in der Subnetzmaske. Diese Eigenschaft wird mit binärem UND mit **cfgRacTuneIpRangeMask** verbunden, um den oberen Teil der erlaubten IP-Adresse zu bestimmen. Jeder IP-Adresse, die dieses Bitmuster in ihrem oberen Bit enthält, wird erlaubt, eine DRAC 5 Sitzung zu beginnen. Anmeldungen von IP-Adressen, die außerhalb dieses Bereichs sind, werden fehlschlagen. Die Standardwerte in jeder Eigenschaft erlauben einen Adressenbereich von 192.168.1.0 bis 192.168.1.255, eine DRAC 5 Sitzung zu bestimmen.
cfgRacTuneIpRangeMask	Definiert die bedeutenden Bitpositionen in der IP-Adresse. Die Subnetzmaske sollte in der Form einer Netzmaske sein, wobei die bedeutenderen Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu Nullen (0) in den niederwertigeren Bits.

IP-Filter aktivieren

Es folgt ein Beispiel-Befehl für den IP-Filter-Setup.

"RACADM verwenden" enthält weitere Informationen über RACADM und RACADM-Befehle.

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

Zur Beschränkung der Anmeldung auf eine einzelne IP-Adresse (zum Beispiel: 192.168.0.57), verwenden Sie die volle Maske, wie unten gezeigt.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

