Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

---

Anmerkungen und Vorsichtshinweise

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

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

2011 - 02

Zurück zum Inhaltsverzeichnis

Übersicht der RACADM-Unterbefehle

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

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

Hilfe

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **An DRAC 5 anmelden** verfügen.

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

Tabelle A-1. Befehl help

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

Zusammenfassung

```
racadm help

racadm help <Unterbefehl>
```

Beschreibung

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

Ausgabe

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

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

arp

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

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

Tabelle A-2. Befehl arp

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

Zusammenfassung

```
racadm arp
```

Unterstützte Schnittstellen

- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

clearasrscreen

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

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

Tabelle A-3. clearasrscreen

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

Zusammenfassung

```
racadm clearasrscreen
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

config

ANMERKUNG: Um den Befehl **getconfig** verwenden zu können, müssen Sie über die Berechtigung **An DRAC 5 anmelden** verfügen.

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

Tabelle A-4. config / getconfig

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

Zusammenfassung

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

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

Beschreibung

Mit dem Unterbefehl **config** kann der Benutzer die Konfigurationsparameter von DRAC 5 einzeln festlegen oder diese als Teil einer Konfigurationsdatei stapelverarbeiten. Wenn sich die Daten unterscheiden, wird das DRAC 5-Objekt mit dem neuen Wert geschrieben.

Eingabe

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

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

Tabelle A-5. Optionen und Beschreibungen des Unterbefehls config

Option	Beschreibung
-f	Mit der Option **-f <Dateiname>** kann **config** den Inhalt der durch **<Dateiname>** angegebenen Datei lesen und DRAC 5 konfigurieren. Die Datei muss Daten enthalten, die dem unter Parsing-Regeln festgelegten Format entsprechen.
-p	Die Option **-p** bzw. die Kennwortoption weist **config** an, die Kennworteinträge in der config-Datei **-f <Dateiname>** zu löschen, sobald die Konfiguration abgeschlossen wurde.
-g	Die Option **-g <Gruppenname>** bzw. die Gruppenoption muss zusammen mit der Option **-o** verwendet werden. Der <*Gruppenname*> gibt die Gruppe an, in der das einzustellende Objekt enthalten ist.
-o	Die Option **-o <Objektname> <Wert>** bzw. die Objektoption muss zusammen mit der Option **-g** verwendet werden. Diese Option legt den Objektnamen fest, der mit der Zeichenkette <*Wert*> geschrieben wird.
-i	Die Option **-i <Index>** bzw. die Indexoption ist nur für indizierte Gruppen gültig und kann zur Bestimmung einer eindeutigen Gruppe verwendet werden. Der <*Index*> ist eine ganze Dezimalzahl von 1 bis 16. Der Index wird hier durch den Indexwert bestimmt und nicht durch einen „benannten" Wert.
-c	Die Option **-c** bzw. die Überprüfungsoption wird zusammen mit dem Unterbefehl **config** verwendet und ermöglicht 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 zu DRAC 5 erfolgen nicht. Diese Option ist nur eine Kontrolle.

Ausgabe

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

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

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

Beispiele

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

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

- `racadm config -f myrac.cfg`

  Konfiguriert DRAC 5 oder konfiguriert diesen neu. Die Datei **myrac.cfg** kann aus dem Befehl **getconfig** erstellt werden. Die Datei **myrac.cfg** kann auch manuell bearbeitet werden, solange die Parsing-Richtlinien befolgt werden.

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

---

getconfig

Beschreibung des Unterbefehls getconfig

Mit dem Unterbefehl **getconfig** kann der Benutzer DRAC 5-Konfigurationsparameter einzeln abrufen, oder es können alle RAC-Konfigurationsgruppen abgerufen und in einer Datei gespeichert werden.

Eingabe

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

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

Tabelle A-6. Optionen des Unterbefehls getconfig

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

Ausgabe

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

- Ungültige Syntax, ungültiger Gruppenname, Objektname, Index oder andere ungültige Datenbankmitglieder
- racadm-CLI-Transportfehler

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

Beispiele

- `racadm getconfig -g cfgLanNetworking`

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

- `racadm getconfig -f myrac.cfg`

  Speichert alle Gruppenkonfigurationsobjekte von RAC in **myrac.cfg**.

- `racadm getconfig -h`

  Zeigt eine Liste der verfügbaren Konfigurationsgruppen in DRAC 5 an.

- `racadm getconfig -u root`

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

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

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

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/RACADM seriell

---

coredump

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

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

Tabelle A-7. coredump

Unterbefehl	Definition
coredump	Zeigt den letzten Core Dump von DRAC 5 an.

Zusammenfassung

`racadm coredump`

Beschreibung

Mit dem Unterbefehl **coredump** werden detaillierte Informationen im Zusammenhang mit kritischen Problemen angezeigt, die kürzlich am RAC aufgetreten sind. Die coredump-Informationen können zur Diagnose dieser kritischen Probleme eingesetzt werden.

Wenn verfügbar, sind die Coredump-Informationen über Ein-/Ausschaltzyklen des RAC beständig und bleiben verfügbar, bis eine der folgenden Bedingungen eintritt:

- Die coredump-Informationen werden mit dem Unterbefehl **coredumpdelete** gelöscht.
- Auf dem RAC tritt ein weiterer kritischer Zustand ein. In diesem Fall beziehen sich die coredump-Informationen auf den zuletzt aufgetretenen kritischen Fehler.

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

Unterstützte Schnittstellen

- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

coredumpdelete

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

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

Tabelle A-8. coredumpdelete

Unterbefehl	Definition
coredumpdelete	Löscht den auf DRAC 5 gespeicherten Core Dump.

Zusammenfassung

```
racadm coredumpdelete
```

Beschreibung

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

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

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

fwupdate

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

ANMERKUNG: Lesen Sie die zusätzlichen Anleitungen unter Verbindung zum verwalteten System über die lokale serielle Schnittstelle oder die Telnet-Management Station (Kundensystem) herstellen, bevor Sie mit der Firmware-Aktualisierung beginnen.

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

Tabelle A-9. fwupdate

Unterbefehl	Definition
fwupdate	Aktualisiert die Firmware von DRAC 5.

Zusammenfassung

```
racadm fwupdate -s

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

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

Beschreibung

Mit dem Unterbefehl **fwupdate** können Benutzer die Firmware von 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/RACADM seriell

Eingabe

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

ANMERKUNG: Die Option **-p** wird vom lokalen und Remote-RACADM unterstützt, nicht jedoch durch die seriellen/Telnet/SSH-Konsole. Die Option **-p** wird auf der Linux-Plattform nicht unterstützt.

Tabelle A-10. Optionen des Unterbefehls fwupdate

Option	Beschreibung
-u	Die Option **Aktualisierung** führt einen Prüfsummentest der Firmware-Aktualisierungsdatei durch und startet das eigentliche Aktualisierungsverfahren. Diese Option kann zusammen mit den Optionen **-g** oder **-p** verwendet werden. Nach der Aktualisierung führt DRAC 5 einen Soft-Reset durch.
-s	Die Option **Status** gibt Informationen zum derzeitigen Status des Aktualisierungsverfahrens aus. Diese Option wird immer allein verwendet.
-g	Die Option **get** weist die Firmware an, die Firmware-Aktualisierungsdatei vom TFTP-Server abzurufen. Der Benutzer muss auch die Optionen **-a** und **-d** angeben. Da die Option **-a** nicht zur Verfügung steht, werden die Standardeinstellungen in den Eigenschaften der Gruppe **cfgRemoteHosts** gelesen, wobei die Eigenschaften **cfgRhostsFwUpdateIpAddr** und **cfgRhostsFwUpdatePath** verwendet werden.
-a	Die Option **IP-Adresse** gibt die IP-Adresse des TFTP-Servers an.
-d	Die Option **-d** bzw. **Verzeichnis** bestimmt das Verzeichnis auf dem TFTP-Server oder auf dem Hostserver von DRAC 5, auf dem sich die Firmware-Aktualisierungsdatei befindet.
-p	Die Option **-p** bzw. **put** wird zum Aktualisieren der Firmware-Datei vom verwalteten System zu 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 a**ngegeben) auf dem TFTP-Server auf eine bestimmte IP-Adresse (durch die Option **-a** angegeben) herunterzuladen. Nachdem die Abbilddatei vom TFTP-Server heruntergeladen wurde, beginnt der Aktualisierungsvorgang. Nach Abschluss dieses Vorgangs wird DRAC 5 zurückgesetzt.

  Wenn der Download länger als 15 Minuten dauert und das Zeitlimit überschreitet, übertragen Sie das Firmware-Flash-Abbild 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 aus.

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

  In diesem Beispiel wird das Firmware-Abbild 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 <Abbilder>`

  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 vom lokalen und Remote-RACADM unterstützt, nicht jedoch durch die seriellen/Telnet/SSH-Konsole. Die Option **-p** wird auf der Linux-Plattform nicht unterstützt.

---

getssninfo

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **An DRAC 5 anmelden** verfügen.

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

Tabelle A-11. Unterbefehl getssninfo

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

Zusammenfassung

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

Beschreibung

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

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

Eingabe

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

Tabelle A-12. Optionen des Unterbefehls getssninfo

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

Beispiele

- racadm getssninfo

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

Tabelle A-13. Ausgabebeispiel des Unterbefehls getssninfo

Benutzer	IP-Adresse	Typ	Konsolen
root	192.168.0.10	Telnet	Virtuelle KVM

- racadm getssninfo -A

  "root" 143.166.174.19 "Telnet" "KEINE"

- racadm getssninfo -A -u *

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

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

---

getsysinfo

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **An DRAC 5 anmelden** verfügen.

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

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 im Zusammenhang mit der Konfiguration des RAC, verwalteten Systems und Watchdogs angezeigt.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

Eingabe

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

Tabelle A-15. Optionen des Unterbefehls getsysinfo

Option	Beschreibung

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

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

Ausgabe

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

Beispielausgabe

```
RAC-Informationen:

RAC Datum/Zeit             = Mon 26. Okt 19:05:33 2009

Firmware-Version           = 1.50

Firmware-Build             = 09.10.21

Letztes Firmware Update    = Mit 21. Okt 21:57:33 2009

Hardware-Version           = A00

Aktuelle IP-Adresse        = 192.168.1.21

Aktuelles IP-Gateway       = 0.0.0.0

Aktuelle IP-Netzmaske      = 255.255.255.0

DHCP Aktiviert             = 1

MAC-Adresse                = 00:1c:23:d7:1a:d9

Aktueller DNS-Server 1     = 0.0.0.0

Aktueller DNS-Server 2     = 0.0.0.0

DNS-Server vom DHCP        = 0

DNS-RAC-Name registrieren  = 0

DNS-RAC-Name               = rac-297GP1S

Aktuelle DNS-Domäne        =

Systeminformationen:

Systemmodell              = PowerEdge 2950

Systemrevision            = [-]

System-BIOS-Version       = 1.3.7

BMC-Firmware-Version      = 02.28

Service-Tag               = 297GP1S

Express-Servicenummer     = 4910296528

Hostname                  =

BS-Name                       =

Stromstatus                   = EIN

Watchdog-Informationen:

Wiederherstellungsmaßnahme     = Keine

Aktueller Countdown-Wert       = 15 Sekunden

Anfänglicher Countdown-Wert    = 15 Sekunden

Integrierte NIC-MAC-Adressen:
```

```
NIC1-Ethernet                 = 00:1A:A0:11:93:68

NIC2-Ethernet                 = 00:1A:A0:11:93:6A
```

Beispiele

```
racadm getsysinfo -A -s

"Systeminformationen:" "PowerEdge 2900" "A08" "1.0" "EF23VQ-0023" "Hostname"

"Microsoft Windows 2000 Version 5.0, Build-Nr. 2195, Service Pack 2" "EIN"

racadm getsysinfo -w -s

Systeminformationen:
Systemmodell                  = PowerEdge 2900
System-BIOS-Version           = 0.2.3
BMC-Firmware-Version          = 0.17
Service-Tag-Nummer            = 48192
Express-Servicenummer         = 4910296528
Host-Name                     = racdev103
BS-Name                       = Microsoft Windows Server 2003
Stromstatus                   = AUS


Watchdog-Informationen:
Wiederherstellungsmaßnahme    = Keine
Aktueller Countdown-Wert      = 0 Sekunden
Anfänglicher Countdown-Wert   = 0 Sekunden
```

Einschränkungen

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

---

getractime

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **An DRAC 5 anmelden** verfügen.

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

Tabelle A-16. getractime

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

Zusammenfassung

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

Beschreibung

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

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

Ausgabe

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

Beispielausgabe

```
racadm getractime

Don Dez 8 20:15:26 2005

racadm getractime -d

20051208201542.000000
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

ifconfig

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **Diagnosebefehle ausführen** oder **DRAC 5 konfigurieren** verfügen.

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

Tabelle A-17. ifconfig

Unterbefehl	Definition
ifconfig	Zeigt den Inhalt der Netzwerkschnittstellentabelle an.

Zusammenfassung

```
racadm ifconfig
```

---

netstat

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

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

Tabelle A-18. netstat

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

Zusammenfassung

```
racadm netstat
```

Unterstützte Schnittstellen

- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

ping

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **Diagnosebefehle ausführen** oder **DRAC 5 konfigurieren** verfügen.

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

Tabelle A-19. ping

Unterbefehl	Definition
ping	Überprüft, ob die Ziel-IP-Adresse von DRAC 5 aus mit dem aktuellen Routingtabelleninhalt erreichbar ist. Eine Ziel-IP-Adresse ist erforderlich. Ein ICMP-Echo-Paket wird zur Ziel-IP-Adresse gesendet, basierend auf dem Inhalt der aktuellen Routingtabelle.

Zusammenfassung

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

Unterstützte Schnittstellen

- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

setniccfg

ANMERKUNG: Um den Befehl **setniccfg** verwenden zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

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

Tabelle A-20. setniccfg

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

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

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-Verwaltungs-Port (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 entsprechende Fehlermeldung angezeigt, wenn der Vorgang nicht erfolgreich ist. Wenn erfolgreich, wird eine Meldung angezeigt.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

getniccfg

ANMERKUNG: Um den Befehl **getniccfg** verwenden zu können, müssen Sie über die Berechtigung **An DRAC 5 anmelden** verfügen.

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

Tabelle A-21. setniccfg / getniccfg

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

Zusammenfassung

```
racadm getniccfg
```

Beschreibung

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

Beispielausgabe

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

```
NIC Aktiviert     = 1

DHCP Aktiviert    = 1

IP-Adresse        = 192.168.0.1

Subnetzmaske      = 255.255.255.0

Gateway           = 192.168.0.1
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

getsvctag

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **An DRAC 5 anmelden** verfügen.

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

Tabelle A-22. getsvctag

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

Zusammenfassung

```
racadm getsvctag
```

Beschreibung

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

Beispiel

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

```
Y76TP0G
```

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

racdump

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

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

Tabelle A-23. racdump

Unterbefehl	Definition
racdump	Zeigt Status- und allgemeine Informationen zu DRAC 5 an.

Zusammenfassung

```
racadm racdump
```

Beschreibung

Der Unterbefehl **racdump** enthält einen einzigen Befehl, mit dem Informationen zu Dump und Status sowie allgemeine DRAC 5-Karteninformationen abgerufen werden können.

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

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

Unterstützte Schnittstellen

- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

racreset

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

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

Tabelle A-24. racreset

Unterbefehl	Definition
racreset	Setzt DRAC 5 zurück.

VORSICHTSHINWEIS: Wenn Sie einen racreset-Unterbefehl ausgeben, kann DRAC bis zu einer Minute benötigen, um zu einem einsatzfähigen Zustand zurückzukehren.

Zusammenfassung

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

Beschreibung

Der Unterbefehl **racreset** gibt einen Reset an 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.

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

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

Tabelle A-25. Optionen des Unterbefehls racreset

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

---

racresetcfg

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

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

Tabelle A-26. racresetcfg

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

Zusammenfassung

```
racadm racresetcfg
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

Beschreibung

Der Befehl **racresetcfg** entfernt alle vom Benutzer konfigurierten Einträge der Datenbankeigenschaften. 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 DRAC 5 automatisch zurückgesetzt.

VORSICHTSHINWEIS: Mit diesem Befehl wird die aktuelle RAC-Konfiguration gelöscht und der RAC sowie die serielle Konfiguration werden auf die ursprünglichen Standardeinstellungen zurückgesetzt. Nach dem Reset lauten der Standardname und das Standardkennwort root bzw. calvin, und die IP-Adresse 192.168.0.120. Wenn Sie den Befehl racresetcfg von einem Netzwerk-Client (z. B. einem unterstützten Internet-Browser, Telnet/ssh oder Remote-RACADM) ausgeben, müssen Sie die Standard-IP-Adresse verwenden.

ANMERKUNG: Mit diesem Unterbefehl wird auch die serielle Schnittstelle auf ihre Standard-Baudrate (57600) und auf ihren standardmäßigen COM-Anschluss zurückgesetzt. Die seriellen Einstellungen müssen eventuell über den BIOS-Setup-Bildschirm für den Server neu konfiguriert werden, damit über die serielle Schnittstelle auf den RAC zugegriffen werden kann.

---

serveraction

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

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

Tabelle A-27. serveraction

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

Zusammenfassung

```
racadm serveraction <Maßnahme>
```

Beschreibung

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

Tabelle A-28. Optionen des Unterbefehls serveraction

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

Ausgabe

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

getraclog

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **An DRAC 5 anmelden** verfügen.

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-Protokolleinträge an.

Zusammenfassung

```
racadm getraclog -i

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

Beschreibung

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

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

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

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

Ausgabe

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

Beispielausgabe

```
Datensatz:        1
Datum/Uhrzeit:    8. Dez 08:10:11
Quelle:           Anmeldung[433]
Beschreibung:     root-Anmeldung von 143.166.157.103
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

clrraclog

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

Zusammenfassung

```
racadm clrraclog
```

Beschreibung

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

---

getsel

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **An DRAC 5 anmelden** verfügen.

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

Tabelle A-30. getsel

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

Zusammenfassung

```
racadm getsel-i

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

Beschreibung

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

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

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

-c - Zeigt die Höchstanzahl der zurückzugebenden Einträge an.

-o - Zeigt die Ausgabe auf einer Zeile an.

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

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

-R - Es werden nur die unformatierten Daten gedruckt.

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

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

Ausgabe

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

Beispiel:

```
Datensatz:       1
Datum/Uhrzeit:   16.11.05 22:40:43
Schweregrad:     OK
Beschreibung:    Systemplatinen-SEL: Ereignisprotokollsensor für Systemplatine, gelöschtes Protokoll wurde bestätigt
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

clrsel

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

Zusammenfassung

```
racadm clrsel
```

Beschreibung

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

gettracelog

ANMERKUNG: Um diesen Befehl verwenden zu können, müssen Sie über die Berechtigung **An DRAC 5 anmelden** verfügen.

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

Tabelle A-31. gettracelog

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

Zusammenfassung

```
racadm gettracelog -i

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

Beschreibung

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

-i – Zeigt die Anzahl der Einträge im DRAC 5-Ablaufverfolgungsprotokoll an.

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

-o – Zeigt die Ausgabe auf einer Zeile an.

-c – Gibt die Anzahl der anzuzeigenden Datensätze an.

-s – Gibt den anzuzeigenden Startdatensatz an.

-A – Zeigt Kopfzeilen oder Kennzeichnungen nicht an.

Ausgabe

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

Beispiel:

```
Datensatz:        1

Datum/Uhrzeit:    Dez 8 08:21:30

Quelle:           ssnmgrd[175]

Beschreibung:     root von 143.166.157.103: Sitzungszeitüberschreibung sid 0be0aef4
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

sslcsrgen

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

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

Tabelle A-32. sslcsrgen

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

Zusammenfassung

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

racadm sslcsrgen -s
```

Beschreibung

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

Optionen

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

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

Tabelle A-33. Optionen des Unterbefehls sslcsrgen

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

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

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

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

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

Einschränkungen

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

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

Beispiele

```
racadm sslcsrgen -s

oder

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

sslcertupload

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

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

Tabelle A-34. sslcertupload

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

Zusammenfassung

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

Optionen

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

Tabelle A-35. Optionen des Unterbefehls sslcertupload

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

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

Einschränkungen

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

Beispiel

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

sslcertdownload

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

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

Tabelle A-36. sslcertdownload

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

Zusammenfassung

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

Optionen

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

Tabelle A-37. Optionen des Unterbefehls sslcertdownload

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

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

Einschränkungen

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

Beispiel

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

sslcertview

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

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

Tabelle A-38. sslcertview

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

Zusammenfassung

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

Optionen

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

Tabelle A-39. Optionen des Unterbefehls sslcertview

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

Ausgabebeispiel

```
racadm sslcertview -t 1

Seriennummer                    : 00

Informationen des Antragstellers :
Landescode (CC)                 : USA
Staat (S)                       : Texas
Standort (L)                    : Round Rock
Organisation (O)                : Dell Inc.
Organisationseinheit (OU)       : Remote-Zugriffs-Gruppe
Allgemeiner Name (CN)           : DRAC5-Standardzertifikat

Informationen des Ausstellers:
Landescode (CC)                 : USA
Staat (S)                       : Texas
Standort (L)                    : Round Rock
Organisation (O)                : Dell Inc.
Organisationseinheit (OU)       : Remote-Zugriffs-Gruppe
Allgemeiner Name (CN)           : DRAC5-Standardzertifikat

Gültig ab                  : 8. Jul 16:21:56 2005 MGZ
Gültig bis                 : 7. Jul 16:21:56 2010 MGZ

racadm sslcertview -t 1 -A

00
USA
Texas
Round Rock
Dell Inc.
Remote-Zugriffs-Gruppe
DRAC5-Standardzertifikat
USA
Texas
Round Rock
Dell Inc.
Remote-Zugriffs-Gruppe
DRAC5-Standardzertifikat
8. Jul 16:21:56 2005 MGZ
7. Jul 16:21:56 2010 MGZ
```

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

sslkeyupload

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

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

Tabelle A-40. sslkeyupload

Unterbefehl	Beschreibung
sslkeyupload	Lädt den SSL-Schlüssel vom Client zu DRAC 5.

Zusammenfassung

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

Optionen

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

Tabelle A-41. Optionen des Unterbefehls sslkeyupload

Option	Beschreibung
-t	Gibt den hochzuladenden Schlüssel an. 1 = Serverzertifikat
-f	Gibt den Dateinamen des hochzuladenden Zertifikats an. Wenn die Datei nicht angegeben wird, wird die Datei **sslcert** im aktuellen Verzeichnis ausgewählt.

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

Einschränkungen

Der Unterbefehl **sslkeyupload** kann nur von einem lokalen oder einem Remote-RACADM-Client aus ausgeführt werden. Der Unterbefehl **sslcsrgen** kann nicht über die serielle, Telnet- oder SSH-Schnittstelle verwendet werden.

Beispiel

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

sslresetcfg

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

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

Tabelle A-42. sslresetcfg

Unterbefehl	Beschreibung
sslresetcfg	Setzt das Web-Server-Zertifikat auf die werkseitigen Standardwerte zurück und startet den Web-Server neu. Das Zertifikat wird 30 Sekunden nach Eingabe des Befehls gültig.

Zusammenfassung