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

Zur Beschränkung der Anmeldung auf einen kleinen Satz von vier angrenzenden IP-Adressen (zum Beispiel: 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
```

IP-Filter - Richtlinien

Verwenden Sie die folgenden Richtlinien, wenn Sie den IP-Filter aktivieren:

- Stellen Sie sicher, dass **cfgRacTuneIpRangeMask** in der Form einer Netzmaske konfiguriert wird, wo alle höchstwertigen Bits Einsen (1) sind (was das Subnetz in der Maske definiert), mit einem Übergang zu nur Nullen (0) in den niederwertigen Bits.
- Verwenden Sie die Basisadresse des gewünschten Bereiches 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-Blockieren

IP-Blockieren stellt dynamisch fest, wenn übermäßige Anmeldungsfehlschläge von einer bestimmten IP-Adresse auftreten und blockiert (oder hindert) die Adresse eine bestimmte Zeit lang an der Anmeldung am DRAC 5.

Der IP-Blockierungsparameter wendet **cfgRacTuning**-Gruppenfunktionen an, die umfassen:

- Die Anzahl von zulässigen Anmeldungsfehlschlägen (**cfgRacTuneIpBlkFailcount**)
- Der Zeitrahmen in Sekunden, während dessen diese Fehler auftreten müssen (**cfgRacTuneIpBlkFailWindow**)
- Die Zeit in Sekunden, die die "schuldige" IP-Adresse gehindert wird, eine Sitzung zu beginnen, nachdem die zulässige Anzahl von Fehlern überschritten wird (**cfgRacTuneIpBlkPenaltyTime**)

Wenn sich Anmeldungsfehler von einer spezifischen IP-Adresse ansammeln, werden sie durch einen internen Schalter "gealtert". Wenn sich der Benutzer erfolgreich anmeldet, wird das Fehlerprotokoll gelöscht, und der interne Zähler wird zurückgesetzt.

ANMERKUNG: Wenn Anmeldungsversuche von der Client-IP-Adresse abgelehnt werden, können einige SSH-Clients die folgende Meldung anzeigen: ssh exchange identification: Verbindung vom Remote Host geschlossen.

Siehe "DRAC 5 Eigenschaften-Datenbankgruppe und Objektdefinitionen" für eine vollständige Liste der **cfgRacTune**-Eigenschaften.

Tabelle 3-8 führt die benutzerdefinierten Parameter auf.

Tabelle 3-8. Anmeldungswiederholungs-Beschränkungseigenschaften

Eigenschaft	Definition
cfgRacTuneIpBlkEnable	Aktiviert die IP-Blockierungsfunktion. Wenn aufeinander folgende Fehler (**cfgRacTuneIpBlkFailCount**) von einer einzelnen IP-Adresse innerhalb eines spezifischen Zeitraums festgestellt werden (**cfgRacTuneIpBlkFailWindow**), werden alle weiteren Versuche, von dieser Adresse eine Sitzung zu beginnen, für einen bestimmten Zeitraum zurückgewiesen (**cfgRacTuneIpBlkPenaltyTime)**.
cfgRacTuneIpBlkFailCount	Legt die Anzahl von Anmeldungsfehlern einer IP-Adresse fest, bevor die Anmeldungsversuche zurückgewiesen werden.
cfgRacTuneIpBlkFailWindow	Der Zeitrahmen in Sekunden, wenn die Fehlversuche gezählt werden. Wenn die Fehler diese Grenze überschreiten, werden sie aus dem Zähler gelöscht.
crgRacTuneIpBlkPenaltyTime	Legt den Zeitraum in Sekunden fest, wenn alle Anmeldungsversuche von einer IP-Adresse aufgrund übermäßiger Fehler zurückgewiesen werden.

IP-Blockieren aktivieren

Das folgende Beispiel hindert eine Client-IP-Adresse fünf Minuten lang daran, eine Sitzung zu beginnen, wenn dieser Client innerhalb einer Minute fünf fehlerhafte Anmeldungsversuche durchführt.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

Das folgende Beispiel verhindert mehr als drei fehlerhafte Versuche innerhalb einer Minute, und verhindert eine Stunde lang zusätzliche Anmeldungsversuche.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

Das verwaltete System über die lokale serielle Schnittstelle oder Telnet-Verwaltungsstation (Client-System) verbinden

Das verwaltete System bietet Zugriff zwischen dem DRAC 5 und der seriellen Schnittstelle auf Ihrem System, damit Sie das verwaltete System einschalten, ausschalten oder neu einrichten können und Zugriff auf die Protokolle haben.

Die serielle Konsole ist auf dem DRAC 5 über den externen seriellen Stecker des verwalteten Systems verfügbar. Nur jeweils ein serielles Client-System (Verwaltungsstation) kann aktiv sein. Die Telnet- und SSH-Konsolen sind auf dem DRAC 5 durch die DRAC-Modi verfügbar (siehe "DRAC-Modi"). Bis zu vier Telnet-Clientsysteme und vier SSH-Clients können zu jeder gegebenen Zeit angeschlossen werden. Die Verbindung der Verwaltungsstation zur seriellen oder Telnet-Konsole des verwalteten Systems erfordert Verwaltungsstation-Terminalemulationssoftware. "Verwaltungsstation-Terminalemulationssoftware konfigurieren" enthält weitere Informationen.

Die folgenden Unterabschnitte erklären, wie die Verwaltungsstation mittels der folgenden Methoden mit dem verwalteten System verbunden wird:

- Eine externe serielle Schnittstelle des verwalteten Systems mit Terminal-Software und einem Null-Modemkabel
- Eine Telnet-Verbindung mit Terminal-Software über die DRAC 5-NIC des verwalteten Systems oder die freigegebene Team-NIC

DB 9-Kabel für die serielle Konsole

Um mit einer seriellen Textkonsole auf das verwaltete System zuzugreifen, schließen Sie ein DB 9-Null-Modemkabel an den COM-Port auf dem verwalteten System an. Nicht alle DB-9-Kabel führen das Pinout/die Signale das/die für diese Verbindung benötigt werden. Das DB-9-Kabel für diese Verbindung muss der in Tabelle 3-9 gezeigten Spezifikation entsprechen.

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

Tabelle 3-9. Erforderliches Pinout für das DB-9-Null-Modem-Kabel

Signalname	DB-9 Pin (Server-Pin)	DB-9-Pin (Workstation-Pin)

FG (Gehäusemasse)	–	–
TD (Daten senden)	3	2
RD (Daten empfangen)	2	3
RTS (Aufforderung zu senden)	7	8
CTS (Frei zum Senden)	8	7
SG (Betriebserde)	5	5
DSR (Datensatz bereit)	6	4
CD (Trägerermittlung)	1	4
DTR (Datenterminal bereit)	4	1 und 6

Verwaltungsstation-Terminalemulationssoftware konfigurieren

Ihre DRAC 5 unterstützt eine serielle oder Telnet-Textkonsole einer Verwaltungsstation, auf der einer der folgenden Typen der Terminalemulationssoftware ausgeführt wird:

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

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

Linux Minicom für die serielle Konsolenemulation konfigurieren

Minicom ist das serielle Schnittstellenzugriffdienstprogramm für Linux. Die folgenden Schritte sind gültig, um Minicom Version 2.0 zu konfigurieren. Andere Minicom Versionen können ein bisschen unterschiedlich sein, aber dieselben grundlegenden Einstellungen benötigen. Verwenden Sie die Informationen in "Erforderliche Minicom-Einstellungen für die Emulation der seriellen Konsole", um andere Versionen von Minicom zu konfigurieren.

Minicom Version 2.0 für die Emulation der seriellen Konsole konfigurieren

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

1. Um eine neue Xterm-Sitzung zu starten, geben Sie anzufangen `xterm &` an der Befehlseingabeaufforderung ein.
2. Im Xterm-Fenster bewegen Sie Ihren Maus-Pfeil in die untere rechte Ecke des Fensters und ändern die Größe des Fensters zu 80 x 25.
3. Wenn Sie keine Minicom-Konfigurationsdatei haben, fahren Sie mit dem folgenden Schritt fort.

   Wenn Sie eine Minicom-Konfigurationsdatei haben, geben Sie `minicom <Minicom Konfigurationsdateiname>` ein und fahren Sie mit Schritt 17 fort.
4. An der Xterm-Befehlseingabeaufforderung, geben Sie `minicom -s` ein.
5. Wählen Sie den **Setup der seriellen Schnittstelle** und drücken Sie auf <Eingabe>.
6. Drücken Sie <a> und wählen Sie das entsprechende serielle Gerät aus (Beispiel: **/dev/ttyS0**).
7. Drücken Sie <e> und stellen Sie die Option **Bps/Par/Bits** auf **57600 8N1**.
8. Drücken Sie <f> und stellen Sie die **Hardwaredatenflusssteuerung** auf **Ja** und die **Softwaredatenflusssteuerung** auf **Nein**.
9. Um das Menü **Setup der seriellen Schnittstelle** zu beenden, drücken Sie auf<Eingabe>.
10. Wählen Sie **Modem und Wählen** und drücken Sie auf <Eingabe>.
11. Im Menü **Modem-Wählen und Parameter-Setup**, drücken Sie auf <Rücktaste> um die Einstellungen **init**, **reset**, **connect** und **hangup**, sodass Sie leer sind.
12. Drücken Sie <Eingabe>, um jeden leeren Wert zu speichern.
13. Wenn alle angegebenen Felder gelöscht sind, drücken Sie auf <Eingabe>, um das Menü **Modem-Wählen und Parameter-Setup** zu beenden.

14. Wählen Sie **Setup als config_name speichern** und drücken Sie auf <Eingabe>.

15. Wählen Sie **Minicom beenden** und drücken Sie auf <Eingabe>

16. An der Befehls-Shell-Eingabeaufforderung geben Sie `minicom <Minicom Config-Dateiname>`. ein

17. Um das Minicom-Fenster auf 80 x 25 zu erweitern, verwenden Sie die Drag-Funktion an der Ecke des Fensters.

18. Drücken Sie <Strg+a>, <z>, <x>, um Minicom zu beenden.

ANMERKUNG: Wenn Sie Minicom für die serielle Textkonsolenumleitung verwenden, um das verwaltete System-BIOS zu konfigurieren, wird empfohlen, in Minicom Farbe einzuschalten. Zum Einschalten der Farbe geben Sie den folgenden Befehl in die Eingabeaufforderung ein: `minicom -c on`

Stellen Sie sicher, dass das Minicom Fenster eine Befehlseingabeaufforderung wie z. B. `[DRAC 5\root]#` anzeigt. Wenn die Befehlseingabeaufforderung erscheint, ist Ihre Verbindung erfolgreich, und Sie sind bereit, zur Konsole des verwalteten Systems mit Hilfe des seriellen Befehls **Verbinden** zu verbinden.

Erforderliche Minicom-Einstellungen für die Emulation der seriellen Konsole

Verwenden Sie Tabelle 3-10, um jede Version von Minicom zu konfigurieren.

Tabelle 3-10. Minicom-Einstellungen für die Emulation der seriellen Konsole

Einstellung der Beschreibung	Erforderliche Einstellung
Bps/Par/Bits	57600 8N1
Hardwaredatenflusssteuerung	Ja
Softwaredatenflusssteuerung	Nein
Terminalemulation	ANSI
Modemwählen und Parameter-Einstellungen	Löschen Sie die Einstellungen **init**, **Reset**, **Verbinden** und **hangup,** sodass sie leer sind
Fenstergröße	80 x 25 (um wieder nach Größe zu ordnen, ziehen Sie die Ecke des Fensters)

Hyperterminal für die serielle Konsolenumleitung konfigurieren

Hyperterminal ist das Zugriffsdienstprogramm für die serielle Schnittstelle von Microsoft Windows. Um die Größe Ihres Konsolenbildschirms entsprechend einzustellen, verwenden Sie die Hilgraeve's HyperTerminal Private Edition version 6.3.

Um Hyperterminal für die serielle Konsolenumleitung zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Starten Sie das Hyper Terminal-Programm.

2. Geben Sie einen Namen für die neue Verbindung ein und klicken Sie auf **OK**.

3. Neben **Verwenden verbinden:** die COM-Schnittstelle auf der Verwaltungsstation (z. B. COM2) auswählen zu dem Sie das DB-9-Null-Modem-Kabel verbunden haben und klicken Sie auf **OK**.

4. Konfigurieren Sie die COM-Schnittstelleneinstellungen, wie in Tabelle 3-11 gezeigt.

5. Klicken Sie auf **OK.**

6. Klicken Sie auf die **Datei** → **Eigenschaften** und dann auf das **Einstellungen**-Register.

7. Setzen Sie die **Telnet-Terminal-ID:** auf **ANSI**.

8. Klicken Sie auf **Terminal-Setup** und stellen Sie die **Bildschirmzeilen** auf **26**.

9. Stellen Sie die **Spalten** auf **80** und klicken Sie **OK**.

Tabelle 3-11. Einstellungen der Verwaltungsstation COM-Schnittstelle

Einstellung der Beschreibung	Erforderliche Einstellung
Bits pro Sekunde	57600
Datenbits	8
Parität	Keine
Stoppbits	1

Ablaufsteuerung	Hardware

Das Hyper Terminal-Fenster zeigt eine Befehlseingabeaufforderung wie z. B. [DRAC 5\root]# an. Wenn die Befehlseingabeaufforderung erscheint, ist Ihre Verbindung erfolgreich, und Sie sind bereit, zur Konsole des verwalteten Systems zu verbinden, die den seriellen Befehl **connect com2** verwendet.

Linux XTerm für die Telnet-Konsolenumleitung konfigurieren

Verwenden Sie die folgenden Richtlinien, wenn Sie die Schritte in diesem Abschnitt ausführen:

- Wenn Sie den Befehl **connect com2** über eine Telnet-Konsole verwenden, um die System-Setup-Bildschirme anzuzeigen, stellen Sie den Terminal-Typ auf **ANSI** im System-Setup und für die Telnet-Sitzung.
- ANMERKUNG: Um sicherzustellen, dass der Text ordnungsgemäß angezeigt wird, empfiehlt Dell, dass Sie ein Xterm-Fenster zur Anzeige der Telnet-Konsole statt der in der Linux-Installation enthaltenen Standardkonsole verwenden.

Um Telnet mit Linux auszuführen, führen Sie die folgenden Schritte aus:

1. Beginnen Sie eine neue Xterm-Sitzung.

   An der Eingabeaufforderung geben Sie `xterm &ein`

2. Bewegen Sie Ihren Maus-Pfeil in die rechte untere Ecke des XTerm-Fensters und stellen Sie es auf 80 x 25 ein.

3. Bauen Sie eine Verbindung mit dem DRAC 5 im verwalteten System auf.

   An der Xterm-Eingabeaufforderung geben Sie `telnet <DRAC 5-IP-Adresse>` ein

Microsoft Telnet für die Telnet-Konsolenumleitung aktivieren

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

1. **Telnet** in **Windows Komponenten-Dienste** aktivieren.

2. Bauen Sie eine Verbindung mit dem DRAC 5 in der Verwaltungsstation auf.

   Öffnen Sie eine Eingabeaufforderung, geben Sie folgendes ein und drücken Sie <Eingabe>:

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

   wobei *IP-Adresse* die IP-Adresse für den DRAC 5 und *Schnittstellennummer* die Telnet-Schnittstellennummer ist (wenn Sie eine neue Schnittstelle verwenden).

Die Rücktaste für die Telnet-Sitzung konfigurieren

Abhängig vom Telnet-Client kann die Verwendung der <Rücktaste> zu unerwarteten Ergebnissen führen. Zum Beispiel kann die Sitzung ein Echo ^h verursachen. Jedoch können die meisten Microsoft und Linux Telnet-Clients 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 Eingabeaufforderungsfenster (falls erforderlich).

2. Wenn Sie keine Telnet-Sitzung ausführen, geben Sie folgendes ein:

   `telnet`

   Wenn Sie eine Telnet-Sitzung ausführen, drücken Sie <Strg><] >.

3. An der Eingabeaufforderung folgendes eingeben:

   `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 Eingabeaufforderung und geben Sie folgendes ein:

   ```
   stty erase ^h
   ```

2. An der Eingabeaufforderung folgendes eingeben:

   ```
   telnet
   ```

Eine serielle oder Telnet-Konsole verwenden

Serielle und **Telnet**-Befehle und RACADM-CLI können in einer seriellen oder Telnet-Konsole eingegeben und auf dem Server lokal oder im Remote-Zugriff ausgeführt werden. Der lokale RACADM-CLI wird für den Gebrauch nur durch einen root-Benutzer installiert.

Weitere Informationen über **serial/telnet/ssh-**Befehle und RACADM-CLI finden Sie in "RACADM Befehlszeilenoberfläche verwenden".

Telnet mittels Windows XP oder Windows 2003 ausführen

Wenn Ihre Verwaltungsstation Windows XP oder Windows 2003 ausführt, kann ein Problem mit den Zeichen in einer DRAC 5-Telnet-Sitzung auftreten. Dieses Problem kann als eine eingefrorene Anmeldung auftreten, wobei die Eingabetaste nicht reagiert und keine Kennwort-Eingabeaufforderung erscheint.

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

Telnet mittels Windows 2000 ausführen

Wenn Ihre Verwaltungsstation Windows 2000 ausführt, können Sie nicht mittels der <F2> Taste auf den BIOS-Setup zugreifen. Dieses Problem wird mit dem mit den Windows-Services für UNIX® 3.5 gelieferten Telnet-Client gelöst - einem empfohlenen Gratis-Download von Microsoft. Sie können Windows-Services für UNIX 3.5 von **www.microsoft.com/windows/sfu/downloads/default.asp** herunterladen.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5 mittels der Internet-Benutzeroberfläche konfigurieren

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Der DRAC 5 enthält eine webbasierte Schnittstelle und RACADM (eine Befehlszeilenschnittstelle), mit denen Sie die DRAC 5-Eigenschaften und -Benutzer konfigurieren, Remote-Verwaltungstasks ausführen, und Probleme an einem Remote (Managed) System beheben können. Für das tägliche System-Management verwenden Sie die webbasierte DRAC 5-Schnittstelle. Dieses Kapitel gibt Auskunft darüber, wie man allgemeine System-Verwaltungstasks mit der webbasierten DRAC 5 Schnittstelle ausführt, und enthält Verknüpfungen zu verwandten Informationen.

Alle webbasierten Schnittstellenkonfigurationstasks können auch mit RACADM ausgeführt werden. Eine Liste aller Racadm-CLI und serieller/telnet/ssh-Konsolenbefehle, mit denen die textbasierten Entsprechungen jeder Aufgabe ausgeführt werden können, finden Sie in "Serielle und Racadm-Befehle verwenden".

Die DRAC 5 Online-Hilfe enthält kontextempfindliche Informationen über jede webbasierte Schnittstellenseite.

Auf die webbasierte Schnittstelle zugreifen

Zum Zugriff auf die webbasierte DRAC 5-Schnittstelle führen Sie die folgenden Schritte aus:

1. Öffnen Sie ein unterstütztes Internetbrowser-Fenster.

   Weitere Informationen finden Sie in "Unterstützte Internetbrowser".

2. Geben sie folgendes in das Feld **Adresse** ein und drücken Sie <Eingabe>:

   `https://<IP-Adresse>`

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

   `https://<IP-Adresse>:<Schnittstellennummer>`

   wobei *IP-Adresse* die IP-Adresse des DRAC 5 und *Schnittstellennummer* die HTTPS Schnittstellennummer ist.

   Der DRAC 5-Fenster **Anmelden** erscheint.

Anmeldung

Sie können sich entweder als DRAC 5-Benutzer oder als ein Microsoft® Active Directory® Benutzer anmelden. Standardbenutzername und -kennwort sind **root** bzw. **calvin**.

Bevor Sie sich am DRAC 5 anmelden, prüfen Sie, ob Sie die Berechtigung **An DRAC 5 anmelden** haben.

Um sich anzumelden, führen Sie die folgenden Schritte aus.

1. Geben Sie eine der folgenden Eingaben in das Feld **Benutzername** ein:
   - Ihren DRAC 5-Benutzernamen.

     Beispiel: <*Benutzername*>

     Der DRAC 5-Benutzername für lokale Benutzer ist groß-/kleinschreibungsabhängig
   - Ihren Active Directory-Benutzernamen

     Beispiel: <*Domäne*>\<*Benutzername*> <*Domäne*>/<*Benutzername*> oder <*Benutzer*>@<*Domäne*>.

     Beispiele eines Active Directory-Benutzernamens sind: **dell.com\john_doe** oder **john_doe@dell.com**.

     Der Active Directory-Benutzername ist nicht groß-/kleinschreibungsabhängig.

2. Geben Sie Ihr DRAC 5-Benutzerkennwort oder Active Directory-Benutzerkennwort in das Feld **Kennwort** ein.

Dieses Feld unterscheidet Groß- und Kleinschreibung

3. Klicken Sie auf **OK** oder drücken Sie auf <Eingabe>.

Abmeldung

1. Klicken Sie auf **Abmelden** in der rechten oberen Ecke des Fensters der webbasierten DRAC 5-Schnittstelle, um die Sitzung zu schließen.
2. Schließen Sie das Browser-Fenster.

ANMERKUNG: Die Schaltfläche **Abmelden** erscheint erst, wenn Sie sich anmelden.

ANMERKUNG: Schließen des Browser ohne sich ordnungsgemäß abzumelden, führt dazu, dass die Sitzung geöffnet bleibt, bis die Zeitüberschreitung erreicht wurde. Es wird empfohlen, dass Sie zum Beenden der Sitzung auf die Abmeldungsschaltfläche klicken, ansonsten bleibt die Sitzung aktiv, bis die Sitzungszeitüberschreitung erreicht wird.

ANMERKUNG: Das Schließen der DRAC 5-webbasierten Schnittstelle in Microsoft Internet Explorer mithilfe der Schließen-Schaltfläche ("x") in der oberen rechten Ecke des Fensters kann zu einem Anwendungsfehler führen. Um dieses Problem zu lösen, laden Sie von der Support-Website von Microsoft unter support.microsoft.com die neueste kumulative Sicherheitsaktualisierung für Internet Explorer herunter.

DRAC 5-NIC konfigurieren

Netzwerk- und IPMI-LAN-Einstellungen konfigurieren

ANMERKUNG: Zur Ausführung der folgenden Schritte müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

ANMERKUNG: Die meisten DHCP Server erfordern, dass ein Server ein Client-ID-Token in seiner Reservierungstabelle speichert. Der Client (DRAC 5, zum Beispiel) muss dieses Token während der DHCP-Verhandlung beitragen. Für RACs liefert der DRAC 5 die Client-ID-Option mit einer Ein-Byte-Schnittstellennummer (0), gefolgt von einer Sechs-Byte MAC-Adresse.

ANMERKUNG: Wenn Ihr Managed DRAC-System DRAC im Modus **Freigegeben** oder **Freigegeben für Failover** konfiguriert ist und der DRAC bei aktiviertem Bereichsstrukturprotokoll (STP) an einen Schalter angeschlossen ist, werden Netzwerk-Clients eine 20 bis 30 Sekunden lange Verzögerung in der Konnektivität feststellen, wenn sich der LOM-Verknüpfungsstatus der Verwaltungssation während der STP-Konvergenz ändert.

1. In **System**struktur klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das **Konfiguration**-Register und dann auf **Netzwerk**.
3. Konfigurieren Sie die DRAC 5 NIC-Einstellungen auf der Seite **Netzwerkkonfiguration**.

   Tabelle 4-1 und Tabelle 4-2 beschreiben **Netzwerk-Einstellungen** und **IPMI-Einstellungen** auf der Seite **Netzwerkkonfiguration**.
4. Wenn dies abgeschlossen ist, klicken Sie auf **Änderungen anwenden**.
5. Klicken Sie auf die Schaltfläche der entsprechenden **Netzwerkkonfiguration-**Seite, um fortzufahren. Siehe Tabelle 4-3.

Tabelle 4-1. Netzwerkeinstellungen

Einstellung	Beschreibung
NIC-Auswahl	Zeigt den ausgewählten NIC-Modus an (**Reserviert**, **Freigegeben für Failover**, oder **Freigegeben**). Die Standardeinstellung ist **Reserviert**.
MAC-Adresse	Zeigt die DRAC 5 MAC-Adresse an.
NIC aktivieren	Aktiviert die DRAC 5-NIC und die restlichen Steuerungen in dieser Gruppe. Die Standardeinstellung ist **Aktiviert**.
DHCP verwenden (für die NIC-IP-Adresse)	Aktiviert Dell OpenManage™ Server Administrator, um die DRAC 5 NIC-IP-Adresse vom Server des dynamischen Host-Konfigurationsprotokolls (DHCP) zu erhalten. Die Auswahl des Kontrollkästchens deaktiviert die Steuerung der **statischen IP-Adresse**, des **statischen Gateway** und der **statischen Subnetzmaske**. Die Standardeinstellung ist **Deaktiviert**.
Statische IP-Adresse	Bestimmt oder bearbeitet die statische IP-Adresse für die DRAC 5-NIC. Um diese Einstellung zu ändern, wählen Sie das Kontrollkästchen **DHCP (für die NIC-IP-Adresse) verwenden** ab.
Statischer Gateway	Bestimmt oder bearbeitet das statische Gateway für die DRAC 5-NIC. Um diese Einstellung zu ändern, wählen Sie das Kontrollkästchen **DHCP (für die NIC-IP-Adresse) verwenden** ab.
Statische Subnetzmaske	Bestimmt oder bearbeitet die statische Subnetzmaske für die DRAC 5-NIC. Um diese Einstellung zu ändern, wählen Sie das Kontrollkästchen **DHCP (für die NIC-IP-Adresse) verwenden** ab.
DHCP zum Abrufen von DNS-Serveradressen verwenden	Ruft die primären und sekundären DNS Server-Adressen an Stelle der der statischen Einstellungen vom DHCP Server ab.

	Die Standardeinstellung ist **Deaktiviert**.
Statischer bevorzugter DNS-Server	Verwendet die primäre DNS Server-IP-Adresse nur, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden nicht ausgewählt** ist.
Statischer alternativer DNS-Server	Verwendet die sekundäre DNS Server-IP-Adresse, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden nicht ausgewählt** ist. Sie können in eine IP-Adresse von 0.0.0.0 eingeben, wenn Sie keinen wechselnden DNS-Server haben.
DRAC auf DNS registrieren	Registriert den DRAC 5-Namen auf dem DNS-Server. Die Standardeinstellung ist **Deaktiviert**.
DNS DRAC-Name	Zeigt den DRAC 5-Namen nur, wenn **DRAC 5 auf DNS registrieren** ausgewählt ist. Der Standardname des DRAC 5 ist RAC-*Service-Tag-Nummer*, wobei *Service-Tag-Nummer* die Service-Tag-Nummer des Dell Servers ist (Beispiel: RAC-ek00002).
DHCP für den DNS-Domänennamen verwenden	Verwendet den Standard-DNS-Domänenname. Wenn das Kästchen nicht gewählt ist und die Option **DRAC 5 auf DNS registrieren** gewählt wird, können Sie den DNS-Domänennamen im Feld **DNS-Domänenname** modifizieren. Die Standardeinstellung ist **Deaktiviert**.
DNS-Domänenname	Die Standardeinstellung des DNS-Domänennamens ist **MYDOMAIN**. Wenn das Kontrollkästchen **DHCP für den DNS-Domänennamen verwenden** ausgewählt ist, können Sie dieses Feld nicht modifizieren, und es wird "ausgegraut".
Automatische Aushandlung	Bestimmt, ob der DRAC 5 den **Duplexmodus** und die **Netzwerktaktrate** automatisch einstellt, indem er mit dem nächsten Router oder Hub kommuniziert (**Ein**) oder Sie den **Duplexmodus** und die **Netzwerktaktrate** manuell einstellen können (**Aus**).
Netzwerktaktrate	Stellt die Netzwerkgeschwindigkeit entsprechend der Netzwerkumgebung auf 100 MB oder 10 MB ein. Diese Option ist nicht vorhanden, wenn **Automatische Aushandlung** auf **Ein** eingestellt ist.
Duplexmodus	Stellt den Duplexbetrieb entsprechend der Netzwerkumgebung auf Voll oder Halb ein. Diese Auswahl ist nicht vorhanden, wenn **Automatische Aushandlung** auf **Ein** gestellt ist.

Tabelle 4-2. IPMI LAN-Einstellungen

Einstellung	**Beschreibung**
IPMI über LAN aktivieren	Aktiviert den IPMI LAN-Kanal.
Beschränkung der Channel-Berechtigungsebene	Konfiguriert die höchste Berechtigungsebene des Benutzers, die auf dem LAN-Kanal akzeptiert werden kann. Wählen Sie eine der folgenden Optionen aus: Administrator, Operator oder Benutzer.
Verschlüsselungsschlüssel	Bestimmt das Verschlüsselungsschlüssel-Zeichenformat: 0 bis 20 Hexadezimalzeichen (keine Leerstellen erlaubt). Die Standardeinstellung ist **0000000000000000000**.
VLAN-ID aktivieren	Aktiviert die VLAN-ID. Wenn aktiviert, wird nur abgestimmter VLAN ID-Verkehr akzeptiert.
VLAN-ID	Das VLAN ID-Feld von 802.1g Feldern.
Priorität	Das Prioritätsfeld von 802.1g Feldern.

Tabelle 4-3. Netzwerkkonfiguration-Seitenschaltflächen

Schaltfläche	**Beschreibung**
Drucken	Druckt die Seite **Netzwerkkonfiguration**
Aktualisieren	Lädt die Seite **Netzwerkkonfiguration** erneut
Erweiterte Einstellungen	Zeigt die Seite **Netzwerksicherheit** an.
Änderungen anwenden	Speichert die an der Netzwerkkonfiguration vorgenommenen Änderungen. **ANMERKUNG:** Bei Änderungen an den NIC-IP-Adresseneinstellungen werden alle Benutzersitzungen geschlossen und Benutzer müssen mit den aktualisierten IP-Adresseneinstellungen eine neue Verbindung zur webbasierten DRAC 5-Schnittstelle aufbauen. Alle anderen Änderungen erfordern, dass die NIC zurückgesetzt wird, was einen kurzen Verlust der Konnektivität verursachen kann.

Netzwerksicherheitseinstellungen konfigurieren

ANMERKUNG: Zur Ausführung der folgenden Schritte müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben.

1. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**.
3. Auf der Seite **Netzwerkkonfiguration** klicken Sie auf **Erweiterte Einstellungen**.
4. Konfigurieren Sie die Attributwerte auf der Seite **Netzwerksicherheit** und klicken Sie dann auf **Änderungen anwenden**.

   Tabelle 4-4 beschreibt die Einstellungen auf der Seite **Netzwerksicherheit**.

5. Klicken Sie auf die Schaltfläche der entsprechenden **Netzwerk-Sicherheit**-Seite, um fortzufahren. Siehe Tabelle 4-5.

Tabelle 4-4. Einstellungen der Seite Netzwerksicherheit

Einstellungen	Beschreibung
IP-Bereich aktiviert	Aktiviert die Funktion IP-Bereichsüberprüfung, die einen spezifischen Bereich von IP-Adressen definiert, die auf den DRAC 5 zugreifen können.
IP-Bereichsadresse	Bestimmt die akzeptable IP-Subnetzadresse.
IP-Bereich-Subnetzmaske	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Subnetzmaske sollte in der Form einer Netzmaske sein, wobei die bedeutenderen Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu Nullen (0) in den niederwertigeren Bits. Zum Beispiel: **255.255.255.0**
IP-Blockieren aktiviert	Aktiviert die IP-Adressen-Blockierungsfunktion, mit der die Anzahl von fehlerhaften Anmeldungsversuchen von einer spezifischen IP-Adresse für einen bestimmten Zeitraum beschränkt wird.
IP-Blockierungsausfall	Stellt die Anzahl von Anmeldungsfehlschlägen von einer IP-Adresse ein, bevor die Anmeldungsversuche von dieser Adresse zurückgewiesen werden.
Fenster IP-Blockierungsausfall	Bestimmt den Zeitraum in Sekunden, während dessen die Fehler der Zählung IP-Blockausfall auftreten müssen, um die Penalty-Zeit IP-Block auszulösen.
Penalty-Zeit IP-Block	Legt den Zeitraum in Sekunden fest, während dessen Anmeldungsversuche von einer IP-Adresse aufgrund übermäßiger Fehler zurückgewiesen werden.

Tabelle 4-5. Schaltflächen Netzwerksicherheitsseite

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Netzwerksicherheit**
Aktualisieren	Lädt die Seite **Netzwerksicherheit** neu
Änderungen anwenden	Speichert die Änderungen, die auf der Seite **Netzwerksicherheit** eingegeben wurden.
Zurück zur Netzwerkkonfigurationsseite	Rückkehr zur Seite **Netzwerkkonfiguration**.

DRAC 5-Benutzer hinzufügen und konfigurieren

Zur Verwaltung des Systems mit dem DRAC 5 und zur Aufrechterhaltung der Systemsicherheit erstellen Sie eindeutige Benutzer mit spezifischen Verwaltungsberechtigungen (oder *rollenbasierter Autorität*). Für zusätzliche Sicherheit können Sie auch Warnungen konfigurieren, die spezifischen Benutzern per E-Mail geschickt werden, wenn ein spezifisches Systemereignis auftritt.

Um DRAC 5-Benutzer hinzuzufügen und zu konfigurieren, führen Sie die folgenden Schritte aus:

ANMERKUNG: Zur Ausführung der folgenden Schritte müssen Sie die Berechtigung DRAC 5 konfigurieren haben.

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.

2. Klicken Sie auf das Register **Konfiguration** und dann auf **Benutzer**.

   Die Seite **Benutzer** wird eingeblendet, die **Status**, **RAC-Berechtigung**, **IPMI LAN-Berechtigung** und **serielle IPMI-Berechtigung** jedes Benutzers enthält.

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

4. Auf der Seite **Anwenderkonfiguration** konfigurieren Sie die Eigenschaften und Berechtigungen des Benutzers.

   Tabelle 4-6 beschreibt die **Allgemeinen** Einstellungen zur Konfiguration eines neuen oder bestehenden DRAC-Benutzernamens und -Kennworts.

   Tabelle 4-7 beschreibt **IPMI-Benutzerberechtigungen** zum Konfigurieren der Benutzer-LAN-Berechtigungen.

   Tabelle 4-8 beschreibt die **Benutzergruppenberechtigungen** für die Einstellung der **IPMI-Benutzerberechtigungen** und der **DRAC-Benutzerberechtigungen**.

   Tabelle 4-9 beschreibt die **DRAC-Gruppenberechtigungen**. Wenn Sie dem Administrator, Hauptbenutzer oder Gastbenutzer eine DRAC-Benutzerberechtigung hinzufügen, wird die **DRAC-Gruppe** zur **Benutzerdefinierten** Gruppe geändert.

5. Wenn dies abgeschlossen ist, klicken Sie auf **Änderungen anwenden**.

6. Klicken Sie auf die Schaltfläche der entsprechenden **Benutzerkonfiguration**-Seite, um fortzufahren. Siehe Tabelle 4-10.

Tabelle 4-6. Allgemeine Eigenschaften

Eigenschaft	Beschreibung
Benutzer-ID	Gibt eine von 16 voreingestellten Benutzer-ID-Nummern an. Wenn Sie Informationen für den Benutzer 'root' bearbeiten, ist dieses Feld statisch. Sie können den Benutzernamen für 'root' nicht bearbeiten.
Benutzer aktivieren	Ermöglicht dem Benutzer, auf den DRAC 5 zuzugreifen. Wenn dies nicht markiert ist, kann der Benutzername nicht geändert werden.
Benutzername	Gibt einen DRAC 5-Benutzernamen mit bis zu 16 Zeichen an. Jeder Benutzer muss einen eindeutigen Benutzernamen haben. **ANMERKUNG:** Benutzernamen auf dem lokalen DRAC 5 können keinen **/** (Vorwärts-Schrägstrich) oder **.** (Punkt) enthalten. **ANMERKUNG:** Wenn der Benutzername geändert wird, erscheint der neue Name erst in der Benutzeroberfläche, wenn sich der nächste Benutzer anmeldet.
Kennwort ändern	Aktiviert die Felder **Neues Kennwort** und **Neues Kennwort bestätigen**. Wenn dies nicht markiert ist, kann das **Kennwort** des Benutzers nicht geändert werden.
Neues Kennwort	Definiert oder bearbeitet das DRAC 5-Benutzerkennwort.
Neues Kennwort bestätigen	Es ist erforderlich, dass Sie das Kennwort des DRAC 5-Benutzers nochmals eingeben, um zu bestätigen.

Tabelle 4-7. IPMI-Benutzerberechtigungen

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

Tabelle 4-8. DRAC-Benutzerberechtigungen

Eigenschaft	Beschreibung
DRAC-Gruppe	Legt die maximale DRAC-Benutzerberechtigung auf dem seriellen IPMI-Kanal für eine der folgenden Möglichkeiten fest: **Administrator**, **Hauptbenutzer**, **Gastbenutzer** oder **Benutzerdefiniert**. Tabelle 4-9 enthält die **DRAC-Gruppenberechtigungen**.
Anmeldung an DRAC	Ermöglicht dem Benutzer, sich am DRAC anzumelden.
DRAC konfigurieren	Ermöglicht dem Benutzer, den DRAC zu konfigurieren.
Benutzer konfigurieren	Ermöglicht dem Benutzer, spezifischen Benutzern zu erlauben, auf das System zuzugreifen.
Protokolle löschen	Ermöglicht dem Benutzer, die DRAC-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, den virtuellen Datenträger auszuführen und zu verwenden.
Testwarnungen	Ermöglicht dem Benutzer, einem spezifischen Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnostische Befehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Tabelle 4-9. DRAC-Gruppenberechtigungen

Benutzergruppe	Berechtigungen gewährt
Administrator	**Anmeldung bei DRAC**, **DRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Hauptbenutzer	**Anmeldung bei DRAC**, **Protokoll löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**
Gastbenutzer	**Anmeldung an DRAC**
Benutzerdefiniert	Auswahl einer beliebigen Kombination der folgenden Berechtigungen: **Anmeldung bei DRAC**, **DRAC konfigurieren**, **Benutzer konfigurieren**, **Protokoll löschen**, **Server-Maßnahmenbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Keine	Keine zugewiesenen Berechtigungen

Tabelle 4-10. Schaltflächen der Benutzerkonfigurationsseite

Schaltfläche	Maßnahme
Drucken	Druckt die Seite **Anwenderkonfiguration**
Aktualisieren	Lädt die Seite **Anwenderkonfiguration** neu
Zurück zur Benutzerseite	Wechselt zurück zur **Benutzerseite**.
Änderungen anwenden	Speichert die an der Netzwerkkonfiguration vorgenommenen Änderungen.

Active Directory-Zertifikate (Standardschema und Erweitertes Schema) konfigurieren und verwalten

ANMERKUNG: Sie müssen die Berechtigung **DRAC 5 konfigurieren** haben, um Active Directory zu konfigurieren und um ein Active Directory-Zertifikat hochzuladen, herunterzuladen und anzusehen.

ANMERKUNG: Weitere Informationen über die Konfiguration von Active Directory und wie Sie Active Directory mit Standardschema oder Erweitertem Schema konfigurieren, finden Sie unter "DRAC 5 mit Microsoft Active Directory verwenden".

Verwenden Sie den Microsoft® Active Directory® Dienst, um Ihre Software für den Zugriff auf den DRAC 5 zu konfigurieren. Der Dienst erlaubt Ihnen, die DRAC5 Benutzerberechtigungen Ihrer vorhandenen Benutzer hinzuzufügen und zu kontrollieren.

Weitere Informationen enthält "DRAC 5 mit Microsoft Active Directory verwenden".

Auf das Active Directory-Hauptmenü zugreifen:

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** und dann auf **Active Directory**.

Tabelle 4-11 enthält die Optionen der Seite **Active Directory**-**Hauptmenü.** Die Schaltflächen in Tabelle 4-12 sind verfügbar auf der Seite **Active Directory**-**Hauptmenü**.

Tabelle 4-11. Optionen der Seite Active Directory-Hauptmenü

Feld	Beschreibung
Active Directory konfigurieren	Konfiguriert den DRAC-Namen von Active Directory, den Root-Domänennamen, den DRAC-Domänennamen, die Active Directory-Authentifizierungszeitüberschreitung, die Auswahl des Active Directory-Schemas und Rollengruppeneinstellungen.
Active Directory CA-Zertifikat hochladen	Lädt ein Active Directory-Zertifikat zum DRAC hoch.
DRAC-Server-Zertifikat herunterladen	Der Windows Download-Manager ermöglicht, ein DRAC-Serverzertifikat zu Ihrem System herunterzuladen.
Active Directory CA-Zertifikat ansehen	Zeigt das Active Directory-Zertifikat an, das zum DRAC hochgeladen wurde.

Tabelle 4-12. Schaltflächen der Seite Active Directory-Hauptmenü

Schaltfläche	Definition
Drucken	Druckt den Inhalt des offenen Fensters auf Ihrem Standarddrucker
Weiter	Weiter zur nächsten gewählten Seite **Option**.

Active Directory (Standardschema und Erweitertes Schema) konfigurieren

1. Auf der Seite **Active Directory**-**Hauptmenü** wählen Sie **Active Directory konfigurieren** und klicken Sie auf **Weiter**.
2. Auf der Seite **Active Directory-Konfiguration und Verwaltung** die Active Directory-Einstellungen eingeben.

   Tabelle 4-13 beschreibt die Seiteneinstellungen für **Active Directory-Konfiguration und Verwaltung**.
3. Auf **Anwenden klicken**, um die Einstellungen zu speichern.
4. Klicken Sie auf die Schaltfläche der entsprechenden **Active Directory**-**Konfiguration-**Seite, um fortzufahren. Siehe Tabelle 4-14.
5. Um die Rollengruppen für das Active Directory-Standardschema zu konfigurieren, klicken Sie auf die einzelne Rollengruppe (1-5). Siehe Tabelle 4-15 und Tabelle 4-16.

ANMERKUNG: Um Einstellungen auf der Seite **Active Directory-Konfiguration und Verwaltung** zu speichern, müssen Sie auf **Anwenden** klicken, bevor Sie mit der Seite **Benutzerdefinierte Rollengruppe** fortfahren.

Tabelle 4-13. Seite zur Einstellung der Active Directory-Konfiguration und Verwaltung

Einstellung	Beschreibung
Active Directory aktivieren	Aktiviert Active Directory. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
ROOT-Domänenname	Der Active Directory ROOT-Domänenname. Dieser Wert ist standardmäßig **NULL**. Der Name muss ein gültiger Domänenname sein und aus *x.y* bestehen, wobei *x* eine ASCII Zeichenkette mit 1 bis -254 Zeichen ohne Leerstellen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net, org ist.
Zeitüberschreitung	Die Wartezeit in Sekunden, bis die Active Directory-Abfragen beendet. Minimaler Wert ist gleich oder größer als 15 Sekunden. Der Standardwert ist 120 Sekunden.
Verwenden Sie Standardschema	Verwendet Standardschema mit Active Directory
Verwenden Sie Erweitertes Schema	Verwendet Erweitertes Schema mit Active Directory
DRAC-Name	Der Name, der die DRAC 5-Karte in Active Directory eindeutig identifiziert. Dieser Wert ist standardmäßig **NULL**. Der Name muss eine ASCII Zeichenkette mit 1 bis -254 Zeichen ohne Leerstellen sein.
DRAC-Domänenname	Der DNS-Name (Zeichenkette) der Domäne, wo sich das Active Directory DRAC 5-Objekt befindet. Dieser Wert ist standardmäßig **NULL**. Der Name muss ein gültiger Domänenname sein und aus *x.y* bestehen, wobei *x* eine ASCII Zeichenkette mit 1 bis -254 Zeichen ohne Leerstellen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net, org ist.
Rollengruppen	Die Liste von Rollengruppen, die mit der DRAC 5-Karte verbunden sind. Um die Einstellungen für eine Rollengruppe zu ändern, klicken Sie auf ihre Rollengruppennummer in der Rollengruppenliste. Das Fenster **Konfigurieren Sie die Rollengruppe** wird angezeigt. **ANMERKUNG:** Wenn Sie auf den Rollengruppenlink klicken, bevor Sie die Einstellungen für die Seite **Active Directory-Konfiguration und Verwaltung** anwenden, werden diese Einstellungen verloren gehen.
Gruppenname	Der Name, der die Rollengruppe im Active Directory identifiziert, das mit der DRAC 5-Karte verbunden ist.
Gruppedomäne	Die Domäne, in der die Gruppe ist.
Gruppenberechtigung	Die Berechtigungsstufe für die Gruppe.

Tabelle 4-14. Schaltflächen der Active Directory-Konfiguration und Verwaltung-Seite

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Active Directory-Konfiguration und Verwaltung**.
Anwenden	Speichert die Änderungen, die an der Seite **Active Directory-Konfiguration und Verwaltung** vorgenommen wurden.
Zurück zum Active Directory-Hauptmenü	Wechselt zurück zur Seite **Active Directory-Hauptmenü**.

Tabelle 4-15. Rollengruppenberechtigungen

Einstellung	Beschreibung
Rollengruppenberechtigungsstufe	Legt die maximale DRAC-Benutzerberechtigung auf dem seriellen IPMI-Kanal für eine der folgenden Möglichkeiten fest: Administrator, Hauptbenutzer, Gastbenutzer oder Benutzerdefiniert. Tabelle 4-16 enthält die **Rollengruppenberechtigungen**.