```
racadm sslresetcfg
```

Beispiel

```
$ racadm sslresetcfg
```

Das Zertifikat wurde erfolgreich generiert und der Webserver neu gestartet.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/Seriell

---

krbkeytabupload

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

Tabelle A-43 beschreibt den Unterbefehl **krbkeytabupload**.

Tabelle A-43. kerbkeytabupload

Unterbefehl	Beschreibung
krbkeytabupload	Eine Kerberos-Keytab-Datei hochladen.

Zusammenfassung

```
racadm krbkeytabupload [-f <Dateiname>]
```

Optionen

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

Tabelle A-44. krbkeytabupload-Unterbefehlsoptionen

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

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

Einschränkungen

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

Beispiel

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

testemail

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

Tabelle A-45. testemail-Konfiguration

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

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-Gruppe cfgEmailAlert aktiviert und ordnungsgemäß konfiguriert ist. Tabelle A-46 enthält eine Liste und zugehörige Befehle für die **cfgEmailAlert**-Gruppe.

Tabelle A-46. testemail-Konfiguration

Maßnahme	Befehl
Aktiviert die Warnung	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
Legen Sie die Ziel-E-Mail-Adresse fest	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 Benutzer1@meineFirma.com
Legen Sie die benutzerdefinierte Nachricht fest, die zur Ziel-E-Mail-Adresse gesendet werden soll	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "Dies ist ein Test!"
Stellen Sie sicher, dass die SNMP-IP-Adresse korrekt konfiguriert ist	racadm config -g cfgRemoteHosts -o cfgRhostsSmptServerIpAddr -i 192.168.0.152
Zeigen Sie die aktuellen E-Mail-Warnungseinstellungen an	racadm getconfig -g cfgEmailAlert -i <*Index*> wobei <*Index*> eine Zahl von 1 bis 4 ist

Optionen

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

Tabelle A-47. testemail-Unterbefehle

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

Ausgabe

Keine.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

testtrap

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

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

Tabelle A-48. testtrap

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

Zusammenfassung

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

Beschreibung

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

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

Tabelle A-49 enthält eine Liste und zugehörige Befehle für die Gruppe cfgIpmiPet.

Tabelle A-49. cfgEmailAlert-Befehle

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

Eingabe

Tabelle A-50 beschreibt die Optionen des Unterbefehls **testtrap**.

Tabelle A-50. Optionen des Unterbefehls testtrap

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

vmdisconnect

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

Tabelle A-51 beschreibt den Unterbefehl **vmdisconnect**.

Tabelle A-51. vmdisconnect

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

Zusammenfassung

```
racadm vmdisconnect
```

Beschreibung

Mit dem Unterbefehl **vmdisconnect** kann ein Benutzer die Sitzung des virtuellen Datenträgers eines anderen Benutzers unterbrechen. Wenn unterbrochen, spiegelt die Internet-basierte Benutzeroberfläche den korrekten Verbindungsstatus wider. Diese Funktion steht nur über die Anwendung des lokalen oder Remote-racadm zur Verfügung.

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 über die Internet-basierte RAC-Schnittstelle oder durch Verwendung des Unterbefehls **getsysinfo** racadm angezeigt werden.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

vmkey

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

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

Tabelle A-52. vmkey

Unterbefehl	Beschreibung
vmkey	Führt schlüsselbezogene Vorgänge des virtuellen Datenträgers aus.

Zusammenfassung

```
racadm vmkey <Maßnahme>
```

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

Beschreibung

Wenn ein benutzerdefiniertes Schlüsselimage des virtuellen Datenträgers zum RAC hochgeladen wird, wird die Schlüsselgröße zur Imagegröße. Der vmkey-Unterbefehl kann verwendet werden, um den Schlüssel auf seine ursprüngliche Standardgröße zurückzusetzen, d. h. 16 MB auf dem DRAC 5.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

usercertupload

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

Tabelle A-53 beschreibt den Unterbefehl **usercertupload**.

Tabelle A-53. usercertupload

Unterbefehl	Beschreibung
usercertupload	Lädt ein Benutzer- oder CA-Zertifikat vom Client zu DRAC hoch.

Zusammenfassung

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

Optionen

Tabelle A-54 beschreibt die Optionen des Unterbefehls **usercertupload**.

Tabelle A-54. Optionen des Unterbefehls usercertupload

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

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

Einschränkungen

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

Beispiel

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

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM

---

usercertview

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

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

Tabelle A-55. usercertview

Unterbefehl	Beschreibung
usercertview	Zeigt das das auf DRAC vorhandene Benutzer- oder CA-Zertifikat an.

Zusammenfassung

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

Optionen

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

Tabelle A-56. Optionen des Unterbefehls sslcertview

Option	Beschreibung
-t	Gibt den Typ des anzuzeigenden Zertifikats an, entweder das Benutzerzertifikat oder das Benutzer-Zertifizierungsstellenzertifikat. 1 = Benutzerzertifikat 2 = Benutzer-Zertifizierungsstellenzertifikat
-A	Verhindert das Drucken von Kopfzeilen/Bezeichnungen.
-i	Indexnummer des Benutzers. Gültige Werte sind 1 - 16.

Unterstützte Schnittstellen

- Lokaler RACADM
- Remote-RACADM
- Telnet/SSH/RACADM seriell

---

localConRedirDisable

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

Tabelle A-57 beschreibt den Unterbefehl **localConRedirDisable**.

Tabelle A-57. localConRedirDisable

Unterbefehl	Beschreibung
localConRedirDisable	Deaktiviert die Konsolenumleitung auf die Management Station.

Zusammenfassung

`racadm localConRedirDisable <Option>`

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

Unterstützte Schnittstellen

- Lokaler RACADM

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Gruppen- und Objektdefinitionen der DRAC 5-Eigenschaftendatenbank

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Die DRAC 5-Eigenschaftendatenbank enthält die Konfigurationsinformationen für 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 Eigenschaftendatenbank unterstützt werden, werden in diesem Abschnitt aufgeführt.

Verwenden Sie die Gruppe und Objekt-IDs mit dem Dienstprogramm racadm, um DRAC 5 zu konfigurieren. Die folgenden Abschnitte beschreiben jedes Objekt und zeigen an, ob das Objekt schreibbar oder lesbar oder beides ist.

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

Anzeigbare Zeichen

Anzeigbare Zeichen umfassen den folgenden Satz:

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

---

idRacInfo

Diese Gruppe enthält Anzeigeparameter, um Informationen über die Einzelheiten des abgefragten DRAC 5 zu geben.

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 eine Zeichenkette, 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 Dell PowerEdge-Server."

Beschreibung

Eine Textbeschreibung des RAC-Typs.

idRacVersionInfo (nur Lesen)

Zulässige Werte

Zeichenkette mit bis zu 63 ASCII-Zeichen.

Standardeinstellung

„1.0"

Beschreibung

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

idRacBuildInfo (schreibgeschützt)

Zulässige Werte

Zeichenkette mit bis zu 16 ASCII-Zeichen.

Standardeinstellung

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

Beschreibung

Eine Zeichenkette mit der aktuellen Build-Version des Produkts.

idRacName (schreibgeschützt)

Zulässige Werte

Zeichenkette mit bis zu 15 ASCII-Zeichen

Standardeinstellung

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 DRAC 5.

---

cfgLanNetworking

Diese Gruppe enthält Parameter zum Konfigurieren des DRAC 5-NIC.

Es ist eine Instanz der Gruppe zulässig. Für alle an den Objekten dieser Gruppe vorgenommenen Änderungen/Aktualisierungen ist ein Reset des DRAC 5-NIC erforderlich, was zu einem kurzen Verlust der Konnektivität führen kann. Objekte, die die DRAC 5-NIC-IP-Adresseneinstellungen ändern, schließen alle aktiven Benutzersitzungen und erfordern, dass Benutzer mittels der aktualisierten IP-Adresseneinstellungen eine neue Verbindung aufbauen.

cfgDNSDomainNameFromDHCP (Lesen/Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

Bestimmt, dass der RAC-DNS-Domänenname über den Netzwerk-DHCP-Server zugeteilt werden soll.

cfgDNSDomainName (Lesen/Schreiben)

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

Zulässige Werte

Zeichenkette mit bis zu 254 ASCII-Zeichen Zeichen müssen alphanumerisch, '-' oder '.' sein.

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

Standardeinstellung

""

Beschreibung

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

cfgDNSRacName (Lesen/Schreiben)

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

Zulässige Werte

Zeichenkette mit bis zu 63 ASCII-Zeichen.

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

Standardeinstellung

rac-*Service-Tag-Nummer*

Beschreibung

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

cfgDNSRegisterRac (Lesen/Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

cfgDNSServersFromDHCP (Lesen/Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

cfgDNSServer1 (Lesen/Schreiben)

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

Zulässige Werte

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

Beschreibung

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

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

cfgDNSServer2 (Lesen/Schreiben)

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

Zulässige Werte

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

Standardeinstellung

0.0.0.0

Beschreibung

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

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

cfgNicEnable (Lesen/Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

cfgNicIpAddress (Lesen/Schreiben)

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

Zulässige Werte

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

Standardeinstellung

192.168.0.120

Beschreibung

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

cfgNicNetmask (Lesen/Schreiben)

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

Zulässige Werte

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

Standardeinstellung

255.255.255.0

Beschreibung

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

cfgNicGateway (Lesen/Schreiben)

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

Zulässige Werte

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

Standardeinstellung

192.168.0.1

Beschreibung

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

cfgNicUseDhcp (Lesen/Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Gibt an, ob DHCP verwendet wird, um die RAC-IP-Adresse zuzuweisen. Wenn diese Eigenschaft auf 1 (TRUE) eingestellt wird, werden die RAC-IP-Adresse, die Subnetzmaske und das Gateway über den DHCP-Server auf dem Netzwerk zugewiesen. Wenn diese Eigenschaft auf **0** (FALSE) eingestellt wird, werden die statische IP-Adresse, die Subnetzmaske und der Gateway über die Eigenschaften **cfgNicIpAddress**, **cfgNicNetmask** und **cfgNicGateway** zugewiesen.

ANMERKUNG: Verwenden Sie den Befehl setniccfg, wenn Sie Ihr System im Remote-Zugriff aktualisieren.

cfgNicSelection (Lesen/Schreiben)

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

Zulässige Werte

0 (freigegeben)

1 (freigegeben mit Failover)

2 (dediziert)

Standardeinstellung

2

Beschreibung

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

Tabelle B-1. cfgNicSelection Unterstützte Modi

Modus	Beschreibung
Freigegeben	Wird verwendet, wenn der integrierte Host-Server-NIC an den RAC auf dem Host-Server freigegeben wird. Dieser Modus ermöglicht, dass Konfigurationen zum Zweck der allgemeinen Zugänglichkeit im Netzwerk dieselbe IP-Adresse auf dem Host-Server und dem RAC verwenden.
Freigegeben mit Failover	Aktiviert Teaming-Fähigkeiten zwischen integrierten Netzwerkschnittstellen-Controllern des Host-Servers.
Dediziert	Legt fest, dass der RAC-NIC zum Zweck der Remote-Zugänglichkeit als dedizierter NIC verwendet wird.

cfgNicMacAddress (schreibgeschützt)

Zulässige Werte

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

Standardeinstellung

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

Beschreibung

Die RAC-NIC-MAC-Adresse.

cfgNicVLanEnable (Lesen/Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

cfgNicVLanId (Lesen/Schreiben)

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

Zulässige Werte

0 – 4094

Standardeinstellung

0

Beschreibung

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

cfgNicVLanPriority (Lesen/Schreiben)

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

Zulässige Werte

0 - 7

Standardeinstellung

0

Beschreibung

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

---

cfgRemoteHosts

Diese Gruppe enthält Eigenschaften, die die Konfiguration verschiedener Remote-Komponenten ermöglichen, z. B. des SMTP-Servers für E-Mail-Warnungen und der TFTP-Server-IP-Adressen für Firmware-Aktualisierungen.

cfgRhostsSmtpServerIpAddr (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

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 die Warnungen konfiguriert und aktiviert sind.

cfgRhostsFwUpdateTftpEnable (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

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

cfgRhostsFwUpdateIpAddr (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

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 des Netzwerk-TFTP-Servers an, die für TFTP-RAC-Firmware-Aktualisierungsvorgänge verwendet wird.

cfgRhostsFwUpdatePath (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

""

Beschreibung

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

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

---

cfgUserAdmin

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

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

cfgUserAdminIpmiLanPrivilege (Lesen/Schreiben)

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

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

15 (Kein Zugriff)

Standardeinstellung

4 (Benutzer 2)

15 (Alle anderen)

Beschreibung

Die maximale Berechtigung auf dem IPMI-LAN-Kanal.

cfgUserAdminIpmiSerialPrivilege (Lesen/Schreiben)

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

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

15 (Kein Zugriff)

Standardeinstellung

4 (Benutzer 2)

15 (Alle anderen)

Beschreibung

Die maximale Berechtigung auf dem seriellen IPMI-Kanal.

cfgUserAdminPrivilege (Lesen/Schreiben)

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

Zulässige Werte

0x0000000 bis 0x00001ff und 0x0

Standardeinstellung

0x0000000

Beschreibung

Diese Eigenschaft legt die für den Benutzer erlaubten rollenbasierten Autoritätsberechtigungen fest. Der Wert wird als Bitmaske dargestellt, die eine beliebige Kombination von Berechtigungswerten ermöglicht. Tabelle B-2 beschreibt die Bitmasken für die zulässigen Benutzerberechtigungen.

Tabelle B-2. Bit-Masken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
An DRAC 5 anmelden	0x0000001
DRAC 5 konfigurieren	0x0000002
Benutzer konfigurieren	0x0000004
Protokolle löschen	0x0000008
Serversteuerungsbefehle ausführen	0x0000010
Auf die Konsolenumleitung zugreifen	0x0000020
Zugriff auf virtuelle Datenträger	0x0000040
Testwarnungen	0x0000080
Debug-Befehle ausführen	0x0000100

Beispiele

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

Tabelle B-3. Beispiel-Bitmasken für Benutzerberechtigungen

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

cfgUserAdminUserName (Lesen/Schreiben)

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

Zulässige Werte

Zeichenkette. Maximale Länge = 16.

Standardeinstellung

""

Beschreibung

Der Name des Benutzers dieses Indexes. Der Benutzerindex wird durch Schreiben einer Zeichenkette in dieses Namensfeld erzeugt, falls der Index leer ist. Das Schreiben einer Zeichenkette von doppelten Anführungszeichen ("") löscht den Benutzer an diesem Index. Der Name kann nicht geändert werden. Sie müssen den Namen löschen und dann neu erstellen. Die folgenden Zeichen dürfen nicht in der Zeichenkette enthalten sein: „/" (Forwardslash, „\" (Backslash), „." (Punkt), Symbol „@" oder Anführungszeichen.

ANMERKUNG: Dieser Eigenschaftswert MUSS sich eindeutig von anderen Benutzerinstanzen unterscheiden.

cfgUserAdminPassword (Nur Schreiben)

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

Zulässige Werte

Eine Zeichenkette mit bis zu 20 ASCII-Zeichen

Standardeinstellung

""

Beschreibung

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

cfgUserAdminEnable

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert einen einzelnen Benutzer.

cfgUserAdminSolEnable

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

---

cfgEmailAlert

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

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

cfgEmailAlertIndex (schreibgeschützt)

Zulässige Werte

1 - 4

Standardeinstellung

Dieser Parameter wird beruhend auf den vorhandenen Instanzen bestückt.

Beschreibung

Der eindeutige Index einer Warnungsinstanz.

cfgEmailAlertEnable (Lesen/Schreiben)

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Gibt die Ziel-E-Mail-Adresse für E-Mail-Warnungen an. Beispiel: `Benutzer1@Firma.com`.

cfgEmailAlertAddress (schreibgeschützt)

Zulässige Werte

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

Standardeinstellung

""

Beschreibung

Die E-Mail-Adresse der Warnungsquelle.

cfgEmailAlertCustomMsg (schreibgeschützt)

Zulässige Werte

Zeichenkette. Maximale Länge = 32.

Standardeinstellung

""

Beschreibung

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

---

cfgSessionManagement

Diese Gruppe enthält Parameter zum Konfigurieren der Anzahl von Sitzungen, 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 über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 – 2

Standardeinstellung

2

Beschreibung

Legt die Höchstanzahl der Konsolenumleitungssitzungen fest, die für den RAC gestattet sind.

cfgSsnMgtRacadmTimeout (Lesen / Schreiben)

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

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 im festgelegten Zeitraum angegeben inaktiv bleibt, wird die Sitzung geschlossen.

cfgSsnMgtWebserverTimeout (Lesen/Schreiben)

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

Zulässige Werte

60 - 1920

Standardeinstellung

300

Beschreibung

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

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

cfgSsnMgtSshIdleTimeout (Lesen/Schreiben)

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

Zulässige Werte

0 (Keine Zeitlimit)

60 - 1920

Standardeinstellung

300

Beschreibung

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

Eine abgelaufene Secure Shell-Sitzung zeigt die folgende Fehlermeldung erst an, wenn Sie auf die Eingabetaste drücken:

```
Warnung: Sitzung nicht mehr gültig, Zeitüberschreitung kann aufgetreten sein
```

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

cfgSsnMgtTelnetTimeout (Lesen/Schreiben)

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

Zulässige Werte

0 (Kein Zeitlimit)

60 - 1920

Standardeinstellung

0

Beschreibung

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

Eine abgelaufene Telnet-Sitzung zeigt die folgende Fehlermeldung erst an, wenn Sie auf die Eingabetaste drücken:

```
Warnung: Sitzung nicht mehr gültig, Zeitüberschreitung kann aufgetreten sein
```

Nachdem die Meldung angezeigt wurde, 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: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

9600, 28800, 57600, 115200

Standardeinstellung

57600

Beschreibung

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

cfgSerialConsoleEnable (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die serielle RAC-Konsolenschnittstelle.

cfgSerialConsoleQuitKey (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

ZEICHENKETTE

MaxLen = 2

Standardeinstellung

^\ (<Strg><\>)

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

Beschreibung

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

- ASCII-Wert - Beispiel: „^a"

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

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

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

cfgSerialConsoleIdleTimeout (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 = kein Zeitlimit

60 - 1920

Standardeinstellung

300

Beschreibung

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

cfgSerialConsoleNoAuth (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 (aktiviert serielle Anmeldungsauthentifizierung)

1 (deaktiviert serielle Anmeldungsauthentifizierung)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Anmeldungsauthentifizierung der seriellen RAC-Konsole.

cfgSerialConsoleCommand (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Beschreibung

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

Standardeinstellung

""

Beispiel

„connect com2"

cfgSerialHistorySize (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 - 8192

Standardeinstellung

8192

Beschreibung

Gibt die maximale Größe des seriellen Verlaufspuffers an.

cfgSerialSshEnable (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

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

cfgSerialTelnetEnable (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die telnet-Konsolenschnittstelle auf dem RAC.

cfgSerialCom2RedirEnable (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Standardeinstellung

1

Zulässige Werte

1 (TRUE)

0 (FALSE)

Beschreibung

Aktiviert oder deaktiviert die Konsole für COM 2-Anschlussumleitung.

---

cfgNetTuning

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

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

cfgNetTuningNicAutoneg (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (Aktiviert)

0 (Deaktiviert)

Standardeinstellung

1

Beschreibung

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

cfgNetTuningNic100MB (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 (10 MBit)

1 (100 MBit)

Standardeinstellung

1

Beschreibung

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

cfgNetTuningNicFullDuplex (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 (Halb-Duplex)

1 (Voll-Duplex)

Standardeinstellung

1

Beschreibung

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

cfgNetTuningNicMtu (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

576 - 1500

Standardeinstellung

1500

Beschreibung

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

cfgNetTuningTcpSrttDflt (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

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 zum Konfigurieren 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: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 31.

Standardeinstellung

public

Beschreibung

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

cfgOobSnmpAgentEnable (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert den SNMP-Agenten im RAC.

---

cfgRacTuning

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

cfgRacTunePluginType

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE) – Java-Plug-in

0 (FALSE) – Systemeigenes Plug-in

Standardeinstellung

0

Beschreibung

Konfiguriert den Plug-in-Typ des virtuellen KVM (vKVM).

cfgRacTuneHttpPort (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

10 - 65535

Standardeinstellung

80

Beschreibung

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

cfgRacTuneHttpsPort (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

10 - 65535

Standardeinstellung

443

Beschreibung

Gibt die Port-Nummer an, die für die HTTPS-Netzwerkkommunikation mit dem RAC verwendet werden soll.

cfgRacTuneIpRangeEnable

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

cfgRacTuneIpRangeAddr

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

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

Standardeinstellung

`192.168.1.1`

Beschreibung

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

cfgRacTuneIpRangeMask

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Standard-IP-Maskenwerte mit linksbündigen Bits

Standardeinstellung

255.255.255.0

Beschreibung

Zeichenkette, formatierte IP-Adresse. Beispiel: 255.255.255.0.

cfgRacTuneIpBlkEnable

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

cfgRacTuneIpBlkFailcount

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

2 - 16

Standardeinstellung

5

Beschreibung

Die Höchstanzahl an Anmeldungsfehlern im Fenster, bevor die Anmeldungsversuche von der IP-Adresse zurückgewiesen werden.

cfgRacTuneIpBlkFailWindow

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

2 – 65535

Standardeinstellung

60

Beschreibung

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

cfgRacTuneIpBlkPenaltyTime

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

2 – 65535

Standardeinstellung

300

Beschreibung

Legt die Zeitspanne in Sekunden fest, während der Sitzungsaufforderungen von einer IP-Adresse aufgrund übermäßiger Fehlversuche zurückgewiesen werden.

cfgRacTuneSshPort (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 - 65535

Standardeinstellung

22

Beschreibung

Gibt die für die RAC-SSH-Schnittstelle verwendete Port-Nummer an.

cfgRacTuneTelnetPort (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 - 65535

Standardeinstellung

23

Beschreibung

Gibt die für die RAC-Telnet-Schnittstelle verwendete Port-Nummer an.

cfgRacTuneRemoteRacadmEnable (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

1

Beschreibung

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

cfgRacTuneConRedirEncryptEnable (Lesen / Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Verschlüsselt das Video in einer Konsolenumleitungssitzung.

cfgRacTuneConRedirPort(Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 - 65535

Standardeinstellung

5901

Beschreibung

Gibt das Port an, das für den Tastatur- und Maus-Datenverkehr während der Konsolenumleitungsaktivität mit dem RAC verwendet wird.

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

cfgRacTuneConRedirVideoPort (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 - 65535

Standardeinstellung

5901

Beschreibung

Gibt das Port an, das für Video-Datenverkehr während der Konsolenumleitungsaktivität mit dem RAC verwendet wird.

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

cfgRacTuneAsrEnable (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die RAC-Funktion zur Erfassung des Absturzbildschirms.

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

cfgRacTuneDaylightOffset (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

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: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

-720 – 780

Standardeinstellung

0

Beschreibung

Gibt den Zeitzonen-Offset (in Minuten) von MGZ/UTC an, der für die RAC-Zeit zu verwenden ist. Einige allgemeine Zeitzonen-Offsets für Zeitzonen in den Vereinigten Staaten sind unten stehend aufgeführt:

-480 (PST – Pacific Standard Time)

-420 (MST – Mountain Standard Time)

-360 (CST – Central Standard Time)

-300 (EST – Eastern Standard Time)

cfgRacTuneWebserverEnable (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert und deaktiviert den RAC-Web-Server. Wenn diese Eigenschaft deaktiviert wird, ist der RAC bei Verwendung von Client-Internet-Browsern oder Remote-RACADM nicht zugänglich. Diese Eigenschaft hat keine Auswirkung auf die Telnet-/SSH-/serielle oder lokale RACADM-Schnittstelle.

cfgRacTuneLocalServerVideo (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (aktiviert)

0 (deaktiviert)

Standardeinstellung

1

Beschreibung

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

cfgRacTuneLocalConfigDisable

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Fähigkeit eines lokalen Benutzers, DRAC 5 unter Verwendung des lokalen racadm oder mittels der Dell OpenManage Server Administrator-Dienstprogramme zu konfigurieren.

cfgRacTuneCtrlEConfigDisable

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Fähigkeit des lokalen Benutzers, DRAC 5 über den BIOS-POST-Options-ROM zu konfigurieren.

cfgRacTuneVirtualConsoleAuthorizeMultipleSessions (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen. Dieses Objekt kann nur mit Remote- oder Firmware- (SSH oder Telnet) RACADM und nicht mit lokalem RACADM oder mit früheren DRAC-Produkten verwendet werden.

Zulässige Werte

0 (Wenn der Benutzer der ersten Sitzung auf die Sitzungsfreigabeanforderung des folgenden Benutzers nicht reagiert hat, erhält der Benutzer der nächsten Sitzung nach dem Standardzeitüberschreitungswert von 30 Sekunden einen Zugang verweigert-Fehler).

1 (Wenn der Benutzer der ersten Sitzung auf die Sitzungsfreigabeanforderung des folgenden Benutzers nicht reagiert hat, erhält der Benutzer der nächsten Sitzung nach dem Standardzeitüberschreitungswert von 30 Sekunden einen schreibgeschützten Zugang).

2 (Wenn der Benutzer der ersten Sitzung auf die Sitzungsfreigabeanforderung des folgenden Benutzers nicht reagiert hat, erhält der Benutzer der nächsten Sitzung nach dem Standardzeitüberschreitungswert von 30 Sekunden einen Administratorzugang).

Standardeinstellung

0

Beschreibung

Wenn ein Erstbenutzer bereits die virtuelle Konsole verwendet, beeinflusst der Wert dieses Objekts die Berechtigungen, die der Freigabanforderung des folgenden Benutzers nach der Zeitüberschreitung von 30 Sekunden gewährt werden.

---

ifcRacManagedNodeOs

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

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

ifcRacMnOsHostname (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

""

Beschreibung

Der Host-Name des verwalteten Systems.

ifcRacMnOsOsName (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

""

Beschreibung

Der Betriebssystemname des verwalteten Systems.

---

cfgRacSecurity

Diese Gruppe wird verwendet, um Einstellungen zu konfigurieren, die mit der RAC-SSL-CSR-Funktion (Zertifikatsignierungsanforderung) in Verbindung stehen. Die Eigenschaften in dieser Gruppe MÜSSEN vor dem Erstellen einer CSR über den RAC konfiguriert werden.

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

cfgRacSecCsrCommonName (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den allgemeinen Namen (CN) der CSR an.

cfgRacSecCsrOrganizationName (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Organisationsnamen (O) an.

cfgRacSecCsrOrganizationUnit (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt die CSR-Organisationseinheit (OU) an.

cfgRacSecCsrLocalityName (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Standort (L) an.

cfgRacSecCsrStateName (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Zustandsnamen (S) an.

cfgRacSecCsrCountryCode (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 2.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Landescode (CC) an

cfgRacSecCsrEmailAddr (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Legt die CSR-E-Mail-Adresse fest.

cfgRacSecCsrKeySize (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1024

2048

4096

Standardeinstellung

1024

Beschreibung

Gibt die asymmetrische SSL-Schlüsselgröße für die CSR an.

---

cfgRacVirtual

Diese Gruppe enthält Parameter zum Konfigurieren der DRAC 5-Funktion des virtuellen Datenträgers. 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 über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Dieses Objekt wird verwendet, um die virtuellen Komponenten über den USB-Bus mit dem System zu verbinden. Wenn die Komponenten mit dem Server verbunden sind, erkennt der Server gültige, mit dem System verbundene USB-Massenspeichergeräte. Dies entspricht dem Herstellen einer Verbindung eines lokalen USB-CDROM/Diskettenlaufwerks mit einem USB-Anschluss am System. Wenn die Komponenten angeschlossen sind, können Sie dann im Remote-Zugriff über die Internet-basierte DRAC5-Schnittstelle oder die CLI eine Verbindung zu den virtuellen Komponenten herstellen. Durch die Einstellung dieses Objekts auf **0** werden die Geräte veranlasst, die USB-Verbindung zu trennen.

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

cfgVirAtapiSvrPort (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **Zugriff auf virtuellen Datenträger** verfügen.

Zulässige Werte

1 - 65535

Standardeinstellung

3669

Beschreibung

Gibt die Port-Nummer an, die für verschlüsselte Verbindungen des virtuellen Datenträgers mit dem RAC verwendet werden.

cfgVirAtapiSvrPortSsl (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

Eine beliebige unbenutzte Port-Nummer zwischen 0 und 65535 dezimal.

Standardeinstellung

3669

Beschreibung

Stellt den für SSL-Verbindungen des virtuellen Datenträgers verwendeten Anschluss ein.

cfgVirMediaKeyEnable (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

cfgVirMediaPluginTypr (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (Java-Plugin)

0 (Native-Plugin)

Standardeinstellung

0

Beschreibung

Legt den Plugin-Typ des virtuellen Datenträgers fest.

cfgVirtualBootOnce (Lesen / Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 – Deaktivieren: Deaktiviert diese Option.

1 – Virtual Flash/Virtueller Datenträger: Starten vom Virtual Flash oder eines virtuellen Datenträgers.

2 – Virtuelle Floppy: Starten von einem virtuellen Diskettenlaufwerk.

3 – Virtuelle CD/DVD/ISO: Starten von einer virtuellen CD/DVD/ISO.

4 – PXE: PXE (Netzwerk) Starten vom Server.

5 – Festplatte: Starten von der Standardfestplatte.

6 – Dienstprogrammpartition: Starten von der Dienstprogrammpartition. Es muss eine Dienstprogrammpartition vorhanden sein.

7 – Standard-CD/DVD: Standard-CD/DVD-Laufwerk des Servers.

8 – BIOS-Setup: BIOS-Setup-Bildschirm.

9 – Primärer Wechseldatenträger: Starten von einem USB-Wechseldatenträger, der als startfähige Diskette emuliert wird.

Standardeinstellung

0

Beschreibung

Legt das Einmal-Startgerät fest. Wird diese Eigenschaft auf ein unterstütztes Gerät eingestellt und das Hostsystem neu gestartet, versucht das System, vom ausgewählten Gerät zu starten (wenn sich der entsprechende Datenträger im Gerät befindet).

ANMERKUNG: Wechseln Sie zum Aktivieren der Einmal-Start-Funktion für das *Virtual Flash*-Gerät zum BIOS-Setup, und nehmen Sie während des Systemneustarts eine manuelle Änderung der Startreihenfolge vor.

ANMERKUNG: Andere Einmal-Startgeräte als *Virtual Flash (1)*, *PXE (4)* und *Deaktivieren (0)* werden nur auf einigen Systemen mit unterstütztem BIOS und BMC-Firmware-Versionen (Baseboard Management Controller) unterstützt. Auf der Website von Dell (**www.dell.com**) können Sie überprüfen, ob Ihr System alle Einmalstart-Geräte unterstützt.

ANMERKUNG: Bei Systemen, die *Virtuelle Floppy* und *Virtuelle CD/DVD/ISO* nicht unterstützen, verwenden Sie '1' (*Virtual Flash/Virtueller Datenträger*) zum Ausführen des Einmal-Starts auf *Virtuelle Floppy* oder *Virtuelle CD/DVD/ISO* oder *Virtual Flash*. Legen Sie in diesem Fall das erforderliche virtuelle Gerät als erstes Startgerät im BIOS-Setup fest. DRAC 5 trennt dieses Gerät automatisch, wenn das System vom Gerät neu startet. Es wird ein anderer Neustart für das System angewendet.

ANMERKUNG: Bei Systemen, die *Virtuelle Floppy* und *Virtuelle CD/DVD/ISO* als separate Optionen unterstützen, trennt DRAC 5 die virtuelle Datenträgerverbindung nach dem einmaligen Start nicht automatisch.

cfgFloppyEmulation (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

1 (True)

0 (False)

Standardeinstellung

0

Beschreibung

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

---

cfgActiveDirectory

Diese Gruppe enthält Parameter zum Konfigurieren der Active Directory-Funktion für DRAC 5.

cfgADRacDomain (Lesen/Schreiben)

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

Zulässige Werte

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

Standardeinstellung

""

Beschreibung

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

cfgADRacName (Lesen/Schreiben)

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

Zulässige Werte

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

Standardeinstellung

""

Beschreibung

Name von DRAC, wie dieser in der Active Directory-Gesamtstruktur verzeichnet ist.

cfgADEnable (Lesen/Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

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

cfgADSpecifyServerEnable (Lesen/Schreiben)

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

Zulässige Werte

1 oder 0 (True oder False)

Standardeinstellung

0

Beschreibung

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

cfgADDomainController (Lesen/Schreiben)

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

Zulässige Werte

Gültige IP-Adresse oder vollständig qualifizierter Domänenname (FQDN)

Standardeinstellung

Keine Standardwerte

Beschreibung

DRAC 5 verwendet den angegebenen Wert zum Durchsuchen des LDAP-Servers nach Benutzernamen.

cfgADGlobalCatalog (Lesen/Schreiben)

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

Zulässige Werte

Gültige IP-Adresse oder vollständig qualifizierter Domänenname (FQDN)

Standardeinstellung

Keine Standardwerte

Beschreibung

DRAC 5 verwendet den angegebenen Wert zum Durchsuchen des Servers, der den globalen Katalog enthält, nach Benutzernamen.

cfgAODomain (Lesen/Schreiben)

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

Zulässige Werte

Gültige IP-Adresse oder vollständig qualifizierter Domänenname (FQDN)

Formatieren

<Domäne>:<IP oder FQDN>

Standardeinstellung

Keine Standardwerte

Beschreibung

DRAC 5 verwendet den von Ihnen angegebenen Wert zum Durchsuchen des Zuordnungsobjekts nach Benutzernamen.

cfgADSmartCardLogonEnable (Lesen/Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Smart Card-Anmeldung an DRAC 5.

cfgADCRLEnable (Lesen/Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Überprüfung der Zertifikatsperrliste (CRL) von Active Directory-basierten Smart Card-Benutzern.

cfgADAuthTimeout (Lesen/Schreiben)

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

Zulässige Werte

15 – 300

Standardeinstellung

120

Beschreibung

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

cfgADRootDomain (Lesen/Schreiben)

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

Zulässige Werte

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

Standardeinstellung

""

Beschreibung

Root-Domäne der Domänengesamtstruktur.

cfgADType (Lesen/Schreiben)

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

Zulässige Werte

1 = Aktiviert das erweiterte Schema mit Active Directory.

2 = Aktiviert das Standardschema mit Active Directory.

Standardeinstellung

1 = Erweitertes Schema

Beschreibung

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

cfgADSSOEnable (Lesen/Schreiben)

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

Zulässige Werte

1 (TRUE)

0 (FALSE)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die einfache Anmeldungsauthentifizierung mittels Active Directory auf dem RAC.

cfgStandardSchema

Diese Gruppe enthält Parameter zum Konfigurieren der Einstellungen des Standardschemas.

cfgSSADRoleGroupIndex (schreibgeschützt)

Zulässige Werte

Ganzzahl von 1 bis 5.

Beschreibung

Index der Rollengruppe, wie im Active Directory verzeichnet.

cfgSSADRoleGroupName (Lesen/Schreiben)

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

Zulässige Werte

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

Standardeinstellung

(leer)

Beschreibung

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

cfgSSADRoleGroupDomain (Lesen/Schreiben)

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

Zulässige Werte

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

Standardeinstellung

(leer)

Beschreibung

Active Directory-Domäne, in der sich die Rollengruppe befindet

cfgSSADRoleGroupPrivilege (Lesen/Schreiben)

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

Zulässige Werte

0x00000000 bis **0x000001ff**

Standardeinstellung

(leer)

Beschreibung

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

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

Rollengruppenberechtigung	Bitmaske
An DRAC 5 anmelden	0x00000001
DRAC 5 konfigurieren	0x00000002
Benutzer konfigurieren	0x00000004
Protokolle löschen	0x00000008
Serversteuerungsbefehle ausführen	0x00000010
Auf die Konsolenumleitung zugreifen	0x00000020
Zugriff auf virtuelle Datenträger	0x00000040
Testwarnungen	0x00000080
Debug-Befehle ausführen	0x00000100

---

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 über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 (Terminal)

1 (Basic)

Standardeinstellung

1

Beschreibung

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

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

cfgIpmiSerialBaudRate (Lesen/Schreiben)

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

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 über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

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

cfgIpmiSerialFlowControl (Lesen/Schreiben)

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

Zulässige Werte

0 (Kein)

1 (CTS/RTS)

2 (XON/XOFF)

Standardeinstellung

1

Beschreibung

Gibt die Einstellung der Datenflusssteuerung für die serielle IPMI-Schnittstelle an.

cfgIpmiSerialHandshakeControl (Lesen/Schreiben)

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

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

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

cfgIpmiSerialLineEdit (Lesen/Schreiben)

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

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

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

cfgIpmiSerialEchoControl (Lesen/Schreiben)

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

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert die Echosteuerung der seriellen IPMI-Schnittstelle.

cfgIpmiSerialDeleteControl (Lesen/Schreiben)

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

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

0

Beschreibung

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

cfgIpmiSerialNewLineSequence (Lesen/Schreiben)

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

Zulässige Werte

0 (Kein)

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

Standardeinstellung

1

Beschreibung

Gibt die Spezifikation der Zeilenumbruchssequenz für die serielle IPMI-Schnittstelle an.

cfgIpmiSerialInputNewLineSequence (Lesen/Schreiben)

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

Zulässige Werte

0 (<EINGABE>)

1 (NULL)

Standardeinstellung

1

Beschreibung

Gibt die Spezifikation der Eingabe-Zeilenumbruchssequenz für die serielle IPMI-Schnittstelle an.

---

cfgIpmiSol

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

cfgIpmiSolEnable (Lesen/Schreiben)

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

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert Seriell über LAN (SOL).

cfgIpmiSolBaudRate (Lesen/Schreiben)

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

Zulässige Werte

9600, 19200, 57600, 115200

Standardeinstellung

57600

Beschreibung

Die Baudrate für die serielle Datenübertragung über LAN.

cfgIpmiSolMinPrivilege (Lesen/Schreiben)

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

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

Gibt die für den Zugriff auf Seriell über LAN erforderliche Mindestzugriffsstufe an.

cfgIpmiSolAccumulateInterval (Lesen/Schreiben)

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

Zulässige Werte

1 – 255.

Standardeinstellung

10

Beschreibung

Gibt die typische Zeitspanne an, die der BMC vor dem Senden eines Teildatenpakets von SOL-Zeichen wartet. Dieser Wert besteht aus 1-basierten 5-ms-Schritten.

cfgIpmiSolSendThreshold (Lesen/Schreiben)

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

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 über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

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

cfgIpmiLanPrivLimit (Lesen/Schreiben)

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

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

0

Beschreibung

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

cfgIpmiLanAlertEnable (Lesen/Schreiben)

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

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

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

cfgIpmiEncryptionKey (Lesen/Schreiben)

ANMERKUNG: Um diese Eigenschaft anzeigen oder ändern zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** sowie über Administratorrechte verfügen.

Zulässige Werte

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

Standardeinstellung

„00000000000000000000"

Beschreibung

IPMI-Verschlüsselungsschlüssel.

cfgIpmiPetCommunityName (Lesen/Schreiben)

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

Zulässige Werte

Eine Zeichenkette mit bis zu 18 Zeichen.

Standardeinstellung

„public"

Beschreibung

Der SNMP-Community-Name für Traps.

---

cfgIpmiPef

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

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

cfgIpmiPefName (schreibgeschützt)

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

Der Name des Index-Filters.

Beschreibung

Gibt den Namen des Plattformereignisfilters an.

cfgIpmiPefIndex (schreibgeschützt)

Zulässige Werte

1 – 17

Standardeinstellung

Der Indexwert eines Plattformereignisfilter-Objekts.

Beschreibung

Gibt den Index eines spezifischen Plattformereignisfilters an.

cfgIpmiPefAction (Lesen/Schreiben)

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

Zulässige Werte

0 (Kein)

1 (Herunterfahren)

2 (Rücksetzen)

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 über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert einen spezifischen Plattformereignisfilter.

---

cfgIpmiPet

Diese Gruppe wird zum Konfigurieren von Plattformereignis-Traps auf dem verwalteten System verwendet.

cfgIpmiPetIndex (Lesen/Schreiben)

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

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 über die Berechtigung **DRAC 5 konfigurieren** verfügen.

Zulässige Werte

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

Standardeinstellung

0.0.0.0

Beschreibung

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

cfgIpmiPetAlertEnable (Lesen/Schreiben)

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

Zulässige Werte

0 (FALSE)

1 (TRUE)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert einen spezifischen Trap.

---

cfgLogging

Diese Gruppe wird zur Aktivierung oder Deaktivierung der OEM-Ereignisprotokollfilterung verwendet.

cfgLoggingSELOEMEventFilterEnable (Lesen/Schreiben)

Zulässige Werte

0 (SEL Protokollfilterung ist deaktiviert)

1 (SEL Protokollfilterung ist aktiviert)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die SEL-Protokollfilterung.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Unterstützte RACADM-Schnittstellen

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Die folgende Tabelle enthält eine Übersicht über RACADM-Unterbefehle und die entsprechende Schnittstellenunterstützung.

Tabelle C-1. Schnittstellenunterstützung für RACADM-Unterbefehle

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

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5: Übersicht

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Der Dell Remote Access Controller 5 (DRAC 5) ist eine Hardware- und Softwarelösung zur Systemverwaltung und ermöglicht die Remoteverwaltung, die Wiederherstellung eines abgestürzten Systems und die Stromsteuerung für Dell-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 Spannungen, Temperaturen, Eingriffen und Lüfterdrehzahlen zusenden. DRAC 5 protokolliert auch Ereignisdaten und den neuesten Absturzbildschirm (nur für Systeme, die das Microsoft Windows-Betriebssystem ausführen), um Ihnen zu helfen, die wahrscheinliche Ursache eines Systemausfalls zu diagnostizieren.

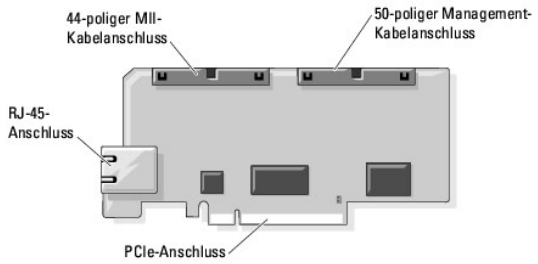
DRAC 5 verfügt über einen eigenen Mikroprozessor und Speicher und wird durch das System versorgt, in dem DARC 5 installiert ist. DRAC 5 kann auf dem System vorinstalliert werden oder ist getrennt in einem Kit erhältlich.

Informationen zum Einstieg mit DRAC 5 finden Sie unter Zum Einstieg mit DRAC 5.

DRAC 5 – Technisch Daten und Funktionen

Abbildung 1-1 zeigt die DRAC 5-Hardware.

Abbildung 1-1. DRAC 5-Hardwarefunktionen



Technische Daten von DRAC 5

Technische Daten der Spannungsversorgung

Tabelle 1-1 enthät Informationen zur Stromaufnahme von DRAC 5.

Tabelle 1-1. DRAC 5 – Technische Daten der Spannungsversorgung

Systemversorgung
(Max.) 1,2 A bei +3,3 V AUX
(Max.) 550 mA bei +3,3 V Main
(Max.) 0 mA bei +5V Main

Anschlüsse

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

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

Das 50-polige Verwaltungskabel ist die Hauptschnittstelle zum DRAC, die den Anschluss an USB, serielle Schnittstelle, Video und einem integrierten

Schaltungsbus (I2C) bietet. 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 DRAC 5 im **dedizierten NIC**-Modus konfiguriert wird.

Abhängig von Ihren Anforderungen können Sie die Verwaltungs- und MII-Kabel verwenden, um DRAC in drei separaten Modi zu konfigurieren. Weitere Informationen finden Sie unter DRAC-Modi.

DRAC 5-Ports

Tabelle 1-2 kennzeichnet die von DRAC 5 verwendeten Ports, die auf eine Serververbindung abgehört wird. Tabelle 1-3 kennzeichnet die Ports, die 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, Abhör-Ports

Schnittstellennummer	Funktion
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
161	SNMP-Agent
443*	HTTPS
623	RMCP/RMCP+
3668*	Server für virtuelle Datenträger
3669*	Virtueller Datenträger - Sicherer Dienst
5900*	Konsolenumleitung: Tastatur/Maus
5901*	Konsolenumleitung: Video
* Konfigurierbare Schnittstelle	

Tabelle 1-3. DRAC 5-Client-Port

Schnittstellennummer	Funktion
25	SMTP
53	DNS
68	DHCP-zugewiesene IP-Adresse
69	TFTP
162	SNMP-Trap
636	LDAPS
3269	LDAPS für 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 MBits/s Ethernet • DHCP-Unterstützung • SNMP-Traps und E-Mail-Ereignisbenachrichtigung • Dedizierte Netzwerkschnittstelle für die DRAC 5-Internet-basierte Schnittstelle • Unterstützung der Telnet/ssh-Konsole und RACADM-CLI-Befehle, einschließlich der Befehle für Systemstart, Reset, Hochfahren und Herunterfahren
Serielle Schnittstelle	• Unterstützung der seriellen Konsole und RACADM-CLI-Befehle, einschließlich der Befehle für Systemstart, Reset, Hochfahren und Herunterfahren • Unterstützung für die Text-Only-Konsolenumleitung zu einem VT-100-Terminal oder Terminalemulator

DRAC 5-Standardfunktionen

DRAC 5 bietet die folgenden Funktionen:

- Zweifaktor-Authentifizierung, die über die Smart Card-Anmeldung erfolgt. Die Zweifaktor-Authentifizierung basiert auf dem, was der Benutzer hat (die Smart Card), und auf dem, was der Benutzer weiß (die PIN).
- Benutzerauthentifizierung durch Microsoft Active Directory (optional) oder durch hardwaregespeicherte Benutzer-IDs und Kennwörter.
- Rollenbasierte Autorität, die es einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren.
- Benutzer-ID- und Kennwort-Konfiguration über die Internet-basierte Schnittstelle oder RACADM-CLI.
- Dynamische DNS-Registrierung (Domänennamensystem).
- Remote-Systemverwaltung und -Überwachung mittels Internet-basierter Benutzeroberfläche, serieller Verbindung, Remote-RACADM oder Telnet-Verbindung.
- Unterstützung der Active Directory-Authentifizierung – Fasst unter Verwendung des Standardschemas und des erweiterten Schemas alle DRAC 5-Benutzer-IDs und -Kennwörter im Active Directory zusammen.
- Konsolenumleitung – Enthält Remote-Systemfunktionen für Tastatur, Video und Maus.
- Virtueller Datenträger – Ermöglicht einem verwalteten System den Zugriff auf ein Datenträgerlaufwerk auf der Management Station.
- Zugriff auf Systemereignisprotokolle – Ermöglicht den Zugriff auf das Systemereignisprotokoll (SEL), das DRAC 5-Protokoll und den „Bildschirm Letzter Absturz" des abgestürzten oder nicht reagierenden Systems, unabhängig vom Zustand des Betriebssystems.
- Dell OpenManage-Softwareintegration – Ermöglicht, die Internet-basierte 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 – Ermöglicht eine lokale und Remote-Konfiguration mittels des RACADM-Befehlszeilendienstprogramms.
- Remote-Energieverwaltung – Ermöglicht die Ausführung von Remote-Energieverwaltungsfunktionen, wie Herunterfahren und Reset, über Verwaltungskonsole.
- IPMI-Unterstützung.
- Auf Standards beruhende Verwaltung mitels IPMI über LAN und SM-CLP.
- Sensoren zur Überwachung der Leistungsaufnahme. DRAC 5 verwendet die Daten, um die Leistungsaufnahme des Systems durch Diagramme und Statistiken bildlich darzustellen.
- SSL-Verschlüsselung (Secure Sockets Layer) – Ermöglicht sichere Remote-Systemverwaltung über die Internet-basierte Schnittstelle.
- Sicherheitsverwaltung auf Kennwortebene – Verhindert den unberechtigten Zugriff auf ein Remote-System.
- Rollenbasierte Autorität – Enthält zuweisbare Berechtigungen für verschiedene Systemverwaltungs-Tasks.

Weitere nützliche Dokumente

Zusätzlich zu diesem *Benutzerhandbuch* bieten die folgenden Dokumente weiterführende Informationen über das Setup und den Betrieb von DRAC 5 in Ihrem System.

- DRAC 5-Online-Hilfe bietet Informationen über die Anwendung der Internet-basierten Schnittstelle.
- Das *Dell OpenManage IT Assistant-Benutzerhandbuch* enthält Informationen zu IT Assistant.
- Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen über die Installation und Anwendung von Server Administrator.
- Das *Dell OpenManage Server Administrator SNMP-Referenzhandbuch* dokumentiert die SNMP-MIB (Management Information Base). MIB definiert Variablen, die die Standard-MIB erweitern, so dass diese die Fähigkeiten von Systemverwaltungsagenten erhalten.
- Im *Benutzerhandbuch zum Dell OpenManage Baseboard-Management-Controller-Dienstprogramm* finden Sie Informationen über die Konfiguration des Baseboard-Management-Controllers (BMC), die Konfiguration des verwalteten Systems mittels des BMC-Verwaltungsdienstprogramms sowie weitere BMC-Informationen.
- Das *Benutzerhandbuch zu Dell Aktualisierungspakete* enthält Informationen zum Bezug und zur Verwenden von Dell Aktualisierungspakete als Teil Ihrer Systemaktualisierungsstrategie.
- Die *Dell Systems Software Support-Matrix* bietet Informationen über verschiedene Dell-Systeme, über die von diesen Systemen unterstützten Betriebssysteme und über die Dell OpenManage-Komponenten, die auf diesen Systemen installiert werden können.
- Das *Glossar* auf der Dell Support-Website enthält Informationen zu den in diesem Dokument verwendeten Begriffen.

Die folgenden Systemdokumente stehen außerdem zur Verfügung, um weitere Informationen über das System zu bieten, in dem Ihr DRAC 5 installiert ist.

- In den mit dem System gelieferten Sicherheitshinweisen finden Sie wichtige Informationen zur Sicherheit und zu den Betriebsbestimmungen. Weitere Betriebsbestimmungen finden Sie auf der Website zur Einhaltung gesetzlicher Vorschriften unter **www.dell.com/regulatory_compliance**. Garantiebestimmungen können als separates Dokument beigelegt sein.
- Im zusammen mit der Rack-Lösung gelieferten *Rack-Installationshandbuch* bzw. in der *Rack-Installationsanleitung* ist beschrieben, wie das System in einem Rack installiert wird.
- Das *Handbuch zum Einstieg* enthält eine Übersicht über die Systemfunktionen, die Einrichtung des Systems und technische Daten.
- Im *Hardware-Benutzerhandbuch* finden Sie Informationen über Systemfunktionen, Fehlerbehebung im System und zum Installieren oder Austauschen von Systemkomponenten.
- In der Dokumentation zur Systemverwaltungssoftware sind die Merkmale, die Anforderungen, die Installation und die grundlegende Funktion der Software beschrieben.

- In der Dokumentation zum Betriebssystem ist beschrieben, wie das Betriebssystem installiert (sofern erforderlich), konfiguriert und verwendet wird.
- Die Dokumentation für alle separat erworbenen Komponenten enthält Informationen zur Konfiguration und zur Installation dieser Optionen.
- Möglicherweise sind auch Aktualisierungen beigelegt, in denen Änderungen am System, an der Software und/oder an der Dokumentation beschrieben sind.

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

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Virtuellen Datenträger verwenden und konfigurieren

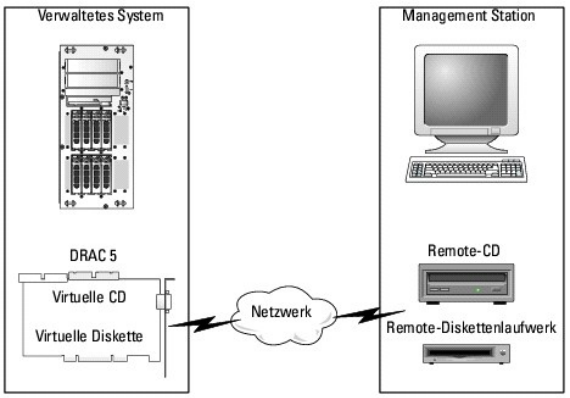
Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

---

Übersicht

Die Funktion Virtueller Datenträger stellt dem verwalteten System ein virtuelles CD-Laufwerk zur Verfügung, das von jeder Stelle des Netzwerks aus Standarddatenträger verwenden kann. Abbildung 11-1 zeigt die gesamte Architektur des virtuellen Datenträgers.

Abbildung 11-1. 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 verfügbare Netzwerkbandbreite von mindestens 128 Kbit/s.

Das verwaltete System wird mit einer DRAC 5-Karte konfiguriert. Die virtuellen CD- und Disketten-Laufwerke sind zwei im DRAC 5 integrierte elektronische Komponenten, die durch die DRAC 5-Firmware gesteuert werden. Diese beiden Komponenten sind im Betriebssystem und dem BIOS des verwalteten Systems zu jeder Zeit vorhanden, wobei es keine Rolle spielt, ob ein virtueller Datenträger verbunden ist oder nicht.

Die Management Station stellt den physischen Datenträger oder die Imagedatei über das Netzwerk bereit. Wenn Sie den RAC-Browser zum ersten Mal starten und auf die Seite des virtuellen Datenträgers zugreifen, wird das Plug-In des virtuellen Datenträgers vom DRAC 5-Web-Server heruntergeladen und automatisch auf der Management Station installiert. Für eine ordnungsgemäße Funktion des virtuellen Datenträgers muss das Plug-In des virtuellen Datenträgers auf der Management Station installiert werden.

Wird eine Verbindung zu einem virtuellen Datenträger hergestellt, werden alle Zugriffsanforderungen auf die virtuelle CD/das virtuelle Diskettenlaufwerk vom verwalteten System über das Netzwerk zur Management Station geleitet. Das Verbinden eines virtuellen Datenträgers ist identisch mit dem Einsetzen von Datenträgern in virtuelle Komponenten. Wenn kein virtueller Datenträger verbunden ist, verhalten sich virtuelle Komponenten auf dem verwalteten System wie zwei Laufwerke ohne Datenträger.

ANMERKUNG: Sie können mit dem Browser- oder Java-Plug-In einen virtuellen Datenträger verbinden.

Tabelle 11-1 listet die unterstützten Laufwerkverbindungen für virtuelle Diskettenlaufwerke und virtuelle optische Laufwerke auf.

ANMERKUNG: Werden virtuelle Datenträger gewechselt, während eine Verbindung vorhanden ist, kann dies die System-Startsequenz anhalten.

Tabelle 11-1. Unterstützte Laufwerkverbindungen

Unterstützte Verbindungen virtueller Diskettenlaufwerke	Unterstützte Verbindungen virtueller optischer Laufwerke
1,44 Zoll Legacy-Diskettenlaufwerk mit 1,44 Zoll-Diskette	CD-ROM, DVD, CDRW, Kombinationslaufwerk mit CD-ROM-Datenträger
USB-Diskettenlaufwerk mit 1,44 Zoll-Diskette	CD-ROM-Abbilddatei im

	ISO9660-Format
1,44 Zoll-Disketten-Image	USB-CD-ROM-Laufwerk mit CD-ROM-Datenträger.

Browser-Plug-In des virtuellen Datenträgers installieren

Zur Verwendung der Funktion des virtuellen Datenträgers muss das Browser-Plug-In auf der Management Station installiert werden. Nachdem Sie die DRAC 5-Benutzeroberfläche geöffnet und die Seite Virtueller Datenträger gestartet haben, lädt der Browser automatisch das Plug-In herunter, falls erforderlich. Nach der erfolgreichen Installation des Plug-Ins zeigt die Seite Virtueller Datenträger eine Liste von Disketten und optischen Laufwerken an, mit denen das virtuelle Laufwerk verbunden werden kann.

Windows-basierte Management Station

Installieren Sie, um die Funktion des virtuellen Datenträgers auf einer Management Station mit Microsoft Windows-Betriebssystem auszuführen, eine unterstützte Internet Explorer-Version mit dem ActiveX-Steuerungs-Plug-In. Stellen Sie die Browser-Sicherheit auf **Mittelhoch** oder auf eine niedrigere Einstellung ein, damit Internet Explorer signierte ActiveX-Steuerelemente herunterladen und installieren kann.

Außerdem ist es erforderlich, dass Sie über Administratorrechte verfügen, um die Funktion des virtuellen Datenträgers installieren und verwenden zu können. Vor der Installation des ActiveX-Steuerelements kann Internet Explorer eventuell eine Sicherheitswarnung anzeigen. Akzeptieren Sie die ActiveX-Steuerung, um das Installationsverfahren abzuschließen, wenn der Internet Explorer Sie mit einer Sicherheitswarnung dazu auffordert.

Linux-basierte Management Station

Installieren Sie eine unterstützte Version von Mozilla oder Firefox, um die Funktion des virtuellen Datenträgers auf einer Management Station mit Linux-Betriebssystem auszuführen. Ist das Plug-In des virtuellen Datenträgers nicht installiert oder ist eine neuere Version verfügbar, wird während des Installationsverfahrens ein Dialogfeld eingeblendet, um die Plug-In-Installation auf der Management Station zu bestätigen. Stellen Sie sicher, dass die Benutzer-ID, unter der der Browser ausgeführt wird, in der Verzeichnisstruktur des Browser schreibberechtigt ist. Hat die Benutzer-ID keine Schreibberechtigung, können Sie das Plug-In des virtuellen Datenträgers nicht installieren.

Weitere Informationen befinden sich auf der *Support-Matrix der Dell-Systemsoftware* auf der Dell Support-Website unter **support.dell.com/manuals**.

Virtuellen Datenträger ausführen

△ **VORSICHTSHINWEIS: Geben Sie keinen racreset-Befehl aus, wenn eine virtuelle Datenträger-Sitzung ausgeführt wird. Andernfalls können unerwünschte Ergebnisse, einschließlich eines Datenverlustes, auftreten.**

Mit dem virtuellen Datenträger können Sie ein Diskettenabbild oder -laufwerk „virtualisieren", wodurch ein Diskettenabbild, ein Diskettenlaufwerk oder ein optisches Laufwerk auf der Verwaltungskonsole zu einem verfügbaren Laufwerk auf dem Remote-System werden kann. Sie können mit dem Browser- oder Java-Plug-In einen virtuellen Datenträger verbinden. Stellen Sie, wenn Sie das Java-Plug-In verwenden, sicher, dass auf dem Verwaltungssystem das Java Runtime Environment (JRE) 1.6 oder höher installiert ist.

Unterstützte Konfigurationen des virtuellen Datenträgers

Sie können den virtuellen Datenträger für ein Floppy-Laufwerk und ein optisches Laufwerk aktivieren. Es kann für jeden Datenträgertyp nur ein einziges Laufwerk auf einmal virtualisiert werden.

Unterstützte Floppy-Laufwerke umfassen ein Floppy-Image oder ein verfügbares Floppy-Laufwerk. Unterstützte optische Laufwerke umfassen maximal ein verfügbares optisches Laufwerk oder eine einzige ISO-Imagedatei.

Virtuellen Datenträger mittels der Internet-Benutzeroberfläche verwenden

Verbindung zu virtuellem Datenträger mit dem Native-Plug-In

1. Öffnen Sie einen unterstützten Internet-Browser auf der Management Station. Eine Liste der unterstützten Webbrowser finden Sie in der *Dell Systems Software Support Matrix* auf der Dell Support-Website unter **support.dell.com/manuals**.

△ **VORSICHTSHINWEIS: Konsolenumleitung und Virtueller Datenträger unterstützen nur 32-Bit-Webbrowser. Das Verwenden von 64-Bit-Internet-Browsern kann zu unerwarteten Ergebnissen oder einem Fehlschlagen von Vorgängen führen.**

2. Stellen Sie eine Verbindung zu DRAC 5 her, und melden Sie sich an. Weitere Informationen finden Sie unter Auf die Internet-basierte Schnittstelle zugreifen.

3. Klicken Sie auf das Register **Datenträger** und dann auf **Virtueller Datenträger**.

Die Seite **Virtueller Datenträger** wird mit den Client-Laufwerken eingeblendet, die virtualisiert werden können.

ANMERKUNG: Die **Disketten-Imagedatei** unter **Diskettenlaufwerk** (falls zutreffend) kann u. U. angezeigt werden, da dieses Gerät als virtuelle Diskette virtualisiert werden kann. Sie können ein optisches Laufwerk und gleichzeitig eine Diskette oder ein einzelnes Laufwerk auswählen.

ANMERKUNG: Die Laufwerkbuchstaben der virtuellen Komponente auf dem verwalteten System entsprechen nicht den Buchstaben des physikalischen Laufwerks auf der Management Station.

4. Befolgen Sie, bei entsprechender Aufforderung, die Bildschirmanleitungen zum Installieren des Plug-Ins des virtuellen Datenträgers.

5. Führen Sie im **Attribut**-Feld die folgenden Schritte aus:

   a. Stellen Sie sicher, dass in der Spalte **Wert** der Statuswert **Verbindung herstellen/Verbindung abtrennen Verbindung hergestellt** lautet.

      Wenn der Wert **Verbindung getrennt** lautet, führen Sie die folgenden Schritte aus:

      - Klicken Sie im Register **Datenträger** auf **Konfiguration**.
      - Stellen Sie sicher, dass in der Spalte **Wert** das Kontrollkästchen **Verbindung mit virtuellem Datenträger herstellen** gewählt ist.
      - Klicken Sie auf **Änderungen übernehmen**.
      - Klicken Sie im Register **Virtueller Datenträger** auf **Virtueller Datenträger**.
      - Stellen Sie sicher, dass in der Spalte **Wert** der Statuswert **Verbindung herstellen/Verbindung abtrennen Verbindung hergestellt** lautet.

   ANMERKUNG: Nachdem der virtuelle Datenträger verbunden wurde, können Sie durch RACADM die Startreihenfolge ändern; die **Konfigurationsseite** ermöglicht Ihnen keinerlei Änderung der Konfiguration des Startreihenfolgegerätes.

   b. Stellen Sie sicher, dass der Wert für **Aktueller Status Nicht angeschlossen** lautet. Wenn das Feld **Wert** „Verbunden" anzeigt, müssen Sie die Verbindung vom Abbild oder Laufwerk trennen, bevor Sie erneut eine Verbindung herstellen. Dieser Status kennzeichnet nur den aktuellen Status der Verbindung des virtuellen Datenträgers auf der aktuellen Internet-basierten Schnittstelle.

   c. Stellen Sie sicher, dass der Wert für **Aktive Sitzung Verfügbar** lautet. Wenn das Feld **Wert** die Meldung **In Verwendung** anzeigt, müssen Sie warten, bis die bestehende Sitzung des virtuellen Datenträgers freigegeben wird, oder beenden Sie diese, indem Sie unter Remote- Zugriff zum Register Sitzungsverwaltung wechseln, und beenden Sie die aktive Sitzung des virtuellen Datenträgers.

      Es ist nur eine aktive Sitzung des virtuellen Datenträgers auf einmal zulässig. Diese Sitzung konnte von einer beliebigen Internet-basierten Schnittstelle oder einem VM-CLI-Dienstprogramm erstellt worden sein.

   d. Wählen Sie das Kontrollkästchen **Verschlüsselung aktiviert** aus, um eine verschlüsselte Verbindung zwischen dem Remote-System und der Management Station (falls gewünscht) herzustellen.

6. Wenn Sie ein Disketten- oder ISO-Abbild virtualisieren, wählen Sie **Floppy-Abbilddatei** oder **ISO-Abbilddatei** aus, und geben Sie den Namen der Abbilddatei ein bzw. suchen Sie die Abbilddatei, die virtualisiert werden soll.

   Wenn Sie ein Diskettenlaufwerk oder ein optisches Laufwerk virtualisieren, wählen Sie die Schaltfläche neben den Laufwerken, die Sie virtualisieren möchten.

7. Klicken Sie auf **Connect** (Verbinden).

   Nach der Authentifizierung der Verbindung wechselt der Verbindungsstatus zu **Verbunden**, und eine Liste aller verbundenen Laufwerke wird angezeigt. Alle verfügbaren Diskettenabbilder und -laufwerke, die Sie ausgewählt haben, werden auf der Konsole des verwalteten Systems verfügbar, als wären sie echte Laufwerke.

ANMERKUNG: Der zugeordnete Buchstabe des virtuellen Laufwerks (für Microsoft Windows-Systeme) oder die komponentenspezifische Datei (für Linux-Systeme) ist eventuell nicht mit dem Laufwerkbuchstaben auf der Verwaltungskonsole identisch.

ANMERKUNG: Der virtuelle Datenträger funktioniert u. U. nicht ordnungsgemäß auf Clients des Windows-Betriebssystems, die mit Internet Explorer Enhanced Security konfiguriert wurden. Ziehen Sie die Dokumentation zu Ihrem Microsoft-Betriebssystem zurate oder setzen sich mit Ihrem Administrator in Verbindung, um dieses Problem zu lösen.

Verbindung des virtuellen Datenträgers trennen

Klicken Sie auf **Unterbrechen**, um alle virtualisierten Abbilder und Laufwerke von der Management Station zu trennen. Die Verbindung zu **allen** virtualisierten Abbildern oder Laufwerken wird unterbrochen, und sie stehen auf dem verwalteten System nicht mehr zur Verfügung.

Verbindung zu virtuellem Datenträger mit dem Java-Plug-In herstellen

1. Öffnen Sie einen unterstützten Internet-Browser auf der Management Station. Eine Liste der unterstützten Webbrowser finden Sie in der *Dell Systems Software Support Matrix* auf der Dell Support-Website unter **support.dell.com/manuals**.

2. Stellen Sie eine Verbindung zu DRAC 5 her, und melden Sie sich an. Weitere Informationen finden Sie unter Auf die Internet-basierte Schnittstelle zugreifen.

3. Klicken Sie auf das Register **Datenträger** und dann auf **Virtueller Datenträger**.

   Die Seite **Virtueller Datenträger** wird mit den Client-Laufwerken angezeigt, die virtualisiert werden können.

ANMERKUNG: Das Plug-In, mit dem Sie sich mit einem virtuellen Datenträger verbinden können, ist vom Plug-In-Typ abhängig, den Sie auf der Registerkarte **Konfiguration** ausgewählt haben.

4. Führen Sie im **Attribut**-Feld die folgenden Schritte aus:

   a. Stellen Sie sicher, dass in der Spalte **Wert** der Statuswert **Verbindung herstellen / Verbindung abtrennen Verbindung hergestellt** lautet.

   Wenn der Wert **Verbindung getrennt** lautet, führen Sie die folgenden Schritte aus:

   - Klicken Sie im Register **Datenträger** auf **Konfiguration**.
   - Stellen Sie sicher, dass in der Spalte **Wert** die Option **Verbindung mit virtuellem Datenträger herstellen** auf „Verbinden" eingestellt ist.
   - Wählen Sie in der Spalte **Wert** den **Plug-In-Typ Java Plug-In** aus.
   - Klicken Sie auf **Änderungen übernehmen**.
   - Klicken Sie im Register **Virtueller Datenträger** auf **Virtueller Datenträger**.

   ANMERKUNG: Stellen Sie sicher, dass auf dem Verwaltungssystem Java Runtime Environment (JRE) 1.6 oder höher installiert ist.

   b. Stellen Sie sicher, dass der Wert für **Aktive Sitzung 0** ist. Wenn das Feld **Wert** den Wert **1** anzeigt, müssen Sie warten, bis die Sitzung des virtuellen Datenträgers freigegeben wird, oder beenden Sie diese, indem Sie unter **Remote-Zugriff** zum Register **Sitzungsverwaltung** wechseln. Es ist nur eine aktive Sitzung des virtuellen Datenträgers auf einmal zulässig. Diese Sitzung wurde möglicherweise von einer beliebigen Internet-basierten Schnittstelle oder einem VM-CLI- Dienstprogramm erstellt.

5. Klicken Sie auf **VM starten**.

   Das Popup-Fenster **Virtuelle Datenträgersitzung** wird angezeigt. Das Popup-Fenster zeigt die Treiber an, die Sie virtualisieren können.

6. Ist ein Gerät bereits virtualisiert, so trennen Sie es, indem Sie das zum Treiber gehörende Kontrollkästchen **Zugewiesen** deaktivieren.

7. Um ein Diskettenabbild oder ISO-Abbild zu virtualisieren, klicken Sie auf **Abbild hinzufügen**, und wählen Sie ein Abbild aus.

8. Klicken Sie auf das Kontrollkästchen **Zugewiesen**, das zum Treiber oder Abbild gehört, den/das Sie verbinden möchten.

   Das Gerät im verwalteten System, mit dem der *Treiber oder das Abbild verbunden ist*, wird in der **Details-***Tabelle* angezeigt.

Verbindung des virtuellen Datenträgers trennen

Deaktivieren Sie das zu einem Treiber oder Abbild gehörende Kontrollkästchen **Zugewiesen**.

Verbindung zur Funktion des virtuellen Datenträgers herstellen und trennen

Die Funktion des virtuellen DRAC 5-Datenträgers basiert auf der USB-Technologie und kann die USB-Plug-and-Play-Funktionen nutzen. DRAC 5 fügt die Option zum Herstellen und Trennen einer Verbindung der virtuellen Komponenten vom USB-Bus hinzu. Wird die Verbindung der Komponenten getrennt, können das Betriebssystem oder BIOS keine verbundenen Laufwerke sehen. Sind die virtuellen Komponenten verbunden, sind die Laufwerke sichtbar. Im Unterschied zu DRAC 4, bei dem die Laufwerke nur mit dem nächsten Systemstart aktiviert oder deaktiviert werden konnten, kann die Verbindung mit virtuellen DRAC-5-Komponenten jederzeit hergestellt oder getrennt werden.

Die Verbindung virtueller Komponenten kann unter Verwendung von Folgendem hergestellt bzw. getrennt werden: Internet-Browser, lokaler racadm, Remote-racadm, Telnet und die serielle Schnittstelle. Um den virtuellen Datenträger mithilfe eines Internet-Browsers zu konfigurieren, können Sie zur Seite **Datenträger** wechseln und dann zur Seite **Konfiguration**, wo Sie Einstellungsänderungen vornehmen und anwenden können. Sie können auch die **Port-Nummer für den virtuellen Datenträger** sowie die **SSL-Port-Nummer für den virtuellen Datenträger** festlegen. Zusätzlich können Sie auch die Funktionen Virtual Flash und Einmaliger Start aktivieren oder deaktivieren. Informationen zur Funktion Einmaliger Start finden Sie unter cfgVirtualBootOnce (Lesen/Schreiben). Ist diese Eigenschaft für ein unterstütztes Gerät eingestellt, und wird der Hostserver neu gestartet, versucht die Funktion, vom ausgewählten Gerät zu starten (wenn sich der entsprechende Datenträger im Gerät befindet).

Automatisches Verbinden des virtuellen Datenträgers

Die DRAC 5-Firmware, Version 1.30 und höher, unterstützt die Funktion des automatischen Verbindens des virtuellen Datenträgers. Wenn Sie diese Funktion aktivieren, verbindet DRAC 5 nur dann automatisch eine virtuelle Komponente mit dem System, wenn eine Komponente auf einem unterstützten Client virtualisiert (verbunden) wird.

DRAC 5 trennt virtuelle Datenträgergeräte, wenn die Sitzung des virtuellen Datenträgergers unterbrochen wird.

Verbindung des virtuellen Datenträgers mittels des Internet-Browsers herstellen, automatisch herstellen oder trennen

Der Status eines virtuellen Datenträgers kann auf „Verbinden", „Automatisch verbinden" oder „Trennen" eingestellt werden. Basierend auf diesem Status werden die Geräte im Remote-System in der DRAC 5-GUI angezeigt.

- **Verbinden** – Wenn der Status „Verbinden" ist, verbindet DRAC 5 automatische alle Geräte des Remote-Systems mit dem Server. Wenn Sie eine Verbindung zum Server herstellen, werden die im Remote-System verfügbare Geräte in der DRAC 5-GUI angezeigt.
- **Automatisch verbinden** – Wenn der Status „Automatisch verbinden" ist, verbindet DRAC 5 ein Gerät nur mit dem Server, wenn das Gerät virtualisiert ist. Wenn Sie beispielsweise eine Verbindung zum Server von einem Remote-System aus herstellen, das über ein CD-Laufwerk verfügt, wird das CD-Laufwerk nur angezeigt, wenn es virtualisiert ist. Andernfalls wird das CD-Laufwerk in der DRAC 5-GUI nicht angezeigt.

- **Trennen** – Wenn der Status „Trennen" ist, wird das virtuelle Gerät nicht im Server angezeigt.

Führen Sie Folgendes aus, um eine Verbindung zum virtuellen Datenträger herzustellen:

1. Klicken Sie auf **System**→ **Konsole/Datenträger**→ **Konfiguration**.
2. Ändern Sie den Wert von **Verbindung mit virtuellem Datenträger herstellen** auf **Verbinden**.
3. Klicken Sie auf **Änderungen anwenden**.

Führen Sie Folgendes aus, um den virtuellen Datenträgers zu trennen:

1. Klicken Sie auf **System**→ **Konsole/Datenträger**→ **Konfiguration**.
2. Ändern Sie den Wert von **Verbindung mit virtuellem Datenträger herstellen** auf **Trennen**.
3. Klicken Sie auf **Änderungen anwenden**.

Verbindung des virtuellen Datenträgers mittels RACADM herstellen, automatisch herstellen oder trennen

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein, und drücken Sie auf die Eingabetaste <Enter>, um eine Verbindung zum virtuellen Datenträger herzustellen:

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 1
```