Anmeldung an DRAC	Ermöglicht dem Benutzer, sich am DRAC anzumelden.
DRAC konfigurieren	Ermöglicht dem Benutzer, den DRAC zu konfigurieren.
Benutzer konfigurieren	Ermöglicht dem Benutzer, spezifischen Benutzern zu erlauben, auf das System zuzugreifen.
Protokolle löschen	Ermöglicht dem Benutzer, die DRAC-Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer, Racadm-Befehle auszuführen.
Zugriff auf Konsolenumleitung	Ermöglicht dem Benutzer, die Konsolenumleitung auszuführen.
Zugriff auf Virtueller Datenträger	Ermöglicht dem Benutzer, den virtuellen Datenträger auszuführen und zu verwenden.
Testwarnungen	Ermöglicht dem Benutzer, einem spezifischen Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Tabelle 4-16. Rollengruppenberechtigungen

Eigenschaft	Beschreibung
Administrator	**Anmeldung bei DRAC**, **DRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Hauptbenutzer	**Anmeldung bei DRAC**, **Protokoll löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**
Gastbenutzer	**Anmeldung an DRAC**
Benutzerdefiniert	Auswahl einer beliebigen Kombination der folgenden Berechtigungen: **Anmeldung bei DRAC**, **DRAC konfigurieren**, **Benutzer konfigurieren**, **Protokoll löschen**, **Server-Maßnahmenbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Keine	Keine zugewiesenen Berechtigungen

Ein Active Directory CA-Zertifikat hochladen

1. Auf der Seite **Active Directory**-**Hauptmenü** wählen Sie **Active Directory-Zertifikat hochladen** und klicken Sie auf **Weiter**.
2. Auf der Seite **Zertifikat Hochladen** geben Sie den Dateipfad des Zertifikats in das **Dateipfad-**Feld ein oder klicken Sie auf **Durchsuchen**, um zu der Zertifikat-Datei zu wechseln.

ANMERKUNG: Der **Dateipfad**-Wert zeigt den relativen Pfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad einschließlich des vollständigen Pfads und Dateinamens und des Dateinamenszusatzes eingeben.

3. Klicken Sie auf **Anwenden**.
4. Klicken Sie auf die entsprechende **Zertifikat Hochladen**-Seitenschaltfläche, um fortzufahren. Siehe Tabelle 4-17.

Tabelle 4-17. Seitenschaltflächen Zertifikat hochladen

Schaltfläche	Beschreibung
Drucken	Seite **Zertifikat hochladen** drucken.
Zurück zum Active Directory-Hauptmenü	Zum **Active Directory-Hauptmenü** zurückkehren.
Anwenden	Wenden Sie das Zertifikat auf die DRAC 5-Firmware an.

DRAC Server-Zertifikat herunterladen

1. Auf der Seite **Active Directory**-**Hauptmenü** wählen Sie **DRAC Server-Zertifikat herunterladen** und klicken Sie auf **Weiter**.
2. Im Fenster **Datei herunterladen** auf **Speichern** klicken und die Datei zu einem Verzeichnis auf Ihrem System speichern.
3. Im Fenster **Herunterladen abgeschlossen** auf **Schließen** klicken.

Active Directory CA-Zertifikat ansehen

Verwenden Sie die Seite **Active Directory-Hauptmenü**, um ein CA-Serverzertifikat für Ihren DRAC 5 anzusehen.

1. Auf der Seite **Active Directory**-**Hauptmenü** wählen Sie **Active Directory-Zertifikat ansehen** und klicken Sie auf **Weiter**.

   Tabelle 4-18 enthält die Felder und zugehörigen Beschreibungen, die im **Zertifikat-**Fenster aufgeführt werden.

   Tabelle 4-19 beschreibt die verfügbaren Seitenschaltflächen auf der Seite **Active Directory CA Zertifikat ansehen**.

2. Klicken Sie auf die entsprechende Schaltfläche der Seite **Active Directory CA-Zertifikat ansehen**, um fortzufahren. Siehe Tabelle 4-19.

Tabelle 4-18. Active Directory CA Zertifikat-Informationen

Feld	Beschreibung
Seriennummer	Zertifikat-Seriennummer.
Subjektinformationen	Vom Subjekt eingegebene Zertifikat-Attribute.
Aussteller-Informationen	Vom Aussteller zurückgegebene Zertifikat-Attribute.
Gültig von	Zertifikat-Ausstellungsdatum.

Gültig bis	Zertifikat-Verfallsdatum.

Tabelle 4-19. Active Directory CA-Zertifikat-Seitenschaltflächen ansehen

Schaltfläche	Beschreibung
Drucken	Druckt das **Active Directory CA-Zertifikat**.
Zurück zum Active Directory-Hauptmenü	Zurück zur Seite **Active Directory-Hauptmenü**.

DRAC 5 Kommunikationen mit SSL- und digitalen Zertifikaten sichern

Dieser Unterabschnitt enthält Informationen über die folgenden Datensicherheitsfunktionen, die in Ihrem DRAC 5 integriert sind:

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

Secure Sockets Layer (SSL)

Der DRAC enthält einen Web Server, der zur Verwendung des Industriestandard-SSL-Sicherheitsprotokolls zur Übertragung verschlüsselter Daten über das Internet konfiguriert ist. SSL ist aufgebaut auf öffentlicher und privater Verschlüsselungstechnologie und eine allgemein akzeptierte Technik, um authentifizierte und verschlüsselte Kommunikationen zwischen Clients und Servern zu bieten, und unbefugtes Lauschen auf dem Netzwerk zu verhindern.

SSL erlaubt einem SSL-aktivierten System, die folgenden Tasks auszuführen:

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

Dieses Verschlüsselungsverfahren gewährt eine hohe Datenschutz-Stufe. Der DRAC verwendet den SSL 128-Bit-Verschlüsselungsstandard, die sicherste Form der Verschlüsselung, die für Internetbrowser in Nordamerika allgemein verfügbar ist.

Der DRAC-Webserver enthält ein selbstsigniertes Dell SSL Digitalzertifikat (Server-ID). Um hohe Sicherheit über das Internet zu sichern, ersetzen Sie das Webserver SSL-Zertifikat, indem eine Anforderung an den DRAC gesendet wird, eine neue Zertifikatssignierungsanforderung (CSR) zu erstellen.

Zertifikatssignierungsanforderung (CSR)

Ein CSR ist eine digitale Anforderung an eine Zertifizierungsstelle (CA) für ein sicheres Server-Zertifikat. Sichere Serverzertifikate sichern die Identität eines Remote-Systems und gewährleisten, dass mit dem Remote-System ausgetauschte Informationen nicht von anderen gesehen oder geändert werden können. Um die Sicherheit für Ihren DRAC 5 zu sichern, wird empfohlen, dass Sie eine CSR erstellen, die CSR an ein CA senden und das von der CA zurückgesendete Zertifikat hochladen.

Eine Zertifizierungsstelle ist ein Geschäftsunternehmen, das in der IT-Industrie dafür anerkannt ist, hohe Standards der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger Sicherheitskriterien zu treffen. Beispiele von CAs schließen Thawte und VeriSign ein. Nachdem die CA Ihre CSR erhält, prüfen und überprüfen die in der CSR enthaltenen Informationen. Wenn der Bewerber die Sicherheitsstandards von CA erfüllt, gibt die CA ein Zertifikat an den Bewerber aus, das diesen Bewerber identifiziert, um Transaktionen über Netzwerke und auf dem Internet vorzunehmen.

Nachdem die CA die CSR genehmigt und Ihnen ein Zertifikat sendet, müssen Sie das Zertifikat zur DRAC-Firmware hochladen. Die auf der DRAC-Firmware gespeicherten CSR-Informationen müssen mit den im Zertifikat enthaltenen Informationen übereinstimmen.

Zugriff auf das SSL-Hauptmenü

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** und dann auf **SSL**.

Verwenden Sie die Optionen auf der Seite **SSL-Hauptmenü** (siehe Tabelle 4-20), um eine CSR zu erstellen, die an einen CA gesendet wird.Die CSR-Informationen werden auf der DRAC 5-Firmware gespeichert. Die Schaltflächen in Tabelle 4-21 sind verfügbar auf der Seite **SSL-Hauptmenü**.

Tabelle 4-20. SSL-Hauptmenüoptionen

Feld	Beschreibung
Eine neue Zertifikatsignierungsanforderung erstellen (CSR)	Klicken Sie auf **Weiter**, um die Seite **Erstellung einer Zertifikatsignierungsanforderung** zu öffnen, die Ihnen ermöglicht, eine CSR zu erstellen, die an eine CA gesendet werden kann, um ein sicheres Webzertifikat anzufordern. **HINWEIS:** Jede neue CSR überschreibt jede vorherige CSR auf der Firmware. Damit eine CA Ihre CSR annimmt, muss die CSR in der Firmware mit dem zurückgesendeten Zertifikat von der CA übereinstimmen.
Server-Zertifikat hochladen	Klicken Sie auf **Weiter,** um ein vorhandenes Zertifikat hochzuladen, für das Ihre Firma den Titel besitzt und dazu verwendet, Zugang zum DRAC 5 zu kontrollieren. **HINWEIS:** Nur X509 Base 64-kodierte Zertifikate werden vom DRAC 5 akzeptiert. DER-kodierte Zertifikate werden nicht akzeptiert. Das Hochladen eines neuen Zertifikats ersetzt das Standardzertifikat, das Sie mit Ihrem DRAC 5 erhalten haben.
Serverzertifikat anzeigen	Klicken Sie auf **Weiter**, um ein vorhandenes Serverzertifikat anzuzeigen.

Tabelle 4-21. SSL-Hauptmenüschaltflächen

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **SSL-Hauptmenü**.
Weiter	Wechselt zur nächsten Seite.

Neue Zertifikatssignierungsanforderung erstellen

ANMERKUNG: Jede neue CSR überschreibt jede vorherige CSR auf der Firmware. Bevor eine CA (Zertifizierungsstelle) Ihre CSR akzeptieren kann, muss die letzte in der Firmware erstellte CSR mit dem von der CA zurückgesendeten Zertifikat übereinstimmen. Ansonsten wird der DRAC 5 das Zertifikat nicht hochladen.

1. Wählen Sie auf der Seite **SSL-Hauptmenü** die Option **Neue Zertifikatssignierungsanforderung (CSR) erstellen** und klicken Sie auf **Weiter**.
2. Geben Sie auf der Seite **Zertifikatssignierungsanforderung (CSR) erstellen** einen Wert für jeden CSR-Attributwert ein.

   Tabelle 4-22 beschreibt die Seitenoptionen für **Zertifikatssignierungsanforderung (CSR) erstellen**.
3. Klicken Sie auf **Erstellen**, um die CSR zu speichern oder anzusehen.
4. Klicken Sie auf die entsprechende Seitenschaltfläche **Zertifikatssignierungsanforderung (CSR) erstellen**, um fortzufahren. Siehe Tabelle 4-23.

Tabelle 4-22. Zertifikatssignierungsanforderung (CSR) -Seitenoptionen erstellen

Feld	Beschreibung
Allgemeiner Name	Der genaue Name, der zertifiziert werden soll (normalerweise der Webserver-Domänenname, z. B. **www.xyzFirma.com**). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen und Punkte sind gültig. Leerstellen sind nicht gültig.
Organisationsname	Der mit dieser Organisation assoziierte Name (z. B. XYZ Unternehmen). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Organisationseinheit	Der mit einer organisatorischen Einheit assoziierte Name, wie z. B. eine Abteilung (zum Beispiel, Unternehmensgruppe). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Ort	Die Stadt oder ein anderer Standort des Unternehmens, das zertifiziert wird (z. B. München). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie keine Unterstreichungszeichen oder andere Zeichen, um Wörter zu trennen.
Zustandsname	Das Bundesland oder die Provinz, in der sich das Unternehmen, das sich für eine Zertifizierung bewirbt, befindet (z. B. Bayern). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie keine Abkürzungen.
Landescode	Der Name des Landes, wo sich das Unternehmen, das sich um Zertifikat bewirbt, befindet. Verwenden Sie das Drop-Down-Menü, um das Land auszuwählen.
E-Mail	Die der CSR zugeordnete E-Mail-Adresse. Sie können die E-Mail-Adresse Ihrer Firma eingeben oder eine E-Mail-Adresse, die mit der CSR assoziiert sein soll. Dieses Feld ist optional.

Tabelle 4-23. Zertifikatssignierungsanforderung (CSR) -Seitenschaltflächen erstellen

Schaltfläche	Beschreibung
Drucken	Die Seite **Zertifikatssignierungsanforderung (CSR) erstellen** drucken.
Zurück zum Sicherheitshauptmenü	Zurück zur Seite **SSL-Hauptmenü**.
Erstellen	Eine CSR erstellen

Ein Server-Zertifikat hochladen

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

   Die Seite **Zertifikat hochladen** wird eingeblendet.

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

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

3. Klicken Sie auf **Anwenden**.

4. Klicken Sie auf die entsprechende Seitenschaltfläche, um fortzufahren. Siehe Tabelle 4-24.

Tabelle 4-24. Seitenschaltflächen Zertifikat hochladen

Schaltfläche	Beschreibung
Drucken	Seite **Zertifikat hochladen** drucken.
Zurück zum SSL Hauptmenü	Zurück zur Seite **SSL-Hauptmenü**.
Anwenden	Wenden Sie das Zertifikat auf die DRAC 5-Firmware an.

Ein Serverzertifikat anzeigen

1. Wählen Sie auf der Seite **SSL-Hauptmenü** die Option **Server-Zertifikat ansehen** und klicken Sie auf **Weiter**.

   Tabelle 4-25 enthält die Felder und zugehörigen Beschreibungen, die im **Zertifikat-**Fenster aufgeführt werden.

2. Klicken Sie auf die entsprechende Seitenschaltfläche **Server-Zertifikat ansehen**, um fortzufahren. Siehe Tabelle 4-26.

Tabelle 4-25. Zertifikat-Informationen

Feld	Beschreibung
Seriennummer	Zertifikatseriennummer
Subjektinformationen	Vom Antragsteller eingegebene Zertifikat-Attribute
Aussteller-Informationen	Zertifikatattribute vom Aussteller zurückgesendet
Gültig von	Ausgabedatum des Zertifikats
Gültig bis	Ablaufdatum des Zertifikats

Tabelle 4-26. Schaltflächen der Seite Serverzertifikat anzeigen

Schaltfläche	Beschreibung
Drucken	Seite **Ansicht-Serverzertifikat** drucken.
Zurück zum SSL Hauptmenü	Zurück zur Seite **SSL-Hauptmenü**.

Seriellen und Terminal-Modus konfigurieren

IPMI und serielles RAC konfigurieren

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.

2. Klicken Sie auf das Register **Konfiguration** und dann auf **Seriell**.

3. Konfigurieren Sie die seriellen IPMI-Einstellungen.

Tabelle 4-27 enthält Informationen über die seriellen IPMI-Einstellungen.

4. Konfigurieren Sie die seriellen RAC-Einstellungen.

   Tabelle 4-28 enthält Informationen über die seriellen RAC-Einstellungen.

5. Klicken Sie auf **Änderungen anwenden**.

6. Klicken Sie auf die entsprechende Seitenschaltfläche von **Serielle Konfiguration**, um fortzufahren. Siehe Tabelle 4-29.

Tabelle 4-27. Serielle IPMI-Einstellungen

Einstellung	Beschreibung
Verbindungsmoduseinstellung	ı Direktverbindung - grundlegender Modus - serieller IPMI-grundlegender Modus ı Direktverbindung Terminalmodus - serieller IPMI-Terminalmodus
Baudrate	Setzt die Datengeschwindigkeit. Wählen Sie **9600 Bit/s**, **19,2 kBit/s**, **57,6 kBit/s** oder **115,2 kBit/s**.
Ablaufsteuerung	ı Keine - Hardware-Ablaufsteuerung Aus ı RTS/CTS - Hardware-Ablaufsteuerung Ein
Beschränkung der Channel-Berechtigungsebene	ı Administrator ı Operator ı Benutzer

Tabelle 4-28. Serielle RAC-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert die serielle RAC-Konsole. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Maximale Sitzungen	Die maximale Anzahl von gleichzeitigen Sitzungen, die für dieses System zulässig sind.
Zeitüberschreitung	Die maximale Sekundenzahl der Bereitschaftszeit, bevor die Leitung getrennt wird. Der Bereich ist 60 bis 1920 Sekunden. Die Standardeinstellung ist 300 Sekunden. Verwenden Sie 0 Sekunden, um die Zeitüberschreitungsfunktion zu deaktivieren.
Umleitung aktiviert	Aktiviert oder deaktiviert die Konsolenumleitung. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Baudrate	Die Datengeschwindigkeit auf der externen seriellen Schnittstelle. Werte sind **9600 Bit/s**, **28,8 kBit/s**, **57,6 kBit/s** und **115,2 k Bit/s**. Die Standardeinstellung ist **57,6 kbps**.
Escape-Taste	Gibt die <Esc> Taste an. Die Standardeinstellung sind die ^ \ Zeichen.
Größe Verlaufspuffer	Die Größe des seriellen Verlaufspuffers, der die letzten zur Konsole geschriebenen Zeichen hält. Maximum und Standard = 8192 Zeichen.
Anmeldungsbefehl	Die auf die gültige Anmeldung auszuführende DRAC-Befehlszeile.

Tabelle 4-29. Serielle Konfigurationsseiteneinstellungen

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Serielle Konfiguration**.
Aktualisieren	Die Seite **Serielle Konfiguration** aktualisieren.
Änderungen anwenden	Die IPMI und seriellen RAC-Änderungen anwenden.
Terminalmoduseinstellungen	Öffnet die Seite **Terminalmodus-Einstellungen**.

Terminalmodus konfigurieren

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.

2. Klicken Sie auf das Register **Konfiguration** und dann auf **Seriell**.

3. Auf der Seite **Serielle Konfiguration** klicken Sie auf **Terminalmodus-Einstellungen**.

4. Seite Terminalmodus-Einstellungen konfigurieren.

   Tabelle 4-30 enthält Informationen über die Terminalmodus-Einstellungen.

5. Klicken Sie auf **Änderungen anwenden**.

6. Klicken Sie auf die entsprechende **Endmoduseinstellungen-Seitenschaltfläche**, um fortzufahren. Siehe Tabelle 4-31.

Tabelle 4-30. Terminalmodus-Einstellungen

Einstellung	Beschreibung
Zeilenbearbeitung	Aktiviert oder deaktiviert die Zeilenbearbeitung.
Löschsteuerung	Wählen Sie eine der folgenden Optionen: • **BMC gibt ein <bksp><sp><bksp> Zeichen aus, wenn <bksp> oder <del> empfangen wird**- • **BMC gibt ein <del> Zeichen aus, wenn <bksp> oder <del> empfangen wird** --
Echo-Steuerung	Aktiviert oder deaktiviert Echo.
Handshaking-Steuerung	Aktiviert oder deaktiviert Handshaking.
Neue Zeilenreihenfolge	**Keine**, **<CR-LF>**, **<NULL>**, **<CR>**, **<LF-CR>** oder **<LF>** wählen.
Neue Zeilenreihenfolge eingeben	**<CR>** oder **<NULL>** auswählen.

Tabelle 4-31. Schaltflächen der Terminalmoduseinstellungsseiten

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Terminalmodus-Einstellungen**.
Aktualisieren	Aktualisiert die Seite **Terminalmodus-Einstellungen**.
Zurück zur Konfiguration der seriellen Schnittstelle	Zur Seite **Konfiguration der seriellen Schnittstelle** zurückkehren.
Änderungen anwenden	Terminalmoduseinstellungsänderungen anwenden.

Seriell über LAN konfigurieren

ANMERKUNG: Vollständige Informationen über Seriell über LAN finden Sie im *Dell OpenManage Baseboard-Verwaltungs-Controller Benutzerhandbuch*.

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** und dann auf **Seriell über LAN**.
3. Seriell über LAN-Einstellungen konfigurieren.

   Tabelle 4-32 enthält Informationen über die Einstellung der Seite **Seriell über LAN-Konfiguration**.
4. Klicken Sie auf **Änderungen anwenden**.
5. Konfigurieren Sie die erweiterten Einstellungen, falls erforderlich. Ansonsten klicken Sie auf die entsprechende Schaltfläche **Seriell über LAN-Konfiguration**, um fortzufahren (siehe Tabelle 4-33).

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

   a. Klicken Sie auf **Erweiterte Einstellungen**.

   b. Konfigurieren Sie auf der Seite **Seriell über LAN-Konfiguration** - **Erweiterte Einstellungen** die erweiterten Einstellungen nach Bedarf. Siehe Tabelle 4-34.

   c. Klicken Sie auf **Änderungen anwenden**.

   d. Klicken Sie auf die entsprechende Seitenschaltfläche für **Seriell über LAN-Konfiguration - erweiterte Einstellungen**, um fortzufahren. Siehe Tabelle 4-35.

Tabelle 4-32. Seriell über LAN-Konfigurationsseiteneinstellungen

Einstellung	Beschreibung
Seriell über LAN aktivieren	Aktiviert Seriell über LAN. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Baudrate	Die IPMI-Datengeschwindigkeit. Wählen Sie **9600 Bit/s**, **19,2 kBit/s**, **57,6 kBit/s** oder **115,2 kBit/s**.
Beschränkung der Channel-Berechtigungsebene	Stellt die IPMI Seriell über LAN-Mindestbenutzerberechtigung ein: **Administrator**, **Operator** oder **Benutzer**.

Tabelle 4-33. Schaltflächen der Seriell über LAN-Konfigurationsseiten

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Seriell über LAN - Konfiguration**.
Aktualisieren	Aktualisiert die Seite **Seriell über LAN - Konfiguration**.
Erweiterte Einstellungen	Öffnet die Seite **Seriell über LAN Konfiguration - erweiterte Einstellungen**.
Änderungen anwenden	Wendet die Seiteneinstellungen für **Seriell über LAN - Konfiguration** an.

Tabelle 4-34. Einstellungen der Seite Seriell über LAN Konfiguration - erweiterte Einstellungen

Einstellung	Beschreibung
Intervall der Zeichenakkumulation	Die Zeitspanne, die der BMC vor dem Übertragen eines teilweisen SOL Zeichen-Datenpakets wartet. 1-basierte 5-ms-Schritte.
Schwellenwert der gesendeten Zeichen	Der BMC sendet ein SOL Zeichen-Datenpaket mit den Zeichen, sobald diese Anzahl von Zeichen (oder mehr) akzeptiert worden ist. 1-basierte Einheiten.

Tabelle 4-35. Seriell über LAN-Konfiguration - erweiterte Einstellung-Seitenschaltflächen

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Seriell über LAN - Konfiguration - erweiterte Einstellungen**.
Aktualisieren	Aktualisiert die Seite **Seriell über LAN - Konfiguration - erweiterte Einstellungen**.
Zurück zur Seite Seriell über LAN - Konfiguration	Rückkehr zur Seite **Seriell über LAN - Konfiguration**.
Änderungen anwenden	Wendet die Seiteneinstellungen für **Seriell über LAN - Konfiguration - erweiterte Einstellungen** an.

Dienste konfigurieren

ANMERKUNG: Zur Änderung dieser Einstellungen müssen Sie die Berechtigung **DRAC 5 konfigurieren** haben. Zusätzlich kann das Remote-RACADM Befehlszeilendienstprogramm nur aktiviert werden, wenn der Benutzer als **root** angemeldet wird.

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** und dann auf **Dienste**.
3. Konfigurieren Sie die folgenden Dienstleistungen nach Bedarf:
   - Web Server (Tabelle 4-36)
   - SSH (Tabelle 4-37)
   - Telnet (Tabelle 4-38)
   - Remote-RACADM (Tabelle 4-39)
   - SNMP-Agent (Tabelle 4-40)
   - Automatisierter Systemwiederherstellungsagent (Tabelle 4-41)

   Verwenden Sie den **Automatisierten Systemwiederherstellungsagent**, um die Funktion **Bildschirm Letzter Absturz** des DRAC 5 zu aktivieren.

   ANMERKUNG: Server Administrator muss mit der Funktion **Autom. Wiederherstellung** installiert werden, die durch Einstellen der **Maßnahme** auf entweder: **System neu starten**, **System ausschalten** oder **System aus- und einschalten** aktiviert wird, so dass **Bildschirm Letzter Absturz** im DRAC 5 funktioniert.
4. Klicken Sie auf **Änderungen anwenden**.
5. Klicken Sie auf die entsprechende Seitenschaltfläche **Dienste**, um fortzufahren. Siehe Tabelle 4-42.

Tabelle 4-36. Webservereinstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert den Webserver. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Max. Sitzungen	Die maximale Anzahl von gleichzeitigen Sitzungen, die für dieses System zulässig sind.
Aktive Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich **Max. Sitzungen**.
Zeitüberschreitung	Die Zeit in Sekunden, die eine Verbindung inaktiv bleiben darf. Die Sitzung wird abgebrochen, wenn das Zeitlimit erreicht wird. Änderungen an der Zeitlimiteinstellung haben keine Auswirkung auf die aktuelle Sitzung. Wenn Sie die Zeitlimiteinstellung ändern, müssen Sie sich abmelden und wieder anmelden, um die neue Einstellung wirksam zu machen. Der Zeitüberschreitungsbereich ist 60 bis 1920 Sekunden.

HTTP-Schnittstellennummer	Die vom DRAC verwendete Schnittstelle, die auf eine Server-Verbindung hört. Die Standardeinstellung ist **80**.
HTTPS-Schnittstellennummer	Die vom DRAC verwendete Schnittstelle, die auf eine Server-Verbindung hört. Die Standardeinstellung ist **443**.

Tabelle 4-37. SSH-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert SSH. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Max. Sitzungen	Die maximale Anzahl von gleichzeitigen Sitzungen, die für dieses System zulässig sind. Bis zu vier Sitzungen werden unterstützt.
Aktive Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich **Max. Sitzungen**.
Zeitüberschreitung	Secure Shell Inaktivitäts-Zeitlimit, in Sekunden. Bereich = 60 bis 1920 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitlimitfunktion zu deaktivieren. Die Standardeinstellung ist 300.
Schnittstellennummer	Die vom DRAC verwendete Schnittstelle, die auf eine Server-Verbindung hört. Die Standardeinstellung ist 22.

Tabelle 4-38. Telnet-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert Telnet. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Max. Sitzungen	Die maximale Anzahl von gleichzeitigen Sitzungen, die für dieses System zulässig sind. Bis zu vier Sitzungen werden unterstützt.
Aktive Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich **Max. Sitzungen**.
Zeitüberschreitung	Secure Shell Inaktivitäts-Zeitlimit, in Sekunden. Bereich = 60 bis 1920 Sekunden. Geben Sie 0 Sekunden ein, um die Zeitlimitfunktion zu deaktivieren. Die Standardeinstellung ist 0.
Schnittstellennummer	Die vom DRAC verwendete Schnittstelle, die auf eine Server-Verbindung hört. Die Standardeinstellung ist 23.

Tabelle 4-39. Remote-RACADM- Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert Remote-RACADM. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Max. Sitzungen	Die maximale Anzahl von gleichzeitigen Sitzungen, die für dieses System zulässig sind. Bis zu vier Sitzungen werden unterstützt.
Aktive Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich **Max. Sitzungen**.

Tabelle 4-40. SNMP-Agent-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert den Agent. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Community-Name	Der Name der Community, die die IP-Adresse für das SNMP-Warnungsziel enthält. Der Community-Name kann bis zu 31 Zeichen (keine Leerzeichen) lang sein. Die Standardeinstellung ist **public**.

Tabelle 4-41. Automatisierte Systemwiederherstellungsagenteinstellung

Einstellung	Beschreibung
Aktiviert	Aktiviert den Automatisierten Systemwiederherstellungsagenten.

Tabelle 4-42. Schaltflächen der Dienstleistungsseite

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

Häufig gestellte Fragen

Tabelle 4-43 listet häufig gestellte Fragen und Antworten auf.

Tabelle 4-43. Remote-System verwalten und wiederherstellen: Häufig gestellte Fragen

Frage	Antwort
Wenn ich auf die webbasierte DRAC 5 Schnittstelle zugreife, bekomme ich eine Sicherheitswarnung, die besagt, dass der Hostname des SSL-Zertifikats nicht mit dem Hostnamen des DRAC 5 übereinstimmt.	Der DRAC 5 enthält ein Standard-DRAC 5 Server-Zertifikat zur Sicherung der Netzwerksicherheit für die webbasierte Schnittstelle und die Remote-RACADM-Funktionen. Wenn dieses Zertifikat verwendet wird, zeigt der Internetbrowser eine Sicherheitswarnung an, weil das Standardzertifikat an das **DRAC5 Standardzertifikat** ausgegeben wird, was nicht dem Hostnamen des DRAC 5 (Beispiel IP-Adresse) entspricht. Um dieses Sicherheitsbedenken anzusprechen, laden Sie ein DRAC 5-Serverzertifikat zur IP-Adresse des DRAC 5 hoch. Wenn Sie die Zertifikatssignierungsanforderung (CSR) zur Ausgabe des Zertifikats erstellen, stellen Sie sicher, dass der allgemeine Name (CN) des CSR der IP-Adresse des DRAC 5 (Beispiel: 192.168.0.120) oder dem eingetragenen DNS-DRAC-Namen entspricht. Um sicherzustellen, dass der CSR dem eingetragenen DNS-DRAC-Namen entspricht, führen Sie die folgenden Schritte aus: 1. In der **System-**Struktur klicken Sie auf **Remote-Zugriff**. 2. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**. 3. Führen Sie auf der Seite **Netzwerk-Einstellungen** die folgenden Schritte aus: a. Wählen Sie das Kontrollkästchen **DRAC auf DNS registrieren**. b. Geben Sie den DRAC-Namen in das Feld **DNS DRAC-Name** ein. 4. Klicken Sie auf **Änderungen anwenden**. Weitere Informationen über das Erstellen von CSRs und die Ausgabe von Zertifikaten finden Sie in "DRAC 5-Kommunikationen mit SSL und digitalen Zertifikaten sichern".
Warum sind der remote racadm und webbasierte Services nach einer Eigenschaftenänderung nicht verfügbar?	Es kann etwa eine Minute dauern, bis die Remote-RACADM-Services und die webbasierte Schnittstelle nach einem Reset des DRAC 5 Web Server wieder verfügbar sind Der DRAC 5 Web Server führt nach den folgenden Ereignissen einen Reset durch: - Wenn die Netzwerkkonfiguration oder Netzwerksicherheitseigenschaften mittels der DRAC 5 Internet-Benutzeroberfläche geändert werden - Wenn die Eigenschaft **cfgRacTuneHttpsPort** geändert wird (einschließlich wenn eine config -f <Konfigurations*datei*> sie ändert) - Wenn **racresetcfg** verwendet wird - Wenn der DRAC 5 einen Reset durchführt - Wenn ein neues SSL Server-Zertifikat hochgeladen wird
Warum registriert mein DNS-Server meinen DRAC 5 nicht?	Einige DNS-Server registrieren nur Namen von 31 Zeichen oder weniger.
Wenn ich auf die DRAC 5 webbasierte Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die aussagt, dass das SSL-Zertifikats durch eine nicht zuverlässige Zertifizierungsstelle (CA) ausgegeben wurde.	DRAC 5 schließt ein Standard-DRAC 5-Serverzertifikat ein, um Netzwerksicherheit für die webbasierte Schnittstelle und Remote-racadm-Funktionen sicherzustellen. Dieses Zertifikat wurde durch eine nicht zuverlässige CA ausgegeben. Um dieses Sicherheitsbedenken anzusprechen, laden Sie ein von einer zuverlässigen CA (z. B. Thawte oder Verisign) ausgegebenes DRAC 5-Serverzertifikat hoch. Weitere Informationen über die Ausgabe von Zertifikaten finden Sie in "DRAC 5-Kommunikationen mit SSL und digitalen Zertifikaten sichern".

Die folgende Meldung wird aus unbekannten Gründen angezeigt:
 	
`Remote Access: SNMP Authentication Failure`
 	
`(Remote-Zugriff: SNMP-Authentifizierungsfehler)`
 	
Warum geschieht dies?
	Als Teil der Ermittlung versucht IT Assistant, die Get- und Set-Community-Namen zu überprüfen. Im IT Assistant ist der Get-**Community-Name = public** und der Set-**Community-Name = private.** Standardmäßig ist der Community-Name für den DRAC 5-Agenten "public". Wenn IT Assistant eine Set-Aufforderung aussendet, erstellt der DRAC 5-Agent den SNMP-Authentifizierungsfehler, weil er nur Aufforderungen von **Community = public** annimmt.
	
	Sie können den DRAC 5 Community-Namen mit RACADM ändern.
	
	Um den DRAC 5 Community-Namen zu sehen, verwenden Sie den folgenden Befehl:
	
	`racadm getconfig -g cfgOobSnmp`
	
	Um den DRAC 5 Community-Name einzustellen, verwenden Sie den folgenden Befehl:
	
	`racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <Community-Name>`
	
	Um SNMP-Authentifizierungs-Traps daran zu hindern erstellt zu werden, müssen Sie Community-Namen eingeben, die vom Agenten akzeptiert werden. Da der DRAC 5 nur einen Community-Namen zulässt, müssen Sie den gleichen **Get** und **Set** Community-Namen für das IT Assistant-Ermittlungs-Setup eingeben.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Wiederherstellung und Fehlerbehebung am verwalteten System

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Dieser Abschnitt erklärt, wie man Aufgaben, die in Beziehung mit Wiederherstellung und Störungen beheben in einem abgestürzten System mit Hilfe des DRAC 5 webbasierten Interface ausführt. Informationen über die Fehlerbehebung Ihres DRAC 5 finden Sie in "Betriebssystem mit VM-CLI bereitstellen".

- Fehlerbehebung an einem Remote-System
- Netzstrom auf einem Remote-System verwalten
- Systemereignisprotokoll (SEL) verwenden
- Bildschirm Letzter Systemabsturz anzeigen
- RAC-Protokoll verwenden
- Diagnosekonsole verwenden

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

Die folgenden Fragen werden im Allgemeinen für Probleme auf höchster Ebene beim Beheben von Störungen im verwalteten System verwendet:

1. Ist das System ein- oder ausgeschaltet?
2. Wenn eingeschaltet, funktioniert das System, ist es abgestürzt oder nur blockiert?
3. Wenn ausgeschaltet, wurde der Strom unerwartet ausgeschaltet?

Für abgestürzte Systeme können Sie den Bildschirm Letzter Absturz überprüfen (siehe "Anzeige des Bildschirms Letzter Systemabsturz") und Konsolenumleitung verwenden ("Unterstützte Bildschirmauflösungs-Bildwiederholfrequenzen auf dem verwalteten System") und Remote-Stromverwaltung (siehe "Netzstrom auf einem Remote-System verwalten"), um das System neu zu starten und den Neustartvorgang zu beobachten.

Netzstrom auf einem Remote-System verwalten

Der DRAC 5 ermöglicht, dass Sie im Remote-Zugriff mehrere Netzstromverwaltungsmaßnahmen auf dem verwalteten System ausführen können, so dass Sie nach einem Systemausfall oder anderen Systemereignis wiederherstellen können.

Die Seite **Stromverwaltung** wird für folgende Aktivitäten verwendet:

- Durchführung eines ordnungsgemäßen Herunterfahrens seitens des Betriebssystems beim Neustart und Ein- oder Ausschalten des Systems.
- Aktuellen **Stromstatus** des Systems ansehen - entweder **EIN** oder **AUS**.

Zum Zugriff auf die Seite **Stromverwaltung** von der **System**struktur klicken Sie auf **System** und dann auf das Register **Stromverwaltung**.

ANMERKUNG: Sie müssen die **Berechtigung Server-Maßnahmenbefehle ausführen** besitzen, um Stromverwaltungsmaßnahmen auszuführen.

Stromregelungsmaßnahmen auswählen

1. Wählen Sie eine der folgenden **Stromsteuerungsmaßnahmen** aus.
   - **System einschalten**- Schaltet den Systemstrom ein (entspricht dem Drücken des Netzschalters, wenn der Systemstrom ausgeschaltet ist).
   - **System ausschalten** - Schaltet den Systemnetzstrom aus und schaltet ihn wieder ein (entspricht dem Drücken der Reset-Schaltfläche wenn das System eingeschaltet ist).
   - **System zurücksetzen** - Führt einen Reset des Systems (entspricht dem Drücken der Reset-Schaltfläche) aus; der Netzstrom wird nicht ausgeschaltet, wenn diese Funktion verwendet wird.
   - **System aus- und einschalten** - Schaltet das System aus und startet es dann neu (Hardwareneustart).

2. Klicken Sie auf **Anwenden,** um die Stromverwaltungsmaßnahme (z. B. das System zum ein- und ausschalten zu veranlassen) ausführen.

3. Klicken Sie auf die Schaltfläche der entsprechenden Seite **Stromverwaltung**, um fortzufahren (siehe Tabelle 5-1).

Tabelle 5-1. Schaltflächen der Seite Stromverwaltung (oben rechts)

Schaltfläche	Maßnahme
Drucken	Druckt die Seite **Stromverwaltung**
Aktualisieren	Lädt die Seite **Stromverwaltung** neu

Systeminformationen anzeigen

Die Seite **Systemzusammenfassung** enthält Informationen über die folgenden Systemkomponenten:

- Hauptsystemgehäuse
- Remote Access Controller
- Baseboard-Verwaltungs-Controller

Um auf die Systeminformationen zuzugreifen, erweitern Sie die **System**struktur und klicken Sie auf **Eigenschaften**.

Hauptsystemgehäuse

Tabelle 5-2 und Tabelle 5-3 beschreiben die Hauptsystemgehäuseeigenschaften.

ANMERKUNG: Um Informationen zu **Hostname** und **BS-Name** zu erhalten, müssen DRAC 5-Dienste auf dem verwalteten System installiert sein.

Tabelle 5-2. Systeminformationsfelder

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

Tabelle 5-3. Autom. Wiederherstellungsfelder

Feld	Beschreibung
Wiederherstellungsmaßnahme	Wenn ein "hängendes System" festgestellt wird, kann der DRAC auf eine der folgenden Maßnahmen eingestellt werden: Keine Maßnahme, Hardware-Reset, Herunterfahren oder Aus- und Einschalten.
Anfänglicher Countdown	Die Anzahl von Sekunden nach der Feststellung eines "hängenden Systems", bis der DRAC eine Wiederherstellungsmaßnahme ausführt.
Vorhandener Countdown	Der aktuelle Wert, in Sekunden, des Countdown-Zeitgebers.

Remote Access Controller

Tabelle 5-4 beschreibt die Eigenschaften des Remote Access Controllers.

Tabelle 5-4. RAC-Informationsfelder

Feld	Beschreibung
Name	Kurzer Name.
Produktinformationen	Ausführlicher Name.
Hardware-Version	Version der Remote Access Controller-Karte oder "unbekannt".
Firmware-Version	Aktuelle DRAC 5 Firmware-Versionsstufe.
Aktualisierte Firmware	Datum und Uhrzeit, zu dem/der die Firmware zuletzt aktualisiert wurde.

RAC-Zeit	Systemzeiteinstellung.

Baseboard-Verwaltungs-Controller

Tabelle 5-5 beschreibt die Eigenschaften des Baseboard-Verwaltungs-Controllers.

Tabelle 5-5. BMC-Informationsfelder

Feld	Beschreibung
Name	"Baseboard-Management Controller".
IPMI-Version	Intelligente Plattformverwaltungsschnittstelle (IPMI) Version.
Anzahl von möglichen aktiven Sitzungen	Die maximale Anzahl an Sitzungen, die zur gleichen Zeit aktiv sein können.
Anzahl von aktuellen aktiven Sitzungen	Gesamtanzahl von aktuellen aktiven Sitzungen.
Firmware-Version	Version der BMC-Firmware.
LAN aktiviert	LAN aktiviert oder LAN deaktiviert.

Systemereignisprotokoll (SEL) verwenden

Auf der Seite **SEL-Protokoll** werden systemkritische Ereignisse angezeigt, die auf dem verwalteten System auftreten.

Um das Systemereignisprotokoll anzusehen, führen Sie die folgenden Schritte aus:

1. In der **System**struktur klicken Sie auf **System**.
2. Klicken Sie auf das Register **Protokolle** und dann auf **Systemereignisprotokoll**.

   Auf der Seite **Systemereignisprotokoll** werden der Ereignisschweregrad und weitere Informationen angezeigt, siehe Tabelle 5-6.
3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Systemereignisprotokoll**, um fortzufahren (siehe Tabelle 5-7).

Tabelle 5-6. Statusanzeigesymbole

Symbol/Kategorie	Beschreibung
	Eine grüne Markierung zeigt eine gesunde (normale) Status-Bedingung an.
	Ein gelbes Dreieck, das ein Ausrufezeichen enthält, zeigt eine Warnungs (nichtkritische) -Status-Bedingung an.
	Ein rotes X zeigt eine kritische (Misserfolg) Status-Bedingung an.
	Ein Fragezeichen-Symbol zeigt an, dass der Status unbekannt ist.
Datum/-uhrzeit	Datum und Uhrzeit des Ereigniseintritts. Wenn das Datumsfeld leer ist, dann trat das Ereignis am Systemstart auf. Das Format ist mm/tt/jjjj hh:mm:ss, basierend auf 24 Stunden-Zeit.
Beschreibung	Eine kurze Beschreibung des Ereignisses

Tabelle 5-7. SEL-Seitenschaltflächen

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

Bildschirm Letzter Systemabsturz anzeigen

HINWEIS: Die Funktion Bildschirm Letzter Absturz erfordert, dass das verwalteten System mit der Funktion **Autom. Wiederherstellung** im Server Administrator konfiguriert wird. Stellen Sie außerdem sicher, dass die Funktion **Automatisierte Systemwiederherstellung** mittels DRAC aktiviert wird. Wechseln Sie zur Seite **Dienstleistungen** im Register **Konfiguration** im Abschnitt **Remote-Zugriff**, um diese Funktion zu aktivieren.

Auf der Seite **Bildschirm Letzter Absturz** wird der letzte Absturzbildschirm mit Informationen über die Ereignisse vor dem Systemausfall angezeigt. Die letzten Systemausfallinformationen werden im DRAC 5-Speicher gespeichert und sind im Remote-Zugriff zugänglich.

Zur Ansicht der Seite **Bildschirm Letzter Absturz** führen Sie die folgenden Schritte aus:

1. In der **System**struktur klicken Sie auf **System**.
2. Klicken Sie auf das Register **Protokolle** und dann auf **Letzter Absturz**.

Die Seite **Bildschirm Letzter Absturz** enthält die folgenden Schaltflächen (siehe Tabelle 5-8) in der rechten oberen Ecke des Bildschirms:

Tabelle 5-8. Schaltflächen des Bildschirms Letzter Absturz

Schaltfläche	Maßnahme
Drucken	Druckt die Seite **Bildschirm Letzter Absturz.**
Speichern	Öffnet ein Pop-Up-Fenster, das Ihnen ermöglicht, den Bildschirm Letzter Absturz zu einem Verzeichnis Ihrer Wahl zu speichern.
Löschen	Löscht die Seite **Bildschirm Letzter Absturz.**
Aktualisieren	Lädt die Seite **Bildschirm Letzter Absturz** hoch.

ANMERKUNG: Aufgrund von Schwankungen im Zeitgeber für Autom. Wiederherstellung kann der **Bildschirm Letzter Absturz** nicht erfasst werden, wenn der System-Reset-Zeitgeber auf weniger als 30 Sekunden eingestellt wird. Stellen Sie den System-Reset-Zeitgeber mit dem Server Administrator oder IT Assistant auf mindestens 30 Sekunden ein und vergewissern Sie sich, dass der **Bildschirm Letzter Absturz** ordnungsgemäß arbeitet. Weitere Informationen erhalten Sie unter "Konfigurieren des verwalteten Systems, um den Bildschirm Letzter Absturz zu erfassen".

RAC-Protokoll verwenden

Das **RAC-Protokoll** ist ein beständiges Protokoll, das in der DRAC 5-Firmware geführt wird. Das Protokoll enthält eine Liste von Benutzermaßnahmen (An- und Abmelden, Änderungen der Sicherheitsregeln) und Warnungen, die vom DRAC 5 ausgegeben werden. Die ältesten Einträge werden überschrieben, wenn das Protokoll voll wird.