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein, und drücken Sie auf die Eingabetaste <Enter>, um eine Verbindung zum virtuellen Datenträger zu trennen:

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 0
```

öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein, und drücken Sie auf die Eingabetaste <Enter>, um eine automatische Verbindung zum virtuellen Datenträger herzustellen:

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 2
```

Starten vom virtuellen Datenträger

Auf unterstützten Systemen ermöglicht Ihnen das System-BIOS das Starten von virtuellen optischen Laufwerken oder von virtuellen Diskettenlaufwerken. Öffnen Sie während des POST das BIOS-Setup-Fenster und überprüfen Sie, ob die virtuellen Laufwerke aktiviert und in der richtigen Reihenfolge aufgeführt sind.

So ändern Sie die BIOS-Einstellung:

1. Starten Sie das verwaltete System.
2. Drücken Sie <F2>, um das BIOS-Setup-Fenster aufzurufen.
3. Scrollen Sie zur Startsequenz und drücken Sie die Eingabetaste.

   Im Popup-Fenster werden die virtuellen optischen Laufwerke und virtuellen Diskettenlaufwerke mit den Standard-Startgeräten aufgeführt.
4. Stellen Sie sicher, dass das virtuelle Laufwerk aktiviert und als erstes Gerät mit startfähigem Datenträger aufgelistet wird. Falls erforderlich, folgen Sie den Bildschirmanleitungen zur Änderung der Startreihenfolge.
5. Speichern Sie die Änderungen und beenden Sie.

   Das verwaltete System wird neu gestartet.

   Das verwaltete System versucht, basierend auf der Startreihenfolge, von einem startfähigen Gerät zu starten. Ist das virtuelle Gerät angeschlossen und ein startfähiger Datenträger vorhanden, startet das System vom virtuellen Gerät. Ansonsten ignoriert das System die Komponente – ähnlich wie bei einer physischen Komponente ohne startfähigen Datenträger.

Installation von Betriebssystemen mittels virtuellem Datenträger

In diesem Abschnitt wird eine manuelle, interaktive Methode zum Installieren des Betriebssystems auf der Management Station beschrieben. Das Verfahren kann mehrere Stunden in Anspruch nehmen. Ein geskriptetes Betriebssystem-Installationsverfahren unter Verwendung des virtuellen Datenträgers kann weniger als 15 Minuten beanspruchen. Weitere Informationen finden Sie unter Betriebssystem mittels VM-CLI bereitstellen.

1. Überprüfen Sie folgende Punkte:
   - Die Installations-CD des Betriebssystems ist in das CD-Laufwerk der Management Station eingelegt.

- Das lokale CD-Laufwerk ist ausgewählt.
- Sie sind mit den virtuellen Laufwerken verbunden.

2. Befolgen Sie die Schritte zum Starten über den virtuellen Datenträger im Abschnitt Starten vom virtuellen Datenträger, um sicherzustellen, dass das BIOS so eingestellt ist, dass es vom CD-Laufwerk startet, von dem aus Sie die Installation vornehmen.

3. Folgen Sie den Bildschirmanleitungen, um die Installation abzuschließen.

Virtuelle Datenträger verwenden, wenn das Betriebssystem des Servers ausgeführt wird

Windows-basierte Systeme

Auf Windows-Systemen werden die Laufwerke der virtuellen Datenträger automatisch gemountet und mit einem Laufwerkbuchstaben konfiguriert.

Die Verwendung der virtuellen Laufwerke innerhalb von Windows ist der Verwendung der physischen Laufwerke ähnlich. Wenn Sie eine Verbindung zu den Datenträgern an einer Management Station aufbauen, werden die Datenträger am System verfügbar, indem Sie auf das Laufwerk klicken und dessen Inhalt durchsuchen.

Linux-basierte Systeme

Auf Linux-Systemen werden die Laufwerke der virtuellen Datenträger nicht mit einem Laufwerkbuchstaben konfiguriert. Abhängig von der auf dem System installierten Software können die Laufwerke der virtuellen Datenträger eventuell nicht automatisch gemountet werden. Wenn die Laufwerke nicht automatisch gemountet werden, mounten Sie die Laufwerke manuell.

Virtual Flash verwenden

DRAC 5 verfügt über nicht flüchtigen virtuellen Flash-Speicher – einen 16-MB-Flash-Speicher im DRAC 5-Dateisystem, der für zur beständigen Speicherung verwendet werden und auf den das System zugreifen kann. Bei Aktivierung wird Virtual Flash als ein drittes virtuelles Laufwerk konfiguriert und in der BIOS-Startreihenfolge angezeigt, was einem Benutzer ermöglicht, vom Virtual Flash zu starten.

ANMERKUNG: Um vom Virtual Flash aus zu starten, muss das Virtual Flash-Abbild ein startfähiges Abbild sein.

Anders als eine CD oder ein Diskettenlaufwerk, die eine externe Client-Verbindung oder eine funktionsfähige Komponente 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 unformatiertes, entfernbares USB-Laufwerk in der Host-Umgebung.

Verwenden Sie die folgenden Richtlinien, wenn Sie Virtual Flash implementieren:

- Durch das Herstellen oder Trennen der Virtual Flash-Verbindung wird eine USB-Umnummerierung durchgeführt, bei der die Verbindung aller Komponenten des virtuellen Datenträgers hergestellt bzw. getrennt werden (Beispiel: CD-Laufwerk und Diskettenlaufwerk).
- Der Verbindungsstatus des CD/Diskettenlaufwerks des virtuellen Datenträgers ändert sich nicht, wenn Sie Virtual Flash aktivieren oder deaktivieren.

VORSICHTSHINWEIS: Die Verfahren zum Trennen und Herstellen von Verbindungen unterbrechen aktive Lese- und Schreibvorgänge des virtuellen Datenträgers.

Virtual Flash aktivieren

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein, und drücken Sie auf die Eingabetaste, um Virtual Flash zu aktivieren:

```
racadm config -g cfgRacVirtual -o cfgVirMediaKeyEnable 1
```

Virtual Flash deaktivieren

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein, und drücken Sie auf die Eingabetaste, um Virtual Flash zu deaktivieren:

```
racadm config -gcfgRacVirtual -o cfgVirMediaKeyEnable 0
```

Abbilder in Virtual Flash speichern

Virtual Flash kann vom verwalteten Host aus formatiert werden. Wenn Sie das Windows-Betriebssystem ausführen, klicken Sie mit der rechten Maustaste auf das Laufwerk-Symbol, und wählen Sie **Format** aus. Wenn Sie Linux ausführen, ermöglichen Systemdienstprogramme wie **format** und **fdisk** die Partitionierung und Formatierung des USB.

Stellen Sie, bevor Sie ein Abbild vom RAC-Internet-Browser zum Virtual Flash hochladen, sicher, dass die Größe der Abbilddatei zwischen 1,44 MB und maximal 16 MB liegt, und Virtual Flash deaktiviert ist. Nachdem Sie das Abbild heruntergeladen und das Virtual Flash-Laufwerk wieder aktiviert haben, erkennen das

System und das 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 das System neu, und booten Sie das ausgewählte Datenträgerlaufwerk.
3. Legen Sie im Virtual Flash eine Partition an, und aktivieren Sie die Partition.

   Wenden Sie **fdisk** an, wenn Virtual Flash eine Festplatte emuliert. Ist Virtual Flash als Laufwerk B: konfiguriert, emuliert Virtual Flash eine Diskette und benötigt keine Partition bei der Konfiguration von Virtual Flash als startfähiges Laufwerk.
4. Formatieren Sie das Laufwerk mittels des Befehls **format** mit dem Schalter **/s**, um die Systemdateien auf den virtuellen Flash-Speicher zu übertragen.

   Beispiel:

   `format /s x`

   wobei *x* der dem Virtual Flash zugeteilte Laufwerkbuchstabe ist.
5. Fahren Sie das System herunter, und nehmen Sie die startfähige Diskette oder CD aus dem entsprechenden Laufwerk.
6. Schalten Sie das System ein, und überprüfen Sie, ob das System vom Virtual Flash mit der `C:\`- oder `A:\`-Eingabeaufforderung startet.

Befehlszeilendienstprogramm des virtuellen Datenträgers verwenden

Das Dienstprogramm der Befehlszeilenoberfläche des virtuellen Datenträgers (VM-CLI) ist eine Script-Befehlszeilenschnittstelle, die Funktionen des virtuellen Datenträgers der Management Station für DRAC 5 im Remote-System ermöglicht.

Das VM-CLI-Dienstprogramm enthält die folgenden Funktionen:

- Unterstützt mehrfache gleichzeitig aktive Sitzungen.

  ANMERKUNG: Beim Virtualisieren von schreibgeschützten Imagedateien können sich mehrere Sitzungen dieselben Imagedatenträger teilen. Beim Virtualisieren von physischen Laufwerken kann zu einem bestimmten Zeitpunkt jeweils nur eine Sitzung auf ein gegebenes physisches Laufwerk zugreifen.
- Wechseldatenträgergeräte oder Imagedateien, die mit den Plugins des virtuellen Datenträgers übereinstimmen.
- Automatische Terminierung, wenn die DRAC-Firmware-Option Einmaliger Start aktiviert ist.
- Sichere Datenübertragungen zu DRAC 5 mittels Secure Sockets Layer (SSL).

Stellen Sie vor dem Ausführen des Dienstprogramms sicher, dass Sie über die DRAC 5-Benutzerberechtigung des virtuellen Datenträgers im Remote-System verfügen.

Unterstützt das Betriebssystem Administratorrechte oder eine betriebssystemspezifische Berechtigung oder Gruppenmitgliedschaft, sind Administratorrechte auch zum Ausführen des VM-CLI-Befehls erforderlich.

Der Administrator des Client-Systems steuert Benutzergruppen und -berechtigungen und dadurch auch die Benutzer, die das Dienstprogramm ausführen können.

Für Windows-Systeme müssen Sie über Hauptbenutzerberechtigungen verfügen, um das VM-CLI-Dienstprogramm ausführen zu können.

Für Linux-Systeme können Sie ohne Administratorrechte auf das VM-CLI-Dienstprogramm zugreifen, indem Sie den Befehl **sudo** verwenden. Dieser Befehl ist ein zentrales Mittel zur Bereitstellung von Nicht-Administrator-Zugriff und protokolliert alle Benutzerbefehle. Um Benutzer zu der VM-CLI-Gruppe hinzuzufügen oder zu bearbeiten verwendet der Administrator den Befehl **visudo**. Benutzer ohne Administratorrechte können den Befehl **sudo** als Präfix zur VM-CLI-Befehlszeile (oder zum VM-CLI-Script) hinzufügen, um Zugriff auf DRAC 5 im Remote-System zu erhalten und das Dienstprogramm auszuführen.

Dienstprogramm-Installation

Das VM-CLI-Dienstprogramm befindet sich auf der DVD *Dell Systems Management Tools and Documentation*, die im Dell OpenManage System Management-Softwarepaket enthalten ist. Legen Sie zum Installieren des Dienstprogramms die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk des Systems ein, und befolgen Sie die Anleitungen auf dem Bildschirm.

Die DVD *Dell Systems Management Tools and Documentation* enthält die neuesten Systemverwaltungs-Softwareprodukte einschließlich Diagnose, Speicherverwaltung, Remote-Zugriffs-Dienst und dem RACADM-Dienstprogramm. Diese DVD enthält auch Infodateien mit den neuesten Produktinformationen über die Systems Management Software.

Darüber hinaus enthält die DVD *Dell Systems Management Tools and Documentation* das Beispielscript **vmdeploy**, das illustriert, wie die VM-CLI- und RACADM-Dienstprogramme zum Bereitstellen von Software für mehrere Remote-Systeme verwendet werden. Weitere Informationen finden Sie unter Betriebssystem mittels VM-CLI bereitstellen.

Befehlszeilenoptionen

Die VM-CLI-Schnittstelle ist auf Windows- und Linux-Systemen identisch. Das Dienstprogramm verwendet Optionen, die mit den RACADM-Dienstprogramm-Optionen übereinstimmen. Beispielsweise erfordert eine Option zur Angabe der DRAC 5-IP-Adresse dieselbe Syntax für das RACADM-Dienstprogramm und das VM-CLI-Dienstprogramm.

Das Format eines VM-CLI-Befehls lautet wie folgt:

`racvmcli [parameter] [operating_system_shell_options]`

ANMERKUNG: Um den Befehl `racvmcli` ausführen zu können, benötigen Sie **Administrator**rechte.

Bei der Befehlszeilensyntax wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter VM-CLI-Parameter.

Wenn das Remote-System die Befehle akzeptiert und DRAC 5 die Verbindung autorisiert, wird der Befehl so lange weiter ausgeführt, bis eine der folgenden Situationen eintritt:

- Die VM-CLI-Verbindung wird aus einem beliebigen Grund abgebrochen.
- Der Prozess wird mit einer Betriebssystemsteuerung manuell abgebrochen. Beispiel: In Windows können Sie den Task Manager verwenden, um den Prozess abzubrechen.

VM-CLI-Parameter

DRAC 5-IP-Adresse

`-r <RAC-IP-Adresse>[:<RAC-SSL-Anschluss>]`

wobei *<RAC-IP-Adresse>* eine gültige, eindeutige IP-Adresse oder der DRAC 5-DDNS-Name (dynamisches Domänennamensystem) ist, falls dieses unterstützt wird.

Dieser Parameter enthält die DRAC 5-IP-Adresse und den SSL-Port. Das VM-CLI-Dienstprogramm benötigt diese Informationen, um eine Verbindung des virtuellen Datenträgers mit dem Ziel-DRAC 5 aufbauen zu können. Wenn Sie eine ungültige IP-Adresse oder einen ungültigen DDNS-Namen eingeben, wird eine Fehlermeldung angezeigt, und der Befehl wird abgebrochen.

Wenn *<RAC-SSL-Port>* ausgelassen wird, wird Port 443 (der Standard-Port) verwendet. Solange der Standard-SSL-Port von DRAC 5 nicht geändert wird, ist der optionale SSL-Port nicht erforderlich.

DRAC 5-Benutzername

`-u <DRAC-Benutzername>`

Dieser Parameter enthält den DRAC 5-Benutzernamen, mit dem der virtuelle Datenträger ausgeführt wird.

Der *<DRAC-Benutzername>* muss die folgenden Attribute aufweisen:

- Gültiger Benutzername
- Benutzerberechtigung für virtuelle DRAC-Datenträger

Schlägt die DRAC 5-Authentifizierung fehl, wird eine Fehlermeldung angezeigt, und der Befehl wird abgebrochen.

DRAC-Benutzerkennwort

`-p <DRAC-Benutzerkennwort>`

Dieser Parameter enthält das Kennwort für den angegebenen DRAC 5-Benutzer.

Schlägt die DRAC 5-Authentifizierung fehl, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.

Disketten-/Festplattengerät oder Imagedatei

`-f {<Gerätename> | <Abbilddatei>}`

wobei *<Gerätename>* ein gültiger Laufwerkbuchstabe (für Windows-Systeme) oder ein gültiger Gerätename ist, einschließlich der Dateisystem-Partitionsnummer zum Mounten, falls anwendbar (für Linux-Systeme), und wobei *<Abbilddatei>* der Dateiname und Pfad einer gültigen Abbilddatei ist.

Dieser Parameter bestimmt das Gerät oder die Datei, das/die den virtuellen Disketten-/Festplatten-Datenträger liefert.

Beispiel: Eine Imagedatei wird wie folgt angegeben:

`-f c:\temp\myfloppy.img` (Windows-System)

`-f /tmp/myfloppy.img` (Linux-System)

Wenn die Datei nicht schreibgeschützt ist, kann der virtuelle Datenträger in die Imagedatei schreiben. Konfigurieren Sie das Betriebssystem so, dass eine Disketten-Imagedatei, die nicht überschrieben werden soll, mit einem Schreibschutz versehen wird.

Beispiel: Ein Gerät wird wie folgt angegeben:

`-f a:\` (Windows-System)

`-f /dev/sdb4 # 4th partition on device /dev/sdb` (Linux-System)

Wenn das Gerät eine Schreibschutzoption anbietet, können Sie diese verwenden, um sicherzustellen, dass der virtuelle Datenträger nicht auf den Datenträger schreibt.

Lassen Sie außerdem diesen Parameter aus der Befehlszeile weg, wenn Sie keine Diskettendatenträger virtualisieren. Wenn ein ungültiger Wert festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl wird abgebrochen.

CD/DVD-Gerät oder -Imagedatei

`-c {<Gerätename> | <Abbilddatei>}`

wobei <*Gerätename*> ein gültiger CD/DVD-Laufwerkbuchstabe (Windows-Systeme) oder ein gültiger CD/DVD-Komponenten-Dateiname (Linux-Systeme) ist, und wobei <*Abbilddatei*> der Dateiname und Pfad einer gültigen ISO-9660-Abbilddatei ist.

Dieser Parameter bestimmt das Gerät oder die Datei, das/die die virtuellen CD/DVD-ROM-Datenträger liefert:

Beispiel: Eine Imagedatei wird wie folgt angegeben:

`-c c:\temp\mydvd.img` (Windows-Systeme)

`-c /tmp/mydvd.img` (Linux-Systeme)

Beispiel: Ein Gerät wird wie folgt angegeben:

`-c d:\` (Windows-Systeme)

`-c /dev/cdrom` (Linux-Systeme)

Dieser Parameter kann auf der Befehlszeile entfallen, wenn Sie keine CD/DVD-Datenträger virtualisieren. Wenn ein ungültiger Wert festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl bricht ab.

Geben Sie mit dem Befehl mindestens einen Datenträgertyp (Disketten- oder CD/DVD-Laufwerk) an, es sei denn, es werden nur Switch-Optionen vorgegeben. Andernfalls wird eine Fehlermeldung angezeigt und der Befehl wird mit einem Fehler abgebrochen.

Versionsanzeige

`-v`

Dieser Parameter wird zur Anzeige der Version des VM-CLI-Dienstprogramms verwendet. Wenn keine anderen Nicht-Switch-Optionen geboten werden, wird der Befehl ohne Fehlermeldung abgebrochen.

Hilfeanzeige

`-h`

Dieser Parameter zeigt eine Zusammenfassung der VM-CLI-Dienstprogrammparameter an. Werden keine anderen Nichtschalteroptionen spezifiziert, wird der Befehl ohne Fehler abgebrochen.

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 Management Station und DRAC 5 im Remote-System. Wenn dieser Parameter nicht in der Befehlszeile enthalten ist, wird die Datenübertragung nicht verschlüsselt.

Shell-Optionen des VM-CLI-Betriebssystems

Die folgenden Betriebssystem-Funktionen können auf 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 von der Standardeingabe (**stdin**). Infolgedessen ist keine **stdin**-Umleitung erforderlich.

- Ausführung im Hintergrund – Standardmäßig wird das VM-CLI-Dienstprogramm im Vordergrund ausgeführt. Verwenden Sie die Shell-Funktionen des Betriebssystems, um zu veranlassen, dass das Dienstprogramm im Hintergrund ausgeführt wird. Unter einem Linux-Betriebssystem wird z. B. durch das auf den Befehl folgende Et-Zeichen (&) veranlasst, dass das Programm als neuer Hintergrundprozess gestartet wird.

Diese letztere Methode ist in Script-Programmen nützlich, da das Script hierdurch fortgesetzt werden kann, nachdem für den VM-CLI-Befehl ein neues Verfahren begonnen wurde (das Script würde andernfalls blockieren, bis das VM-CLI-Programm abgebrochen wird). Wenn mehrfache VM-CLI-Instanzen auf diese Weise gestartet werden und eine oder mehrere Befehls-Instanzen manuell abgebrochen werden müssen, verwenden Sie die betriebssystemspezifischen Einrichtungen zum Aufführen und Beenden von Verfahren.

VM-CLI-Rückgabecodes

0 = Kein Fehler

1 = Kann keine Verbindung herstellen

2 = VM-CLI-Befehlszeilenfehler

3 = RAC-Firmware-Verbindung abgebrochen

Immer wenn Fehler auftreten, werden neben der Standardfehlerausgabe auch Textmeldungen auf Englisch ausgegeben.

Betriebssystem mittels VM-CLI bereitstellen

Das Dienstprogramm der Befehlszeilenoberfläche des virtuellen Datenträgers (VM-CLI) ist eine Befehlszeilenschnittstelle, die Funktionen des virtuellen Datenträgers der Management Station für DRAC 5 im Remote-System ermöglicht. Mit VM-CLI und Scriptmethoden können Sie das Betriebssystem auf mehreren Remote-Systemen im Netzwerk einsetzen.

Dieser Abschnitt enthält Informationen über die Integrierung des VM-CLI-Dienstprogramms in Ihrem Unternehmensnetzwerk.

Bevor Sie beginnen

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

Remote-System-Anforderungen

- Die DRAC 5-Karte ist in jedem Remote-System installiert
- Die virtuelle Komponente in jedem Remote-System ist die erste Komponente in der BIOS-Startreihenfolge.

Dell Custom Factory Integration

Wenn Sie Ihr Dell-System mit Dell-CFI-Optionen (Custom Factory Integration) 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 den Komponenten des virtuellen Datenträgers aus zu starten, nachdem das System in Ihrem Unternehmensnetzwerk installiert wurde.

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

Netzwerkanforderungen

Sie müssen über eine Netzwerkfreigabe verfügen, die Folgendes enthält:

- Betriebssystemdateien
- Erforderliche Treiber
- Start-Imagedatei(en) des Betriebssystems

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

Startfähige Imagedatei erstellen

Bevor Sie die Imagedatei für die Remote-Systeme bereitstellen, ist sicherzustellen, dass ein unterstütztes System von der Datei gestartet werden kann. Um die Abbilddatei zu testen, übertragen Sie sie auf ein Testsystem mit der DRAC 5-Internet-Benutzeroberfläche, und starten Sie dann das System neu.

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

Imagedatei für Linux-Systeme erstellen

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

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

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

Beispiel:

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

Imagedatei für Windows-Systeme erstellen

Achten Sie bei der Auswahl eines Datenreplikator-Dienstprogramms für Windows-Imagedateien darauf, dass es sich um ein Dienstprogramm handelt, welches die Imagedatei und die CD/DVD-Startsektoren kopiert.

Vorbereitung auf die Bereitstellung

Remote-Systeme konfigurieren

1. Erstellen Sie eine Netzwerkfreigabe, auf die über die Management Station zugegriffen werden kann.
2. Kopieren Sie die Betriebssystemdateien zur Netzwerkfreigabe.
3. Wenn Sie über eine startfähige, vorkonfigurierte Imagedatei zur Bereitstellung des Betriebssystems an die Remote-Systeme verfügen, können Sie diesen Schritt überspringen.

   Wenn Sie über keine startfähige, vorkonfigurierte Imagedatei verfügen, erstellen Sie die Datei. Schließen Sie alle für die Betriebssystem-Bereitstellungsverfahren verwendeten Programme und/oder Scripts ein.

   Um z. B. das Microsoft Windows-Betriebssystem bereitzustellen, kann die Imagedatei Programme enthalten, die den von Microsoft Systems Management Server (SMS) verwendeten Bereitstellungsmethoden ähnlich sind.

   Stellen Sie beim Erstellen der Abbilddatei sicher, dass Sie:

   - Befolgen Sie netzwerkbasierte Standardinstallationsverfahren.
   - Das Bereitstellungs-Abbild als „schreibgeschützt" kennzeichnen, um sicherzustellen, dass jedes Zielsystem startet und dasselbe Bereitstellungsverfahren ausführt.

4. Führen Sie eines der folgenden Verfahren aus:

   - RACADM und die Befehlszeilenoberfläche des virtuellen Datenträgers (VM-CLI) in Ihre vorhandene Betriebssystem-Bereitstellungsanwendung integrieren. Das Beispiel-Bereitstellungsscript als Richtlinie verwenden, wenn Sie die DRAC 5-Dienstprogramme in Ihre vorhandene Betriebssystem-Bereitstellungsanwendung integrieren.
   - Das vorhandene **vmdeploy**-Script verwenden, um Ihr Betriebssystem bereitzustellen.

Bereitstellen des Betriebssystems

Verwenden Sie das VM-CLI-Dienstprogramm und das im Dienstprogramm enthaltene **vmdeploy**-Script, um das Betriebssystem für die Remote-Systeme bereitzustellen.

Bevor Sie beginnen, sehen Sie sich das zum VM-CLI-Dienstprogramm gehörende **vmdeploy**-Beispielscript an. Das Script bietet ausführliche Voraussetzungen für die Bereitstellung des Betriebssystems für die Remote-Systeme im Netzwerk.

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

1. Identifizieren Sie die Remote-Systeme, die bereitgestellt werden sollen.
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 Zielsystem einbezieht:
    - DRAC 5-IP-Adresse oder DDNS-Name
    - Name der startfähigen Bereitstellungs-Abbilddatei
    - DRAC 5-Benutzername
    - DRAC 5-Benutzerkennwort
b. Stellen Sie die Ziel-DRAC 5-Option **Einmaliger Start** mittels RACADM ein.
c. Starten Sie das DRAC 5-System mithilfe von RACADM neu.

Häufig gestellte Fragen

Ich habe bemerkt, dass meine Verbindung des virtuellen Datenträger-Clients manchmal abbricht. Warum?

Wenn bei einem Netzwerk eine Zeitüberschreitung eintritt, trennt die DRAC 5-Firmware die Verbindung, wobei die Verbindung zwischen dem Server und dem virtuellen Laufwerk unterbrochen wird. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie die Funktion Virtueller Datenträger.

Welche Betriebssysteme unterstützen den DRAC 5?

Eine Liste unterstützter Betriebssysteme befindet sich auf der *Support-Matrix der Dell-Systemsoftware* auf der Dell Support-Website unter **support.dell.com/manuals**.

Welche Internet-Browser unterstützen den DRAC 5?

Eine Liste unterstützter Internet-Browser befindet sich auf der *Support-Matrix der Dell-Systemsoftware* auf der Support-Website von Dell unter **support.dell.com/manuals**.

Warum bricht meine Client-Verbindung manchmal ab?

- Es kann sein, dass Ihre Client-Verbindung von Zeit zu Zeit unterbrochen wird, wenn das Netzwerk langsam ist, oder wenn Sie die CD im CD-Laufwerk des Client-Systems wechseln. Beispiel: Wenn Sie die CD im CD-Laufwerk des Client-Systems wechseln, weist die neue CD eventuell eine Autostart-Funktion auf. Wenn dies der Fall ist, kann für die Firmware eine Zeitüberschreitung eintreten und die Verbindung kann verloren gehen, wenn das Client-System zu viel Zeit in Anspruch nimmt, bevor es zum Lesen der CD bereit ist. Wenn eine Verbindung verloren geht, können Sie sie über die GUI wieder herstellen und mit dem vorherigen Vorgang fortfahren.
- Wenn bei einem Netzwerk eine Zeitüberschreitung eintritt, trennt die DRAC 5-Firmware die Verbindung, wobei die Verbindung zwischen dem Server und dem virtuellen Laufwerk unterbrochen wird. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie die Funktion Virtueller Datenträger.

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 das System während des Installationsverfahrens eventuell vorübergehend seine Verbindung zum CD-Laufwerk verlieren, und eine korrekte Installation des Betriebssystems kann 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 Sie das Programm nur auf den Systemen aus, auf die sich das Problem bezieht. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 823086.

Warum kann ich Windows 2000 nicht lokal oder im Remote-Zugriff installieren?

Dieses Problem tritt normalerweise dann auf, wenn Virtual Flash aktiviert ist und kein gültiges Abbild enthält, z. B. wenn Virtual Flash ein beschädigtes oder zufälliges Abbild enthält, kann es sein, dass Sie Windows 2000 weder lokal noch im Remote-Zugriff installieren können. Um dieses Problem zu lösen, installieren Sie ein gültiges Abbild auf Virtual Flash, oder deaktivieren Sie 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 wurde?

Die Installation von Netzwerk- und Chipsatz-Treibern auf dem Server führt zu einem Abbruch der Verbindung des virtuellen Datenträgers bei Konfiguration im freigegebenen NIC-Modus. Die Installation der Netzwerk- oder Chipsatz-Treiber verursacht, dass LOM zurückgesetzt wird, was wiederum zu Zeitüberschreitungen bei Netzwerkpaketen und zu Zeitüberschreitungen und einem Abbruch der Verbindung des virtuellen Datenträgers führt. Um dieses Problem zu umgehen, kopieren Sie die Treiber vom 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 DVD *Dell Systems Management Tools and Documentation* und über eine langsame Netzwerkverbindung installieren, kann es sein, dass das Installationsverfahren aufgrund der Netzwerklatenzzeit mehr Zeit in Anspruch nimmt, um auf die DRAC 5-Internet-basierte Schnittstelle zuzugreifen. Obwohl das Installationsfenster den Installationsfortschritt nicht anzeigt, befindet sich das Installationsverfahren in Ausführung.

Ich sehe den Inhalt eines Diskettenlaufwerks oder eines USB-Speicherschlüssels an. Wenn ich versuche, über das gleiche Laufwerk eine Verbindung zum virtuellen Datenträger herzustellen, erhalte ich eine Verbindungs-Fehlermeldung und werde gebeten, den Vorgang zu wiederholen. Warum?

Ein gleichzeitiger Zugriff auf virtuelle Diskettenlaufwerke ist nicht erlaubt. 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 nach Bedarf. Um z. B. von einem CD-Laufwerk aus zu starten, konfigurieren Sie das CD-Laufwerk als erstes Laufwerk in der Startreihenfolge.

Von welchen Arten von Datenträgern kann ich starten?

Mit DRAC 5 können Sie von den folgenden startfähigen Datenträgern aus starten:

- CD-ROM/DVD-Datenträger

- ISO 9660-Image
- 1,44 Zoll-Diskette oder Disketten-Image
- DRAC 5-integrierter Virtual Flash
- USB-Schlüssel, der vom Betriebssystem als Wechsellaufwerk erkannt wird
- Ein USB-Schlüssel-Image

Wie kann ich meinen USB-Schlüssel startfähig machen?

Nur USB-Speicher-Sticks mit Windows 98 DOS können von der virtuellen Diskette starten. Um Ihren eigenen startfähigen USB-Speicher-Stick zu konfigurieren, starten Sie mit einer Windows 98-Startdiskette, und kopieren Sie Systemdateien von der Startdiskette auf den USB-Speicher-Stick. Geben Sie z. B. an der DOS-Eingabeaufforderung den folgenden Befehl ein:

```
sys a: x: /s
```

wobei „x:" der USB-Speicher-Stick ist, der startfähig gemacht werden soll.

Sie können auch das Startdienstprogramm von Dell verwenden, um einen startfähigen USB-Speicher-Stick zu erstellen. Dieses Dienstprogramm ist nur mit USB-Speicher-Stick der Marke Dell kompatibel. Öffnen Sie zum Herunterladen des Dienstprogramms einen unterstützten Internet-Browser, wechseln Sie zur Support-Website von Dell, die sich unter **support.dell.com** befindet, und machen Sie die Datei „R122672.exe" ausfindig.

Brauche ich Administratorrechte, um das ActiveX-Plug-In installieren zu können?

Um das Plug-In des virtuellen Datenträgers installieren zu können, müssen Sie auf Windows-Systemen Administratorrechte oder Hauptbenutzerberechtigungen besitzen.

Welche Berechtigungen brauche ich, um das Plug-In des virtuellen Datenträgers auf einer Red Hat Linux-Management Station zu installieren und verwenden?

Sie müssen in der Verzeichnisstruktur des Browsers Schreibberechtigungen besitzen, um das Plug-In des virtuellen Datenträgers erfolgreich installieren zu können.

Ich kann meine virtuelle Diskettenkomponente 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 meinem Remote-Diskettenlaufwerk verbunden. Was soll ich tun?

Bei einigen Linux-Versionen werden virtuelle Diskettenlaufwerke und virtuelle CD-Laufwerke nicht in gleicher Weise automatisch geladen. Um das virtuelle Diskettenlaufwerk zu mounten, machen Sie den Komponentenknoten ausfindig, den Linux dem virtuellen Diskettenlaufwerk zuordnet. Führen Sie die folgenden Schritte aus, um das virtuelle Diskettenlaufwerk korrekt ausfindig zu machen und zu mounten:

1. Öffnen Sie eine Linux-Eingabeaufforderung und führen Sie den folgenden Befehl aus:

   ```
   grep "Virtual Floppy" /var/log/messages
   ```

2. Machen Sie den letzten Eintrag zu dieser Meldung ausfindig und notieren Sie die Zeit.

3. Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:

   ```
   grep "hh:mm:ss" /var/log/messages
   ```
   wobei

   hh:mm:ss der Zeitstempel der Meldung ist, die von grep in Schritt 1 zurückgegeben wurde.

4. Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls, und machen Sie den Komponentennamen ausfindig, den die „virtuelle Dell-Floppy" trägt.

5. Stellen Sie sicher, dass das virtuelle Diskettenlaufwerk angeschlossen ist und eine Verbindung dazu besteht.

6. Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:

   ```
   mount /dev/sdx /mnt/floppy
   ```

   wobei

   /dev/sdx ist der in Schritt 4 gefundene Gerätename.

   /mnt/floppy ist der Bereitstellungspunkt.

Welche Dateisystemtypen werden auf meinem virtuellen Diskettenlaufwerk oder auf Virtual Flash unterstützt?

Ihr virtuelles Diskettenlaufwerk oder Virtual Flash unterstützt FAT16- oder FAT32-Dateisysteme.

Als ich im Remote-Zugriff anhand der DRAC 5-Internet-basierten Schnittstelle eine Firmware-Aktualisierung ausführte, wurden meine virtuellen Laufwerke im Server entfernt. Warum?

Firmware-Aktualisierungen führen zu einem Reset von DRAC 5, einem Abbruch der Remote-Verbindung sowie zum Unmount 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 getrennt und dann wieder mit ihm verbunden werden.

Wie kann ich einen Internet-Browser auf meiner Management Station installieren, auf der sich ein schreibgeschütztes Dateisystem befindet?

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

VORSICHTSHINWEIS: In einer schreibgeschützten Client-Umgebung wird das installierte VM-Plug-In betriebsunfähig, wenn die DRAC 5-Firmware auf eine neuere Version des Plug-Ins aktualisiert wird. Dies ist der Fall, weil früheren Plug-In-Funktionen nicht erlaubt wird, zu funktionieren, wenn die Firmware eine neuere Plug-In-Version enthält. In diesem Fall werden Sie zur Plug-In-Installation aufgefordert. Da das Dateisystem schreibgeschützt ist, schlägt die Installation fehl, und die Plug-In-Funktionen sind nicht verfügbar.

So erhalten Sie das Plug-In-Installationspaket:

1. Melden Sie sich an einem vorhandenen DRAC 5 an.
2. Ändern Sie die URL in der Adresszeile des Browsers von

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

   in

   `https://<RAC_IP>/Plug-Ins/ # Achten Sie darauf, auch den abschließenden Schrägstrich zu verwenden.`
3. Machen Sie die beiden Unterverzeichnisse vm und vkvm ausfindig. Wechseln Sie zum entsprechenden Unterverzeichnis, klicken Sie mit der rechten Maustaste auf die Datei rac5XXX.xpi, und wählen Sie **Link- Ziel speichern unter...** aus.
4. Wählen Sie einen Speicherort für die Datei des Plug-In- Installationspakets aus.

So installieren Sie das Plug-In-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 auf der Browser-Adresszeile den Dateipfad zum Plug-In- Installationspaket ein. Beispiel:

   Datei:///tmp/rac5vm.xpi
4. Der Browser führt den Benutzer durch die Plug-In-Installation.

Wenn die Installation einmal durchgeführt wurde, fordert der Browser diese Plug-In-Installation nicht erneut an, solange die Ziel-DRAC5-Firmware keine neuere Version des Plug-Ins enthält.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Sicherheitsfunktionen konfigurieren

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

DRAC 5 bietet die folgenden Sicherheitsfunktionen:

- Erweiterte Sicherheitsoptionen für den DRAC-Aministrator:
  - Mittels der Deaktivierungsoption für die Konsolenumleitung können Benutzer des *lokalen* Systems die Konsolenumleitung anhand der DRAC 5-Konsolenumleitungsfunktion deaktivieren.
  - Die Deaktivierungsfunktionen für die lokale Konfiguration ermöglichen dem *Remote*-DRAC-Administrator, die Fähigkeit zum Konfigurieren des DRAC 5 über folgende Möglichkeiten selektiv zu deaktivieren:
    - BIOS-POST, Options-ROM
    - dem Betriebssystem unter Verwendung des lokalen racadm und der Dell OpenManage Server Administrator-Dienstprogramme
  - RACADM-CLI und Internet-basierte Schnittstellenvorgänge, die eine SSL-128-Bit-Verschlüsselung und SSL-40-Bit-Verschlüsselung (für Länder, in denen 128 Bit nicht annehmbar ist) unterstützen.

  ANMERKUNG: Telnet unterstützt keine SSL-Verschlüsselung.

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

Sicherheitsoptionen für den DRAC-Aministrator

Lokale DRAC 5-Konfiguration deaktivieren

Administratoren können die lokale Konfiguration über die DRAC 5-GUI (Grafische Benutzeroberfläche) deaktivieren, indem sie **Remote-Zugriff**→ **Konfiguration**→ **Dienste** auswählen. Wenn das Kontrollkästchen für **Lokale DRAC-Konfiguration mittels Options-ROM deaktiveren** ausgewählt ist, wird das Dienstprogramm für die Remote-Zugriffs-Konfiguration (auf das Sie durch Drücken auf Strg+E während des Systemstarts zugreifen können) im schreibgeschützten Modus betrieben, wodurch lokale Benutzer daran gehindert werden, die Komponente zu konfigurieren. Wenn der Administrator das Kontrollkästchen **Lokale DRAC-Konfiguration mittels RACADM deaktiveren** auswählt, können lokale Benutzer den DRAC 5 nicht über das racadm-Dienstprogramm oder mittels des Dell OpenManage Server Administrator konfigurieren, obwohl die Konfigurationseinstellungen noch immer abgelesen werden können.

Administratoren können eine oder beide dieser Optionen gleichzeitig aktivieren. Zusätzlich zum Aktivieren über die GUI können Administratoren Optionen auch unter Verwendung lokaler racadm-Befehle aktivieren.

Lokale Konfigurationen während des Systemneustarts deaktivieren

Durch diese Funktion wird die Fähigkeit des Benutzers des verwalteten Systems deaktiviert, DRAC 5 während des Systemneustarts zu konfigurieren.

```
racadm config -g cfgRacTune -o

cfgRacTuneCtrlEConfigDisable 1
```

ANMERKUNG: Diese Option wird nur im Remote-Zugriffs-Konfigurationsdienstprogramm Version 1.13 und später unterstützt. Um ein Upgrade auf diese Version vorzunehmen, erweitern Sie das BIOS unter Verwendung des BIOS-Aktualisierungspakets, das sowohl auf der DVD *Dell Server Updates* als auch auf der Support-Website von Dell unter **support.dell.com** zur Verfügung steht.

Lokale Konfiguration über lokalen racadm deaktivieren

Durch diese Funktion wird die Fähigkeit des Benutzers des verwalteten Systems deaktiviert, DRAC 5 unter Verwendung des lokalen racadm oder mittels der Dell OpenManage Server Administrator-Dienstprogramme zu konfigurieren.

```
racadm config -g cfgRacTune -o cfgRacTuneLocalConfigDisable 1
```

VORSICHTSHINWEIS: Durch diese Funktionen wird die Fähigkeit des lokalen Benutzers, DRAC 5 über das lokale System zu konfigurieren sowie einen Reset auf die Standardeinstellung der Konfiguration vorzunehmen, stark eingeschränkt. Dell empfiehlt, die Verwendung dieser Funktionen gut abzuwägen und nur eine Schnittstelle auf einmal zu deaktivieren, um einem vollständigen Verlust der Anmeldungsberechtigungen vorzubeugen.