Um auf das RAC-Protokoll zuzugreifen, führen Sie die folgenden Schritte aus:

1. In **System**struktur klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Protokolle** und dann auf **RAC-Protokolle**.

Das **RAC-Protokoll** enthält die in Tabelle 5-9 aufgeführten Informationen.

Tabelle 5-9. Informationen der RAC-Protokollseite

Feld	Beschreibung
Datum/-uhrzeit	Datum und Uhrzeit (z. B. 19. Dez. 16:55:47). Wenn der DRAC 5 startet nicht mit dem verwalteten System kommunizieren kann, wird die Zeit als System-Start angezeigt.
Quelle	Die Schnittstelle, die das Ereignis verursachte.
Beschreibung	Eine kurze Beschreibung des Ereignisses und des Namens des Benutzers, der am DRAC 5 angemeldet war.

Verwendung der Seitenschaltflächen des RAC-Protokolls

Die Seite **RAC-Protokoll** enthält die folgenden Schaltflächen (siehe Tabelle 10-5).

Tabelle 10-5. Schaltflächen des RAC-Protokolls

Schaltfläche	Maßnahme
Drucken	Druckt die Seite **RAC-Protokoll** aus.
Protokoll löschen	Löscht die **RAC-Protokoll**-Einträge.

	ANMERKUNG: Die Schaltfläche **Protokoll löschen** erscheint nur, wenn Sie die Berechtigung **Protokolle löschen** besitzen.
Speichern unter	Öffnet ein Popup-Fenster, das Ihnen ermöglicht, das **RAC-Protokoll** in einem Verzeichnis Ihrer Wahl zu speichern. **ANMERKUNG:** Wenn Sie Internet Explorer verwenden und beim Speichern auf ein Problem stoßen, laden Sie die kumulative Sicherheitsaktualisierung für Internet Explorer herunter, die auf der Support-Website von Microsoft unter support.microsoft.com verfügbar ist.
Aktualisieren	Lädt die Seite **RAC-Protokoll** neu.

Diagnosekonsole verwenden

Der DRAC 5 enthält einen Standardsatz von Netzwerkdiagnosehilfsprogrammen (siehe Tabelle 5-11) die den mit Microsoft® Windows®- oder Linux-basierten Systemen gelieferten Hilfsprogrammen ähnlich sind. Mit der webbasierten DRAC 5-Schnittstelle können Sie auf die Hilfsprogramme zum Netzwerk-Debuggen zugreifen.

Zum Zugriff auf die Seite **Diagnosekonsole** führen Sie die folgenden Schritte aus:

1. In **System**struktur klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das **Diagnose**-Register.

Tabelle 5-11 beschreibt die Optionen, die auf der Seite **Diagnosekonsole** verfügbar sind. Geben Sie einen Befehl ein und klicken Sie auf **Senden**. Die Debug-Ergebnisse werden auf der Seite **Diagnosekonsole** angezeigt.

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

Tabelle 5-11. 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 Routing-Tabelle. Wenn die optionale Schnittstellenzahl im Textfeld rechts von der Option **netstat** angegeben wird, dann druckt NetStat zusätzliche Informationen bezüglich des Verkehrs durch die Schnittstelle, Puffergebrauch, und anderen Netzwerkschnittstelleninformationen.
ping *<IP-Adresse>*	Prüft nach, dass das Ziel-IP-Adresse vom DRAC 5 mit dem aktuellen Routing-Tabelleninhalt erreichbar ist. Ein Ziel-IP-Adresse muss im Feld rechts von dieser Option eingegeben werden. Ein ICMP- (Internetsteuerungsmeldungsprotokoll) Echo-Paket wird zur Ziel-IP-Adresse basierend auf dem aktuellen Inhalt der Routing-Tabelle gesendet.
gettracelog	Zeigt das DRAC 5-Ablaufverfolgungsprotokoll. Weitere Informationen erhalten Sie in "gettracelog".

Fehlerbeseitigungsnetzwerkprobleme

Das interne DRAC 5-Ablaufverfolgungsprotokoll wird von Administratoren verwendet, um den DRAC 5-Alarm oder den Netzwerkbetrieb zu debuggen. Sie können von der webbasierten DRAC 5-Schnittstelle auf das Ablaufverfolgungsprotokoll zugreifen, indem Sie auf das Register **Diagnose** klicken und den Befehl **gettracelog** oder den Befehl **racadm gettracelog** eingeben. Weitere Informationen erhalten Sie in "gettracelog".

Das Ablaufverfolgungsprotokoll verfolgt die folgenden Informationen:

- DHCP - Verfolgt Pakete, die an einen DHCP-Server gesendet und von ihm empfangen werden.
- IP - Verfolgt gesendete und empfangene IP Pakete.

Das Ablaufverfolgungsprotokoll kann auch DRAC 5 Firmware-spezifische Fehlerkontrollen enthalten, die mit der internen DRAC 5-Firmware, nicht mit dem Betriebssystem des verwalteten Systems verbunden sind.

ANMERKUNG: Der DRAC 5 gibt kein Echo eines ICMP (Ping) mit einer Paketgröße über 1500 Bytes zurück.

Probleme mit der Warnung bei Störungen beheben

Zur Fehlerbehebung eines bestimmten Typs von DRAC 5-Warnungen verwenden Sie protokollierte SNMP-Trap-Informationen. SNMP-Trap-Übergaben werden im Ablaufverfolgungsprotokoll standardmäßig protokolliert Da SNMP jedoch die Übergabe von Traps nicht bestätigt, ist es am besten, die Pakete auf dem verwalteten System mit Hilfe eines Netzwerkanalysators oder eines Hilfsprogramms wie **snmputil** von Microsoft zu verfolgen.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5 mit Microsoft Active Directory verwenden

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Ein Verzeichnisdienst wird verwendet, um eine allgemeine Datenbank aller Informationen aufrechtzuerhalten, die erforderlich sind, um Benutzer, Computer, Drucker etc. auf einem Netzwerk zu kontrollieren. Wenn Ihre Firma die Microsoft® Active Directory® Service-Software verwendet, kann diese dahingehend konfiguriert werden, dass Sie Zugang zum DRAC 5 erhalten, wodurch Sie bestehenden Benutzern in der Active Directory-Software DRAC 5-Benutzerberechtigungen zuteilen und diese regeln können

ANMERKUNG: Die Verwendung von Active Directory zur Anerkennung von DRAC 5-Benutzern wird auf den Microsoft Windows® 2000- und Windows-Server® 2003-Betriebssystemen unterstützt.

Sie können Active Directory verwenden, um Benutzerzugang auf DRAC 5 durch zwei Methoden zu definieren: Sie können die Lösung des erweiterten Schemas verwenden, die Dell-definierte Active Directory-Objekte verwendet, oder eine Standardschema-Lösung, die nur Active Directory-Gruppenobjekte verwendet.

Vorteile und Nachteile des Erweiterten Schemas und Standardschemas

Wenn Sie Active Directory verwenden, um den Zugang zum DRAC 5 zu konfigurieren, müssen Sie entweder das erweiterte Schema oder die Standardschema-Lösung wählen.

Die Vorteile, die Lösung des erweiterten Schemas zu verwenden, sind:

- Alle Access Control-Objekte werden in Active Directory aufrechterhalten.
- Maximale Flexibilität bei der Konfiguration des Benutzerzugriffs auf verschiedene DRAC 5-Karten mit verschiedenen Berechtigungsebenen.

Die Vorteile, die Standardschema-Lösung zu verwenden, sind:

- Es ist keine Schema-Erweiterung erforderlich, weil das Standardschema nur Active Directory-Objekte verwendet.
- Die Konfiguration auf der Active Directory-Seite ist einfach.

Übersicht über Erweitertes Schema von Active Directory

Es gibt zwei Wege, Erweitertes Schema von Active Directory zu aktivieren:

- Mit der webbasierten DRAC 5-Benutzerschnittstelle. Siehe "DRAC 5 mit dem Erweiterten Schema von Active Directory und webbasierter Schnittstelle konfigurieren".
- Mit dem RACADM CLI-Hilfsprogramm. Siehe "DRAC 5 mit dem Erweiterten Schema von Active Directory und RACADM konfigurieren".

Active Directory-Schema-Verlängerungen

Die Active Directory-Daten sind eine dezentrale Datenbank von Attributen und Klassen. Das Active Directory-Schema enthält die Regeln, die den Typ der Daten bestimmen, die hinzugefügt oder in die Datenbank 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 einzigartigen Attribute und Klassen hinzufügen, um Umgebungsspezifische Bedürfnisse zu lösen. Dell hat das Schema erweitert, um die erforderlichen Änderungen zur Unterstützung der Remote-Verwaltungsauthentifizierung und Autorisierung einzuschließen.

Jede(s) Attribut oder Klasse, das/die einem existierenden Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert werden. Um einzigartige IDs innerhalb der Industrie aufrechtzuerhalten, erhält Microsoft eine Datenbank von Active Directory-Objektbezeichnern aufrecht, sodass es garantiert ist, dass hinzugefügte Verlängerungen des Schemas einzigartig ist und nicht miteinander in Konflikt stehen. Um das Schema im Active Directory von Microsoft zu erweitern, erhielt Dell einzigartige OIDs, einzigartige Namensverlängerungen und einzigartige verbundene Attribut-IDs für unsere Attribute und Klassen, die dem Verzeichnisdienst hinzugefügt werden.

Die Dell-Erweiterung ist: dell

Der Grund-OID von Dell ist: 1.2.840.113556.1.8000.1280

Der RAC-LinkID-Bereich ist: 12070 bis 12079

Die von Microsoft aufrechterhaltene Datenbank von Active Directory-OIDs kann unter **http://msdn.microsoft.com/certification/ADAcctInfo.asp** eingesehen werden, indem unsere Verlängerung Dell eingegeben wird.

Übersicht von RAC-Schema-Verlängerungen

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

Objektübersicht des Active Directory

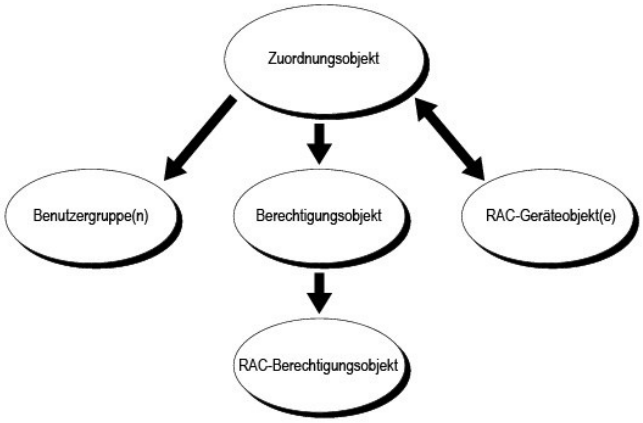
Für jedes der physischen RACs auf dem Netzwerk, das Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein RAC-Geräteobjekt erstellen. Sie können so viele Zuordnungsobjekte erstellen, wie gewünscht, und jedes Zuordnungsobjekt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

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

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

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

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



ANMERKUNG: Das RAC-Berechtigungsobjekt gilt für DRAC 4 und DRAC 5.

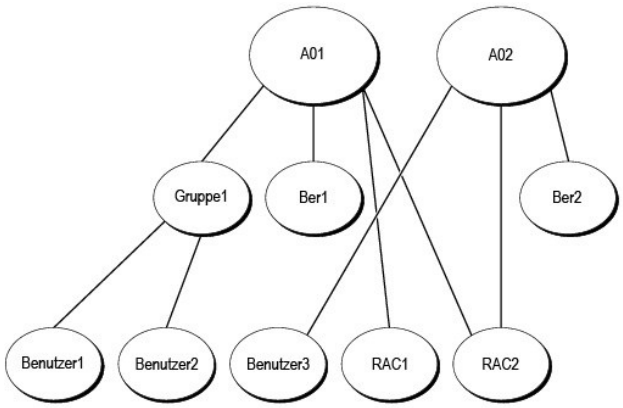
Sie können eine beliebige Anzahl an Zuordnungsobjekten erstellen. Jedoch müssen Sie mindestens ein Zuordnungsobjekt erstellen und Sie müssen ein RAC-Geräteobjekt für jeden RAC (DRAC 5) auf dem Netzwerk haben, das Sie mit Active Directory für die Authentifizierung und Genehmigung mit dem RAC (DRAC 5) integrieren wollen.

Das Zuordungsobjekt berücksichtigt so viele oder wenige Benutzer und/oder Gruppen sowie RAC-Geräteobjekte. Aber das Zuordnungsobjekt enthält nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die "Benutzer", die "Berechtigungen" haben auf den RACs (DRAC 5s).

Außerdem können Sie Active Directory-Objekte in einer einzelnen Domäne oder in mehreren Domänen einrichten. Z. B. haben Sie zwei DRAC 5-Karten (RAC1 und RAC2) und drei existierende Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Sie wollen Benutzer1 und Benutzer2 eine Administratorberechtigung für sowohl DRAC 5-Karten geben, als auch Benutzer3 eine Anmeldungsberechtigung zur RAC2-Karte. Abbildung 6-2 zeigt, wie die Active Directory-Objekte in diesem Fall eingestellt werden.

Wenn Sie Universalgruppen von unterschiedlichen Domänen hinzufügen, erstellen Sie ein Zuordnungsobjekt mit der Universalreichweite. Die durch das Dell Schema-Erweiterungsdienstprogramm erstellten Standardzuordnungsobjekte sind domänenlokale Gruppen und arbeiten nicht mit Universalgruppen von anderen Domänen.

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



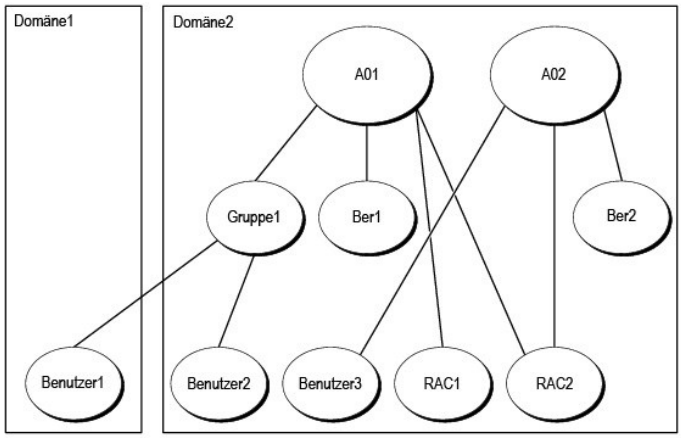
Um die Objekte für das Einzeldomänen-Szenario zu konfigurieren, führen Sie die folgenden Tasks aus:

1. Erstellen Sie zwei Zuordnungsobjekt.
2. Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die zwei DRAC 5-Karten darstellen.
3. Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) und Ber2 Anmeldungsberechtigungen hat.
4. Gruppieren Sie Benutzer1 und Benutzer2 in Gruppe1.
5. Fügen Sie Group1 als Mitglieder im Zuordnungsobjekt 1 (AO1), Ber1 als Berechtigungsobjekte in AO1, und RAC1, RAC2 als RAC-Geräte in AO1 hinzu.
6. Fügen Sie User3 als Mitglied im Zuordnungsobjekt 2 (AO2), Ber2 als Berechtigungsobjekte in AO2, und RAC2 als RAC-Geräte in AO2 hinzu.

Ausführliche Anleitungen erhalten Sie unter "DRAC 5-Benutzer und -Berechtigungen zum Active Directory hinzufügen"

Abbildung 6-3 enthält ein Beispiel von Active Directory-Objekten in mehreren Domänen. Z. B. haben Sie zwei DRAC 5-Karten (RAC1 und RAC2) und drei existierende Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Benutzer1 ist in Domäne1 und Benutzer2 und Benutzer3 sind in Domäne2. In diesem Fallbeispiel konfigurieren Sie Benutzer1 und Benutzer2 mit Administratorberechtigungen für beide DRAC 5-Karten und Benutzer3 mit Anmeldungsberechtigungen an der RAC2-Karte.

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



Um die Objekte für das Szenario für eine einzelne Domäne zu konfigurieren, führen Sie die folgenden Aufgaben aus:

1. Stellen Sie sicher, dass die Domänenfunktion im nativen oder Windows-2003-Modus ist.
2. Erstellen Sie zwei Zuordnungsobjekte, AO1 (mit universellem Bereich) und AO2 in jeder Domäne.

   Abbildung 6-3 zeigt die Objekte in Domain2.
3. Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die zwei DRAC 5-Karten darstellen.

4. Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) und Ber2 Anmeldungsberechtigung hat.

5. Gruppieren Sie Benutzer1 und Benutzer2 in Gruppe1. Der Gruppenbereich von Gruppe1 muss universal sein.

6. Fügen Sie Gruppe1 als Mitglieder in Zuordnungsobjekt 1 (AO1), Ber1 als Berechtigungsobjekte in AO1, und RAC1, RAC2 als RAC-Geräte in AO1 hinzu.

7. Fügen Sie User3 als Mitglied im Zuordnungsobjekt 2 (AO2), Ber2 als Berechtigungsobjekte in AO2, und RAC2 als RAC-Geräte in AO2 hinzu.

Erweitertes Schema von Active Directory konfigurieren um auf Ihren DRAC 5 zuzugreifen

Bevor Sie Active Directory verwenden, um auf Ihren DRAC 5 zuzugreifen, konfigurieren Sie die Active Directory-Software und den DRAC 5, indem Sie die folgenden Schritte in der vorgegebenen Reihenfolge ausführen:

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

2. Erweitern Sie die Active Directory-Benutzer und Computer-Snap-Ins (siehe "Installieren der Dell Erweiterung für Active Directory-Benutzer und Computer-Snap-Ins").

3. Fügen Sie dem Active Directory DRAC 5-Benutzer und deren Berechtigungen hinzu (siehe "DRAC 5-Benutzer und Berechtigungen zum Active Directory hinzufügen").

4. Aktivieren Sie SSL auf jedem Ihrer Domänen-Controller (siehe "SSL auf einem Domänen-Controller aktivieren").

5. Konfigurieren Sie die DRAC 5 Active Directory-Eigenschaften, die entweder die DRAC 5-webbasierte Schnittstelle oder RACADM verwenden (siehe "DRAC 5 mit dem Erweiterten Schema von Active Directory und webbasierter Schnittstelle konfigurieren" oder "DRAC 5 mit dem Erweiterten Schema von Active Directory und RACADM konfigurieren").

Erweiterung des Active Directory-Schemas

Mit der Erweiterung des Active Directory-Schemas werden eine Dell organisatorische Einheit, Schemaklassen und -attribute und Beispielsberechtigungen und Zuordnungsobjekte zum Active Directory-Schema hinzugefügt. Bevor Sie das Schema erweitern, vergewissern Sie sich, dass Sie Schema-Admin-Berechtigungen auf dem Schema Master Flexible Single Master Operation (FSMO)-Rollenbesitzer des Domänenwaldes haben.

Sie können das Schema mit einer der folgenden Methoden erweitern.

- Dell Schemaerweiterungsdienstprogramm
- LDIF-Skript-Datei

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

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

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

Zur Verwendung der LDIF-Dateien siehe die Anleitungen in der Infodatei im Verzeichnis **LDIF_Dateien**. Um das Active Directory-Schema mit Hilfe der Dell-Schema-Erweiterung zu erweitern, führen Sie die Schritte unter "Dell Schema-Erweiterung verwenden" aus.

Sie können die Schema-Erweiterung oder LDIF-Dateien kopieren und von jedem Standort aus ausführen.

Dell Schema-Erweiterung verwenden

HINWEIS: Die Dell Schema-Erweiterung verwendet die Datei **SchemaExtenderOem.ini**. Um sicherzustellen, dass das Dell Schemaerweiterungsdienstprogramm richtig funktioniert, modifizieren Sie den Namen dieser Datei nicht.

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

2. Lesen Sie die Warnung und klicken Sie wieder auf **Weiter**.

3. Wählen Sie **Aktuelle Anmeldungszeugnisse verwenden** oder geben Sie einen Benutzernamen und Kennwort mit Schema-Administratorberechtigungen ein.

4. Klicken Sie auf **Weiter**, um die Dell Schemaerweiterung auszuführen.

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

   Das Schema wird erweitert. Um die Schema-Erweiterung zu überprüfen, verwenden Sie die Microsoft Verwaltungskonsole (MMC) und das Active Directory Schema-Snap-In, um die Existenz der folgenden Elemente zu überprüfen:

   - Klassen (siehe Tabelle 6-1 bis Tabelle 6-6)

- Attribute (Tabelle 6-7)

Weitere Informationen über das Aktivieren und die Verwendung von Active Directory-Schema-Snap-In im MCC erhalten Sie in Ihrer Microsoft-Dokumentation.

Tabelle 6-1. Klassendefinitionen für Klassen, die dem Active Directory-Schema hinzugefügt wurden

Klassenname	Zugewiesene Objektkennnummer (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabelle 6-2. DellRacDevice-Klasse

OID	**1.2.840.113556.1.8000.1280.1.1.1.1**
Beschreibung	Repräsentiert das Dell RAC-Gerät. Das RAC-Gerät muss als dellRacDevice im Active Directory konfiguriert werden. Mit dieser Konfiguration kann der DRAC 5 Lightweight Directory Access Protocol (LDAP)-Fragen an das Active Directory senden.
Klassentyp	Strukturklasse
Superklassen	dellProduct
Attribute	**dellSchemaVersion** **dellRacType**

Tabelle 6-3. DellAssociationObject-Klasse

OID	**1.2.840.113556.1.8000.1280.1.1.1.2**
Beschreibung	Repräsentiert das Dell Zuordnungsobjekt. Das Zuordungsobjekt enthält die Verbindung zwischen den Benutzern und den Geräten.
Klassentyp	Strukturklasse
Superklassen	Gruppe
Attribute	**dellProductMembers** **dellPrivilegeMember**

Tabelle 6-4. DellRAC4Privileges-Klasse

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
Beschreibung	Wird verwendet, um die Berechtigungen (Autorisierungsrechte) für das DRAC 5-Gerät zu definieren.
Klassentyp	Hilfsklasse
Superklassen	Keine
Attribute	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Tabelle 6-5. DellPrivileges-Klasse

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
Superklassen	Benutzer
Attribute	**dellRAC4Privileges**

Tabelle 6-6. DellProduct-Klasse

OID	**1.2.840.113556.1.8000.1280.1.1.1.5**
Beschreibung	Die Hauptklasse, von der alle Dell Produkte abgeleitet werden.
Klassentyp	Strukturklasse
Superklassen	Computer
Attribute	**dellAssociationMembers**

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

Attributname/Beschreibung	Zugewiesene OID/Syntax-Objektbezeichner	Einzeln geschätzt
dellPrivilegeMember Liste von Dell Berechtigungsobjekten, die zu diesem Attribut gehören.	1.2.840.113556.1.8000.1280.1.1.2.1 Bemerkenswerter Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Die Liste von Dell Rac-Geräten, 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 Bemerkenswerter 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 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.4 Boolean (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 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE, wenn der Benutzer Protokolllöschrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolean (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 Boolean (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 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE, wenn der Benutzer Virtuelle Datenträgerrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolean (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 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE, wenn der Benutzer Debug-Befehlsadministratorenrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolean (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 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Dieses Attribut ist der aktuelle RAC-Typ für das DellRacDevice-Objekt und die rückwärts gerichtete Verknüpfung zur Vorwärtsverknüpfung von dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers	1.2.840.113556.1.8000.1280.1.1.2.14	FALSE

Die Liste von dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist die Rückwärtsverbindung zum dellProductMembers verbundenen Attribut. Link-ID: 12071	Bemerkenswerter Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	

Dell Erweiterung auf die Active Directory-Benutzer und das Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch die Active Directory-Benutzer und das Computer-Snap-In erweitern, so dass der Administrator RAC (DRAC 5)-Geräte, Benutzer und Benutzergruppen, RAC-Zuordnungen und RAC-Berechtigungen verwalten kann.

Wenn Sie die Systems Management Software mit der CD *Dell Systems Management Consoles* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsverfahrens die **Dell Erweiterung** für die Option **Active Directory Benutzer- und Computer-Snap-In** auswählen. Das *Dell OpenManage-Software: Schnellinstallationshandbuch* enthält weitere Anweisungen Zusatzbefehle über die Installation von Systems Management-Software.

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

Administrator-Pack installieren

Sie müssen das Administrator-Pack auf jedem System installieren, das die Active Directory-DRAC 5-Objekte verwaltet. Wenn Sie den Administrator-Pack nicht installieren, können Sie das Dell RAC-Objekt im Container nicht ansehen.

Weitere Informationen enthält "Active Directory Benutzer- und Computer-Snap-In".

Active Directory-Benutzer und Computer-Snap-In öffnen

Um die Active Directory-Benutzer und Computer-Snap-In zu öffnen, führen Sie die folgenden Schritte aus:

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 Administrator-Pack auf dem lokalen System installiert sein. Um diesen Administrator-Satz zu installieren, klicken Sie auf **Start** → **Ausführen**, geben Sie `MMC` ein und drücken Sie auf **Eingabe**.

   Die Verwaltungskonsole von Microsoft (MMC) wird eingeblendet.

2. Klicken Sie auf **Datei** (oder **Konsole** auf Systemen unter Windows 2000) im Fenster **Konsole 1**.

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 klicken Sie auf **OK**.

DRAC 5-Benutzer und -Berechtigungen zum Active Directory hinzufügen

Mit dem Dell Erweiterten Active Directory-Benutzer- und Computer-Snap-In können Sie DRAC 5-Benutzer und -Berechtigungen hinzuzufügen, indem Sie RAC-, Zuordnungs- und Berechtigungsobjekte erstellen. Um jede Objektart hinzuzufügen, führen Sie die folgenden Verfahren aus:

- Ein RAC-Geräteobjekt erstellen
- Ein Berechtigungsobjekt erstellen
- Zuordnungsobjekt erstellen
- Einem Zuordnungsobjekt Objekte hinzufügen

Ein RAC-Geräteobjekt erstellen

1. Im Fenster MMC-**Konsolenstamm** klicken Sie mit der rechten Maustaste auf einen Container.

2. Wählen Sie **Neues**→ **Dell RAC-Objekt**.

   Das Fenster **Neues Objekt** wird geöffnet.

3. Geben Sie einen Namen für das neue Objekt ein. Der Name muss mit dem DRAC 5-Namen identisch sein, den Sie im Schritt a von "DRAC 5 mit dem Erweiterten Schema von Active Directory und webbasierter Schnittstelle konfigurieren" eintippen werden.

4. Wählen Sie **RAC-Geräteobjekt**.

5. Klicken Sie auf **OK.**

Ein Berechtigungsobjekt erstellen

ANMERKUNG: Ein Berechtigungsobjekt muss in der gleichen Domäne wie das verwandte Zuordnungsobjekt erstellt werden.

1. Im Fenster **Konsolenstamm** (MCC), klicken Sie mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neues→ Dell RAC-Objekt**.

   Das Fenster **Neues Objekt** wird geöffnet.
3. Geben Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Berechtigungsobjekt**.
5. Klicken Sie auf **OK.**
6. Klicken Sie mit der rechten Maustaste auf das von Ihnen erstellte Objekt und wählen Sie **Eigenschaften**.
7. Klicken Sie auf das Register **RAC-Berechtigungen** und wählen Sie die Berechtigungen, die der Benutzer besitzen soll (weitere Informationen erhalten Sie in Tabelle 4-8).

Zuordnungsobjekt erstellen

Das Zuordnungsobjekt wird aus einer Gruppe abgeleitet und muss einen Gruppentyp enthalten. Die Zuordnungsreichweite gibt den Sicherheitsgruppentyp für das Zuordnungsobjekt an. Wenn Sie ein Zuordnungsobjekt erstellen, müssen Sie die Zuordnungsreichweite wählen, die sich auf den Typ der Objekte bezieht, die hinzugefügt werden sollen.

Wenn z. B. **Universal** gewählt wird, bedeutet das, dass Zuordnungsobjekte nur verfügbar sind, wenn die Active Directory-Domäne im Native- oder einem höheren Modus arbeitet.

1. Im Fenster **Konsolenstamm** (MCC), klicken Sie mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neues→ Dell RAC-Objekt**.

   Dadurch 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** aus.
6. Klicken Sie auf **OK.**

Einem Zuordnungsobjekt Objekte hinzufügen

Durch Anwendung des Fensters **Zuordnungsobjekteigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und RAC-Geräte oder RAC-Gerätegruppen zuordnen. Wenn das System den Windows 2000-Modus oder höher verwendet, müssen Sie universale Gruppen verwenden, um Domänen mit Ihren Benutzern oder RAC-Objekten mit einzuschließen.

Sie können Gruppen von Benutzern und RAC-Geräten hinzufügen. Die Verfahren zum Erstellen von Dell-bezogenen Gruppen und nicht-Dell-bezogenen Gruppen sind identisch.

Benutzer oder Benutzergruppen hinzufügen

1. Klicken Sie mit der rechten Maustaste auf das **Zuordnungsobjekt** und wählen Sie **Eigenschaften**.
2. Klicken Sie auf das Register **Benutzer** und klicken Sie **Hinzufügen**.
3. Geben Sie den Benutzer- oder Benutzergruppennamen ein und klicken Sie auf **OK**.

Klicken Sie auf das Register **Berechtigungsobjekt**, um die Berechtigung hinzuzufügen, die die Benutzer- oder Benutzergruppenberechtigungen definiert, während ein RAC-Gerät authentisiert wird. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

Berechtigungen hinzufügen

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

Klicken Sie auf das Register **Produkte**, um ein oder mehrere RAC-Geräte zur Zuordnung hinzuzufügen. Die assoziierten Geräte geben die mit dem Netzwerk verbundenen RAC-Geräte an, die für die definierten Benutzer oder Benutzergruppen verfügbar sind. Mehrere RAC-Geräte können einem Zuordnungsobjekt hinzugefügt werden.

RAC-Geräte oder RAC-Gerätegruppen hinzufügen

Um RAC-Geräte oder RAC-Gerätegruppen hinzuzufügen:

1. Wählen Sie das Register **Produkte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Namen des RAC-Geräts oder der RAC-Gerätegruppe ein und klicken Sie auf **OK**.
3. Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.

DRAC 5 mit dem Erweiterten Schema von Active Directory und webbasierter Schnittstelle konfigurieren

1. Öffnen Sie ein unterstütztes Internetbrowser-Fenster.
2. Melden Sie sich an der webbasierten DRAC 5-Schnittstelle an.
3. Erweitern Sie die **System**-Struktur und klicken Sie auf **Remote-Zugriff**.
4. Klicken Sie auf das Register **Konfiguration** und wählen Sie **Active Directory**.
5. Auf der Seite **Active Directory**-**Hauptmenü** wählen Sie **Active Directory konfigurieren** und klicken Sie auf **Weiter**.
6. Im Abschnitt Allgemeine Einstellungen:
   a. Wählen Sie das Kontrollkästchen **Active Directory aktivieren**
   b. Geben Sie den **Root-Domänennamen** ein. Der **Root-Domänenname** ist der vollständig qualifizierte Root-Domänenname für den Wald.
   c. Geben Sie die **Zeitüberschreitungs**-Zeit in Sekunden ein.
7. Klicken Sie auf **Erweitertes Schema verwenden** im Abschnitt Auswahl des Active Directory-Schemas.
8. Im Abschnitt Erweiterte Schemaeinstellungen:
   a. Geben Sie den **DRAC-Namen** ein. Dieser Name muss derselbe sein, wie der allgemeine Name des neuen RAC-Objekts, das Sie in Ihrem Domänen-Controller erstellt haben (siehe Schritt 3 "RAC-Geräteobjekt erstellen").
   b. Geben Sie den **DRAC-Domänenname** ein (z. B. `drac5.com`). Verwenden Sie den NetBIOS-Namen nicht. Der **DRAC-Domänenname** ist der vollständig qualifizierte Domänenname der Sub-Domäne, in der sich das RAC-Geräteobjekt befindet.
9. Klicken Sie auf **Anwenden** um die Active Directory-Einstellungen zu speichern.
10. Auf **Zurück zum Active Directory-Hauptmenü** klicken.
11. Laden Sie das Domänen-Wald Stamm-CA-Zertifikat in den DRAC 5 hoch.
    a. Wählen Sie das Kontrollkästchen **Active Directory CA Zertifikat hochladen** und klicken Sie dann auf **Weiter**.
    b. Geben Sie auf der Seite **Zertifikat hochladen** den Dateipfad des Zertifikats ein oder suchen Sie die Zertifikat-Datei.

    ANMERKUNG: Der **Dateipfad**-Wert zeigt den relativen Pfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad tippen, mit dem vollständigen Pfad und dem gesamten Dateinamen und Dateinamenszusatz.

    Die SSL-Zertifikate des Domain-Controllers sollten vom Stamm-CA unterzeichnet worden sein. Halten Sie das Stamm-Zertifizierungsstellenzertifikat auf Ihrer Verwaltungsstation bereit, die auf DRAC 5 zugreift (siehe "Domänen-Controller-Stamm-Zertifizierungsstellenzertifikat exportieren").

    c. Klicken Sie auf **Anwenden**.

    Der DRAC 5 Webserver startet automatisch neu, nachdem Sie auf **Anwenden** klicken.

12. Melden Sie sich ab und dann am DRAC 5 an, um die DRAC 5 Active Directory-Funktionskonfiguration abzuschließen.

13. In der **System-**Struktur klicken Sie auf **Remote-Zugriff**.

14. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**.

    Die Seite **Netzwerkkonfiguration** wird eingeblendet.

15. Wenn **DHCP verwenden (für die NIC-IP-Adresse)** unter **Netzwerk-Einstellungen** gewählt wird, dann wählen Sie **DHCP verwenden, um DNS Server-Adresse zu erhalten**.

    Wenn Sie eine DNS-Server-IP-Adresse von Hand eingeben möchten, wählen Sie **DHCP zum Abrufen von DNS-Serveradressen verwenden** ab und geben Sie die primäre und alternative DNS-Server-IP-Adresse ein.

16. Klicken Sie auf **Änderungen anwenden**.

    Die Funktionskonfiguration des DRAC 5 erweiterten Schema von Active Directory ist abgeschlossen.

DRAC 5 mit dem Erweiterten Schema von Active Directory und RACADM konfigurieren

Verwendung der folgenden Befehle, um die DRAC 5-Active Directory-Funktion mit erweitertem Schema mit Hilfe der racadm CLI anstatt der webbasierten Schnittstelle zu konfigurieren.

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

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

   racadm config -g cfgActiveDirectory -o cfgADType 1

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

   racadm config -g cfgActiveDirectory -o cfgADRootDomain <völlig qualifizierter Stammdomänenname>

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

   racadm sslcertupload -t 0x2 -f <ADS Stammzertifizierungsstellenzertifikat>

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

2. Wenn DHCP auf dem DRAC 5 aktiviert wird und Sie den vom DHCP-Server bereitgestellten DNS verwenden wollen, geben Sie den folgenden racadm-Befehl ein:

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

3. Wenn DHCP auf dem DRAC 5 deaktiviert ist oder Sie Ihre DNS-IP-Adresse manuell eingeben wollen, 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. Drücken Sie auf **Eingabe**, um die DRAC 5-Active Directory-Funktionskonfiguration zu abzuschließen.

Übersicht über das Standardschema von Active Directory

Wie in der Abbildung 6-4 gezeigt, erfordert die Verwendung des Standardschemas für Active Directory-Integration die Konfiguration sowohl auf Active Directory als auch auf DRAC 5.Auf der Active Directory-Seite wird ein Standardgruppenobjekt als eine Rollengruppe verwendet. Ein Benutzer, der Zugang zu DRAC 5 hat, wird ein Mitglied der Rollengruppe sein. Um diesem Benutzer Zugriff auf eine spezifische DRAC 5-Karte zu gewähren, müssen der Rollengruppenname und sein Domänenname auf der spezifischen DRAC 5-Karte konfiguriert werden. Im Unterschied zur Lösung des erweiterten Schemas, sind die Rollen- und Berechtigungsstufe auf jeder DRAC 5-Karte und nicht im Active Directory definiert.Bis zu fünf Rollengruppen können in jedem DRAC 5 konfiguriert und definiert werden. Tabelle 4-15 zeigt die Berechtigungsstufe der Rollengruppen an und Tabelle 6-8 zeigt die Standardeinstellungsrollengruppeneinstellungen.

Abbildung 6-4. Konfiguration von DRAC 5 mit Microsoft Active Directory und Standardschema

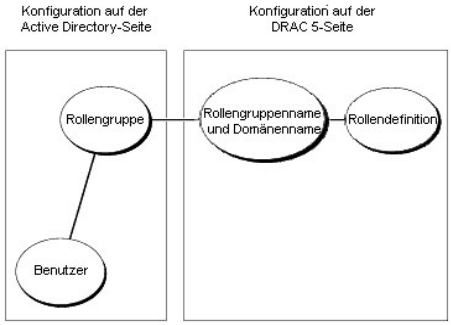


Tabelle 6-8. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppen	Standardeinstellungsberechtigungsstufe	Berechtigungen gewährt	Bit-Maske
Rollengruppe 1	Administrator	**Anmeldung bei DRAC**, **DRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**	0x000001ff
Rollengruppe 2	Hauptbenutzer	**Anmeldung bei DRAC**, **Protokoll löschen**, **Serversteuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**	0x000000f9
Rollengruppe 3	Gastbenutzer	**Anmeldung an DRAC**	0x00000001
Rollengruppe 4	Keine	Keine zugewiesenen Berechtigungen	0x00000000
Rollengruppe 5	Keine	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bit-Maske-Werte werden nur verwendet, wenn das Standardschema mit RACADM eingestellt wird.

Es gibt zwei Wege, das Standardschema von Active Directory zu aktivieren:

- Mit der DRAC 5-webbasierten Benutzerschnittstelle. Siehe "DRAC 5 mit dem Standardschema von Active Directory und webbasierter Schnittstelle konfigurieren".
- Mit dem RACADM CLI-Hilfsprogramm. Siehe "DRAC 5 mit dem Standardschema von Active Directory und RACADM konfigurieren".

Das Standardschema von Active Directory konfigurieren, um auf Ihren DRAC 5 zuzugreifen

Sie müssen die folgenden Schritte ausführen, um Active Directory zu konfigurieren, bevor ein Active Directory-Benutzer auf den DRAC 5 zugreifen kann:

1. Auf einem Active Directory-Server (Domänen-Controller) das Active Directory-Benutzer- und Computer-Snap-In öffnen.
2. Erstellen Sie eine Gruppe oder wählen Sie eine vorhandene Gruppe aus. Der Name der Gruppe und der Namen dieser Domäne muss auf dem DRAC 5 entweder mit der webbasierten Schnittstelle oder RACADM konfiguriert werden (siehe "DRAC 5 mit dem Standardschema von Active Directory und webbasierter Schnittstelle konfigurieren" oder "DRAC 5 mit dem Standardschema von Active Directory und RACADM konfigurieren").
3. Fügen Sie den Active Directory-Benutzer als ein Mitglied der Active Directory-Gruppe hinzu, um auf den DRAC 5 zuzugreifen.

DRAC 5 mit dem Standardschema von Active Directory und webbasierter Schnittstelle konfigurieren

1. Öffnen Sie ein unterstütztes Internetbrowser-Fenster.
2. Melden Sie sich an der webbasierten DRAC 5-Schnittstelle an.
3. Erweitern Sie die **System**-Struktur und klicken Sie auf **Remote-Zugriff**.
4. Klicken Sie auf das Register **Konfiguration** und wählen Sie **Active Directory**.
5. Auf der Seite **Active Directory-Hauptmenü** wählen Sie **Active Directory konfigurieren** und klicken Sie auf **Weiter**.
6. Im Abschnitt Allgemeine Einstellungen:

a. Wählen Sie das Kontrollkästchen **Active Directory aktivieren**

b. Geben Sie den **Root-Domänennamen** ein. Der **Root-Domänenname** ist der vollständig qualifizierte Root-Domänenname für den Wald.

c. Geben Sie die **Zeitüberschreitungs**-Zeit in Sekunden ein.

7. Klicken Sie auf **Standardschema verwenden** im Abschnitt Auswahl des Active Directory-Schemas.

8. Klicken Sie auf **Anwenden** um die Active Directory-Einstellungen zu speichern.

9. In der Spalte **Rollengruppen** des Abschnitts Standardschemaeinstellungen auf eine **Rollengruppe** klicken.

   Die Seite **Rollengruppe konfigurieren** erscheint, die einen **Gruppennamen**, eine **Gruppendomäne** und **Rollengruppenberechtigungen** einer Rollengruppe beinhaltet.

10. Geben Sie den **Gruppennamen** ein. Der Gruppenname identifiziert die Rollengruppe im Active Directory, das mit der DRAC 5-Karte verbunden ist.

11. Geben Sie die **Gruppendomäne** ein. Der **Gruppenomänenname** ist der vollständig qualifizierte Root-Domänenname für den Wald.

12. Auf der Seite **Rollengruppenberechtigungen** die Gruppenberechtigungen einstellen.

    Tabelle 4-15 beschreibt die **Rollengruppenberechtigungen**.

    Tabelle 4-16 beschreibt die **Rollengruppenzulassungen**. Wenn Sie einige der Berechtigungen modifizieren, wird die vorhandene **Rollengruppenberechtigung** (Administrator, Hauptbenutzer oder Gastbenutzer) entweder zur benutzerdefinierten Gruppe oder zur entsprechenden Rollengruppenberechtigung, die auf den modifizierten Berechtigungen basiert, wechseln.

13. Klicken Sie auf **Anwenden** um die Rollengruppeneinstellungen zu speichern.

14. Klicken Sie auf **Zurück zur Active Directory-Konfiguration und Verwaltung**.

15. Auf **Zurück zum Active Directory-Hauptmenü** klicken.

16. Laden Sie das Domänen-Wald Stamm-CA-Zertifikat in den DRAC 5 hoch.

    a. Wählen Sie das Kontrollkästchen **Active Directory CA Zertifikat hochladen** und klicken Sie dann auf **Weiter**.

    b. Geben Sie auf der Seite **Zertifikat hochladen** den Dateipfad des Zertifikats ein oder suchen Sie die Zertifikat-Datei.

    ANMERKUNG: Der **Dateipfad**-Wert zeigt den relativen Pfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad tippen, mit dem vollständigen Pfad und dem gesamten Dateinamen und Dateinamenszusatz.

    Die SSL-Zertifikate des Domänen-Controllers sollten vom Stamm-CA unterzeichnet worden sein. Halten Sie das Stamm-Zertifizierungsstellenzertifikat auf Ihrer Verwaltungsstation bereit, die auf DRAC 5 zugreift (siehe "Domänen-Controller-Stamm-Zertifizierungsstellenzertifikat exportieren").

    c. Klicken Sie auf **Anwenden**.

    Der DRAC 5 Webserver startet automatisch neu, nachdem Sie auf **Anwenden** klicken.

17. Melden Sie sich ab und dann am DRAC 5 an, um die DRAC 5 Active Directory-Funktionskonfiguration abzuschließen.

18. In der **System-**Struktur klicken Sie auf **Remote-Zugriff**.

19. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**.

    Die Seite **Netzwerkkonfiguration** wird eingeblendet.

20. Wenn **DHCP verwenden (für die NIC-IP-Adresse)** unter **Netzwerk-Einstellungen** gewählt wird, dann wählen Sie **DHCP verwenden, um DNS Server-Adresse zu erhalten**.

    Wenn Sie eine DNS-Server-IP-Adresse von Hand eingeben möchten, wählen Sie **DHCP zum Abrufen von DNS-Serveradressen verwenden** ab und geben Sie die primäre und alternative DNS-Server-IP-Adresse ein.

21. Klicken Sie auf **Änderungen anwenden**.

    Die DRAC 5-Standardschema-Funktionskonfiguration von Active Directory ist abgeschlossen.

DRAC 5 mit dem Standardschema von Active Directory und RACADM konfigurieren

Verwenden Sie die folgenden Befehle, um die DRAC 5 Active Directory-Funktion mit dem Standardschema zu konfigurieren, das RACADM CLI anstelle der webbasierten Schnittstelle verwendet.

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

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

   racadm config -g cfgActiveDirectory -o cfgADType 2

   racadm config -g cfgActiveDirectory -o cfgADRootDomain <völlig qualifizierter Stammdomänenname>

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

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

   racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupPrivilege <Bit-Maske-Nummer für spezifische Benutzerberechtigungen>

   racadm sslcertupload -t 0x2 -f <ADS Stammzertifizierungsstellenzertifikat>

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

   ANMERKUNG: Bit-Maske-Nummernwerte finden Sie in der Tabelle B-4.

2. Wenn DHCP auf dem DRAC 5 aktiviert wird und Sie den vom DHCP-Server bereitgestellten DNS verwenden wollen, geben Sie die folgenden racadm-Befehle ein:

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

3. Wenn DHCP auf dem DRAC 5 deaktiviert ist oder Sie Ihre DNS-IP-Adresse manuell eingeben wollen, 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>
   ```

SSL auf einem Domänen-Controller aktivieren

Wenn Sie die Microsoft Enterprise Stamm-CA verwenden, um alle Domänen-Controller-SSL-Zertifikate automatisch zuzuweisen, müssen Sie die folgenden Schritte ausführen, um SSL auf jedem Domänen-Controller zu aktivieren.

1. Installieren Sie eine Microsoft Enterprise-Stamm-CA auf einem Domänen-Controller.
   a. Wählen Sie **Start**→ **Systemsteuerung**→ **Programme Hinzufügen oder Entfernen**.
   b. Wählen Sie **Windows-Komponenten hinzufügen/entfernen**.
   c. Im **Assistent für Windows-Komponenten** wählen Sie das Kontrollkästchen **Zertifikatsdienste**.
   d. Wählen Sie **Enterprise Stamm-CA** als **CA-Typ** und klicken Sie auf **Weiter**.
   e. Geben Sie **Allgemeiner Name dieser Zertifizierungsstelle,** klicken Sie auf **Weiter** und klicken Sie auf **Fertig stellen**.

2. Aktivieren Sie SSL auf jedem Ihrer Domänen-Controller durch Installieren des SSL-Zertifikats für jeden Controller.
   a. Klicken Sie auf **Start**→ **Verwaltung**→ **Domänen-Sicherheitsrichtlinie**.
   b. Erweitern Sie den Ordner **Öffentliche Schlüsselregeln**, klicken Sie mit der rechten Maustaste **Automatische Zertifikatanforderungseinstellungen** und klicken Sie auf **Automatische Zertifikatsanforderung**.
   c. Im **Assistent für automatische Zertifikatsanforderung** klicken Sie auf **Weiter** und wählen Sie **Domänen-Controller**.
   d. Klicken Sie auf **Weiter** und klicken Sie auf **Fertig stellen**.

Domänen-Controller-Stamm-CA-Zertifikat exportieren

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

1. Suchen Sie den Domänen-Controller, der den Microsoft Enterprise CA-Dienst ausführt.
2. Klicken Sie auf **Start**→**Ausführen**.
3. Geben Sie in das Feld **Ausführen** 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**.
5. Im Fenster **Snap-In hinzufügen/entfernen** klicken Sie auf **Hinzufügen**.

6. Im Fenster **Eigenständiges Snap-In hinzufügen** wählen Sie **Zertifikate** und klicken Sie auf **Hinzufügen**.

7. Wählen Sie das Konto **Computer** und klicken sie auf **Weiter**.

8. Wählen Sie **Lokaler Computer** und klicken Sie auf **Fertig stellen**.

9. Klicken Sie auf **OK.**

10. **Im Fenster Konsole 1** erweitern Sie 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** und klicken Sie auf **Exportieren...** .

12. Im **Zertifikatsexport-Assistent** klicken sie auf **Weiter** und wählen Sie **Nein, exportieren Sie nicht den privaten Schlüssel**.

13. Klicken Sie auf **Weiter** und wählen Sie **Base-64 kodierte X.509 (.cer)** als das Format.

14. Auf **Weiter** klicken und das Zertifikat in einem Verzeichnis auf Ihrem System speichern.

15. Laden Sie das in Schritt 14 gespeicherte Zertifikat zum DRAC 5 hoch.

    Um das Zertifikat hochzuladen, das RACADM verwendet, schauen Sie unter "DRAC 5 mit dem Erweiterten Schema von Active Directory und webbasierter Schnittstelle" nach

    Um das Zertifikat mittels der webbasierten Schnittstelle hochzuladen, führen Sie das folgende Verfahren aus:

    a. Öffnen Sie ein unterstütztes Internetbrowser-Fenster.

    b. Melden Sie sich an der webbasierten DRAC 5-Schnittstelle an.

    c. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.

    d. Klicken Sie auf das Register **Konfiguration** und dann auf **Sicherheit**.

    e. Auf der Seite **Sicherheitszertifikat-Hauptmenü** wählen Sie **Server-Zertifikat hochladen** und klicken Sie auf **Anwenden**.

    f. Führen Sie auf dem Bildschirm **Zertifikat hochladen** eins der folgenden Verfahren aus:

       - Klicken Sie auf **Durchsuchen** und wählen Sie das Zertifikat
       - Geben Sie den Pfad zum Zertifikat in das Feld **Wert** ein.

    g. Klicken Sie auf **Anwenden**.

DRAC 5 Firmware SSL-Zertifikat importieren

Verwenden Sie das folgende Verfahren, um das DRAC 5 Firmware SSL-Zertifikat zu allen vertrauenswürdigen Zertifikat-Listen der Domänen-Controller zu importieren.

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

ANMERKUNG: Wenn das DRAC 5 Firmware-SSL-Zertifikat von einer bekannten CA signiert ist, brauchen die in diesem Abschnitt beschriebenen Schritte nicht ausgeführt zu werden.

Das DRAC 5 SSL-Zertifikat ist identisch mit dem Zertifikat, das für den DRAC 5-Webserver verwendet wird. Alle DRAC 5-Controller werden mit einem selbstunterzeichneten Standardzertifikat verladen.

Um auf das Zertifikat zuzugreifen, das die webbasierte DRAC 5-Schnittstelle verwendet, wählen Sie **Konfiguration→ Active Directory→ DRAC 5 Server-Zertifikat herunterladen**.

1. Auf dem Domänen-Controller, öffnen Sie ein Fenster **MMC-Konsole** und wählen Sie **Zertifikate→ zuverlässigen Stammzertifikatszertifizierungsstellen**.

2. Rechts-klicken Sie auf **Zertifikate**, wählen Sie **Alle Aufgaben** und klicken sie auf **Import**.

3. Klicken Sie auf **Weiter** und browsen Sie zur SSL-Zertifikat-Datei.

4. Installieren Sie das RAC-SSL-Zertifikat in der **zuverlässigen Stammzertifikatszertifizierungsstelle** jedes Domänen-Controllers.

   Wenn Sie Ihr eigenes Zertifikat installiert haben, stellen Sie sicher, dass die CA, die Ihr Zertifikat unterschreibt auf der Liste von **zuverlässigen Stammzertifikatzertifizierungsstelle ist.** Wenn die Zertifizierungsstelle nicht auf der Liste ist, müssen Sie sie auf allen Ihren Domänen-Controllern installieren.

5. Klicken Sie auf **Weiter** und wählen Sie, ob Windows die Zertifikatstelle, basierend auf dem Zertifikattyp, automatisch wählen soll oder wechseln Sie zu einer Stelle Ihrer Wahl.

6. Klicken Sie auf **Fertig stellen** und klicken Sie auf **OK**.

Active Directory verwenden, um zum sich beim DRAC 5 anzumelden

Sie können Active Directory verwenden, um sich mittels einer der folgenden Methoden am DRAC 5 anzumelden:

- Webbasiertes Interface
- Remote-RACADM
- Serielle oder Telnet-Konsole.

Die Anmeldungssyntax ist für alle drei Methoden beständig:

<*Benutzername@Domäne*>

oder

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

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

Leerstellen und Sonderzeichen (z.B. \, / oder @) sind weder im Benutzernamen noch im Domänennamen zulässig.

ANMERKUNG: NetBIOS-Domänennamen, z.B. "Americas" können nicht festgelegt werden, da diese Namen nicht gelöst werden können.

Häufig gestellte Fragen

Tabelle 6-9 enthält häufig gestellte Fragen und Antworten.

Tabelle 6-9. DRAC 5 mit Active Directory verwenden: Häufig gestellte Fragen

Frage	Antwort
Kann ich mich beim DRAC 5 anmelden, indem ich Active Directory über mehrfache Strukturen verwende?	Ja. Der DRAC 5-Active Directory-Fragealgorithmus unterstützt nur mehrere Strukturen in einem einzelnen Wald.
Funktioniert die Anmeldung beim DRAC 5 mit Hilfe von Active Directory im gemischten Modus (d. h., die Domänen-Controller im Wald führen verschiedene Betriebssysteme aus, wie z. B. Microsoft Windows NT® 4.0, Windows 2000 oder Windows Server 2003)?	Ja. Im gemischten Modus müssen alle durch das DRAC 5-Frageverfahren verwendeten Objekte (unter dem Benutzer, RAC-Geräteobjekt und Zuordnungsobjekt) in derselben Domäne sein. Das Dell-erweiterte Active Directory Users and Computers Snap-In überprüft den Modus und beschränkt Benutzer, um Objekte über Domänen hinweg zu erstellen, wenn es im Mischmodus ist.
Unterstützt die Verwendung von DRAC 5 mit Active Directory mehrfache Domänenumgebungen?	Ja. Der Domänenwaldfunktionslevel muss im nativen Modus oder Windows-2003-Modus sein. Außerdem müssen die Gruppen unter dem Zuordungsobjekt, RAC-Benutzerobjekte und RAC-Geräteobjekte (einschließlich des Zuordnungsobjekts) universale Gruppen sein.
Können diese Dell-erweiterten Objekte (Dell-Zuordnungsobjekt, Dell RAC-Gerät und Dell-Berechtigungsobjekt) in verschiedenen Domänen sein?	Das Zuordnungsobjekt und das Berechtigungsobjekt müssen in derselben Domäne sein. Mit Dell erweiterten Active Directory-Benutzern und Computer-Snap-In müssen Sie diese zwei Objekte in derselben Domäne erstellen. Andere Objekte können sich in verschiedenen Domänen befinden.
Gibt es irgendwelche Einschränkungen der Domänen-Controller-SSL-Konfiguration?	Ja. SSL-Zertifikate aller Active Directory-Server im Wald müssen von der gleichen Stammzertifizierungsstelle unterzeichnet werden, da DRAC 5 nur zulässt, dass ein CA-SSL-Zertifikat hochgeladen wird.
Ich erstellte und lud ein neues RAC-Zertifikat und jetzt startet die Web-gegründete Schnittstelle nicht.	Wenn Sie Zertifikatsdienste von Microsoft verwenden, um das RAC-Zertifikat zu erstellen, ist eine mögliche Ursache davon dass Sie **Benutzerzertifikat** wählten anstatt **Webzertifikat** als Sie das Zertifikat erstellten. Erstellen Sie zur Wiederherstellung einen CSR und dann ein neues Web-Zertifikat von Microsoft Zertifikats-Dienste und laden Sie es unter Verwendung des RACADM CLI vom verwalteten System, indem Sie die folgenden racadm-Befehle verwenden: racadm sslcsrgen [-g] [-u] [-f {Dateiname}] racadm sslcertupload -t 1 -f {web_sslcert}
Was kann ich tun, wenn ich mich mittels Active Directory-Authentifizierung nicht am DRAC 5 anmelden kann? Wie kann ich eine Lösung für das Problem finden?	1. Stellen Sie sicher, dass Sie die richtige Benutzerdomänenname während einer Anmeldung verwendet wird und nicht der NetBIOS-Name. 2. Wenn Sie ein lokales DRAC-Benutzerkonto haben, melden Sie sich mit Ihren lokalen Anmeldeinformationen am DRAC 5 an. Nachdem Sie angemeldet sind, die folgenden Schritte ausführen: a. Stellen Sie sicher, dass Sie das Kästchen **Active Directory aktivieren** auf der Seite DRAC 5 Active Directory-Konfiguration markiert haben. b. Stellen Sie sicher, dass die DNS-Einstellung auf der DRAC 5-Netzwerkanschlusskonfigurationsseite richtig ist. c. Stellen Sie sicher, dass Sie das Active Directory-Zertifikat von Ihrer Active Directory-Stammzertifizierungsstelle zum DRAC 5 geladen haben. d. Überprüfen Sie die Domänen-Controller SSL-Zertifikate, um sicherzustellen, dass sie nicht abgelaufen sind.

	e. Stellen Sie sicher, dass **DRAC -Name**, **Root-Domänenname** und **DRAC -Domänenname** mit Ihrer Active Directory-Umgebungskonfiguration übereinstimmen. f. Stellen Sie sicher, dass das DRAC 5-Kennwort maximal 127 Zeichen aufweist. Während der DRAC 5 Kennwörter von bis zu 256 Zeichen unterstützt, unterstützt Active Directory nur Kennwörter, die maximal 127 Zeichen lang sind.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

GUI-Konsolenumleitung verwenden

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Dieser Abschnitt enthält Informationen über die Anwendung der DRAC 5-Konsolenumleitungsfunktion.

Übersicht

Mit der DRAC 5-Konsolenumleitungsfunktion können Sie im Remote-Zugriff im grafischen oder Textmodus auf die lokale Serverkonsole zugreifen. Mittels Konsolenumleitung können Sie ein oder mehrere DRAC 5-aktivierte Systeme von einem Standort kontrollieren.

Heutzutage, mit der Macht von Networking und des Internets müssen Sie nicht vor jedem Server sitzen, um die ganze alltägliche Wartung auszuführen. Sie können die Server von einer anderen Stadt oder sogar von der anderen Seite der Welt von Ihrem Desktop oder tragbarem PC verwalten. Sie können die Informationen auch mit anderen teilen - im Remote-Zugriff und sofort.

Konsolenumleitung verwenden

ANMERKUNG: Wenn Sie eine Konsolenumleitungssitzung öffnen, zeigt das verwaltete System nicht an, dass die Konsole umgeleitet worden ist

Die Seite **Konsolenumleitung** ermöglicht Ihnen, das Remote-System zu verwalten, indem Sie die Tastatur, das Video und die Maus auf Ihrer lokalen Verwaltungsstation verwenden, um die entsprechenden Geräte auf einem verwalteten Remote-System zu kontrollieren. Diese Funktion kann in Verbindung mit der virtuellen Datenträgerfunktion verwendet werden, um Remote-Softwareinstallationen auszuführen.

Die folgenden Regeln gelten für eine Konsolenumleitungssitzung:

- Es können nur zwei gleichzeitige Konsolenumleitungssitzungen unterstützt werden.
- Konsolenumleitungssitzungen können nur mit einem Remote-Zielsystem verbunden werden.
- Konsolenumleitungssitzungen können nicht auf dem lokalen System konfiguriert werden.
- Die erforderliche verfügbare Netzwerk-Mindestbandbreite beträgt 1 MB/s.

Unterstützte Bildschirmauflösungswiederholfrequenzen auf dem verwalteten System

Tabelle 7-1 führt die unterstützten Bildschirmauflösungen und entsprechende Bildwiederholfrequenzen für eine Konsolenumleitungssitzung auf, die auf dem verwalteten System ausgeführt wird.

Tabelle 7-1. 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

Verwaltungsstation konfigurieren

Zur Verwendung von Konsolenumleitung auf Ihrer Verwaltungsstation führen Sie die folgenden Verfahren aus:

1. Einen unterstützten Internetbrowser installieren und konfigurieren. Siehe die folgenden Abschnitte für weiterführende Informationen:
   - "Unterstützte Internetbrowser"

     ANMERKUNG: Konsolenumleitung und Virtueller Datenträger unterstützen nur 32-Bit-Internet-Browser. Das Verwenden von 64-Bit-Internet-Browsern kann zu unerwarteten Ergebnissen oder einem Fehlschlagen von Vorgängen führen.
   - "Einen unterstützten Internetbrowser konfigurieren"
2. Stellen Sie die Auflösung des Monitors auf mindestens 1280 x 1024 Pixel bei 60 Hz mit 128 Farben ein. Ansonsten können Sie u. U. die Konsole nicht im

Vollbildmodus sehen.

Konsolenumleitung konfigurieren

1. Öffnen Sie einen unterstützten Internetbrowser auf der Verwaltungsstation und melden Sie sich am DRAC 5 an. "Zugriff auf die webbasierte Schnittstelle" enthält weitere Informationen.

2. In der **System**struktur klicken Sie auf **System**.

3. Klicken Sie auf das Register **Konsole** und dann auf **Konfiguration**.

4. Verwenden Sie auf der Seite **Konsolenumleitungskonfiguration** die Informationen aus Tabelle 7-2 zum Konfigurieren der Konsolenumleitungssitzung, und klicken Sie dann auf **Änderungen anwenden**.

Tabelle 7-2. Informationen zur Konsolenumleitungskonfigurationsseite

Informationen	Beschreibung
Aktiviert	Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Max. Sitzungen	Zeigt die Zahl von Konsolenumleitungssitzungen an, die verfügbar sind.
Aktive Sitzungen	Zeigt die Zahl der aktiven Konsolenumleitungssitzungen an.
Tastatur- und Mausanschlussnummer	Standardeinstellung = 5900
Videoschnittstellennummer	Standardeinstellung = 5901
Videoverschlüsselung aktiviert	Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Lokaler Server-Video aktiviert	Markiert=Aktiviert; Unmarkiert=Deaktiviert.

Die Schaltflächen in Tabelle 7-3 sind auf der Seite **Konsolenumleitungskonfiguration** verfügbar.

Tabelle 7-3. Schaltflächen der Konsolenumleitungskonfigurationsseite

Eigenschaft	Beschreibung
Drucken	Druckt die Seite **Konsolenumleitungskonfiguration**
Aktualisieren	Lädt die Seite **Konsolenumleitungskonfiguration** neu
Änderungen anwenden	Speichert Ihre Konfigurationseinstellungen.

Konsolenumleitungssitzung öffnen

Wenn Sie eine Konsolenumleitungssitzung öffnen, startet die Dell Virtual KVM Viewer-Anwendung, und das Desktop des Remote-Systems wird im Viewer eingeblendet. Mit der virtuellen KVM Viewer-Anwendung können die Maus- und Tastatur-Funktionen des Systems von einer lokalen oder Remote-Verwaltungsstation aus gesteuert werden.

Um eine Konsolenumleitungssitzung zu öffnen, führen Sie die folgenden Schritte aus.

1. Öffnen Sie einen unterstützten Internetbrowser auf der Verwaltungsstation und melden Sie sich am DRAC 5 an. "Zugriff auf die webbasierte Schnittstelle" enthält weitere Informationen.

2. Klicken Sie in der **System**struktur auf **System** und dann im Register **Konsole** auf **Konsolenumleitung**.

ANMERKUNG: Wenn Sie eine Sicherheitswarnung erhalten, die Sie auffordert, das Konsolenumleitungs-Plugin zu installieren und auszuführen, überprüfen Sie die Authentizität des Plugins und klicken dann auf **Ja**, um das Plugin zu installieren und auszuführen. Wenn Sie Firefox ausführen, starten Sie den Browser neu und wechseln dann zu Schritt 1.

3. Verwenden Sie auf der Seite **Konsolenumleitung** die Informationen von Abbildung 7-4, um sicherzustellen, dass eine Konsolenumleitungssitzung verfügbar ist.

Tabelle 7-4. Informationen zur Seite Konsolenumleitung

Eigenschaft	Beschreibung
Aktivierte Konsolenumleitung	Ja/Nein
Videoverschlüsselung aktiviert	Ja/Nein
Lokaler Server-Video aktiviert	Ja/Nein
Status	Verbunden oder Unterbrochen

Max. Sitzungen	Die maximale Anzahl von unterstützten Konsolenumleitungssitzungen
Aktive Sitzungen	Die aktuelle Anzahl von aktiven Konsolenumleitungssitzungen

Die Schaltflächen in Tabelle 7-5 sind auf der Seite **Konsolenumleitung** verfügbar.

Tabelle 7-5. Schaltflächen der Seite Konsolenumleitung

Schaltfläche	Definition
Aktualisieren	Lädt die Seite **Konsolenumleitungskonfiguration** neu
connect	Öffnet eine Konsolenumleitungssitzung auf dem Remote-Ziel-System.
Drucken	Druckt die Seite **Konsolenumleitungskonfiguration**

4. Wenn eine Konsolenumleitungssitzung verfügbar ist, auf **Verbinden** klicken.

   ANMERKUNG: Mehrere Meldungskästen können angezeigt werden, nachdem Sie die Anwendung starten. Um nicht freigegebenen Zugang zur Anwendung zu verhindern, müssen Sie innerhalb drei Minuten durch diese Nachrichtenfenster wechseln. Sonst werden Sie aufgefordert, die Anwendung erneut zu starten.

   ANMERKUNG: Wenn ein oder mehrere Fenster **Sicherheitswarnung** in den folgenden Schritten eingeblendet werden, lesen Sie die Informationen im jeweiligen Fenster und klicken Sie auf **Ja**, um fortzufahren.

   Die Verwaltungsstation wird mit dem DRAC 5 verbunden und der Desktop des Remote Systems erscheint in der Dell Digital-KVM Viewer-Anwendung.

5. Wenn zwei Mauszeiger auf dem Desktop des Remote Systems angezeigt werden, synchronisieren Sie die Mauszeiger auf der Verwaltungsstation und dem Remote-System. Siehe "Mauszeiger synchronisieren".

Lokaler Video deaktivieren oder aktivieren

Um lokaler Video zu deaktivieren oder zu aktivieren, führen Sie das folgende Verfahren aus:

1. Öffnen Sie einen unterstützten Internetbrowser auf der Verwaltungsstation und melden Sie sich am DRAC 5 an. "Zugriff auf die webbasierte Schnittstelle" enthält weitere Informationen.

2. In der **System**struktur klicken Sie auf **System**.

3. Klicken Sie auf das Register **Konsole** und dann auf **Konfiguration**.

4. Wenn Sie lokaler Video auf dem Server aktivieren wollen (EINschalten), wählen Sie auf der Seite **Konfiguration der Konsolenumleitung** das Kontrollkästchen **Lokales Server-Video aktiviert** aus und klicken Sie dann auf **Änderungen anwenden**. Der Standardwert ist EIN.

5. Wenn Sie lokaler Video auf dem Server deaktivieren wollen (AUSschalten), wählen Sie auf der Seite **Konfiguration der Konsolenumleitung** das Kontrollkästchen **Lokales Server-Video aktiviert** ab und klicken Sie dann auf **Änderungen anwenden**.

Die Seite **Konsolenumleitung** zeigt den Status des lokalen Server-Videos an.

ANMERKUNG: Die Funktion lokaler Server-Video aktiviert wird auf allen x9xx PowerEdge-Systemen, außer PowerEdge SC1435 und 6950, unterstützt.

ANMERKUNG: Wenn lokaler Video auf dem Server deaktiviert wird (AUSschalten), wird nur der an den lokalen Server angeschlossene Monitor deaktiviert.

Video Viewer verwenden

Der Video Viewer enthält eine Benutzerschnittstelle zwischen der Verwaltungsstation und dem Remote-System, wodurch der Desktop des Remote-Systems sichtbar wird und die Maus-und Tastaturfunktionen von der Verwaltungsstation gesteuert werden können. Wenn Sie eine Verbindung zum Remote-System erstellen, wird der Video Viewer in einem eigenen Fenster gestartet.

Der Video Viewer enthält verschiedene Steuerungseinstellungen wie Videokalibrierung, Mausbeschleunigung und Snapshots. Klicken Sie auf **Hilfe**, um weitere Informationen über diese Funktionen zu erhalten.

Wenn Sie eine Konsolenumleitungssitzung beginnen und das Fenster des Video Viewers angezeigt wird, können Sie aufgefordert werden, die folgenden Steuerelemente zu regulieren, um das Remote-System ordnungsgemäß ansehen und steuern zu können. Diese Einstellungen umfassen:

- Zugriff auf die Viewer-Menüleiste
- Einstellung der Videoqualität
- Synchronisieren der Mauszeiger

Zugriff auf die Viewer-Menüleiste

Die Viewer-Menüleiste ist eine versteckte Menüleiste. Um auf die Menüleiste zuzugreifen, bewegen Sie Ihren Cursor im Desktop-Fenster des Viewers zur Mitte des oberen Rands.

Die Menüleiste kann außerdem aktiviert werden, indem Sie die Standard-Funktionstaste <F9> drücken. Um diese Funktionstaste einer neuen Funktion zuzuweisen, führen Sie folgende Schritte aus:

1. Drücken Sie auf <F9>, oder bewegen Sie den Maus-Cursor zum oberen Ende des Video Viewers.
2. Drücken Sie auf die "Reißzwecke", um die Viewer-Menüleiste zu sperren.
3. Klicken Sie in der Viewer-Menüleiste auf **Extras**, und wählen Sie **Sitzungsoptionen aus.**
4. Im Fenster **Sitzungsoptionen** klicken Sie auf das Register **Allgemein**.
5. Im Fenster des Registers **Allgemein** im Feld **Menüaktivierungstastenanschlag** klicken Sie auf das Drop-Down-Menü und wählen eine andere Funktionstaste aus.
6. Klicken Sie auf **Anwenden** und dann auf **OK**.

Tabelle 7-6 enthält die Hauptfunktionen, die in der Viewer-Menüleiste für den Gebrauch verfügbar sind.

Tabelle 7-6. Auswahlmöglichkeiten auf der Viewer-Menüleiste

Menüartikel	Artikel	Beschreibung
Datei	Capture zur Datei	Erfasst den aktuellen Remote-System-Bildschirm in einer **.bmp** (Windows) oder **.png** (Linux) -Datei auf dem lokalen System. Ein Dialogfeld wird angezeigt, in dem Sie die Datei zu einem angegebenen Standort speichern können.
	Beenden	Beendet die Seite **Konsolenumleitung.**
Ansicht	Aktualisieren	Aktualisiert den kompletten Remote-Systembildschirm-Viewport.
	Vollbildschirm	Erweitert den Sitzungsbildschirm von einem Fenster zum Vollbildschirm.
Makros	Verschiedene Tastenkombinationen	Führt eine Tastenanschlag-Kombination auf dem Remote-System aus. Um die Tastatur der Verwaltungsstation an das Remote-System anzuschließen und ein Makro auszuführen, führen Sie die folgenden Schritte aus: 1. Auf **Hilfsprogramme** klicken. 2. Im Fenster **Sitzungsoptionen** klicken Sie auf das Register **Allgemein**. 3. Wählen Sie **Alle Tastenanschläge ans Ziel weitergeben**. 4. Klicken Sie auf **OK.** 5. Klicken Sie auf **Makros**. 6. Im **Makros**-Menü klicken Sie auf eine Tastenanschlag-Kombination zur Ausführung auf dem Zielsystem.
Hilfsprogramme	Automatische Videoanpassung	Kalibriert die Session Viewer-Videoausgabe neu.
	Manuelle Video-Einstellung	Enthält einzelne Steuerungen zur manuellen Einstellung der Videoausgabe des Session Viewers. **ANMERKUNG:** Wird die horizontale Position unmittig eingestellt, führt dies zu einer Desynchronisation der Mauszeiger.
	Sitzungsoptionen	Bietet zusätzliche Session Viewer-Steuerungseinstellungen. Das **Maus**-Register ermöglicht die Auswahl des verwendeten Betriebssystems zur Optimierung der Konsolenumleitung-Mausleistung. **Windows**, **Linux** oder **Keine** auswählen. Das Register **Allgemein** enthält die folgenden Optionen: - **Tastatur-Durchreichmodus-** Wählen Sie **Alle Tastenanschläge ans Ziel weitergeben**, um die Tastenanschläge der Verwaltungsstation zum Remote-System weiterzugeben. - **Menüaktivierungstastenanschlag** - Wählt die Funktionstaste aus, mit der die Viewer-Menüleiste aktiviert wird. Mit dem **Symbolleistenregister** können Sie die **Symbolleistenausblendverzögerung** auf zwischen 1 und 10 Sekunden einstellen.
Hilfe	-	Aktiviert das **Hilfe**-Menü.

Einstellung der Videoqualität

Der Video Viewer enthält Videoeinstellungen, mit denen Sie das Video auf die bestmögliche Ansicht optimieren können. Klicken Sie auf **Hilfe**, um weitere Informationen zu erhalten.

Um die Videoqualität automatisch einzustellen, führen Sie die folgenden Schritte aus:

1. Greifen Sie auf die Viewer-Menüleiste zu. Siehe "Zugriff auf die Viewer-Menüleiste".

2. Klicken Sie auf **Hilfsprogramme** und wählen Sie **Automatische Bildregulierung**.

   Die Videoqualität wird neu kalibriert, und der Session Viewer wird wieder angezeigt.

Zur manuellen Einstellung der Videoqualität führen Sie die folgenden Schritte aus:

1. Greifen Sie auf die Viewer-Menüleiste zu. Siehe "Zugriff auf die Viewer-Menüleiste".
2. Klicken Sie auf **Hilfsprogramme** und wählen Sie **Manuelle Bildregulierung**.
3. Klicken Sie im Fenster **Videoeinstellung** auf jede Videoeinstellungsschaltfläche und justieren Sie die Steuerungen nach Bedarf.

Wenn Sie die Videoqualität von Hand einstellen, sind die folgenden Richtlinien einzuhalten:

- Um zu verhindern, dass die Mauszeiger ihre Synchronizität verlieren, justieren Sie die horizontale Einstellung so, dass der Desktop des Remote-Systems im Sitzungsfenster zentriert ist.
- Wenn das Pixel-Rauschverhältnis auf Null gesetzt wird, führt dies zu mehrfachen Videoauffrischungsbefehlen, die übermäßigen Netzwerk-Verkehr und flackerndes Video im Video Viewer-Fenster verursachen. Dell empfiehlt, dass Sie die Einstellung des Pixel/Rauschen-Verhältnisses auf eine Stufe setzen, die optimale Systemleistung und Pixel-Verfeinerung bei minimalem Netzwerkaufkommen bietet.

Synchronisieren der Mauszeiger

Wenn Sie eine Verbindung zu einem PowerEdge Remote-System mittels Konsolenumleitung aufbauen, ist die Mausbeschleunigungsgeschwindigkeit auf dem Remote System u. U. nicht synchron mit dem Mauszeiger auf der Verwaltungsstation, was dazu führt, dass zwei Mauszeiger im Video Viewer-Fenster sichtbar sind.

Um die Mauszeiger zu synchronisieren, führen Sie die folgenden Schritte aus.

1. Greifen Sie auf die Viewer-Menüleiste zu. Siehe "Zugriff auf die Viewer-Menüleiste".
2. Klicken Sie auf **Hilfsprogramme** und wählen Sie **Sitzungsoptionen**.
3. Klicken Sie auf das **Maus**-Register, wählen Sie das Betriebssystem der Verwaltungsstation und klicken Sie auf **OK**.
4. Klicken Sie auf **Hilfsprogramme** und wählen Sie **Manuelle Bildregulierung**.
5. Justieren Sie die horizontalen Steuerungen so, dass der Desktop des Remote-Systems im Sitzungsfenster zentriert ist.
6. Klicken Sie auf **OK.**

Wenn Sie Linux (Red Hat® oder Novell®) verwenden, werden die standardmäßigen Mauseinstellungen des Betriebssystems verwendet, um den Maus-Pfeil im DRAC 5-Konsolenumleitungsbildschirm zu steuern.

ANMERKUNG: Auf Linux (Red Hat oder Novell)-Systemen gibt es bekannte Maus-Pfeil-Synchronisationsprobleme. Um Synchronisationsprobleme der Maus zu minimieren, stellen Sie sicher, dass alle Benutzer die standardmäßigen Mauseinstellungen verwenden.

Häufig gestellte Fragen

Tabelle 7-7 führt häufig gestellte Fragen und Antworten auf.

Tabelle 7-7. Konsolenumleitung verwenden: Häufig gestellte Fragen

Frage	Antwort
Kann eine neue Remote-Konsole-Videositzung begonnen werden, wenn der lokale Video auf dem Server AUSgeschaltet wird?	Ja.
Warum dauert es 15 Sekunden, um den lokalen Video auf dem Server AUSzuschalten, nachdem angefragt wurde, lokaler Video AUSzuschalten?	Es gibt einem lokalen Benutzer eine Gelegenheit, jede Maßnahme durchzuführen, bevor der Video AUSgeschaltet wird.
Gibt es eine Zeitverzögerung, wenn lokaler Video EINgeschaltet wird?	Nein, sobald eine Anfrage von DRAC 5 erhalten wurde, dass lokaler Video EINgeschaltet werden soll, wird der Video sofort EINgeschaltet.
Kann der lokale Benutzer auch den Video AUSschalten?	Ja, ein lokaler Benutzer kann racadm CLI (lokal) verwenden, um den Video AUSzuschalten.
Kann der lokale Benutzer auch den Video EINschalten?	Ja, der Benutzer sollte racadm CLI auf dem Server installiert haben, und nur wenn der Benutzer in der Lage ist, den Server über eine RDP-Verbindung, wie Terminaldienste, Telnet oder SSH zu erreichen. Der Benutzer kann sich dann am Server anmelden und racadm (lokal) ausführen, um den Video EINzuschalten.
Mein lokaler Video wird AUSgeschaltet und aus irgendeinem Grund ist mein DRAC 5 im Remote-Zugriff nicht zugänglich, und der Server kann nicht auf RDP, Telnet oder SSH zugreifen. Wie stelle ich den lokalen Video wiederher?	Der einzige Weg, den lokalen Video wiederherzustellen, ist in diesem Fall, das Netzstromkabel vom Server zu entfernen, den Kriechstrom des Servers abzuleiten und das Netzstromkabel wieder anzuschließen; das wird den lokalen Video auf den Server-Monitor zurückbringen. Außerdem wird die DRAC 5-Konfiguration zu lokaler Video EIN (Standardeinstellung) geändert. Der DRAC 5 muss neu konfiguriert werden, wenn der lokale Video wieder AUSgeschaltet werden muss.