ANMERKUNG: Weitere Informationen finden Sie in der Publikation zum Thema *Lokale Konfiguration und virtuelle Remote-KVM in DRAC deaktivieren* auf der Support-Website von Dell unter **support.dell.com / manuals**.

Obwohl Administratoren die lokalen Konfigurationsoptionen mittels lokaler racadm-Befehle einstellen können, ist es aus Sicherheitsgründen nur möglich, die Optionen über eine bandexterne DRAC 5-GUI oder eine Befehlszeilenschnittstelle zurückzusetzen. Die Option `cfgRacTuneLocalConfigDisable` gilt, sobald der Einschalt-Selbsttest des Systems abgeschlossen ist und das System in eine Betriebssystemumgebung gestartet wurde. Das Betriebssystem kann Microsoft Windows Server oder Enterprise Linux sein (Betriebssysteme, die Befehle des lokalen racadm ausführen können) oder ein beschränkt einsetzbares Betriebssystem wie z. B. Microsoft Windows Preinstallation Environment oder vmlinux, die zum Ausführen von Befehlen des lokalen racadm im Dell OpenManage Deployment Toolkit verwendet werden.

Es gibt verschiedene Situationen, in denen ein Administrator eine lokale Konfiguration u. U. deaktivieren muss. Beispiel: In einem Datenzentrum mit mehreren Administratoren für Server und Remote-Zugriffsgeräte benötigen diejenigen, die für die Wartung von Server-Software-Stacks zuständig sind, eventuell keine Administratorrechte für den Zugriff auf Remote-Zugriffsgeräte. Auf ähnliche Weise haben Techniker während routinemäßigen Systemwartungsarbeiten eventuell direkten Zugriff auf Server und sind dadurch in der Lage, Systeme neu zu starten und auf das kennwortgeschützte BIOS zuzugreifen. Es sollte jedoch nicht möglich sein, dass sie Remote-Zugriffsgeräte konfigurieren. Administratoren von Remote-Zugriffsgeräten sollten in Anbetracht der Möglichkeit solcher Situationen erwägen, die lokale Konfiguration zu deaktivieren.

Administratoren sollten in Betracht ziehen, dass das Deaktivieren lokaler Konfigurationen die Berechtigung zum Ausführen lokaler Konfigurationen stark einschränkt, was auch das Zurücksetzen von DRAC 5 auf die ursprüngliche Konfiguration einschließt. Sie sollten entsprechende Optionen daher nur anwenden, wenn dies wirklich notwendig ist und dabei lediglich eine Schnittstelle auf einmal deaktivieren, um einem vollständigen Verlust ihrer Anmeldungsberechtigung vorzubeugen. Wenn Administratoren z. B. alle lokalen DRAC 5-Benutzer deaktiviert haben und nur Benutzern des Microsoft Active Directory-Verzeichnisdienstes gestatten, sich an DRAC 5 anzumelden und die Infrastruktur der Active Directory-Authentifizierung daraufhin fehlschlägt, ist es möglich, dass sich die Administratoren nicht mehr anmelden können. Eine vergleichbare Situation tritt auf, wenn Administratoren die gesamte lokale Konfiguration deaktiviert haben und einen DRAC 5 mit statischer IP-Adresse einem Netzwerk hinzufügen, das bereits einen DHCP-Server (Dynamisches Host-Konfigurationsprotokoll) enthält und der DHCP-Server die DRAC 5-IP-Adresse daraufhin einer anderen Komponente auf dem Netzwerk zuweist. Durch den sich ergebenden Konflikt kann die bandexterne Konnektivität von DRAC deaktiviert werden, woraufhin Administratoren die Firmware über eine serielle Verbindung auf ihre standardmäßigen Einstellungen zurücksetzen müssen.

Virtuelle DRAC 5-Remote-KVM deaktivieren

Administratoren können DRAC 5-Remote-KVM selektiv deaktivieren und einem lokalen Benutzer somit eine flexible, sichere Methode zur Verfügung stellen, um auf dem System zu arbeiten, ohne dass eine andere Person über die Konsolsenumleitung die Maßnahmen des Benutzers beobachten kann. Damit diese Funktion verwendet werden kann, ist auf dem Server die Installation der DRAC-Software für den verwalteten Knoten erforderlich. Administratoren können die Remote-vKVM unter Verwendung des folgenden Befehls deaktivieren:

```
racadm LocalConRedirDisable 1
```

Der Befehl LocalConRedirDisable deaktiviert die vorhandenen Fenster der Remote-vKVM-Sitzung, wenn er mit Argument 1 ausgeführt wird.

Um zu verhindern, dass ein Remote-Benutzer die Einstellungen des lokalen Benutzers überschreibt, steht dieser Befehl nur für den lokalen racadm zur Verfügung. Administratoren können diesen Befehl auf Betriebssystemen (einschließlich Microsoft Windows Server 2003 und SUSE Linux Enterprise Server 10) verwenden, die den lokalen racadm unterstützen. Da dieser Befehl über Systemneustarts hinweg aufrechterhalten bleibt, müssen Administratoren den Befehl eigens wieder aufheben, um die Remote-vKVM erneut zu aktivieren. Die Aufhebung kann durch die Verwendung des Arguments 0 vorgenommen werden:

```
racadm LocalConRedirDisable 0
```

In verschiedenen Situationen ist die Deaktivierung von DRAC 5-Remote-vKVM erforderlich. Es ist z. B. möglich, dass Administratoren vermeiden möchten, dass ein Remote-DRAC 5-Benutzer die auf einem System konfigurierten BIOS-Einstellungen anzeigen kann. In diesem Falle können Administratoren die Remote-vKVM während des System-POST deaktivieren, indem Sie den Befehl `LocalConRedirDisable` anwenden. Es empfiehlt sich u. U., die Sicherheit zu erhöhen, indem die Remote-vKVM immer dann automatisch deaktiviert wird, wenn sich ein Administrator am System anmeldet. Hierzu ist der Befehl `LocalConRedirDisable` über die Benutzeranmeldungsskripts auszuführen.

ANMERKUNG: Weitere Informationen finden Sie in der Publikation zum Thema *Lokale Konfiguration und virtuelle Remote-KVM in DRAC deaktivieren* auf der Support-Website von Dell unter **support.dell.com / manuals**.

Weitere Informationen zu Anmeldungsskripts sind unter **technet2,microsoft.com / windowsserver / en / library / 31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx** zu finden.

DRAC 5-Kommunikationen mit SSL- und digitalen Zertifikaten sichern

Dieser Unterabschnitt enthält Informationen über die folgenden Datensicherheitsfunktionen, die in DRAC 5 integriert sind:

Secure Sockets Layer (SSL)

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 Methode, um

authentifizierte und verschlüsselte Kommunikationen zwischen Clients und Servern zu bieten und unbefugtes Lauschen auf dem Netzwerk zu verhindern.

Merkmale eines SSL-aktivierten Systems:

- Authentifiziert sich selbst an einem SSL-aktivierten Client
- Ermöglicht dem Client, sich am Server selbst zu authentifizieren
- Ermöglicht beiden Systemen, eine verschlüsselte Verbindung herzustellen

Dieses Verschlüsselungsverfahren gewährleistet ein hohes Maß von Datenschutz. DRAC verwendet den SSL-128-Bit-Verschlüsselungsstandard, die sicherste Form der Verschlüsselung, die für Internet-Browser in Nordamerika allgemein verfügbar ist.

Der DRAC-Web Server enthält ein selbstsigniertes Dell-SSL-Digitalzertifikat (Server-ID). Um hohe Sicherheit über das Internet zu gewährleisten, ersetzen Sie das Web Server-SSL-Zertifikat, indem Sie eine Anforderung an DRAC senden, um eine neue Zertifikatsignierungsanforderung (CSR) zu erstellen.

Zertifikatsignierungsanforderung (CSR)

Eine CSR ist eine digitale Anforderung eines sicheren Serverzertifikats von einer Zertifizierungsstelle (CA). Sichere Serverzertifikate sind erforderlich, um die Identität eines Remote-Systems zu schützen und um sicherzustellen, dass Informationen, die mit dem Remote-System ausgetauscht werden, von anderen weder gesehen noch geändert werden können. Um die Sicherheit für den iDRAC zu gewährleisten, wird dringend empfohlen, eine CSR zu erstellen, die CSR an eine Zertifizierungsstelle zu senden und das von der Zertifizierungsstelle erhaltene Zertifikat hochzuladen.

Bei einer Zertifizierungsstelle handelt es sich um ein Geschäftsunternehmen, das in der IT-Branche auf Grund seiner hohen Standards bezüglich der zuverlässigen Sicherheitsüberprüfung, Identifizierung und weiterer wichtiger Sicherheitskriterien anerkannt ist. Beispiele für CAs umfassen Thawte und VeriSign. Nachdem die CA die CSR empfangen hat, werden die in der CSR enthaltenen Informationen eingesehen und überprüft. Wenn der Bewerber den Sicherheitsstandards der CA genügt, wird für den Bewerber ein Zertifikat ausgestellt, das den Bewerber bei Übertragungen über Netzwerke oder über das Internet eindeutig identifiziert.

Nachdem die CA die CSR überprüft und ein Zertifikat gesendet hat, muss das Zertifikat zur DRAC-Firmware hochgeladen werden. Die in der DRAC-Firmware gespeicherten CSR-Informationen müssen mit den Informationen des Zertifikats übereinstimmen.

Zugriff auf das SSL-Hauptmenü

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **SSL**.

Verwenden Sie die Optionen auf der Seite **SSL-Hauptmenü** (sehen Sie Tabelle 12-1), um eine CSR zu erstellen, die an eine Zertifizierungsstelle gesendet wird. Die Informationen der CSR werden in der DRAC 5-Firmware gespeichert. Tabelle 12-2 beschreibt die auf der Seite **SSL-Hauptmenü** verfügbaren Schaltflächen.

Tabelle 12-1. 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 Zertifizierungsstelle gesendet werden kann, um ein Sicheres-Internet-Zertifikat anzufordern. △ **VORSICHTSHINWEIS: Jede neue CSR überschreibt die vorherige CSR in der Firmware. Damit eine Zertifizierungsstelle Ihre CSR annimmt, muss die CSR in der Firmware mit dem von der Zertifizierungsstelle zurückgesendeten Zertifikat übereinstimmen.**
Serverzertifikat hochladen	Klicken Sie auf **Weiter**, um ein vorhandenes Zertifikat hochzuladen, für das Ihre Firma den Titel besitzt und dazu verwendet, den Zugriff auf DRAC 5 zu steuern. △ **VORSICHTSHINWEIS: Nur X509 Base 64-kodierte Zertifikate werden von DRAC 5 akzeptiert. DER-kodierte Zertifikate werden nicht akzeptiert. Laden Sie ein neues Zertifikats hoch, um das Standardzertifikat, das Sie mit DRAC 5 erhalten haben, zu ersetzen.**
Serverzertifikat anzeigen	Klicken Sie auf **Weiter**, um ein vorhandenes Serverzertifikat anzuzeigen.

Tabelle 12-2. Schaltflächen im SSL-Hauptmenü

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **SSL-Hauptmenü**.
Weiter	Wechselt zur nächsten Seite.

Neue Zertifikatsignierungsanforderung erstellen

ANMERKUNG: Jede neue CSR überschreibt die vorherige CSR in der Firmware. Damit eine Zertifizierungsstelle (CA) Ihre CSR annimmt, muss die CSR in der Firmware mit dem von der Zertifizierungsstelle zurückgesendeten Zertifikat übereinstimmen. Ansonsten wird DRAC 5 das Zertifikat nicht hochladen.

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

   Tabelle 12-3 beschreibt die Optionen der Seite **Zertifikatsignierungsanforderung (CSR) erstellen**.
3. Klicken Sie auf **Erstellen**, um die CSR zu speichern oder anzuzeigen.
4. Klicken Sie auf die entsprechende Schaltfläche der Seite **Zertifikatsignierungsanforderung (CSR) erstellen**, um fortzufahren. Tabelle 12-4 beschreibt die auf der Seite **Zertifikatsignierungsanforderung (CSR) erstellen** verfügbaren Schaltflächen.

Tabelle 12-3. Optionen der Seite „Zertifikatsignierungsanforderung (CSR) erstellen"

Feld	Beschreibung
Allgemeiner Name	Der genaue Name, der zertifiziert werden soll (normalerweise der Web Server-Domänenname, z. B. **www.xyzcompany.com**). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen und Punkte sind gültig. Leerstellen sind nicht gültig.
Name der Organisation	Der mit dieser Organisation assoziierte Name (zum Beispiel, XYZ Corporation). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Organisationseinheit	Der mit einer organisatorischen Einheit assoziierte Name, z. B. eine Abteilung (zum Beispiel IT). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Ort	Die Stadt oder ein anderer Standort des Unternehmens, das zertifiziert wird (z. B. München). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie keine Unterstreichungszeichen oder andere Zeichen, um Wörter zu trennen.
Name des Bundeslands oder Kantons	Das Bundesland oder der Kanton, in dem sich das Unternehmen, das sich für eine Zertifizierung bewirbt, befindet (z. B. Bayern). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie keine Abkürzungen.
Landescode	Der Name des Landes, in dem sich das Unternehmen befindet, das sich um eine Zertifizierung bewirbt. Verwenden Sie das Dropdown-Menü, um das Land auszuwählen.
E-Mail	Die mit der CSR verbundene E-Mail-Adresse. Sie können die E-Mail-Adresse Ihrer Firma eingeben oder eine E-Mail-Adresse, die mit der CSR in Verbindung stehen soll. Dieses Feld ist optional.

Tabelle 12-4. Schaltflächen der Seite „Zertifikatsignierungsanforderung (CSR) erstellen"

Schaltfläche	Beschreibung
Drucken	Die Seite **Zertifikatsignierungsanforderung (CSR) erstellen** drucken.
Zurück zum Sicherheitshauptmenü	Zurück zur Seite **SSL-Hauptmenü**.
Erstellen	Eine CSR erstellen.

Serverzertifikat hochladen

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

   Die Seite **Zertifikat hochladen** wird eingeblendet.
2. Geben Sie im Feld **Dateipfad** den Pfad des Zertifikats in das Feld **Wert** ein, oder klicken Sie auf **Durchsuchen**, um zur Zertifikatdatei zu navigieren.

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

ANMERKUNG: Ein Serverzertifikat kann nur einmal hochgeladen werden. Falls Sie versuchen, ein Serverzertifikat hochzuladen, das bereits einmal hochgeladen wurde, zeigt DRAC die Fehlermeldung „Kein gültiges Zertifikat gefunden" an.

3. Klicken Sie auf **Anwenden**.
4. Klicken Sie auf die entsprechende Seitenschaltfläche, um fortzufahren.

Serverzertifikat anzeigen

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

   Tabelle 12-5 erläutert die Felder und zugehörigen Beschreibungen, die im Fenster **Zertifikat** aufgeführt werden.

2. Klicken Sie auf der Seite **Serverzertifikat anzeigen** auf die entsprechende Schaltfläche, um fortzufahren.

Tabelle 12-5. Zertifikatinformationen

Feld	Beschreibung
Seriennummer	Seriennummer des Zertifikats
Informationen des Antragstellers	Vom Antragsteller eingegebene Zertifikatsattribute
Ausstellerinformationen	Vom Aussteller zurückgegebene Zertifikatsattribute
Gültig von	Ausgabedatum des Zertifikats
Gültig bis	Ablaufdatum des Zertifikats

Secure Shell (SSH) verwenden

Es werden nur vier SSH-Sitzungen gleichzeitig unterstützt. Die Sitzungszeitüberschreitung wird durch die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert, wie unter Gruppen- und Objektdefinitionen der DRAC 5-Eigenschaftendatenbank beschrieben. Sie können die SSH auf 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>
```

Weitere Informationen zu den Eigenschaften `cfgSerialSshEnable` und `cfgRacTuneSshPort` finden Sie unter Gruppen- und Objektdefinitionen der DRAC 5-Eigenschaftendatenbank.

Die DRAC 5-SSH-Umsetzung unterstützt mehrfache Verschlüsselungs-Schemata, wie in Tabelle 12-6 dargestellt.

Tabelle 12-6. Verschlüsselungsschemata

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

ANMERKUNG: SSHv1 wird nicht unterstützt.

Dienste konfigurieren

ANMERKUNG: Zur Änderung dieser Einstellungen müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen. Zusätzlich kann das Remote-RACADM-Befehlszeilen-Dienstprogramm nur aktiviert werden, wenn der Benutzer als **root** angemeldet ist.

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.

2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Dienste**.

3. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Lokale Konfiguration (Tabelle 12-7)
   - Web Server (Tabelle 12-8)
   - SSH (Tabelle 12-9)
   - Telnet (Tabelle 12-10)
   - Remote-RACADM (Tabelle 12-11)
   - SNMP-Agent (Tabelle 12-12)
   - Automatisierter Systeme-Wiederherstellungsagent (Tabelle 12-13)

   Verwenden Sie den **Automatisierten Systemwiederherstellungs-Agent**, um die Funktion **Bildschirm Letzter Absturz** von DRAC 5 zu aktivieren.

   ANMERKUNG: Server Administrator muss mit aktivierter Funktion **Autom. Wiederherstellung** installiert werden, indem die **Maßnahme** entweder auf **System neu starten**, **System ausschalten** oder auf **System aus- und einschalten** eingestellt wird, sodass der **Bildschirm Letzter Absturz** in DRAC 5 funktionieren kann.

4. Klicken Sie auf **Änderungen übernehmen**.

5. Klicken Sie auf der Seite **Dienste** auf die entsprechende Schaltfläche, um fortzufahren. Siehe Tabelle 12-14.

Tabelle 12-7. Einstellungen der lokalen Konfiguration

Einstellung	Beschreibung
Lokale DRAC-Konfiguration mittels Options-ROM deaktivieren	Deaktiviert die lokale DRAC 5-Konfiguration mittels Options-ROM. Das Options-ROM fordert Sie auf, das Setup-Modul während des Systemneustarts durch Drücken von <Strg+E> zu öffnen.
Lokale DRAC-Konfiguration mittels RACADM deaktivieren	Deaktiviert die lokale DRAC 5-Konfiguration mittels lokalem RACADM.

Tabelle 12-8. Web Server-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert den Web Server. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger Sitzungen, die für dieses System zulässig sind.
Aktive Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich **Max. Sitzungen**.
Zeitüberschreitung	Die Zeit in Sekunden, die eine Verbindung inaktiv bleiben darf. Die Sitzung wird abgebrochen, wenn der Zeitüberschreitungswert erreicht wird. Änderungen an der Zeitlimit-Einstellung haben keine Auswirkung auf die aktuelle Sitzung. Wenn Sie die Zeitlimit-Einstellung ändern, müssen Sie sich abmelden und wieder anmelden, um die neue Einstellung wirksam zu machen. Der Zeitüberschreitungsbereich beträgt 60 bis 1920 Sekunden.
HTTP-Schnittstellennummer	Das von DRAC verwendete Port, das auf eine Serververbindung hört. Die Standardeinstellung ist **80**.
HTTPS-Schnittstellennummer	Das von DRAC verwendete Port, das auf eine Serververbindung hört. Die Standardeinstellung ist **443**.

Tabelle 12-9. SSH-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert SSH. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger 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 Zeitüberschreitungsfunktion zu deaktivieren. Die Standardeinstellung ist 300.
Schnittstellennummer	Das von DRAC verwendete Port, das auf eine Serververbindung hört. Die Standardeinstellung ist 22.

Tabelle 12-10. Telnet-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert Telnet. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger 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 Zeitüberschreitungsfunktion zu deaktivieren. Die Standardeinstellung ist 0.
Schnittstellennummer	Das von DRAC verwendete Port, das auf eine Serververbindung hört. Die Standardeinstellung ist 23.

Tabelle 12-11. Remote-RACADM- Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert Remote-RACADM. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Max. Sitzungen	Die maximale Anzahl gleichzeitiger 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 12-12. Einstellungen des SNMP-Agenten

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert den SNMP-Agenten. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
Community-Name	Der Name der Community, welche die IP-Adresse für das SNMP-Warnungsziel enthält. Der Community-Name kann bis zu 31 Zeichen (keine Leerzeichen) lang sein. Die Standardeinstellung ist **public**.

Tabelle 12-13. Einstellung des automatisierten System-Wiederherstellungsagenten

Einstellung	Beschreibung
Aktiviert	Aktiviert den automatisierten Systemwiederherstellungs-Agenten.

Tabelle 12-14. Schaltflächen der Seite „Dienste"

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

Zusätzliche DRAC 5-Sicherheitsoptionen aktivieren

Um einen unberechtigten Zugriff auf das Remote-System zu verhindern, enthält DRAC 5 die folgenden Funktionen:

- IP-Adressenfilter (IPRange) – Definiert einen spezifischen Bereich von IP-Adressen, die auf DRAC 5 zugreifen können.
- Blockierung von IP-Adressen – Beschränkt die Anzahl von fehlgeschlagenen Anmeldeversuchen 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 <Objektname> <Wert>
```

Verwenden Sie diese Funktionen auch in Verbindung mit den entsprechenden Sitzungszeitüberschreitungswerten und einem festgelegten Sicherheitsplan für Ihr Netzwerk.

Die folgenden Unterabschnitte enthalten zusätzliche Informationen über diese Funktionen.

IP-Filter (IpRange)

Die IP-Adressenfilterung (oder *IP-Bereichs-Überprüfung*) gestattet den DRAC 5-Zugriff nur von Clients oder Verwaltungs-Workstations, deren IP-Adressen

innerhalb eines benutzerspezifischen Bereichs liegen. Alle anderen Anmeldeversuche werden abgelehnt.

Die IP-Filterung vergleicht die IP-Adresse einer eingehenden Anmeldung mit dem IP-Adressenbereich, der in den folgenden **cfgRacTuning**-Eigenschaften angegeben ist:

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

Die Eigenschaft **cfgRacTuneIpRangeMask** wird sowohl auf die eingehende IP-Adresse als auch auf die **cfgRacTuneIpRangeAddr**-Eigenschaften angewendet. Sind die Ergebnisse von beiden Eigenschaften identisch, wird der eingehenden Anmeldeanforderung der Zugriff auf DRAC 5 gestattet. Anmeldungen von IP-Adressen außerhalb dieses Bereichs erhalten eine Fehlermeldung.

Die Anmeldung wird fortgeführt, wenn der folgende Ausdruck Null entspricht:

`cfgRacTuneIpRangeMask & (<eingehende_IP-Adresse> ^ cfgRacTuneIpRangeAddr)`

wobei & das binäre UND der Mengen und ^ das binäre ausschließliche ODER ist.

Eine vollständige Liste der **cfgRacTune**-Eigenschaften finden Sie unter Gruppen- und Objektdefinitionen der DRAC 5-Eigenschaftendatenbank.