Werden die lokale Tastatur und Maus auch AUSgeschaltet, wenn der lokale Video AUSgeschaltet wird?	Nein, wenn der lokale Video AUSgeschaltet wird, wird nur der Video AUSgeschaltet, der vom Server-Monitor-Ausgabe-Konnektor kommt; er wird *nicht* die Tastatur und Maus ausschalten, die lokal mit dem Server verbunden sind.
Wird der Video auf der Remote vKVM-Sitzung ausgeschaltet, wenn der lokaler Server-Video ausgeschaltet wird?	Nein, denn das EIN- und AUSschalten des lokalen Videos ist unabhängig von der Remote-Konsole-Sitzung.
Welche Berechtigungen sind für einen DRAC 5-Benutzer erforderlich, um den lokalen Server-Video EIN- oder AUSzuschalten?	Jeder Benutzer mit DRAC 5-Konfigurationsberechtigungen kann den lokalen Server-Video EIN- oder AUSschalten.
Wie kann ich den aktuellen Status des lokalen Server-Videos erhalten?	Der Status wird auf der Seite **Konfiguration der Konsolenumleitung** der DRAC 5-webbasierten Schnittstelle angezeigt. Der racadm CLI-Befehl racadm getconfig –g cfgRacTuning zeigt den Status im Objekt cfgRacTuneLocalServerVideo an. Der Status wird auch vom lokalen Benutzer auf dem Server-LCD-Bildschirm als "Video AUS" oder als "Video AUS in 15" gesehen.
Warum sehe ich manchmal nicht den Status "Video AUS" oder "Video AUS in 15" auf dem Server-LCD-Bildschirm?	Der lokale Videostatus ist eine Meldung mit niedriger Priorität und wird maskiert, wenn ein Server-Ereignis mit hoher Priorität aufgetreten ist. Die LCD-Meldungen basieren auf Priorität; Sie müssen jegliche LCD-Meldungen mit hoher Priorität lösen, und sobald dieses Ereignis gelöscht oder gelöst ist, wird die nächste Meldung mit niedriger Priorität angezeigt.Die Server-Video-Meldung auf dem LCD-Bildschirm ist in der Natur informatorisch.
Wo kann ich mehr Informationen über die Funktion des lokalen Server-Videos bekommen?	Es wird ein weißes Papier geben, das diese Funktion auf der Dell Support-Website, die unter **support.dell.com** zu finden ist, behandelt.
Ich sehe Videoverfälschung auf meinem Bildschirm. Wie kann ich dieses Problem beheben?	Klicken Sie im Fenster **Konsolenumleitung** auf **Aktualisieren**, um den Bildschirm aufzufrischen. **ANMERKUNG:** Es ist u. U. erforderlich, mehrmals auf **Aktualisieren** zu klicken, bis die Videoverfälschung korrigiert ist.
Während der Konsolenumleitung wurden Tastatur und Maus nach der Rückkehr aus dem Schlafmodus auf einem Windows 2000-System verriegelt. Wodurch wurde dies verursacht?	Um dieses Problem zu lösen, müssen Sie einen Reset des DRAC 5 durchführen indem Sie den Befehl **racadm racreset** ausführen.
Ich kann vom Konsolenumleitungsfenster aus die Unterseite des Systembildschirms nicht sehen.	Stellen Sie sicher, dass die Monitorauflösung der Verwaltungsstation auf 1280x1024 eingestellt ist.
Während der Konsolenumleitung wurde die Maus nach der Rückkehr aus dem Schlafmodus auf einem Windows 2000-System verriegelt. Warum geschah dies?	Um dieses Problem zu lösen, wählen Sie ein anderes Betriebssystem als Windows für die Mausbeschleunigung aus dem virtuellen KVM (vKVM)-Pulldown-Menüfenster aus, warten Sie 5 bis 10 Sekunden und wählen Sie Windows erneut. Wenn das Problem noch immer nicht gelöst ist, müssen Sie einen Reset des DRAC 5 durchführen, indem Sie den Befehl **racadm racreset** ausführen. Wenn das Problem noch immer nicht gelöst ist, müssen Sie einen Reset des DRAC 5 durchführen, indem Sie den Befehl **racadm racreset hard** ausführen.
Warum funktioniert die vKVM-Tastatur und der Maus-Mechanismus nicht?	Sie müssen den USB-Controller auf **On with BIOS support (BIOS-Unterstützung ein)** in den BIOS-Einstellungen des verwalteten Systems einstellen. Starten Sie das verwaltete System erneut und drücken Sie <F2>, um Setup einzugeben. Wählen Sie **Integrated Devices (Integrierte Geräte)**, und dann wählen Sie **USB Controller (USB-Controller)**. Speichern Sie Ihre Änderungen, und starten Sie das System neu.
Warum wird der Konsolenbildschirm des verwalteten Systems ausgeblendet, wenn Windows einen blauen Bildschirm hat?	Das verwaltete System hat nicht den richtigen ATI-Videotreiber. Sie müssen den Videotreiber mit Hilfe der *Dell PowerEdge Installation and Server Management* CD aktualisieren.
Warum bekomme ich einen leeren Schirm auf der Remote-Konsole nach dem Beenden einer Windows 2000-Installation?	Das verwaltete System hat nicht den richtigen ATI-Videotreiber. Die DRAC 5-Konsolenumleitung läuft nicht ordnungsgemäß mit einem SVGA Videotreiber von der Windows 2000-Vertriebs-CD. Sie müssen Windows 2000 mit Hilfe der *Dell PowerEdge Installation and Server Management* CD installieren, um sicherzustellen, dass Sie die spätesten, unterstützten Treiber für das verwaltete System haben.
Warum bekomme ich einen leeren Bildschirm auf dem verwalteten System, wenn das Windows 2000-Betriebssystem lädt?	Das verwaltete System hat nicht den richtigen ATI-Videotreiber. Sie müssen den Videotreiber mit Hilfe der *Dell PowerEdge Installation and Server Management* CD aktualisieren.
Warum bekomme ich einen leeren Bildschirm auf dem verwalteten System im Windows-Vollbild-DOS-Fenster?	Das verwaltete System hat nicht den richtigen ATI-Videotreiber. Sie müssen den Videotreiber mit Hilfe der *Dell PowerEdge Installation and Server Management* CD aktualisieren.
Warum kann ich nicht deb BIOS-Setup eingeben, indem ich die <F2> Taste drücke?	Dieses Verhalten ist in einer Windows-Umgebung typisch. Verwenden Sie Ihre Maus, um auf einen Bereich des Konsolenumleitungsfensters zu klicken, um den Fokus zu regulieren. Um den Fokus zum untersten Menübalken des Konsolenumleitungsfensters zu bewegen, verwenden Sie die Maus und klicken Sie eins der Objekte auf dem untersten Menübalken.
Warum synchronisiert die vKVM-Maus nicht, wenn ich die *Dell PowerEdge Installation and Server Management* CD verwende um das Betriebssystem im Remote-Zugriff installieren?	Konsolenumleitung für das auf dem Zielsystem ausführende Betriebssystem konfigurieren. 1. Klicken Sie im vKVM-Symbolleisten-Menü auf **Hilfsprogramme** und wählen Sie **Sitzungsoptionen**. 2. Im Fenster **Sitzungsoptionen** klicken Sie auf das Register **Maus**. 3. Im Feld **Mausbeschleunigung** wählen Sie das Betriebssystem aus, das auf dem Zielsystem ausführt und klicken Sie auf **OK**.
Warum synchronisiert die vKVM-Maus nicht, nachdem sie aus dem Energiesparmodus "Hibernation" auf einem Windows-System zurückkommt?	Wählen Sie ein anderes Betriebssystem für die Mausbeschleunigung aus dem Pulldown-Menü des vKVM-Fensters. Dann kehren Sie zum ursprünglichen Betriebssystem zurück, um die USB-Maus zu initialisieren. 1. Klicken Sie in der vKVM-Symbolleiste auf **Hilfsprogramme** und wählen Sie **Sitzungsoptionen**. 2. Im Fenster **Sitzungsoptionen** klicken Sie auf das Register **Maus**. 3. Im Feld **Mausbeschleunigung** wählen Sie ein anderes Betriebssystem und klicken Sie auf **OK**. 4. Initialisieren Sie die USB-Maus.
Warum synchronisiert die Maus nicht in DOS, wenn die Konsolenumleitung ausgeführt wird?	Der Dell BIOS emuliert den Maustreiber als PS/2-Maus. Die PS/2-Maus verwendet Relativposition für den Mauszeiger, welches die Verzögerung in der Synchronisation verursacht. DRAC 5 hat einen USB Maus-Treiber, der absolute Position und das nähere Verfolgen des Mauszeigers erlaubt. Selbst wenn der DRAC 5 die USB absolute Mausposition zum Dell BIOS durchführt, würde die BIOS-Emulation sie zurück zur Relativposition umwandeln und das Verhalten würde gleichbleiben.
Warum synchronisiert die Maus nicht unter der	Virtueller KVM erfordert den USB Maus-Treiber, aber der USB Maus-Treiber ist nur unter dem X-

Textkonsole von Linux?	Windows-Betriebssystem verfügbar.
Ich habe immer noch Probleme mit der Maus-Synchronisation.	Stellen Sie sicher, dass der Zielsystem-Desktop im Konsolenumleitungsfenster zentriert ist. 1. Klicken Sie in der vKVM-Symbolleiste auf **Hilfsprogramme** und wählen Sie **Manuelle Video-Einstellung**. 2. Justieren Sie die horizontalen und vertikalen Steuerungen wie erforderlich, um den Desktop im Konsolenumleitungsfenster auszurichten. 3. Klicken Sie auf **Schließen**. 4. Bewegen Sie den Zielsystem-Mauszeiger in die linke obere Ecke des Konsolenumleitungsfensters und dann zurück in die Mitte des Fensters. 5. Wiederholen Sie Schritt 2 bis Schritt 4, bis beide Cursor synchronisiert sind.
Warum funktioniert die vKVM-Maus und Tastatur nicht, wenn die Mausbeschleunigung für verschiedene Betriebssysteme geändert wird?	Die USB-vKVM-Tastatur und -Maus sind von 5 bis 10 Sekunden nach dem Ändern der Mausbeschleunigung untätig. Durch die Netzwerklast kann manchmal diese Operation veranlassen, länger zu dauern als sonst (mehr als 10 Sekunden).
Warum kann ich nicht den Boden des Server-Bildschirms des vKVM-Fensters sehen?	Stellen Sie sicher, dass die Server-Bildschirmauflösung 1280 x 1024 Pixel bei 60 Hz mit 128 Farben ist.
Warum kann ich keine Tastatur oder Maus verwenden, während ich ein Microsoft® Betriebssystem mittels DRAC 5-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 **OK** entweder auf dem lokalen System auswählen oder das im Remote-Zugriff verwaltete System neustarten, neu installieren und dann die Konsolenumleitung im BIOS abschalten. Diese Nachricht wird durch Microsoft erstellt, um den Benutzer zu alarmieren, dass Konsolenumleitung aktiviert ist. Um sicherzustellen, dass diese Meldung nicht erscheint, schalten Sie die Konsolenumleitung im BIOS immer aus, bevor Sie ein Betriebssystem im Remote-Zugriff installieren.
Konsolenumleitung zeigt das Betriebssystem-Startmenü nicht in der chinesischen, japanischen und koreanischen Version von Microsoft Windows 2000.	Um dieses Problem auf Systemen zu beheben, auf denen Windows 2000 ausgeführt wird, das zu mehreren Betriebssystemen starten kann, ändern Sie das Standardstartbetriebssystem, indem sie die folgenden Schritte ausführen: 1. Klicken Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz** und wählen Sie **Eigenschaften.** 2. Klicken Sie auf das Register **Erweitert**. 3. Klicken Sie auf **Autostart und Wiederherstellung**. 4. Wählen Sie das neue Standardbetriebssystem aus der Liste **Autostart** aus. 5. In der Liste **Anzeigen** für den Kasten, geben Sie die Anzahl von Sekunden an, für die die Liste von Auswahlen angezeigt werden sollte, bevor das Standardbetriebssystem automatisch gestartet wird.
Warum zeigt der Num Lock-Anzeiger auf meiner Verwaltungsstation nicht den Status des Num Lock auf dem Remote-Server an?	Wenn über den DRAC 5 zugegriffen wird, stimmt der Num Lock-Anzeiger auf der Verwaltungsstation nicht unbedingt mit dem Zustand des Num Lock auf dem Remote-Server überein. Der Zustand von Num Lock ist von der Einstellung auf dem Remote-Server abhängig, wenn die Remote-Sitzung unabhängig vom Zustand des Num Lock auf der Verwaltungsstation verbunden wird.
Warum erscheinen viele Session Viewer-Fenster, wenn ich eine Konsolenumleitungssitzung aufbaue?	Sie konfigurieren eine Konsolenumleitungssitzung zum lokalen System. Konfigurieren Sie die Sitzung zu einem Remote-System.
Erhalte ich eine Warnungsmeldung, wenn ich eine Konsolenumleitungssitzung ausführe und ein lokaler Benutzer auf das Remote-System zugreift?	Nein Wenn ein lokaler Benutzer auf das System zugreift, kann er/sie Ihre Maßnahmen ohne Warnung überschreiben.
Welche Bandbreite brauche ich für eine Konsolenumleitungssitzung?	Dell empfiehlt eine 5 MB/s-Verbindung für gute Leistung. Eine 1 MB/s-Verbindung ist die vorgeschriebene Mindestleistung.
Was sind die Mindestsystemanforderungen für meine Verwaltungsstation für die Ausführung der Konsolenumleitung?	Die Verwaltungsstation erfordert einen Intel Pentium III 500-MHz-Prozessor mit mindestens 256 MB RAM.
Wie viele Konsolenumleitungssitzungen kann ich maximal auf einem Remote-System ausführen?	Der DRAC 5 unterstützt bis zu zwei gleichzeitige Konsolenumleitungssitzungen.
Warum habe ich Maus-Synchronisationsprobleme?	Auf Linux (Red Hat oder Novell)-Systemen gibt es bekannte Maus-Pfeil-Synchronisationsprobleme. Um Synchronisationsprobleme der Maus zu minimieren, stellen Sie sicher, dass alle Benutzer die standardmäßigen Mauseinstellungen verwenden.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Virtuellen Datenträger verwenden und konfigurieren

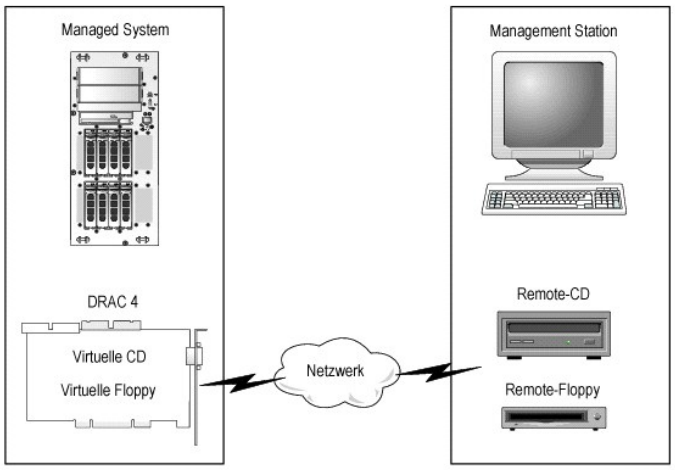
Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

---

Übersicht

Die Funktion Virtueller Datenträger enthält das verwaltete System mit einem virtuellen CD-Laufwerk, das Standarddatenträger von jeder Stelle auf dem Netzwerk verwenden kann. Abbildung 8-1 zeigt die gesamte Architektur des virtuellen Datenträgers.

Abbildung 8-1. Gesamte Architektur des virtuellen Datenträgers



Mit dem virtuellen Datenträger können Administratoren im Remote-Zugriff verwaltete Systeme starten, Anwendungen installieren, Treiber aktualisieren oder sogar neue Betriebssysteme im Remote-Zugriff von virtuellen CD/DVD und Diskettenlaufwerken installieren.

ANMERKUNG: Virtuelle Datenträger erfordern eine minimale verfügbare Netzwerkbandbreite von 128 Kbps.

Das verwaltete System wird mit einer DRAC 5-Karte konfiguriert. Die virtuellen CD- und Disketten-Laufwerke sind zwei elektronische Geräte, die im DRAC 5 eingebettet sind und die durch die DRAC 5 Firmware gesteuert werden. Diese zwei Geräte sind auf dem Betriebssystem des verwalteten Systems und BIOS zu jeder Zeit gegenwärtig, ob ein virtueller Datenträger verbunden ist oder nicht.

Die Verwaltungsstation enthält die physischen Datenträger oder Bilddatei über das Netzwerk. Wenn Sie den RAC Browser zum ersten Mal starten und Sie auf die Seite des virtuellen Datenträgers zugreifen, wird das Plug-In des virtuellen Datenträgers vom DRAC 5-Webserver heruntergeladen und wird auf der Verwaltungsstation automatisch installiert. Damit die Virtual Media-Funktion funktioniert, muss das Plug-In des virtuellen Datenträgers auf der Verwaltungsstation installiert werden.

Wenn der virtuelle Datenträger verbunden wird, werden alle virtuellen Zugriffsaufforderungen des CD-/Disketten-Laufwerks vom verwalteten System zur Verwaltungsstation durch das Netzwerk geleitet. Die Verbindung eines virtuellen Datenträgers ist identisch mit dem Einfügen von Datenträgern in virtuelle Geräte. Wenn der virtuelle Datenträger nicht verbunden ist, verhalten sich virtuelle Geräte auf dem verwalteten System wie zwei Laufwerke ohne Datenträger.

Tabelle 8-1 enthält die unterstützten Laufwerk-Verbindungen für virtuelle Disketten- und virtuelle optische Laufwerke.

ANMERKUNG: Werden virtuelle Datenträger geändert, während sie verbunden sind, kann dies die Systemstartsequenz anhalten.

Tabelle 8-1. Unterstützte Laufwerk-Verbindungen

Unterstützte Virtuelle Diskettenlaufwerk-Verbindungen	Unterstützte Virtuelle Optische Laufwerk-Verbindungen
Legacy 1.44 Diskettenlaufwerk mit einer 1.44 Diskette	CD-ROM, DVD, CDRW, Kombinationslaufwerk mit CD-ROM-Datenträger
USB-Diskettenlaufwerk mit einer 1.44 Diskette	CD-ROM-Abbilddatei im ISO9660-Format
1.44 Diskettenabbild	USB-CD-ROM-Laufwerk mit CD-ROM-Datenträger.

Virtual Media-Plug-In installieren

Zur Verwendung der Virtual Media-Funktion muss das Plug-In des virtuellen Datenträger-Browsers auf der Verwaltungsstation installiert werden. Nachdem Sie die DRAC 5-Benutzeroberfläche öffnen und die Seite des Virtuellen Datenträgers starten, lädt der Browser automatisch das Plug-In herunter, falls erforderlich. Wenn das Plug-In erfolgreich installiert ist, zeigt die Seite des virtuellen Datenträgers eine Liste von Disketten und CDs an, mit denen das virtuelle Laufwerk verbunden ist.

Windows-basierte Verwaltungsstation

Um die Funktion des virtuellen Datenträgers auf einer Verwaltungsstation mit Microsoft Windows-Betriebssystem auszuführen, installieren Sie eine unterstützte Internet Explorer-Version mit dem ActiveX-Steuerung-Plug-In. Setzen Sie die Browsersicherheit auf **Mittel** oder eine niedrigere Einstellung, damit der Internet Explorer signierte ActiveX-Steuerungen herunterladen und installieren kann.

Weitere Informationen finden Sie in "Unterstützte Internetbrowser".

Darüber hinaus müssen Sie Administratorberechtigungen auf Windows-Systemen haben, um die Virtueller Datenträger-Funktion zu installieren und zu verwenden. Vor der Installation der ActiveX-Steuerung kann Internet Explorer eine Sicherheitswarnung zeigen. Um das Installationsverfahren für ActiveX Control abzuschließen, akzeptieren Sie die ActiveX Control, wenn Internet Explorer Sie mit einer Sicherheitswarnung dazu auffordert.

Linux-basierte Verwaltungsstation

Um die Funktion des virtuellen Datenträgers auf einer Verwaltungsstation mit Linux-Betriebssystem auszuführen, installieren Sie eine unterstützte Version von Mozilla oder Firefox. Wenn das virtueller Datenträger-Plug-In nicht installiert ist, oder wenn eine neuere Version verfügbar ist, wird während des Installationsverfahrens ein Dialogfeld eingeblendet, um die Plug-In-Installation auf der Verwaltungsstation zu bestätigen. Stellen Sie sicher, dass die Benutzer-ID, die den Browser ausführt, hat, in der Verzeichnisstruktur des Browser Schreibberechtigung hat. Wenn die Benutzer-ID keine Schreibberechtigung hat, können Sie das Plug-In des virtuellen Datenträgers nicht installieren.

Weitere Informationen finden Sie in "Unterstützte Internetbrowser".

Virtuellen Datenträger ausführen

HINWEIS: Geben Sie keinen **racreset** Befehl, wenn Sie eine Virtueller Datenträger-Sitzung ausführen. Ansonsten können unerwünschte Ergebnisse einschließlich Datenverlust vorkommen.

Mit dem virtuellen Datenträger können Sie ein Diskettenabbild oder Laufwerk "virtualisieren", wodurch ein Diskettenabbild, Diskettenlaufwerk oder optisches Laufwerk auf der Verwaltungskonsole ein verfügbares Laufwerk auf dem Remote-System werden kann.

Unterstützte Virtueller Datenträger-Konfigurationen

Sie können den Virtuellen Datenträger für ein Diskettenlaufwerk und ein optisches Laufwerk aktivieren. Nur ein Laufwerk für jeden Datenträgertyp kann auf einmal virtualisiert werden.

Unterstützte Diskettenlaufwerke umfassen ein Diskettenabbild oder ein verfügbares Diskettenlaufwerk. Unterstützte optische Laufwerke umfassen maximal ein verfügbares optisches Laufwerk oder eine ISO-Abbilddatei.

Virtuellen Datenträger mittels der Internet-Benutzeroberfläche ausführen

Virtuellen Datenträger verbinden

1. Öffnen Sie einen unterstützten Webbrowser auf Ihrer Verwaltungsstation. Siehe "Unterstützte Internetbrowser".

Konsolenumleitung und Virtueller Datenträger unterstützen nur 32-Bit Internetbrowser. Das Verwenden von 64-Bit-Internet-Browsern kann zu unerwarteten Ergebnissen oder einem Fehlschlagen von Vorgängen führen.

2. Verbinden Sie mit DRAC 5 und melden Sie sich an. "Zugriff auf die webbasierte Schnittstelle" enthält weitere Informationen.

3. Klicken Sie auf das Register **Datenträger** und dann auf **Virtueller Datenträger**.

   Die Seite **Virtueller Datenträger** wird mit den Client-Laufwerken eingeblendet, die virtualisiert sein können.

   ANMERKUNG: Die **Disketten-Abbilddatei** unter **Diskettenlaufwerk** (wenn anwendbar) kann erscheinen, da dieses Gerät als virtuelle Diskette virtualisiert sein kann. Sie können ein optisches Laufwerk und eine Floppy gleichzeitig oder ein einzelnes Laufwerk auswählen.

   ANMERKUNG: Die Laufwerksbuchstaben des virtuellen Geräts auf dem verwalteten System entsprechen nicht den physischen Laufwerksbuchstaben auf der Verwaltungsstation.

4. Wenn dazu aufgefordert, folgen Sie den Bildschirmanleitungen, zum Installieren des Plug-In des virtuellen Datenträgers.

5. Im **Attribut**-Kasten führen Sie die folgenden Schritte aus:

   a. Stellen Sie sicher, dass in der Spalte **Wert** der Statuswert **Verbinden / Abtrennen Verbunden ist**.

   Wenn der Wert **Abgetrennt** ist, sind die folgenden Schritte auszuführen:

   - Klicken Sie im Register **Datenträger** auf **Konfiguration**.
   - Stellen Sie sicher, dass in der Spalte **Wert** das Kontrollkästchen **Virtuellen Datenträger verbinden** ausgewählt ist.
   - Klicken Sie auf **Änderungen anwenden**.
   - Im Register **Virtueller Datenträger** auf **Virtueller Datenträger** klicken.
   - Stellen Sie sicher, dass in der Spalte **Wert** der Statuswert **Verbinden / Abtrennen Verbunden ist**.

   - Stellen Sie sicher, dass **Aktueller Status Nicht angeschlossen** ist. Wenn das **Wert**-Feld 'verbunden' anzeigt, müssen Sie vom Image oder Laufwerk abtrennen, bevor sie wieder verbinden. Dieser Status zeigt nur den aktuellen Status der Verbindung des virtuellen Datenträgers auf der aktuellen webbasierten Schnittstelle an.
   - Stellen Sie sicher, dass der Wert **Aktive Sitzung Verfügbar** ist. Wenn das Feld **Wert In Verwendung** anzeigt, müssen Sie warten, dass die vorhandene Sitzung des virtuellen Datenträgers freigegeben wird, oder Sie beenden sie, indem Sie in das Register Sitzungsverwaltung unter Remote-Zugriff gehen und die aktive Sitzung des virtuellen Datenträgers beenden.Nur eine aktiver Sitzung des virtuellen Datenträgers wird auf einmal erlaubt. Diese Sitzung könnte von jeder webbasierten Schnittstelle oder jedem VM-CLI-Dienstprogramm erstellt worden sein.
   - Wählen Sie das Kontrollkästchen **Verschlüsselung aktiviert**, um eine verschlüsselte Verbindung zwischen dem Remote-System und Ihrer Verwaltungsstation (wenn gewünscht) herzustellen.

- Wenn Sie ein Disketten- oder ISO-Abbild virtualisieren, wählen Sie **Diskettenabbilddatei** oder **ISO-Abbilddatei** und geben Sie den Namen der Abbilddatei ein bzw. suchen Sie die Abbilddatei, die Sie virtualisieren wollen.

  Wenn Sie ein Diskettenlaufwerk oder ein optisches Laufwerk virtualisieren, wählen Sie die Schaltfläche neben den Laufwerken aus, die Sie virtualisieren wollen.

7. Klicken Sie auf **Verbinden**.

   Wenn die Verbindung authentifiziert wird, wechselt der Verbindungsstatus zu **Verbunden** und eine Liste aller verbundenen Laufwerke wird angezeigt. Alle verfügbaren Disketten-Images und Laufwerke, die Sie ausgewählt haben, werden verfügbar auf der Konsole des verwalteten Systems, als wären sie echte Laufwerke.

   ANMERKUNG: Der zugeordnete virtuelle Laufwerksbuchstabe (für Microsoft® Windows®- Systeme) oder die gerätespezifische Datei (für Linux-Systeme) kann nicht identisch mit dem Laufwerksbuchstaben auf Ihrer Verwaltungskonsole sein.

   ANMERKUNG: Virtueller Datenträger funktioniert auf Clients des Windows-Betriebssystems eventuell nicht korrekt, die mit Internet Explorer Enhanced Security konfiguriert sind. Um dieses Problem zu lösen, ziehen Sie die Dokumentation zu Ihrem Microsoft-Betriebssystem zurate oder setzen sich mit Ihrem Administratoren in Verbindung.

Virtuellen Datenträger unterbrechen

Klicken Sie auf **Unterbrechen**, um alle virtualisierten Abbilder und Laufwerke von der Verwaltungsstation zu trennen. **Alle** virtualisierten Abbilder oder Laufwerke werden unterbrochen und sind auf dem verwalteten System nicht mehr verfügbar.

Funktion des virtuellen Datenträgers verbinden und abtrennen

Die DRAC 5 Virtueller Datenträger-Funktion basiert auf der USB-Technologie und kann die USB-Plug-and-Play-Funktionen ausnutzen. DRAC 5 fügt die Option zum Verbinden und Unterbrechen der virtuellen Geräte vom USB-Bus hinzu. Wenn die Geräte abgetrennt werden, können Betriebssystem oder BIOS keine verbundenen Laufwerke sehen. Wenn die virtuellen Geräte verbunden sind, sind die Laufwerke sichtbar. Anders als beim DRAC 4, wo die Laufwerke nur mit dem nächsten System-Start aktiviert oder deaktiviert werden konnten, können DRAC-5 virtuelle Geräte jederzeit verbunden oder abgetrennt werden.

Die virtuellen Geräte können mit einem Webbrowser, lokalem racadm, Remote-racadm, Telnet, und seriellen Anschluss verbunden bzw. abgetrennt werden. Um den virtuellen Datenträger mithilfe eines Internetbrowsers zu konfigurieren, können Sie zur Seite **Datenträger** wechseln und dann zur Seite **Konfiguration**, wo Sie Einstellungsänderungen vornehmen und anwenden können. Sie können auch die **Schnittstellennummer für den virtuellen Datenträger** und die **SSL-Schnittstellennummer für den virtuellen Datenträger** angeben. Außerdem können Sie die Funktion **Virtual Flash** und **Einmal starten** aktivieren oder deaktivieren.

Den virtuellen Datenträger mithilfe des Internetbrowsers verbinden und abtrennen

Um die Funktion des virtuellen Datenträgers anzuhängen, führen Sie Folgendes aus:

1. Klicken Sie auf **System** -> **Datenträger** -> **Konfiguration**
2. Wählen Sie das Kontrollkästchen **Wert** für **Virtuellen Datenträger verbinden**
3. Klicken Sie auf **Änderungen anwenden**

Um die Funktion des virtuellen Datenträgers abzutrennen, führen Sie Folgendes aus:

1. Klicken Sie auf **System** -> **Datenträger** -> **Konfiguration**
2. Wählen Sie das Kontrollkästchen **Wert** für **Virtuellen Datenträger verbinden** ab
3. Klicken Sie auf **Änderungen anwenden**

Virtuelle Datenträger mithilfe von RACADM anhängen und abtrennen

Um die Funktion des virtuellen Datenträgers anzuhängen, öffnen Sie eine Eingabeaufforderung, geben den folgenden Befehl ein und drücken auf <Eingabe>:

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 1
```

Um die Funktion des virtuellen Datenträgers abzutrennen, öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie auf <Eingabe>:

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 0
```

Vom virtuellen Datenträger starten

Auf unterstützten Systemen ermöglicht das System-BIOS das Starten von virtuellen optischen Laufwerken oder von virtuellen Diskettenlaufwerken. Während des POST öffnen Sie das BIOS-Setup-Fenster und überprüfen Sie, dass 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 das verwaltete System.
2. Drücken Sie <F2>, um das BIOS Setup-Fenster einzugeben.
3. Rollen Sie zur Startsequenz und drücken Sie auf <Eingabe>.

   Im Popup-Fenster werden die virtuellen optischen Laufwerke und virtuellen Diskettenlaufwerke mit den Standardstartgeräten aufgeführt.
4. Stellen Sie sicher, dass das virtuelle Laufwerk aktiviert ist und als das erste Gerät mit startfähigem Datenträger aufgeführt wird. Falls erforderlich, folgen Sie den Bildschirmanleitungen zur Modifikation der Startreihenfolge.
5. Speichern Sie die Änderungen und beenden Sie.

   Das verwaltete System startet neu.

   Das verwaltete System versucht außerdem von einem startfähigen Gerät auf der Startsequenz basierend zu starten. Wenn ein virtuelles Gerät angeschlossen ist und startfähige Datenträger vorhanden sind, startet das System vom virtuellen Gerät. Ansonsten ignoriert das System das Gerät - ähnlich einem physischen Gerät ohne startfähige Datenträger.

Betriebssysteme mit Hilfe von virtuellen Datenträgern verwenden

In diesem Abschnitt wird eine manuelle, interaktive Methode zum Installieren des Betriebssystems auf der Verwaltungsstation beschrieben, die mehrere Stunden in Anspruch nehmen kann. Ein scripted Betriebssystem-Installationsverfahren mittels Virtuellem Datenträger kann weniger als 15 Minuten dauern. "Weitere Informationen finden Sie in "Betriebssystem mit VM-CLI bereitstellen".

1. Überprüfen Sie folgendes:
   - Die Betriebssystem-Installations-CD ist in das Verwaltungsstation-CD-Laufwerk eingelegt.
   - Das lokale CD-Laufwerk ist ausgewählt.
   - Sie sind mit den virtuellen Laufwerken verbunden.
2. Folgen Sie den Schritten zum Starten vom virtuellen Datenträger im Abschnitt "Vom virtuellen Datenträger starten", um sicherzustellen, dass der BIOS obendrein vom CD-Laufwerk eingestellt wird, von dem Sie installieren.
3. Folgen Sie den Bildschirmanleitungen, um die Installation abzuschließen.

Verwendung des virtuellen Datenträgers, wenn das Betriebssystem des Servers ausgeführt wird

Windows-basierte Systeme

Auf Windows-Systemen werden die virtuellen Datenträger-Laufwerke automatisch geladen und mit einem Laufwerksbuchstaben konfiguriert.

Verwendung der virtuellen Laufwerke von Windows ist der Verwendung Ihrer physischen Laufwerke ähnlich. Wenn Sie die Verbindung zu den Datenträgern an einer Verwaltungsstation aufbauen, sind die Datenträger am System verfügbar, indem man auf das Laufwerk klickt und dessen Inhalt durchsucht.

Linux-basierte Systeme

Auf Linux-Systemen werden die virtuellen Datenträger-Laufwerke nicht mit einem Laufwerksbuchstaben konfiguriert. Abhängig von der auf Ihrem System installierten Software dürfen die virtuellen Datenträger-Laufwerke nicht automatisch geladen werden. Wenn die Laufwerke nicht automatisch geladen werden, laden Sie die Laufwerke manuell.

Virtual Flash verwenden

Der DRAC 5 enthält beständigen Virtual Flash - einen 16 MB Flash-Speicher im DRAC 5-Dateisystem, der für beständige Speicherung verwendet und vom System zugegriffen werden kann. Bei Aktivierung wird Virtual Flash als ein drittes virtuelles Laufwerk konfiguriert und erscheint in der BIOS-Startreihenfolge, wodurch ein Benutzer vom Virtual Flash starten kann

ANMERKUNG: Um vom Virtual Flash zu starten, muss das Virtual Flash-Image ein startfähiges Abbild sein.

Anders als eine CD oder ein Diskettenlaufwerk, die eine externe Client-Verbindung oder ein funktionelles Gerät im Host-System erfordern, erfordert die Bereitstellung von Virtual Flash lediglich die beständige DRAC 5 Virtual Flash-Funktion. Die 16 MB des Flash-Speichers erscheinen als ein unformatiertes, abnehmbares USB-Laufwerk in der Host-Umgebung.

Verwenden Sie die folgenden Richtlinien, wenn Sie Virtual Flash bereitstellen:

- Durch das Verbinden oder Abtrennen des Virtual Flash wird eine USB-Umnumerierung ausgeführt, bei der alle Geräte des virtuellen Datenträgers verbunden und abgetrennt werden (Beispiel: CD-Laufwerk und Diskettenlaufwerk).
- Wenn Sie Virtual Flash aktivieren oder deaktivieren, ändert sich der Verbindungsstatus der CD/Diskettenlaufwerks des Virtuellen Datenträgers nicht.

HINWEIS: Die Verfahren zum Abtrennen und Verbinden stören die aktiven Lese- und Schreibvorgänge des Virtuellen Datenträgers.

Virtual Flash aktivieren

Um Virtual Flash zu aktivieren, öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgRacVirtual -o cfgVirMediaKeyEnable 1
```

Virtual Flash deaktivieren

Um Virtual Flash zu deaktivieren, öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie <Eingabe>:

```
racadm config -g cfgRacVirtual -o cfgVirMediaKeyEnable 0
```

Abbilder in einem Virtual Flash speichern

Der Virtual Flash kann vom Managed Host formatiert werden. Wenn Sie das Windows-Betriebssystem ausführen, klicken Sie mit der rechten Maustaste auf das Laufwerk-Symbol und wählen Sie **Format**. Wenn Sie Linux ausführen, ermöglichen Systemhilfsprogramme wie **format** und **fdisk**, den USB zu partitionieren und zu formatieren.

Bevor Sie ein Abbild vom RAC-Inbernetbrowser zum Virtual Flash hochladen, stellen Sie sicher, dass die Größe der Abbilddatei zwischen 1.44 MB und 16 MB (einschließlich) und Virtual Flash deaktiviert ist. Nachdem Sie das Image heruntergeladen und das Virtual Flash-Laufwerk wieder aktiviert haben, erkennen das System und BIOS den Virtual Flash.

Startfähigen Virtual Flash konfigurieren

1. Legen Sie eine startfähige Diskette in das Diskettenlaufwerk ein oder legen Sie eine startfähige CD in das optische Laufwerk ein.
2. Starten Sie Ihr System neu und starten Sie zum ausgewählten Datenträgerlaufwerk.
3. Fügen Sie eine Partition zum Virtual Flash hinzu und aktivieren Sie die Partition.

   Wenden Sie **fdisk** an, wenn Virtual Flash das Festplattenlaufwerk emuliert. Wenn Virtual Flash als Laufwerk B konfiguriert ist: Der Virtual Flash ist diskettenemuliert und erfordert keine Partition zum Konfigurieren von Virtual Flash als startfähiges Laufwerk.
4. Formatieren Sie das Laufwerk mittels des Befehls **format** mit dem Switch **/s**, um die Systemdateien auf das Virtual Flash zu übertragen.

   Beispiel:

`format /s x`

wobei *x* der dem Virtual Flash zugeteilte Laufwerksbuchstabe ist.

5. Fahren Sie das System herunter und entfernen Sie die startfähige Floppy oder CD vom entsprechenden Laufwerk.

6. Schalten Sie das System ein und überprüfen Sie, ob das System vom Virtual Flash zur `C:\` oder `A:\`-Eingabeaufforderung startet.

Befehlszeilenoberfläche-Dienstprogramm des Virtuellen Datenträgers verwenden

Die Befehlszeilenoberfläche des Virtuellen Datenträgers (VM-CLI) Dienstprogramm ist eine scriptbare Befehlszeilenschnittstelle, die Funktionen des Virtuellen Datenträgers von der Verwaltungsstation zum DRAC 5 im Remote System bereitstellt.

Das VM-CLI-Dienstprogramm enthält die folgenden Funktionen:

- Unterstützt mehrfache gleichzeitig aktive Sitzungen.

  ANMERKUNG: Beim Virtualisieren von schreibgeschützten Abbilddateien, können mehrere Sitzungen dieselben Abbilddatenträger teilen. Beim Virtualisieren von physischen Laufwerken kann nur jeweils eine Sitzung auf ein gegebenes physisches Laufwerk zugreifen.

- Wechselmediengeräte oder Bilddateien, die mit den Plug-Ins des Virtuellen Datenträgers übereinstimmen
- Automatische Terminierung, wenn die DRAC-Firmware startet, wenn die Option aktiviert ist.
- Sichere Kommunikationen zum DRAC 5 mittels Secure Sockets Layer (SSL)

Bevor Sie das Dienstprogramm ausführen, stellen Sie sicher, dass Sie die Berechtigung Virtueller Datenträger-Benutzer zum DRAC 5 im Remote-System haben.

Wenn das Betriebssystem Administrator-Berechtigungen oder eine betriebssystemspezifische Berechtigung oder Gruppenmitgliedschaft unterstützt, sind Administrator-Berechtigungen auch zum Ausführen des VM-CLI-Befehls erfordert.

Der Administrator des Client-Systems kontrolliert Benutzergruppen und Berechtigungen und dadurch die Benutzer, die das Dienstprogramm ausführen können.

Für Windows-Systeme müssen Sie Hauptbenutzerberechtigungen haben, um das VM-CLI Dienstprogramm auszuführen.

Für Linux-Systeme können Sie ohne Administrator-Berechtigungen auf das VM-CLI-Dienstprogramm zugreifen, indem Sie den **sudo** Befehl verwenden. Dieser Befehl enthält ein zentrales Mittel zur Bereitstellung von Nicht-Administrator-Zugang und protokolliert alle Benutzerbefehle. Um Benutzer in der VM-CLI-Gruppe hinzuzufügen oder zu bearbeiten, verwendet der Administrator den **visudo** Befehl. Benutzer ohne Administrator-Berechtigungen können die Befehl **sudo** als Präfix zur VM-CLI-Befehlszeile (oder zum VM-CLI Skript) hinzufügen, um Zugang zum DRAC 5 im Remote-System zu erhalten und das Dienstprogramm auszuführen.

Dienstprogramminstallation

Das VM-CLI Dienstprogramm befindet sich auf de CD *Dell OpenManage™ Systems Management Consoles*, die im Dell OpenManage Systemverwaltungssoftwaresatz enthalten ist. Um das Dienstprogramm zu installieren, legen Sie die CD *System Management Consoles* in das System-CD-Laufwerk und führen Sie die angezeigten Anweisungen aus.

Die CD *Systems Management Consoles* enthält die neuesten Systemverwaltungssoftwareprodukte, einschließlich Diagnose, Speicher-Management, RAS-Dienst und RACADM-Dienstprogramm. Diese CD enthält auch Infodateien mit den neuesten Produktinformationen über die Systemverwaltungssoftware.

Darüber hinaus enthält die CD *Systems Management Consoles* das Beispielscript **vmdeploy**, das illustriert, wie man die VM-CLI- und RACADM-Dienstprogramme zur Bereitstellung von Software an mehrfache Remote-Systeme verwendet. "Weitere Informationen finden Sie in "Betriebssystem mit VM-CLI bereitstellen"".

Befehlszeilenoptionen

Die VM-CLI-Schnittstelle ist auf Windows- und Linux-Systemen identisch. Das Dienstprogramm verwendet Optionen, die mit den RACADM-Dienstprogrammoptionen übereinstimmen. Zum Beispiel erfordert eine Option zur Angabe der DRAC 5 IP-Adresse dieselbe Syntax für die RACADM- und VM-CLI-Dienstprogramme.

Das Format eines VM-CLI-Befehls ist wie folgt:

`racvmcli [Parameter] [Betriebs_system_Shell_Optionen]`

Die Befehlszeilensyntax ist groß/kleinschreibungsabhängig. In "VM-CLI-Parameter" finden Sie weitere Informationen.

Wenn das Remote-System die Befehle akzeptiert und der DRAC 5 die Verbindung autorisiert, führt der Befehl weiter aus, bis einer der folgenden Vorgänge eintritt:

- Die VM-CLI-Verbindung wird aus einem beliebigen Grund terminiert.
- Das Verfahren wird mit einer Betriebssystemsteuerung manuell terminiert. Beispiel: In Windows können Sie den Task-Manager verwenden, um das Verfahren zu beenden.

VM-CLI-Parameter

DRAC 5-IP-Adresse

`-r <RAC-IP-Adresse>[:<RAC-SSL-Schnittstelle>]`

wobei *<RAC-IP-Adresse>* eine gültige, eindeutige IP-Adresse oder der DRAC 5-dynamische Domänennamensystem (DDNS) -Name ist (wenn unterstützt).

Dieser Parameter enthält die DRAC 5 IP-Adresse und SSL-Schnittstelle. Das VM-CLI-Dienstprogramm benötigt diese Informationen, um eine Virtueller Datenträger-Verbindung mit dem Ziel-DRAC 5 aufzubauen. Wenn Sie eine ungültige IP-Adresse oder einen ungültigen DDNS-Namen eingeben, wird eine Fehlermeldung angezeigt, und der Befehl wird terminiert.

Wenn *<RAC-SSL-Schnittstelle>* ausgelassen wird, wird die Standardschnittstelle (443) verwendet. Solange die Standard-SSL-Schnittstelle des DRAC 5 nicht geändert wird, ist die optionale SSL-Schnittstelle nicht erforderlich.

DRAC 5-Benutzername

`-u <DRAC-Benutzername>`

Dieser Parameter enthält den DRAC 5-Benutzernamen, der den Virtuellen Datenträger ausführen wird.

Der *<DRAC-Benutzername>* muss die folgenden Attribute haben:

- Gültiger Benutzername
- DRAC Virtueller Datenträger-Benutzerberechtigung

Wenn die DRAC 5-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt und der Befehl wird terminiert.

DRAC-Benutzerkennwort

`-p <DRAC-Benutzerkennwort>`

Dieser Parameter enthält das Kennwort für den angegebenen DRAC 5-Benutzer.

Wenn die DRAC 5-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt und der Befehl beendet.

Diskette/Festplatten-Gerät oder -Abbilddatei

`-f {<Gerätename> | <Image-Datei>}`

wobei *<Gerätename>* ein gültiger Laufwerksbuchstabe (für Windows-Systeme) oder ein gültiger Gerätekomponentenname ist, einschließlich der bereitstellbaren Dateisystem-Partitionsnummer, wenn anwendbar (für Linux-Systeme); und *<Image-Datei>* der Dateiname und Pfad einer gültigen Abbilddatei ist.

Dieser Parameter bestimmt das Gerät oder die Datei, die die virtuelle Disketten-/Festplattendatenträger liefern.

Beispiel: Eine Abbilddatei wird wie folgt angegeben:

`-f c:\temp\myfloppy.img` (Windows-System)

`-f /tmp/myfloppy.img` (Linux-System)

Wenn die Datei nicht schreibgeschützt ist, kann der virtuelle Datenträger zur Abbilddatei schreiben. Konfigurieren Sie das Betriebssystem, um eine Diskettenabbilddatei, die nicht überschrieben werden soll, mit Schreibschutz zu versehen.

Beispiel: Ein Gerät wird wie folgt angegeben:

`-f a:\` (Windows-System)

`-f /dev/sdb4 # 4. Partition auf dem Gerät` /dev/sdb (Linux-System)

Wenn das Gerät eine Schreibschutzfähigkeit bietet, können Sie diese Fähigkeit zum Sicherstellen verwenden, dass der virtuelle Datenträger nicht zum Datenträger schreiben wird.

Lassen Sie zusätzlich diesen Parameter aus der Befehlszeile weg, wenn Sie keine Diskettendatenträger virtualisieren. Wenn ein ungültiger Wert festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl beendet.

CD/DVD-Gerät oder -Abbilddatei

`-c {<Gerätename> | <Image-Datei>}`

wobei *<Gerätename>* ein gültiger CD/DVD-Laufwerksbuchstabe (für Windows-Systeme) oder ein gültiger Gerätekomponentenname (für Linux-Systeme) und *<Image-Datei>* der Dateiname und Pfad einer gültigen ISO-9660-Abbilddatei ist.

Dieser Parameter bestimmt das Gerät oder die Datei, das/die virtuellen CD/DVD-ROM-Datenträger liefert:

Beispiel: Eine Abbilddatei wird wie folgt angegeben:

`-c c:\temp\mydvd.img` (Windows-Systeme)

`-c /tmp/mydvd.img` (Linux-Systeme)

Beispiel: Ein Gerät wird wie folgt angegeben:

`-c d:\` (Windows-Systeme)

`-c /dev/cdrom` (Linux-Systeme)

Lassen Sie zusätzlich diesen Parameter aus der Befehlszeile weg, wenn Sie keine CD/DVD-Datenträger virtualisieren. Wenn ein ungültiger Wert festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl beendet.

Geben Sie mit dem Befehl mindestens einen Datenträgertyp (Diskette oder CD/DVD-Laufwerk) an, es sei denn, es werden nur Switch-Optionen vorgegeben. Ansonsten wird eine Fehlermeldung angezeigt und der Befehl mit einem Fehler beendet.

Versionsanzeige

`-v`

Dieser Parameter wird zur Anzeige der Version des VM-CLI Dienstprogramms verwendet. Wenn keine anderen Nichtschalteroptionen geboten werden, endet der Befehl ohne Fehlermeldung.

Hilfeanzeige

`-h`

Dieser Parameter wird zur Anzeige einer Zusammenfassung von VM-CLI Dienstprogrammparametern verwendet. Wenn keine anderen Nichtschalteroptionen geboten werden, wird der Befehl ohne Fehler beendet.

Verschlüsselte Daten

`-e`

Wenn dieser Parameter in der Befehlszeile enthalten ist, verwendet das VM-CLI-Dienstprogramm einen SSL-verschlüsselten Kanal zur Übertragung von Daten zwischen der Verwaltungsstation und dem DRAC 5 im Remote-System. Wenn dieser Parameter nicht in der Befehlszeile enthalten ist, wird die Datenübertragung nicht verschlüsselt.

VM-CLI-Betriebssystem Shell-Optionen

Die folgenden Betriebssystem-Funktionen können in der VM-CLI-Befehlszeile verwendet werden:

- stderr/stdout-Umleitung - Leitet jede gedruckte Dienstprogrammausgabe zu einer Datei um.

  Zum Beispiel überschreibt das "größer als"-Zeichen (>), gefolgt von einem Dateinamen, die angegebene Datei mit der gedruckten Ausgabe des VM-CLI-Dienstprogramms.

  ANMERKUNG: Das VM-CLI-Dienstprogramm liest nicht vom Standardeingang (**stdin**). Infolgedessen ist keine **stdin** Umleitung erforderlich.

- Hintergrundausführung - Standardmäßig führt das VM-CLI-Dienstprogramm im Vordergrund aus. Verwenden Sie die Befehlsshell-Funktionen des Betriebssystems, um das Dienstprogramm zu veranlassen, im Hintergrund auszuführen. Zum Beispiel veranlasst unter einem Linux-Betriebssystem das Et-Zeichen (&) nach einem Befehl, dass das Programm als neues Hintergrundverfahren erzeugt wird.

Diese letztere Technik ist in Script-Programmen nützlich, da sie zulässt, dass das Script weiter ausführt, nachdem ein neues Verfahren für den VM-CLI-Befehl begonnen wird (ansonsten würde das Script sperren, bis das VM-CLI-Programm beendet ist). Wenn mehrfache VM-CLI-Instanzen auf diese Weise gestartet werden, und ein oder mehrere Befehls-Instanzen von Hand beendet werden müssen, verwenden Sie die betriebssystemspezifischen Einrichtungen zum Auflisten und Beenden von Verfahren.

VM-CLI-Rückcodes

0 = kein Fehler

1 = kann keine Verbindung aufbauen

2 = VM-CLI-Befehlszeilenfehler

3 = RAC-Firmware-Verbindung abgebrochen

Textmeldungen (nur auf Englisch) werden auch zur Standardfehlerausgabe ausgegeben, wenn Fehler festgestellt werden.

Häufig gestellte Fragen

Tabelle 8-2 Führt häufig gestellte Fragen und Antworten auf.

Tabelle 8-2. Virtuellen Datenträger verwenden: Häufig gestellte Fragen

Frage	Antwort
Manchmal bemerke ich, dass die Clientenverbindung meines virtuellen Datenträgers nachlässt. Warum?	Wenn bei einem Netzwerk eine Zeitüberschreitung eintritt, trennt die DRAC 5-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie die Funktion des virtuellen Datenträgers.
Welche Betriebssysteme unterstützen den DRAC 5?	"Unterstützte Betriebssysteme" enthält eine Liste von unterstützten Betriebssystemen.
Welche Webbrowser unterstützen den DRAC 5?	"Unterstützte Internetbrowser" enthält eine Liste der unterstützten Internetbrowser.
Warum verliere ich manchmal meine Clientverbindung?	• Sie können Ihre Clientverbindung verlieren, wenn das Netzwerk langsam ist oder wenn Sie die CD im Clientsystem-CD-Laufwerk ändern. Beispiel: Wenn Sie die CD im Clientsystem-CD-Laufwerk wechseln, hat die neue CD u. U. eine Autostart-Funktion. Wenn das der Fall ist, kann die Firmware eine Zeitüberschreitung haben und die Verbindung kann verloren gehen, wenn das Clientsystem zu viel Zeit beansprucht, bevor es bereit ist, die CD zu lesen. Wenn eine Verbindung verloren geht, vom GUI wieder anschließen und den vorherigen Vorgang fortfahren. • Wenn bei einem Netzwerk eine Zeitüberschreitung eintritt, trennt die DRAC 5-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie die Funktion des virtuellen Datenträgers.
Wie gehe ich vor, wenn Windows 2000 mit Service Pack 4 nicht korrekt installiert wird?	Wenn Sie den virtuellen Datenträger und die CD des Windows 2000-Betriebssystems verwenden, um Windows 2000 mit Service Pack 4 zu installieren, kann Ihr System während des Installationsverfahrens eventuell vorübergehend seine Verbindung zum CD-Laufwerk verlieren, und eine korrekte Installation des Betriebssystems kann eventuell fehlschlagen. Um dieses Problem zu lösen, laden Sie die Datei **usbstor.sys** von der Support-Website von Microsoft unter support.microsoft.com herunter und führen das Programm nur auf den Systemen aus, auf die sich dieses Problem bezieht. Weitere Informationen finden Sie in Microsoft Knowledge Base-Artikel 823086.
Warum kann ich Windows 2000 nicht lokal oder im Remote-Zugriff installieren?	Wenn Virtual Flash aktiviert ist und kein gültiges Image enthält, z. B.wenn Virtual Flash ein beschädigtes oder zufälliges Image enthält, kann es sein, dass Sie Windows 2000 nicht lokal oder im Remote-Zugriff installieren können. Um dieses Problem zu lösen, installieren Sie ein gültiges Image auf Virtual Flash oder deaktivieren Virtual Flash, wenn es während des Installationsverfahrens nicht verwendet wird.
Warum bricht die Verbindung des virtuellen Datenträgers ab, wenn sie im freigegebenen NIC-Modus konfiguriert wird?	Die Installation von Netzwerk- und Chipsatz-Treibern auf dem Server führt zu einem Abbruch der Verbindung des virtuellen Datenträgers, wenn sie im freigegebenen NIC-Modus konfiguriert wurde. Die Installation der Netzwerk- oder Chipsatz-Treiber verursacht, dass LOM zurückgesetzt wird, was wiederum zu Zeitüberschreitungen bei Netzwerkpaketen und zu Zeitüberschreitungen und Abbruch der Verbindung des virtuellen Datenträgers führt. Um dieses Problem zu umgehen, kopieren Sie die Treiber von Ihrem virtuellen Laufwerk auf die lokale Festplatte des Servers. Um zu verhindern, dass sich eine abgebrochene Verbindung des virtuellen Datenträgers störend auf das Treiberinstallationsverfahren auswirkt, starten Sie die Treiberinstallation direkt vom Server.
Eine Installation des Windows-Betriebssystems scheint zu lange zu dauern. Warum?	Wenn Sie das Windows-Betriebssystem mithilfe der CD *Dell PowerEdge Installation and Server Management* und über eine langsame Netzwerkverbindung installieren, kann es sein, dass das Installationsverfahren aufgrund von Netzwerklatenzzeit mehr Zeit in Anspruch nimmt, um auf die DRAC 5-webbasierte Schnittstelle zuzugreifen. Im Installationsfenster wird der Installationsfortschritt nicht anzeigt, doch das Installationsverfahren wird durchgeführt.
Ich zeige den Inhalt eines Diskettenlaufwerks oder eines USB-Speicherschlüssels an. Wenn ich versuche, über dasselbe Laufwerk eine Verbindung zum virtuellen Datenträger herzustellen, erhalte ich eine Verbindungs-Fehlermeldung and werde gebeten, den Vorgang zu wiederholen. Warum?	Ein Simultanzugriff auf virtuelle Diskettenlaufwerke ist nicht zulässig. Vor dem Versuch, das Laufwerk zu virtualisieren, ist die Anwendung zum Anzeigen des Laufwerkinhalts zu schließen.
Wie konfiguriere ich mein virtuelles Gerät als startfähiges Gerät?	Greifen Sie auf dem verwalteten System auf das BIOS-Setup zu, und wechseln Sie zum Startmenü. Machen Sie die virtuelle CD, die virtuelle Floppy oder den Virtual Flash ausfindig, und ändern Sie die Gerätestartreihenfolge wie erforderlich. Um z. B. von einem CD-Laufwerk zu starten, konfigurieren Sie das CD-Laufwerk als erstes Laufwerk in der Startreihenfolge.
Von welchen Arten von Datenträgern kann ich starten?	Mit DRAC 5 können Sie von den folgenden startfähigen Datenträgern starten: • CDROM/DVD-Datenträger • ISO 9660-Image • 1.44-Diskette oder Floppy-Image • DRAC 5-integrierter Virtual Flash • USB-Schlüssel, der vom Betriebssystem als Wechselplatte erkannt wird • USB-Schlüssel-Image
Wie kann ich meine USB-Taste startfähig machen?	Nur USB-Schlüssel mit Windows 98 DOS können von der virtuellen Floppy starten. Um Ihren eigenen startfähigen USB-Schlüssel zu konfigurieren, starten Sie zu einer Windows 98-Startdiskette und kopieren Systemdateien von der Startdiskette zum USB-Schlüssel. Geben Sie z. B. an der DOS-Eingabeaufforderung den folgenden Befehl ein: `sys a: x: /s` wobei "x:" der USB-Schlüssel ist, der startfähig gemacht werden soll. Sie können auch das Dell Startdienstprogramm verwenden, um einen startfähigen USB-Schlüssel zu erstellen. Dieses Dienstprogramm ist nur mit USB-Schlüsseln kompatibel, die von Dell mit einer Schutzmarke versehen wurden. Um das Dienstprogramm herunterzuladen, öffnen Sie einen unterstützten Web-Browser, wechseln Sie zur Dell Support-Website, die unter **support.dell.com** zu finden ist, und suchen Sie nach "R122672.exe. "
Brauche ich Administratorrechte, um das	Um das Plugin des virtuellen Datenträgers installieren zu können, müssen Sie Administrator- oder

ActiveX-Plugin installieren zu können?	Hauptbenutzerberechtigungen auf Windows-Systemen besitzen.
Welche Berechtigungen brauche ich, um das Plugin des virtuellen Datenträgers auf einer Red Hat Linux-Verwaltungsstation zu installieren und verwenden?	Sie müssen in der Verzeichnisstruktur des Browsers Schreib-Berechtigungen haben, um das Plugin des virtuellen Datenträgers erfolgreich installieren zu können.
Ich kann mein virtuelles Floppy-Gerät auf einem System, das das Red Hat Enterprise Linux- oder SUSE Linux-Betriebssystem ausführt, nicht finden. Mein virtueller Datenträger ist angeschlossen, und ich bin mit meiner Remote-Floppy verbunden. Was soll ich tun?	Bei einigen Linux-Versionen erfolgt die automatische Ladung des virtuellen Diskettenlaufwerks 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 folgenden Schritte aus, um das virtuelle Diskettenlaufwerk korrekt zu finden und zu laden: 1. Öffnen Sie eine Linux-Eingabeaufforderung, und führen Sie den folgenden Befehl aus: grep "Virtual Floppy" /var/log/messages 2. Finden Sie den letzten Eintrag dieser Meldung und notieren Sie die Zeit. 3. An der Linux-Eingabeaufforderung führen Sie den folgenden Befehl aus: grep "hh:mm:ss"/var/log/messages wo: hh:mm:ss ist die Zeitmarke der Meldung, die im Schritt 1 von grep zurückgegeben wurde. 4. Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls und finden Sie den Gerätenamen, der der "Virtuellen Dell-Floppy" gegeben wurde 5. Stellen Sie sicher, dass das virtuelle Diskettenlaufwerk angeschlossen ist und eine Verbindung zu ihm besteht. 6. Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus: mount /dev/sdx /mnt/floppy wo: /dev/sdx ist der Gerätename, der im Schritt 4 gefunden wurde /mnt/floppy ist der Befestigungspunkt.
Welche Dateisystemtypen werden auf meinem virtuellen Diskettenlaufwerk oder Virtual Flash unterstützt?	Ihr virtuelles Diskettenlaufwerk oder Virtual Flash unterstützt FAT16- oder FAT32-Dateisysteme.
Als ich im Remote-Zugriff anhand der DRAC 5-webbasierten Schnittstelle eine Firmware-Aktualisierung ausführte, wurden meine virtuellen Laufwerke am Server entfernt. Warum?	Firmware-Aktualisierungen führen zu einem Reset des DRAC 5, einem Abbruch der Remote-Verbindung sowie zum Entladen der virtuellen Laufwerke. Die Laufwerke werden wieder erscheinen, wenn der DRAC-Reset abgeschlossen ist.
Als ich Virtual Flash aktivierte oder deaktivierte, bemerkte ich, dass alle meine virtuellen Laufwerke verschwanden und dann wieder erschienen. Warum?	Ein Deaktivieren oder Aktivieren des Virtual Flash verursacht einen USB-Reset und bewirkt, dass alle virtuellen Laufwerke vom USB-Bus abgetrennt und dann wieder mit ihm verbunden werden.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

RACADM-Befehlszeilenoberfläche verwenden

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Die serial/telnet/ssh-Konsole enthält eine Reihe von Racadm-Befehlen. Die Racadm-Befehle enthalten Zugang zu den textbasierten Funktionen, die durch die webbasierte DRAC 5-Schnittstelle unterstützt werden.

RACADM ermöglicht, den DRAC 5 lokal oder im Remote-Zugriff zu konfigurieren und zu verwalten. RACADM führt auf der Verwaltungsstation und dem verwalteten System aus. RACADM ist auf der CD *Systems Management Consoles* enthalten.

Sie können RACADM verwenden, um Skripte zu schreiben, um mehrere DRAC 5s automatisch zu konfigurieren. Weitere Informationen über das Konfigurieren mehrerer DRAC 5s finden Sie unter "Mehrere DRAC 5-Karten konfigurieren".

Dieser Abschnitt enthält die folgenden Informationen:

- **Serielle** und **racadm**-Befehle verwenden. Siehe "Serielle oder Telnet-Konsole verwenden" bzw. "RACADM verwenden"
- DRAC 5 mit dem **racadm**-Befehl konfigurieren
- Racadm-Konfigurationsdatei zum Konfigurieren mehrerer DRAC 5- Karten verwenden

---

Eine serielle oder Telnet-Konsole verwenden

Sie können die seriellen Befehle in Tabelle 9-1 im Remote-Zugriff mittels RACADM oder von der seriell/telnet/ssh Eingabeaufforderung ausführen.

Anmeldung bei DRAC 5

Nachdem Sie Ihre Verwaltungsstation-Terminalemulator-Software und den Managed Knoten-BIOS konfiguriert haben, melden Sie sich mit den folgenden Schritten am DRAC 5 an:

1. Stellen Sie eine Verbindung zum DRAC 5 her, indem Sie Ihre Verwaltungsstation-Terminalemulator-Software verwenden.
2. Geben Sie Ihren DRAC 5-Benutzernamen ein und drücken Sie auf <Eingabe>.

   Sie werden am DRAC 5 angemeldet.

Eine Textkonsole starten

Nachdem Sie sich über Ihre Verwaltungsstation-Terminal-Software oder mit Telnet oder SSH beim DRAC 5 angemeldet haben, können Sie die Textkonsole des verwalteten Systems umleiten, indem Sie den seriellen/Telnet-Befehl **connect com2** verwenden. Es wird nur jeweils ein **connect com2**-Client unterstützt.

Zur Verbindung mit der verwalteten System-Textkonsole öffnen Sie eine DRAC 5-Eingabeaufforderung (angezeigt durch eine Telnet- oder SSH-Sitzung) und geben Sie folgendes ein:

```
connect com2
```

Von einer seriellen Sitzung können Sie mit der seriellen Konsole des verwalteten Systems verbunden werden, indem Sie <Esc><Umschalt><Q> drücken, wodurch die serielle Schnittstelle des verwalteten Systems direkt mit der COM2-Schnittstelle des Servers verbunden und der DRAC 5 umgangen wird. Um den DRAC 5 wieder mit dem seriellen Anschluss zu verbinden, drücken Sie <Esc><Umschalt><9>. Die Baudraten der COM2-Schnittstelle des Managed Knotens und der seriellen DRAC 5-Schnittstelle müssen identisch sein.

Der Befehl `connect -h com2` zeigt den Inhalt des seriellen Verlaufspuffers bevor er auf Tastatureingaben oder neue Zeichen von der seriellen Schnittstelle wartet.

ANMERKUNG: Wenn die Option **-h** verwendet wird, müssen der Client- und Server-Terminalemulationstyp (ANSI oder VT100) identisch sein; ansonsten kann die Ausgabe verwirrt sein. Setzen Sie zusätzlich die Client-Terminalzeile auf **25**.

Die Standardgröße (und maximale Größe) des Verlaufspuffers ist 8192 Zeichen. Sie können diese Zahl zu einem kleineren Wert einstellen, indem Sie den folgenden Befehl verwenden:

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

RACADM verwenden

Die RACADM-CLI-Befehle können lokal oder im Remote-Zugriff von der seriellen oder Telnet-Konsolen-Befehlseingabeaufforderung bzw. durch eine normale Befehlseingabeaufforderung ausgeführt werden.

Verwenden Sie den Befehl **racadm**, um DRAC 5-Eigenschaften zu konfigurieren, führen Sie Remote-Verwaltungsaufgaben aus oder stellen Sie ein abgestürztes System wieder her.

Zur Anzeige des racadm-Unterbefehls mit RACADM, geben Sie folgendes ein:

```
racadm help
```

Die Unterbefehlliste enthält alle Befehle, die durch den DRAC 5 unterstützt werden.

Ohne Optionen zeigt der Befehl **racadm** allgemeine Anwendungsinformationen. Geben Sie `racadm help` ein, um eine Liste aller verfügbaren Unterbefehle anzuzeigen. Geben Sie `racadm help <Unterbefehl>` ein, um alle Syntax- und Befehlszeilenoptionen für den Unterbefehl aufzuführen.

Die folgenden Abschnitte bieten Informationen darüber, wie man **racadm**-Befehle verwendet

RACADM im Remote-Zugriff verwenden

ANMERKUNG: Konfigurieren Sie die IP-Adresse auf Ihrem DRAC 5, bevor Sie die Racadm-Remote-Fähigkeit verwenden. Weitere Informationen über die Einrichtung des DRAC 5 und eine Liste von verwandten Dokumenten finden Sie in "DRAC 5 installieren und einrichten".

RACADM verfügt über eine Remote-Fähigkeitsoption (**-r**), mit der eine Verbindung zum verwalteten System hergestellt werden kann und **racadm**-Unterbefehle von einer Remote-Konsole oder einer Verwaltungsstation ausgeführt werden können. Um die Remote-Option zu verwenden, werden ein gültiger Benutzername (**-u** -Option) und ein Kennwort (**-p**-Option) sowie die DRAC 5-IP-Adresse des verwalteten Systems benötigt.

ANMERKUNG: Die racadm-Remote-Fähigkeit wird nur auf Verwaltungsstations unterstützt. Weitere Informationen finden Sie in "Unterstützte Internetbrowser".

ANMERKUNG: Wenn Sie die racadm Remote-Fähigkeit verwenden, müssen Sie Schreiberlaubnis auf den Ordnern haben, auf denen Sie die racadm-Unterbefehle verwenden, die Dateivorgänge einbeziehen, zum Beispiel:

```
racadm getconfig -f <Dateiname>

oder

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

Racadm-Übersicht

```
racadm -r <RACIP-Adresse> -u <Benutzername> -p <Kennwort> <Unterbefehl> <Unterbefehlsoptionen>

racadm -i -r <RAC-IP-Adresse> <Unterbefehl> <Unterbefehlsoptionen>
```

Beispiel:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo

racadm -i -r 192.168.0.120 getsysinfo
```

Wenn die HTTPS-Schnittstellennummer des RAC zu einer von der Standardschnittstelle (443) abweichenden kundenspezifischen Schnittstelle geändert wurde, muss die folgende Syntax verwendet werden:

```
racadm -r <RAC-IP-Adresse>:<Schnittstelle> -u <Benutzername> -p <Kennwort> <Unterbefehl> <Unterbefehlsoptionen>

racadm -i -r <RAC-IP-Adresse>:<Schnittstelle> <Unterbefehl> <Unterbefehlsoptionen>
```

RACADM-Optionen

Tabelle 9-1 führt die Optionen für den Befehl **racadm** auf.

Tabelle 9-1. Racadm-Befehlsoptionen

Option	Beschreibung
-r <racIpAddr>	Bestimmt die Remote-IP-Adresse des Controllers.
-r <racIpAddr>:<*Schnittstellennummer***>**	Verwenden Sie *:<Schnittstellennummer>*, wenn die DRAC 5 Schnittstellennummer nicht die Standardschnittstelle (443) ist
-i	Weist **racadm** an, den Benutzer interaktiv nach dem Benutzernamen und Kennwort zu fragen.
-u <Benutzername>	Bestimmt den Benutzernamen der zur Authentifizierung der Befehlsdurchführung verwendet wird. Wenn die Option **-u** verwendet wird, muss die Option **-p** angegeben werden und die Option **-i** (Interaktiv) ist nicht zulässig.
-p <Kennwort>	Bestimmt das Kennwort das zur Authentifizierung der Befehlsdurchführung verwendet wird. Wenn die Option **-p** verwendet wird, ist die Option **-i** nicht zulässig.

Die RACADM Remote-Option aktivieren und deaktivieren

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

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

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

Zum Deaktivieren der Remote-Fähigkeit geben Sie folgendes ein:

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

RACADM-Unterbefehle

Tabelle 9-2 enthält eine Beschreibung jedes **racadm**-Unterbefehls, den Sie in RACADM ausführen können. Eine ausführliche Auflistung aller racadm-Unterbefehle einschließlich der Syntax und gültiger Einträge finden Sie unter "RACADM-Unterbefehlsübersicht".

Bei der Eingabe eines RACADM-Unterbefehls muss dem Befehl racadm vorausgestellt werden. Beispiel:

```
racadm help
```

Tabelle 9-2. RACADM-Unterbefehle

Befehl	Beschreibung
help	Führt die DRAC 5-Unterbefehle auf.
help <- *Unterbefehl*>	Listet die Verwendungsaussage für den angegebenen Unterbefehl auf.
arp	Zeigt den Inhalt der ARP-Tabelle an. ARP-Tabellen dürfen nicht hinzugefügt oder gelöscht werden.
clearasrscreen	Löscht den letzten Bildschirm Letzter Absturz (letzten blauen Bildschirm).
clrraclog	Löscht das DRAC 5-Protokoll. Es wird ein einzelner Eintrag vorgenommen, um anzuzeigen, von welchem Benutzer und zu welcher Uhrzeit das Protokoll gelöscht wurde.
config	Konfiguriert den RAC.
getconfig	Zeigt die aktuellen RAC-Konfigurationseigenschaften an.
coredump	Zeigt den letzten Coredump des DRAC 5 an.
coredumpdelete	Löscht den im DRAC 5 gespeicherten Coredump.
fwupdate	Führt DRAC 5-Firmware-Aktualisierungen durch zeigt den Status der RAC-Firmware-Aktualisierungen an.
getssninfo	Zeigt Informationen über aktive Sitzungen an
getsysinfo	Zeigt Status- und allgemeine Informationen zum DRAC 5 und zum System an.
getractime	Zeigt die DRAC 5-Uhrzeit.
ifconfig	Zeigt die aktuelle RAC-IP-Konfiguration an.
netstat	Anzeige der Routingtabelle und der aktuellen Verbindungen.
ping	Prüft nach, dass das Ziel-IP-Adresse vom DRAC 5 mit dem aktuellen Routing-Tabelleninhalt erreichbar ist.
setniccfg	Stellt die IP-Konfiguration für den Controller ein.
getniccfg	Zeigt die derzeitige IP-Konfiguration für den Controller an.
getsvctag	Zeigt Service-Tag-Nummern an.
racdump	Liest den DRAC 5-Status sowie Zustandsinformationen für Debuggen aus.
racreset	Stellt den DRAC 5 neu ein.
racresetcfg	Setzt den DRAC 5 auf die Standardkonfiguration zurück.
serveraction	Durchführung der Stromverwaltungsvorgänge auf dem verwalteten System.
getraclog	Anzeige des RAC-Protokolls.
clrsel	Löscht alle Systemereignisprotokolleinträge.
gettracelog	Zeigt das DRAC 5-Ablaufverfolgungsprotokoll. Bei Verwendung mit -i zeigt der Befehl die Anzahl von Einträgen im DRAC 5-Ablaufverfolgungsprotokoll an.
sslcsrgen	Erstellt und lädt die SSL-CSR herunter.
sslcertupload	Lädt ein CA-Zertifikat oder Serverzertifikat zum DRAC 5 hoch.
sslcertdownload	Lädt ein CA-Zertifikat herunter.
sslcertview	Zeigt ein CA-Zertifikat oder Serverzertifikat zum DRAC 5 an.
testemail	Zwingt den DRAC 5, eine E-Mail über die DRAC 5-NIC zu senden.
testtrap	Zwingt den DRAC 5, einen SNMP über die DRAC 5-NIC zu senden.
vmdisconnect	Zwingt eine Verbindung des virtuellen Datenträgers zu schließen.
vmkey	Setzt die Virtual Flash-Größe auf die Standardgröße (16 MB) zurück.

RACADM-Fehlermeldungen

Informationen über racadm-CLI-Fehlermeldungen erhalten Sie unter "Häufig gestellte Fragen" in diesem Kapitel.

Mehrere DRAC 5-Karten konfigurieren

Mit RACADM können Sie eine oder mehrere DRAC 5-Karten mit identischen Eigenschaften konfigurieren. Wenn Sie eine spezifische DRAC 5-Karte mittels ihrer Gruppen-ID und Objekt-ID abfragen, erstellt RACADM die **racadm.cfg**-Konfigurationsdatei aus den abgerufenen Informationen. Wenn Sie die Datei zu einer oder mehreren DRAC 5-Karten exportieren, können Sie in kürzester Zeit Ihre Controller mit identischen Eigenschaften konfigurieren.

ANMERKUNG: Einige Konfigurationsdateien enthalten eindeutige DRAC 5-Informationen (wie die statische IP-Adresse), die vor dem Exportieren der Datei zu anderen DRAC 5-Karten geändert werden müssen.

Zum Konfigurieren mehrerer DRAC 5-Karten führen Sie die folgenden Verfahren aus:

1. Verwenden Sie RACADM, um die Ziel-DRAC 5 abzufragen, die die entsprechende Konfiguration enthält.

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

   Öffnen Sie eine Eingabeaufforderung und geben Sie folgendes ein:

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

   ANMERKUNG: Das Umadressieren der RAC-Konfiguration zu einer Datei mit **getconfig -f** wird nur mit den lokalen und Remote-RACADM-Schnittstellen unterstützt.

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

3. Verwenden Sie die neue Konfigurationsdatei, um ein Ziel-RAC zu modifizieren.

   An der Eingabeaufforderung geben Sie folgendes ein:

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

4. Den konfigurierten Ziel-RAC zurücksetzen.

   An der Eingabeaufforderung geben Sie folgendes ein:

   ```
   Racadm-Reset
   ```

Der Unterbefehl **getconfig -f racadm.cfg** fordert die DRAC 5-Konfiguration an und erstellt die **racadm.cfg**-Datei. Auf Anfrage können Sie die Datei mit einem anderen Namen konfigurieren.

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

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

Der Unterbefehl **config** lädt die Informationen in andere DRAC 5s. Verwenden Sie **config**, um die Benutzer- und Kennwort-Datenbank mit dem Server Administrator zu synchronisieren

Die anfängliche Konfigurationsdatei **racadm.cfg** wird vom Benutzer benannt. Im folgenden Beispiel heißt die Konfigurationsdatei **myfile.cfg**. Um diese Datei zu erstellen, geben Sie folgendes an der Eingabeaufforderung ein:

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

HINWEIS: Es wird empfohlen, dass Sie diese Datei mit einem einfachen Texteditor bearbeiten. Das racadm-Dienstprogramm verwendet einen ASCII-Textparser. Formatierung verwirrt den Parser, wodurch die racadm-Datenbank beschädigt werden kann.

Eine DRAC 5-Konfigurationsdatei erstellen

Die DRAC 5-Konfigurationsdatei **<***Dateiname***>.cfg** wird mit dem Befehl `racadm config -f <Dateiname>.cfg` verwendet. Die Konfigurationsdatei besteht aus einer einfachen Textdatei, mit der der Benutzer eine Konfigurationsdatei erstellen kann (ähnlich zur **.ini**-Datei) und den DRAC 5 mit dieser Datei konfigurieren kann. Es kann ein beliebiger Dateiname verwendet werden und die Datei erfordert keine **.cfg**-Erweiterung (obwohl sich dieser Unterabschnitt auf diese Endung bezieht).

Die **.cfg**-Datei kann:

- Erzeugt werden
- Von einem Befehl `racadm getconfig -f <Dateiname>.cfg` erhalten

- Von einem Befehl `racadm getconfig -f <Dateiname>.cfg` erhalten und dann bearbeiten

ANMERKUNG: Weitere Informationen zu dem Befehl **getconfig**finden Sie unter "getconfig".

Die **.cfg**-Datei wird zuerst analysiert, um zu überprüfen, ob gültige Gruppen- und Objektnamen vorhanden sind und dass einige einfache Syntaxregeln befolgt werden. Fehler werden mit der Zeilennummer markiert, in der der Fehler ermittelt wurde und eine einfache Meldung beschreibt das Problem. Die gesamte Datei wird auf Richtigkeit analysiert und alle Fehler werden angezeigt. Schreibbefehle werden nicht zum DRAC 5 übertragen, wenn ein Fehler in der Datei **.cfg** festgestellt wird. Der Benutzer muss *alle* Fehler korrigieren, bevor eine Konfiguration erfolgen kann. Die Option -**c** kann für den Unterbefehl **config** verwendet werden, wodurch nur die Syntax überprüft wird, jedoch *keine* Schreibvorgänge zum DRAC 5 vorgenommen werden.

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

- Wenn die Analyse auf eine indizierte Gruppe trifft, ist es der Wert des anhängenden Objektes, der die verschiedenen Indizes unterscheidet.

  Die Analyse liest also alle Indizes aus dem DRAC 5 für diese Gruppe aus. Alle Objekte innerhalb dieser Gruppe sind einfache Modifizierungen, wenn der DRAC 5 konfiguriert wird. Wenn ein geändertes Objekt einen neuen Index darstellt, wird der Index während der Konfiguration auf dem DRAC 5 erstellt.

- Der Benutzer kann in einer **.cfg**-Datei keinen gewünschten Index angeben.

  Indizes können erstellt und gelöscht werden, sodass die Gruppe im Laufe der Zeit durch genutzte und ungenutzte Indizes fragmentiert wird. Wenn ein Index vorhanden ist, wird er bearbeitet. 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 RAC zu machen braucht. Neue Benutzer werden dem ersten verfügbaren Index hinzugefügt. Dadurch kann eine **.cfg**-Datei, die auf einem DRAC 5 richtig analysiert und ausgeführt wird, möglicherweise nicht richtig auf einem anderen RAC ausgeführt werden, falls alle Indizes belegt sind und ein neuer Benutzer hinzugefügt werden muss.

- Verwenden Sie den Unterbefehl **racresetcfg**, um alle DRAC 5-Karten mit identischen Eigenschaften zu konfigurieren.

  Verwenden Sie den Unterbefehl **racresetcfg**, um den DRAC 5 auf die ursprünglichen Standardeinstellungen zurückzusetzen, und dann führen Sie den Befehl `racadm config -f <Dateiname>.cfg` aus. Stellen Sie sicher, dass die **.cfg**-Datei alle gewünschten Objekte, Benutzer, Indizes und andere Parameter enthält.

HINWEIS: Verwenden Sie den Unterbefehl **racresetcfg**, um die Datenbank und die DRAC 5-NIC-Einstellungen auf die ursprünglichen Standardeinstellungen zurückzusetzen und alle Benutzer und Benutzerkonfigurationen zu entfernen. Während der Stammbenutzer weiterhin verfügbar ist, werden die Einstellungen anderer Benutzer auch auf die Standardeinstellungen zurückgesetzt.

Analyse-Richtlinien

- Alle Zeilen, die mit dem Zeichen '#' beginnen, werden als Kommentarzeilen behandelt.

  Eine Kommentarzeile muss mit Spalte eins beginnen. Wenn sich das Zeichen '#' in einer anderen Spalte befindet, wird es als das Zeichen # behandelt.

  Einige Modemparameter können #-Zeichen in der Zeichenkette enthalten. Es ist kein Escape-Zeichen erforderlich. Sie können einen **.cfg**-Befehl von einem `racadm getconfig -f <Dateiname>.cfg`-Befehl erstellen und dann einen `racadm config -f <Dateiname>.cfg`-Befehl an einen anderen DRAC 5 ausführen, ohne dass Sie Escape-Zeichen hinzufügen müssen.

  Beispiel:

  ```
  #

  # Das ist eine Anmerkung

  [cfgUserAdmin]

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

- Alle Gruppeneinträge müssen sich zwischen den Zeichen "**[**" und "**]**" befinden.

  Das Anfangszeichen "**[**", das einen Gruppennamen anzeigt, *muss* in Spalte eins beginnen. Dieser Gruppenname *muss* vor allen anderen Objekten in dieser Gruppe angegeben werden. Objekte, denen kein Gruppenname zugewiesen ist, erzeugen Fehler. Diese Konfigurationsdaten werden in Gruppen verwaltet, wie unter "DRAC 5 Eigenschaften-Datenbankgruppe und Objektdefinitionen" definiert.

  Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objektes:

  Beispiel:

  ```
  [cfgLanNetworking] - {Gruppenname}

  cfgNicIpAddress=143.154.133.121 {Objekt-Name}
  ```

- Alle Parameter werden in "Objekt=Wert"-Paaren ohne Leerzeichen zwischen 'Objekt', '=' oder 'Wert' angegeben.

  Leerstellen nach dem Wert werden ignoriert. Eine Leerstelle innerhalb einer Wertzeichenkette bleibt unmodifiziert. Jedes Zeichen rechts neben dem '=' wird wie eingegeben übernommen (z. B. ein zweites '=', ein '#', ein '[', ']', usw.) Bei diesen Zeichen handelt es sich um gültige Modemchat-Scriptzeichen.

  Siehe das Beispiel unter dem vorherigen Punkt.

- Der **.cfg** Parser ignoriert einen Index-Objekteintrag.

  Der Benutzer kann nicht angeben, welcher Index verwendet wird. 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>.cfg` setzt einen Kommentar vor die Index-Objekte, durch die dem Benutzer die enthaltenen Kommentare angezeigt werden.

ANMERKUNG: Der Benutzer kann mit dem folgenden Befehl eine mit einem Index versehene Gruppe manuell erstellen:
racadm config -g <*Gruppenname*> -o <*verankertes Objekt*> -i <*Index 1-16*> <*eindeutiger Ankername*>

- Die Zeile für eine indizierte Gruppe *kann nicht* aus einer **.cfg**-Datei gelöscht werden.

  Der Benutzer muss eine indiziertes Objekt über den folgenden Befehl manuell löschen:

  ```
  racadm config -g <Gruppenname> -o <Objektname> -i <Index 1-16> ""
  ```

ANMERKUNG: Eine NULL-Zeichenkette (zwei "" Zeichen) weist den DRAC 5 dazu an, den Index für die angegebene Gruppe zu löschen.

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

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

- Für indizierte Gruppen *muss* es sich bei dem Objektanker um das erste Objekt nach dem Klammer-[ ]-Paar handeln. Es folgen Beispiele der derzeitigen indizierten Gruppen:

  ```
  [cfgUserAdmin]
  ```

  ```
  cfgUserAdminUserName=<BENUTZERNAME>
  ```

  Wenn Sie `racadm getconfig -f <MeinBeispiel>.cfg` eingeben, erstellt der Befehl eine **.cfg**-Datei für die aktuelle DRAC 5-Konfiguration. Diese Konfigurationsdatei kann als Beispiel sowie als Startpunkt für Ihre **eindeutige.cfg**-Datei verwendet werden.

DRAC 5 IP-Adresse ändern

Wenn Sie die DRAC 5 IP-Adresse in der Konfigurationsdatei modifizieren, entfernen Sie alle unnötigen **<***variable***>**=**Wert**-Einträge. In diesem Fall bleibt lediglich die tatsächliche Bezeichnung der variablen Gruppe mit " [" und "] " zusammen mit den zwei **<***variable***>**=**Wert**-Einträgen erhalten, die der IP-Adressänderung zugeordnet sind.

Beispiel:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Diese Datei wird durch folgende Einträge ergänzt:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored

cfgNicGateway=10.35.9.1
```

Mit dem Befehl **racadm config -f myfile.cfg** wird die Datei geparst und Fehler werden nach Zeilennummer identifiziert. Eine korrekte Datei nimmt die richtigen Einträge vor. Derselbe, im vorhergehenden Beispiel verwendete Befehl **getconfig** kann zur Bestätigung der Aktualisierung verwendet werden.

Diese Datei kann für das Herunterladen von unternehmensweiten Änderungen oder zur Konfiguration neuer Systeme über das Netzwerk verwendet werden.

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

RACADM -Dienstprogramm zur Konfiguration des DRAC 5 verwenden

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

Die webbasierte DRAC 5-Schnittstelle ist die schnellste Art, einen DRAC 5 zu konfigurieren. Wenn Sie Befehlszeilen- oder Skript-Konfiguration bevorzugen oder mehrere DRAC 5 konfigurieren müssen, verwenden Sie RACADM, das mit dem DRAC 5-Agent auf dem verwalteten System installiert wird.

Um mehrere DRAC 5 mit identischen Konfigurationseinstellungen zu konfigurieren, führen Sie eines der folgenden Verfahren aus:

- Erstellen Sie mit Hilfe der RACADM-Beispiele in diesem Abschnitt eine Stapeldatei mit **racadm**-Befehlen und führen Sie dann diese Stapeldatei auf jedem verwalteten System aus.
- Erstellen Sie die DRAC 5-Konfigurationsdatei, wie unter "RACADM-Unterbefehlsübersicht" beschrieben; führen Sie dann den Unterbefehl **racadm config** auf jedem verwalteten System unter Verwendung dieser Konfigurationsdatei aus.

Bevor Sie Beginnen

Sie können bis zu 16 Benutzer in der DRAC 5 Eigenschaften-Datenbank konfigurieren. Bevor Sie einen DRAC 5-Benutzer manuell aktivieren, prüfen Sie, ob aktuelle Benutzer vorhanden sind. Wenn Sie einen neuen DRAC 5 konfigurieren oder den Befehl **racadm racresetcfg** ausgeführt haben, ist der einzige aktuelle Benutzer root mit dem Kennwort calvin. Der Unterbefehl **racresetcfg** setzt den DRAC 5 auf die ursprünglichen Standardeinstellungen zurück.

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

ANMERKUNG: Benutzer können im Lauf der Zeit aktiviert und deaktiviert werden. Infolgedessen kann ein Benutzer auf jedem DRAC 5 eine unterschiedliche Indexnummer besitzen.

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

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

ODER

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

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

ANMERKUNG: Sie können auch racadm getconfig -f <myfile.cfg> eingeben und die Datei **myfile.cfg** ansehen oder bearbeiten, die alle DRAC 5-Konfigurationsparameter umfasst.

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

```
# cfgUserAdminIndex=XX

cfgUserAdminUserName=
```

Wenn das Objekt **cfgUserAdminUserName** keinen Wert besitzt, steht diese Indexnummer, die durch das Objekt **cfgUserAdminIndex** angezeigt wird, zur Verfügung. Wenn hinter dem "=" ein Name erscheint, wird dieser Index von diesem Benutzernamen verwendet.

ANMERKUNG: Wenn Sie einen Benutzer mit dem Unterbefehl **racadm config** manuell aktivieren oder deaktivieren, *muss* der Index mit der Option **-i** angegeben werden. Beobachten Sie, ob das im vorigen Beispiel angezeigte Objekt **cfgUserAdminIndex** das Zeichen '#' enthält. Ebenso: wenn der Befehl **racadm config** -**f racadm.cfg** zur Angabe einer beliebigen Anzahl von zu schreibenden Gruppen/Objekten verwendet wird, kann der Index nicht angegeben werden. Ein neuer Benutzer wird zum ersten verfügbaren Index hinzugefügt. Diese Verfahrensweise bietet eine größere Flexibilität bei der Konfiguration mehrerer DRAC 5 mit gleichen Einstellungen.

DRAC 5-Benutzer hinzufügen

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

1. Geben Sie den Benutzernamen ein.
2. Geben Sie das Kennwort ein.
3. Geben Sie die Benutzerberechtigungen ein.
4. Aktivieren Sie den Benutzer.

Beispiel

Das folgende Beispiel beschreibt, wie man einen neuen Benutzer genannt "John" mit dem Kennwort "123456" und ANMELDUNGS-Berechtigung am RAC hinzufügt.

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

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

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

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

Zur Überprüfung einen der folgenden Befehle verwenden:

```
racadm getconfig -u john
```

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

Einen DRAC 5-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 Befehls-Syntax gezeigt, die zum Löschen eines Benutzers des RAC verwendet werden kann:

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

Eine Null-Kette von Anführungszeichen("") weist den DRAC 5 an, die Anwenderkonfiguration am angegebenen Index zu entfernen und die Anwenderkonfiguration auf die ursprünglichen Fabrikeinstellungen zurückzusetzen.

E-Mail-Warnung prüfen

Mit der RAC-E-Mail-Warnungsfunktion können Benutzer E-Mail-Warnungen erhalten, wenn ein kritisches Ereignis auf dem verwalteten System auftritt. Das folgende Beispiel zeigt, wie man die E-Mail-Warnungsfunktion überprüft, um sicherzustellen, dass der RAC ordnungsgemäß E-Mail-Warnungen über das Netzwerk versenden kann.

```
racadm testemail -i 2
```

ANMERKUNG: Stellen Sie sicher, dass die SMTP- und E-Mail-Warnungseinstellungen konfiguriert sind, bevor die E-Mail-Warnungsfunktion getestet wird. Für weitere Informationen siehe "E-Mail-Warnungen konfigurieren".

RAC-SNMP-Trap-Warnungsfunktion testen

Die RAC-SNMP-Trap-Warnungsfunktion ermöglicht SNMP-Trap-Zuhörerkonfigurationen, Traps für Systemereignisse zu erhalten, die auf dem verwalteten System auftreten.

Das folgende Beispiel zeigt, wie ein Benutzer die SNMP-Trap-Warnungsfunktion des RAC testen kann.

```
racadm testtrap -i 2
```

Bevor Sie die RAC-SNMP-Trap-Warnungsfunktion testen, stellen Sie sicher, dass die SNMP- und Trap-Einstellungen ordnungsgemäß konfiguriert sind. Siehe die **testtrap** und **testemail**-Unterbefehl-Beschreibungen, um diese Einstellungen zu konfigurieren.

DRAC 5-Benutzer mit Berechtigungen aktivieren

Um einen Benutzer mit den spezifischen administrativen Berechtigungen (rollenbasierte Autorität) zu aktivieren, finden Sie zuerst einen vorhandenen Benutzer-Index, indem Sie die Schritte in "Bevor Sie beginnen" ausführen. Geben Sie dann die folgenden Befehlszeilen mit dem neuen Benutzernamen und dem neuen Kennwort ein:

ANMERKUNG: Eine Liste der gültigen Bit-Maskenwerte für spezifische Benutzerberechtigungen finden Sie in Tabelle B-2. Der Standardberechtigungswert ist 0, was anzeigt, dass der Benutzer keine aktivierten Berechtigungen hat.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <Index> <Benutzer Berechtigung Bitmaskwert>
```

DRAC 5-Netzwerkeigenschaften konfigurieren

Geben Sie folgendes ein, um eine Liste verfügbarer Netzwerkeigenschaften zu erhalten:

```
racadm getconfig -g cfgLanNetworking
```

Wenn DHCP zum Erhalt einer IP-Adresse verwendet werden soll, kann der folgende Befehl zum Schreiben des Objekts **cfgNicUseDhcp** und zum Aktivieren dieser Funktion verwendet werden.

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

Die Befehle enthalten dieselbe Konfigurationsfunktionalität wie die Option ROM, wenn beim Systemstart <Strg><e> gedrückt werden soll. Weitere Informationen über die Konfiguration der Netzwerkeigenschaften mit der Option ROM finden Sie unter "DRAC 5-Netzwerkeigenschaften konfigurieren".

Im folgenden Beispiel wird gezeigt, wie der Befehl zur Konfiguration gewünschter LAN-Netzwerkeigenschaften verwendet werden kann.

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

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

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

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

ANMERKUNG: Wenn **cfgNicEnable** auf **0** gesetzt wird, ist das DRAC 5-LAN selbst dann deaktiviert, wenn DHCP aktiviert ist.

DRAC-Modi

Der DRAC 5 kann in einem von drei Modi konfiguriert werden:

- Dediziert
- Freigegeben
- Freigegeben für Failover

Tabelle 9-3 enthält eine Beschreibung jedes dieser Modi.

Tabelle 9-3. DRAC 5 NIC-Konfigurationen

Modus	Beschreibung
Dediziert	Der DRAC verwendet seine eigene NIC- (RJ-45 Anschluss) und die BMC MAC-Adresse für den Netzwerk-Verkehr.
Freigegeben	Der DRAC verwendet Broadcom LOM1 auf dem Planar.
Freigegeben für Failover	Der DRAC verwendet Broadcom LOM1 und LOM2 im Team für das Failover. Das Team verwendet die BMC MAC- Adresse.

Häufig gestellte Fragen

Tabelle 9-4 enthält die häufig gestellten Fragen und Antworten.

Tabelle 9-4. Serielle und Racadm-Befehle verwenden: Häufig gestellte Fragen

Frage	Antwort
Nachdem ich (unter Verwendung des Befehls **racadm racreset**) einen DRAC 5-Reset ausgeführt habe, gebe ich einen Befehl aus, worauf die folgende Meldung eingeblendet wird: racadm <*Befehlsname*> Transport: ERROR: (RC=-1) Was bedeutet diese Meldung?	Sie müssen warten, bis der DRAC 5-Reset abgeschlossen ist, bevor Sie einen anderen Befehl ausstellen.
Wenn ich die Befehle und Unterbefehle **racadm** verwende, bekomme ich Fehler, die ich nicht verstehe.	Bei der Verwendung von **racadm**-Befehlen und Unterbefehlen können ein oder mehrere der folgenden Fehler eintreten: - Lokale Fehlermeldungen - Probleme wie Syntax, typografische Fehler und falsche Namen. Beispiel: ERROR: <Meldung>
Wenn ich die DRAC-IP-Adresse von meinem System 'pinge' und dann meine DRAC 5-Karte zwischen den Modi **Reserviert** und **Freigegeben** während der Ping-Antwort umschalte, erhalte ich keine Antwort.	Löschen Sie die ARP-Tabelle auf Ihrem System.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Glossar

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

Active Directory

Active Directory ist ein zentralisiertes und standardisiertes System, das Netzwerkverwaltung von Benutzerdaten, Sicherheit und verteilten Ressourcen automatisiert, und Interoperation mit anderen Verzeichnissen aktiviert. Active Directory wird insbesondere für verteilte Netzwerkanschlussumgebungen hergestellt.

AGP

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

ARP

Akronym für Address Resolution Protocol (Adressenauflösungsprotokoll), wobei es sich um eine Methode handelt, 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), wobei es sich um den Teil der System-Software handelt, der die Schnittstelle unterster Ebene zu Peripheriegeräten darstellt und der die erste Stufe des Systemstartprozesses steuert, einschließlich des Ladens des Betriebssystems in den Speicher.

BMC

Abkürzung für Baseboard Management Controller (Basisplatinen-Verwaltungs-Controller), wobei es sich um die Controller-Schnittstelle zwischen dem DRAC 5 und dem BMC des verwalteten Systems.

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 zu treffen. Beispiele von CAs schließen Thawte und VeriSign ein. Nachdem die CA Ihre CSR erhält, prüfen und überprüfen die in der CSR enthaltenen Informationen. Wenn der Bewerber die Sicherheitsstandards von CA erfüllt, gibt die CA ein Zertifikat an den Bewerber aus, das diesen Bewerber identifiziert, um Transaktionen über Netzwerke und auf dem Internet vorzunehmen.

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 der 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 die Befehlszeilenschnittstelle.

CLP

Abkürzung für das Befehlszeilenprotokoll.

CSR

Abkürzung für die Zertifikatssignierungsanforderung.

DDNS

Abkürzung für das dynamische 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 die Bibliothek für dynamisches Verbinden, die eine Bibliothek von kleinen Programmen ist, von denen eins, wenn erforderlich, durch ein größeres Programm gerufen werden kann, das im System läuft. Das kleine Programm, das das größere Programm mit einem spezifischen Gerät wie ein Drucker oder Scanner kommunizieren lässt, wird oft als ein DLL-Programm (oder Datei) präsentiert.

DMTF

Abkürzung für Distributed Management Task Force.

DNS

Abkürzung für das Domänennamensystem.

DRAC 5

Abkürzung für den Dell Remote Access Controller 5.

DSU

Abkürzung für Disk Storage Unit (Festplattenspeichereinheit).

erweitertes Schema

Eine mit Active Directory verwendete Lösung, um Benutzerzugriff auf DRAC 5 zu bestimmen; verwendet von Dell definierte Active Directory-Objekte.

FQDN

Akronym für Völlig Qualifizierte Domänennamen. Microsoft® Active Directory® unterstützt nur FQDN bis zu maximal 64 Bytes.

FSMO

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), wobei es sich um die Standard-Uhrzeit handelt, die an jedem Ort der Welt gültig ist. GMT stellt normalerweise die mittlere Sonnenzeit entlang des Nullmeridians dar, der durch das Greenwich Observatory außerhalb von London, GB verläuft.

GPIO

Abkürzung für allgemeine Eingabe/Ausgabe.

GRUB

Akronym für GRand Unified Bootloader, ein neuer und allgemein verwendeter Linux-Lader.

GUI

Abkürzung für Graphical User Interface (Graphische Benutzeroberfläche), die eine Anzeigenoberfläche eines Computers darstellt, in der Elemente wie z. B. Fenster, Dialogfelder und Schaltflächen verwendet werden, im Gegensatz zu einer Befehlsaufforderungsschnittstelle, in der alle Eingaben und Anzeigen als Text dargestellt werden.

Hardwareprotokoll

Zeichnet durch den DRAC 5 und BMC erstellte Ereignisse auf.

ICMB

Abkürzung für Intelligent Chassis Management Bus (Intelligenter Gehäuseverwaltungsbus).

ICMP

Abkürzung für Internet-Steuerungsmeldungsprotokoll.

ID

Abkürzung für Identifier (Bezeichner), wird normalerweise als Bezeichnung für einen Benutzer-Bezeichner (Benutzer-ID) oder Objekt-Bezeichner (Objekt-ID) verwendet.

IP

Abkürzung für Internet Protocol (Internet-Protokoll), wobei es sich um die Netzwerkschicht für TCP/IP handelt. IP ermöglicht Paket-Routing, Fragmentierung und Reorganisation.

IPMB

Abkürzung für den intelligenten Plattformverwaltungsbus, der ein in der Systemverwaltungstechnologie verwendeter Bus ist.

IPMI

Abkürzung für Intelligent Platform Management Interface (Intelligente Plattformverwaltungsschnittstelle), wobei es sich um einen Teil der Systemverwaltungstechnologie handelt.

Kbps

Abkürzung für Kilobits per Second (Kilobit pro Sekunde), wobei es sich um eine Datentransferrate handelt.

Konsolenumleitung

Konsolenumleitung ist eine Funktion, die den Anzeigenbildschirm sowie die Maus- und Tastaturfunktionen eines verwalteten Systems an die entsprechenden Geräte einer Verwaltungsstation umleitet. Dann kann die Systemkonsole der Verwaltungsstation zur Steuerung des verwalteten Systems verwendet werden.

LAN

Abkürzung für Local Area Network (Lokales Netzwerk).

LDAP

Abkürzung für das Leichtgewichtsverzeichniszugriffsprotokoll.

LED

Abkürzung 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), wobei es sich um eine Netzwerkunterschicht zwischen einem Netzwerkknoten und der physikalischen Netzwerkschicht handelt.

MAC-Adresse

Akronym für Datenträger-Access Control-Adresse, die eine einzigartige in den physischen Komponenten einer NIC eingebettete Adresse ist.

MAPE

Abkürzung für Manageability Access Point (Verwaltungsfunktionenzugriffspunkt).

Mbps

Abkürzung für Megabits per Second (Megabit pro Sekunde), wobei es sich um eine Datentransferrate handelt.

MIB

Abkürzung für Management Information Base (Verwaltungsinformationsbasis).

MII

Abkürzung für Media Independent Interface (Datenträgerunabhängige Schnittstelle).

NAS

Abkürzung für dem Netzwerk beigefügter Speicher.

NIC

Abkürzung für die Netzwerkschnittstellenkarte. Eine in einem Computer installierte Adapterleiterplatte, um eine direktleitende Verbindung zu einem Netzwerk zu bieten.

OID

Abkürzung für Objektbezeichner.

PCI

Abkürzung für Peripheral Component Interconnect (Verbindung peripherer Komponenten), wobei es sich um eine Standardschnittstellen- und Bustechnologie zum Anschluss von Peripheriegeräten an ein System und zur Kommunikation mit diesen Peripheriegeräten handelt.

POST

Akronym für Power-On Self-Test (Einschaltselbsttest), wobei es sich um eine Folge von Diagnosetests handelt, die automatisch beim Einschalten eines Systems ausgeführt werden.

PPP

Abkürzung für Point-to-Point Protocol (Punkt-zu-Punkt-Protokoll), wobei es sich um das Standardinternetprotokoll zur Übertragung von Netzwerkschicht-Datagrammen (wie z. B. IP-Pakete) über serielle Punkt-zu-Punkt-Verknüpfungen handelt.

RAC

Abkürzung für Remote Access Controller (Remote Access Controller).

RAM disk

Ein speicherresidentes Programm, das ein Festplattenlaufwerk emuliert. Der DRAC 5 besitzt eine RAM-Disk im Speicher.

RAM

Akronym für Random-Access Memory (Speicher mit wahlfreiem Zugriff). RAM ist der allgemeine lesbare und beschreibbare Speicher in Systemen und im DRAC 5.

ROM

Akronym für Read-Only Memory (Nur-Lesen-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 Packet-Verwaltungssystem 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 den Service-Zugriffspunkt.

SEL

Akronym für das Systemereignisprotokoll.

SMI

Abkürzung für das Systems Management Interrrupt.

SMTP

Abkürzung für Simple Mail Transfer Protocol (Einfaches Mail-Übertragungsprotokoll), das verwendet wird, um elektronische Post zwischen Systemen, gewöhnlich über ein Ethernet, zu übertragen.

SMWG

Abkürzung für Systems Management Working Group (Systems Management- Arbeitsgruppe).

SNMP

Abkürzung für Simple Network Management Protocol (Einfaches Netzwerkverwaltungsprotokoll), wobei es sich um ein Protokoll zur Verwaltung von Knoten in einem IP-Netzwerk handelt. DRAC 5 sind SNMP-verwaltete Geräte (Knoten).

SNMP-Trap

Eine vom DRAC 5 oder von einem BMC erzeugte Meldung (Ereignis), die Informationen über Statusänderungen auf dem verwalteten System oder über mögliche Hardwarestörungen enthält.

SSH

Abkürzung für Secure Shell.

SSL

Abkürzung für die Secure Socket Layer (Sichere Sockelschicht).

Standardschema

Eine mit Active Directory verwendete Lösung, um Benutzerzugriff auf DRAC 5 zu bestimmen; verwendet nur Active Directory-Gruppenobjekte.

TAP

Abkürzung für Telelocator Alphanumeric Protocol (Telelocator alphanumerisches Protokoll), wobei es sich um ein Protokoll zum Senden von Anfragen an einen Funkrufdienst handelt.

TCP/IP

Abkürzung für Transmission Control Protocol/Internet Protocol (Übertragungssteuerungsprotokoll/Internetprotokoll), das den Standard-Ethernetprotokollsatz repräsentiert, der die Protokolle der Netzwerkschicht und der Übertragungsschicht enthält.

TFTP

Abkürzung für Trivial File Transfer Protocol (Trivial-Dateiübertragungsprotokoll), wobei es sich um ein einfaches Dateiübertragungsprotokoll handelt, das zum Herunterladen von Startcode auf datenträgerlose Geräte oder Systeme verwendet wird.

UPS (USV)

Abkürzung für Unterbrechungsfreie Stromversorgung.

USB

Abkürzung für den Universalen Seriellen Bus.

UTC

Abkürzung für Universal Coordinated Time (Koordinierte Weltzeit). *Siehe* GMT.

verwaltetes System

Das verwaltete System ist das System, in dem der DRAC 5 installiert oder eingebettet wird.

Verwaltungsstation

Die Verwaltungsstation ist ein System dass im Remote-Zugriff auf den DRAC 5 zugreift.

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, das von den meisten allgemeinen Terminal-Emulationsprogrammen verwendet wird.

WAN

Abkürzung für Wide Area Network (Weitbereichsnetzwerk).

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Dell™ Remote Access Controller 5 Firmware-Version 1.20: Benutzerhandbuch

ANMERKUNG: Eine ANMERKUNG zeigt wichtige Informationen an, die Ihnen helfen, Ihren Computer effektiver einzusetzen.

HINWEIS: Ein HINWEIS zeigt entweder einen eventuellen Hardwareschaden oder Datenverlust an und weist darauf hin, wie das Problem vermieden werden kann.

Zurück zum Inhaltsverzeichnis