Tabelle 12-15. Eigenschaften der IP-Adressenfilterung (IpRange)

Eigenschaft	Beschreibung
cfgRacTuneIpRangeEnable	Aktiviert die IP-Bereichsüberprüfungsfunktion.
cfgRacTuneIpRangeAddr	Bestimmt das akzeptable IP-Adressen-Bitmuster, abhängig von den Einsen (1) in der Subnetzmaske. Diese Eigenschaft wird mit binärem UND mit **cfgRacTuneIpRangeMask** verbunden, um den oberen Teil der erlaubten IP-Adresse zu bestimmen. Jeder IP-Adresse, die dieses Bitmuster in ihrem oberen Bitbereich enthält, wird erlaubt, eine DRAC 5-Sitzung herzustellen. Anmeldeversuche von IP-Adressen, die sich außerhalb dieses Bereichs befinden, schlagen fehl. Die Standardwerte in jeder Eigenschaft erlauben einem Adressenbereich von 192.168.1.0 bis 192.168.1.255 eine DRAC 5-Sitzung herzustellen.
cfgRacTuneIpRangeMask	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Subnetzmaske sollte in der Form einer Netzmaske sein, wobei die signifikanten Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu Nullen (0) in den niederwertigeren Bits.

IP-Filter aktivieren

Es folgt ein Beispielbefehl für den IP-Filter-Setup.

Unter RACADM im Remote-Zugriff verwenden finden Sie weitere Informationen zu RACADM- und RACADM-Befehlen.

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

Zur Beschränkung der Anmeldung auf eine einzelne IP-Adresse (z. B. 192.168.0.57) verwenden Sie die volle Maske, wie unten gezeigt.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

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

Zur Beschränkung von Anmeldungen auf einen kleinen Satz von vier angrenzenden IP-Adressen (z. B. 192.168.0.212 bis 192.168.0.215) wählen Sie alle außer den niederwertigsten zwei Bits in der Maske aus, wie unten gezeigt:

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

Richtlinien zu IP-Filtern

Verwenden Sie die folgenden Richtlinien, wenn Sie den IP-Filter aktivieren:

- Stellen Sie sicher, dass **cfgRacTuneIpRangeMask** in Form einer Netzmaske konfiguriert ist, wobei alle signifikanten Bits Einsen (1) sind (was das Subnetz in der Maske definiert), mit einem Übergang zu nur Nullen (0) in den niederwertigeren Bits.
- Verwenden Sie die Basisadresse des Bereichs, die Sie als Wert für **cfgRacTuneIpRangeAddr** bevorzugen. Der binäre 32 Bit-Wert dieser Adresse muss Nullen in allen niederwertigen Bits haben, wo Nullen in der Maske sind.

IP-Blockierung

IP-Blockierung stellt dynamisch fest, wenn übermäßige Anmeldungsfehlversuche von einer bestimmten IP-Adresse auftreten und blockiert (oder hindert) die

Adresse während einer zuvor festgelegten Zeitspanne an der Anmeldung an DRAC 5.

Der IP-Blockierungsparameter wendet **cfgRacTuning**-Gruppenfunktionen an, die Folgendes umfassen:

- Anzahl der zulässigen Anmeldefehlversuche
- Zeitrahmen in Sekunden, während dem die Fehlversuche auftreten müssen
- Die Zeitspanne in Sekunden, während der die „schuldige" IP-Adresse gehindert wird, eine Sitzung zu beginnen, nachdem die zulässige Anzahl von Fehlversuchen überschritten wurde

Die Anmeldefehlversuche von einer spezifischen IP-Adresse werden laufend durch einen internen Zähler festgehalten. Wenn sich der Benutzer erfolgreich anmeldet, wird die Aufzeichnung der Fehlversuche gelöscht und der interne Zähler zurückgesetzt.

ANMERKUNG: Wenn Anmeldeversuche von der Client-IP-Adresse abgelehnt werden, zeigen einige SSH-Clients u. U. die folgende Meldung an: ssh exchange identification: Verbindung vom Remote-Host geschlossen.

Eine vollständige Liste der **cfgRacTune**-Eigenschaften finden Sie unter Gruppen- und Objektdefinitionen der DRAC 5-Eigenschaftendatenbank.

Tabelle 12-16 führt die vom Benutzer definierten Parameter auf.

Tabelle 12-16. Anmeldungswiederholungs-Beschränkungseigenschaften

Eigenschaft	Definition
cfgRacTuneIpBlkEnable	Aktiviert die IP-Blockierungsfunktion. Wenn aufeinander folgende Fehlversuche (**cfgRacTuneIpBlkFailCount**) von einer spezifischen IP-Adresse innerhalb eines bestimmten Zeitraums festgestellt werden (**cfgRacTuneIpBlkFailWindow**), werden alle weiteren Versuche, von dieser Adresse eine Sitzung herzustellen, während einer bestimmten Zeitspanne zurückgewiesen (**cfgRacTuneIpBlkPenaltyTime**).
cfgRacTuneIpBlkFailCount	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche zurückgewiesen werden.
cfgRacTuneIpBlkFailWindow	Die Zeitspanne in Sekunden, während der die Fehlversuche gezählt werden. Wenn die Fehlversuche diese Grenze überschreiten, werden sie aus dem Zähler gelöscht.
crgRacTuneIpBlkPenaltyTime	Legt die Zeitspanne in Sekunden fest, während der alle Anmeldeversuche von einer IP-Adresse aufgrund übermäßiger Fehlversuche zurückgewiesen werden.

IP-Blockierung aktivieren

Das folgende Beispiel hindert eine Client-IP-Adresse fünf Minuten lang daran, eine Sitzung herzustellen, wenn dieser Client innerhalb einer Minute fünf fehlerhafte Anmeldeversuche durchgeführt hat.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

Das folgende Beispiel verhindert mehr als drei Fehlversuche innerhalb einer Minute und verhindert für eine Stunde weitere 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
```

Netzwerksicherheitseinstellungen mittels DRAC 5-GUI vornehmen

ANMERKUNG: Um die folgenden Schritte ausführen zu können, müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

1. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.
2. Klicken Sie auf die Registerkarte **Konfiguration**, und klicken Sie auf **Netzwerk**.
3. Klicken Sie auf der Seite **Netzwerkkonfiguration** auf **Erweiterte Einstellungen**.
4. Konfigurieren Sie auf der Seite **Netzwerksicherheit** die Attributwerte und klicken Sie dann auf **Änderungen anwenden**.

Tabelle 12-17 beschreibt die Einstellungen der Seite **Netzwerksicherheit**.

5. Klicken Sie auf der Seite **Netzwerksicherheit** auf die entsprechende Schaltfläche, um fortzufahren. Unter Tabelle 12-18 finden Sie eine Beschreibung der Schaltflächen der Seite **Netzwerksicherheit**.

Tabelle 12-17. Einstellungen der Seite „Netzwerksicherheit"

Einstellungen	Beschreibung
IP-Bereich aktiviert	Aktiviert die Funktion zur IP-Bereichs-Überprüfung, die einen spezifischen Bereich von IP-Adressen definiert, die auf DRAC 5 zugreifen können.
IP-Bereichs-Adresse	Bestimmt die akzeptable IP-Subnetzadresse.
IP-Bereichs-Subnetzmaske	Definiert die bedeutenden Bitstellen in der IP-Adresse. Die Subnetzmaske sollte in der Form einer Netzmaske sein, wobei die signifikanten Bits alles Einsen (1) sind, mit einem einzelnen Übergang zu Nullen (0) in den niederwertigeren Bits. Zum Beispiel: **255.255.255.0**
IP-Blockierung aktiviert	Aktiviert die IP-Adressen-Blockierungsfunktion, mit der während einer festgelegten Zeitspanne die Anzahl von Anmeldungsfehlversuchen einer spezifischen IP-Adresse eingeschränkt wird.
IP-Blockierung, Zählung von Fehlversuchen	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche von dieser Adresse zurückgewiesen werden.
IP-Blockierung, Fenster der Fehlversuche	Bestimmt die Zeitspanne in Sekunden, während der ?die gezählten IP-Blockierungsfehlversuche auftreten müssen, um die IP-Blockierungs-Penalty-Zeit auszulösen.
IP-Blockierung, Strafzeit	Die Zeitspanne in Sekunden, während der Anmeldeversuche von einer IP-Adresse aufgrund übermäßiger Fehlversuche zurückgewiesen werden.

Tabelle 12-18. Schaltflächen der Seite „Netzwerksicherheit"

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Netzwerksicherheit**.
Aktualisieren	Lädt die Seite **Netzwerksicherheit** neu.
Änderungen übernehmen	Speichert die Änderungen, die auf der Seite **Netzwerksicherheit** vorgenommen wurden.
Zurück zur Seite „Netzwerk-konfiguration"	Wechselt zur Seite **Netzwerkkonfiguration** zurück.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5 SM-CLP-Befehlszeilenoberfläche verwenden

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Dieser Abschnitt gibt Auskunft über das Serververwaltungs-Befehlszeilenprotokoll (SM-CLP) der Serververwaltungs-Workgroup (SMWG), 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**.

DRAC 5-SM-CLP ist ein von der DMTF und der SMWG betriebenes Protokoll, das den Standard für Systemverwaltungs-CLI-Umsetzungen setzt. SMWG-SM-CLP ist eine Unterkomponente der gesamten von der DMTF verfolgten SMASH-Bemühungen.

DRAC 5 SM-CLP-Support

DRAC 5 ist das erste RAC-Produkt, das für das auf dem SM-CLP-Standard basierende Befehlszeilenprotokoll Unterstützung bietet. SM-CLP wird von der DRAC 5-Controller-Firmware aus gehostet und unterstützt Telnet, SSH und seriell basierte Schnittstellen. 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 in DRAC 5 verwendet werden.

SM-CLP-Funktionen

Das SM-CLP fördert das Konzept von Verben und Zielen und stellt Systemverwaltungsfunktionen über die CLI bereit. Das Verb zeigt den auszuführenden Vorgang an, und das Ziel bestimmt die Einheit (oder das Objekt), die den Vorgang ausführt.

Es folgt ein Beispiel der SM-CLP-Befehlszeilensyntax.

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

Während einer typischen SM-CLP-Sitzung kann der Benutzer Vorgänge mittels der in Tabelle 13-1 und Tabelle 13-2 aufgeführten Verben ausführen.

Tabelle 13-1. Unterstützte CLI-Verben für System

Verb	Definition
CD	Wechselt durch den MAP mittels der Shell.
delete	Löscht eine Objektinstanz.
Hilfe	Zeigt die Hilfe für ein bestimmtes Ziel an.
reset	Setzt das Ziel zurück.
Anzeigen	Zeigt die Zieleigenschaften, Verben und Unterziele an.
start	Schaltet ein Ziel ein.
stop	Fährt ein Ziel herunter.
Beenden	Beendet die SM-CLP-Shell-Sitzung.
Version	Zeigt die Versionsattribute eines Ziels an.

Tabelle 13-2. Unterstützte CLI-Verben für Lüfter, Batterien, Eingriff, Hardwareleistung, Netzteile, Temperaturen und Spannungen

Verb	Definition
CD	Wechselt durch den MAP mittels der Shell.
Hilfe	Zeigt die Hilfe für ein bestimmtes Ziel an.
Anzeigen	Zeigt die Zieleigenschaften, Verben und Unterziele an.
Beenden	Beendet die SM-CLP-Shell-Sitzung.
Version	Zeigt die Versionsattribute eines Ziels an.

SM-CLP verwenden

1. SSH (oder Telnet) an DRAC 5 mit den richtigen Anmeldeinformationen.
2. Geben Sie in der Befehlszeile `smclp` ein.

   Die SMCLP-Eingabeaufforderung (->) wird angezeigt.

SM-CLP-Verwaltungsvorgänge und Ziele

Verwaltungsvorgänge

DRAC 5-SM-CLP ermöglicht Benutzern die Verwaltung von Folgendem:

- Serverenergieverwaltung – System einschalten, herunterfahren oder neu starten
- Verwaltung des Systemereignisprotokolls (SEL) – SEL-Datensätze anzeigen oder löschen

Optionen

Tabelle 13-3 führt die unterstützten SM-CLP-Optionen auf.

Tabelle 13-3. Unterstützte SM-CLP-Optionen

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

Ziele

Tabelle 13-4 enthält eine Liste der von SM-CLP akzeptierten Ziele, die diese Vorgänge unterstützen.

Tabelle 13-4. SM-CLP-Ziele

Ziel	Definition
/system1	Das Ziel des verwalteten Systems.
/system1/logs1	Das Protokollsammlungsziel.
/system1/logs1/log1	Das Ziel des Systemereignisprotokolls (SEL) auf dem verwalteten System.
/system1/logs1/log1/record1	Eine einzelne SEL-Datensatzinstanz auf dem verwalteten System.
/system1/pwrmgtsvc1	Der Energieverwaltungsdienst für das System.
/system1/pwrmgtsvc1/pwrmgtcap1	Funktionalität des Energieverwaltungsdiensts für das System.
/system1/fan1	Ein Lüfterziel auf dem verwalteten System.
/system1/fan1/tachsensor1	Ein individuelles Sensorziel auf dem Lüfterziel des verwalteten Systems.
/system1/batteries1	Ein Batterieziel auf dem verwalteten System.
/system1/batteries1/sensor1	Ein individuelles Sensorziel auf dem Batterieziel des verwalteten Systems.
/system1/intrusion1	Ein Gehäuseeingriffsziel auf dem verwalteten System.
/system1/intrusion1/sensor1	Ein individuelles Sensorziel auf dem Gehäuseeingriffsziel des verwalteten Systems.
/system1/hardwareperformance1	Ein Hardwareleistungsziel auf dem verwalteten System.
/system1/hardwareperformance1/sensor1	Ein individuelles Sensorziel auf dem Hardwareleistungsziel des verwalteten Systems.
/system1/powersupplies1	Ein Netzteilziel auf dem verwalteten System.
/system1/powersupplies1/sensor1	Ein individuelles Sensorziel auf dem Netzteilziel des verwalteten Systems.
/system1/temperatures1	Ein Temperaturziel auf dem verwalteten System.
/system1/temperatures1/tempsensor1	Ein individuelles Sensorziel auf dem Temperaturziel des verwalteten Systems.

/system1/voltages1	Ein Spannungsziel auf dem verwalteten System.
/system1/voltages1/voltsensor1	Ein individuelles Sensorziel auf dem Spannungsziel des verwalteten Systems.
/system1/chassis1	Ein individuelles Gehäuseziel auf dem System.

SM-CLP-Ausgabeformat

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

DRAC 5-SM-CLP, Beispiele

Die folgenden Unterabschnitte enthalten Beispiele zur Verwendung von SM-CLP zum Ausführen der folgenden Vorgänge:

- Serverenergieverwaltung
- SEL-Verwaltung
- MAP-Zielnavigation
- Eigenschaften des Anzeigesystems

Server-Energieverwaltung

Tabelle 13-5 enthält Beispiele für die Verwendung von SM-CLP zum Ausführen von Energieverwaltungsvorgängen auf einem verwalteten System.

Tabelle 13-5. Stromverwaltungsvorgänge des Servers

Operation	Syntax
Anmeldung am RAC über die Telnet/SSH-Schnittstelle	>ssh 192.168.0.120 >Anmeldung: root >Kennwort:
SM-CLP-Verwaltungs-Shell starten	- >smclp DRAC5-SM-CLP-Systemverwaltungs-Shell, Version 1.0 Copyright (c) 2004-2008 Dell, Inc. Alle Rechte vorbehalten. ->
Schalten Sie den Server aus.	- ->stop /system1 system1 wurde erfolgreich angehalten
Server aus dem ausgeschalteten Zustand hochfahren	- ->start /system1 system1 wurde erfolgreich gestartet
Server neu starten	->reset /system1 system1 wurde erfolgreich zurückgesetzt

SEL-Verwaltung

Tabelle 13-6 enthält Beispiele für die Verwendung des SM-CLP zum Ausführen von SEL-bezogenen Vorgängen auf dem verwalteten System.

Tabelle 13-6. SEL-Verwaltungsvorgänge

Operation	Syntax
SEL anzeigen	->show /system1/logs1/log1 /system1/logs1/log1 Ziele: Record1 Record2 Record3 Record4 Record5 Eigenschaften: 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 Befehle: CD Anzeigen Hilfe Beenden Version
SEL-Datensatz anzeigen	->show /system1/logs1/log1/record4 /system1/logs1/log1/record4 Eigenschaften: LogCreationClassName = CIM_RecordLog CreationClassName = CIM_LogRecord LogName = IPMI SEL RecordID = 1 MessageTimeStamp = 20050620100512,000000-000 Beschreibung = FAN 7 RPM: Lüftersensor, Fehler erkannt ElementName = IPMI SEL Record Befehle: CD Anzeigen Hilfe Beenden Version
SEL löschen	->delete /system1/logs1/log1/record* Alle Einträge wurden erfolgreich gelöscht

Batterieverwaltung

Tabelle 13-7 enthält Beispiele für die Verwendung von SM-CLP zum Ausführen von Vorgängen auf den Batterien.

Tabelle 13-7. Batterieverwaltungsvorgänge

Operation	**Syntax**
Batteriestatus anzeigen	->show system1/batteries1/sensor1 /system1/batteries1/sensor1: Eigenschaften: SystemCreationClassName = CIM_ComputerSystem SystemName = F196P1S CreationClassName = CIM_Sensor DeviceID = BATTERIE 1 SensorType = 1 PossibleStates = {"Gut" "Schlecht" "Unbekannt"} CurrentState = gut ElementName = Systemplatinen-CMOS-Batterie OtherSensorTypeDescription = CMOS-Batteriesensor. EnabledState = 1 Verben: CD Beenden Hilfe Anzeigen Version

MAP-Zielnavigation

Tabelle 13-8 enthält Beispiele für die Verwendung des Verbs **cd**, um innerhalb des MAP zu navigieren. In allen Beispielen wird angenommen, dass das ausgängliche Standardziel '/' ist.

Tabelle 13-8. Map-Zielnavigationsvorgänge

Operation	Syntax

Zum Systemziel wechseln und einen Neustart durchführen	`->cd system1`
	`->reset`
	
	ANMERKUNG: Das aktuelle Standardziel ist /.

Zum SEL-Ziel wechseln und die Protokolldatensätze anzeigen	`->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 13-9 führt die Systemeigenschaften 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-Schemadefinitionen.

Tabelle 13-9. Systemeigenschaften

Objekt	Eigenschaft	Beschreibung
CIM_Computersystem	Name	Eindeutiger Bezeichner einer Systeminstanz, die 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
	Dediziert	Aufzählung, die anzeigt, ob das System ein Spezialsystem oder ein Mehrzwecksystem ist. Werte: 0=Nicht dediziert 1=Unbekannt 2=Andere 3=Speicher 4=Router 5=Schalter 6=Layer 3-Schalter 7=CentralOffice-Schalter 8=Hub

		9=Zugriffsserver 10=Firewall 11=Print 12=E/A 13=Web-Caching 14=Verwaltung 15=Server blockieren 16=Dateiserver 17=Mobiles Benutzergerät, 18=Repeater 19=Bridge/Extender 20=Gateway 21=Speicher-Virtualizer 22=Medienbibliothek 23=Extender-Knoten 24=NAS-Kopf 25=Eigenständiges NAS 26=USV 27=IP-Telefon 28=Verwaltungs-Controller 29=Gehäuseverwalter
	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 diese Instanz 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=Unter Test 8=Verzögert 9=Quiesce 10=Start
	EnabledDefault	Zeigt die Standard-Startkonfiguration 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=Quiesce 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=Unterstützende Einheit fehlerhaft 17=Abgeschlossen 18=Strom-Modus
	Beschreibung	Eine textbasierte Beschreibung des Systems.

Eigenschaftennamen für Lüfter, Temperatur, numerische Spannung, Leistungsaufnahme und Stromsensoren

Unterstützte Eigenschaftennamen für Lüfter, Temperatur, numerische Spannung, Leistungsaufnahme und Stromsensoren

Tabelle 13-10. Sensoren

Objekt	Eigenschaft	Beschreibung
CIM_NumericSensor	SystemCreationClassName	Der Name der Systemerstellungsklasse – CIM_ComputerSystem
	SystemName	Die Service-Tag-Nummer des Systems – eine eindeutige Systemidentifikation, die in der Unternehmensumgebung vorhanden ist
	CreationClassName	Der Name der Erstellungsklasse – CIM_NumericSensor
	DeviceID	Die eindeutige ID des Sensors im System fan1...n (für Drehzahlmesser) temp 1...n (für Temp.-sensor) numerische Spannung 1...n (für numerischen Sensor (Spannung) (nur PMBus-Systeme)) Leistungsaufnahme 1...n (für Leistungsaufnahme (nur PMBus-Systeme)) amperage 1...n (für Strom (nur PMBus-Systeme))
	BaseUnits	Die Maßeinheiten des Sensors RPM=U/min (für Drehzahlmesser) C=Grad (für Temp.-sensor) V=Spannung (für numerischen Sensor) Watt=Leistung (für Leistungsaufnahme) Amp=Ampere (für Strom)
	CurrentReading	Der aktuelle Messwert des Sensors
	LowerThresholdNonCritical	Der nicht kritische untere Schwellenwert
	UpperThresholdNonCritical	Der nicht kritische obere Schwellenwert
	LowerThresholdCritical	Der kritische untere Schwellenwert
	UpperThresholdCritical	Der kritische obere Schwellenwert
	SupportedThreshold	Der unterstützte Schwellenwert des Sensors. { „LowerThresholdCritical" } (für Drehzahlmesser) { „LowerThresholdNonCritical", „UpperThresholdNonCritical", „UpperThresholdCritical", „LowerThresholdCritical" } (für Temp.-sensor) {} (für Spannungssensor (numerischer Sensor)) {„UpperThresholdNonCritical", „UpperThresholdCritical"} (für Leistungsaufnahme {} für Strom)
	SettableThreshold	Die Schwellenwerte, die für einen Sensor festgelegt werden können. { } (keine Sensorunterstützung zum Festlegen von Schwellenwerten)
	SensorTypes	Sensortyp: 5=U/min (für Drehzahlmesser) 2=Grad (für Temperatur) 3=V (für Spannung) 1=W (für Leistungsaufnahme) 1=A (für Strom)
	PossibleStates	Die möglichen Zustände des Sensors. { „unbekannt", „Warnung", „fehlerhaft", „nicht wiederherstellbar" }
	CurrentState	Der aktuelle Zustand, wie er von einem Sensor gemeldet wird
	ElementName	Der Name des Sensors
	OtherSensorTypeDescription	Wenn die Eigenschaft sensortype einen Wert von „1" (andere) aufweist, bietet diese Eigenschaft eine zusätzliche Beschreibung des entsprechenden Sensors

		„Leistungsaufnahmesensor.“ für Leistungsaufnahme „Stromsensor.“ für Strom
	EnabledState	Zeigt an, ob der Sensor aktiviert oder deaktiviert ist 1=Aktiviert

Eigenschaftennamen für Netzteilsensoren

Tabelle 13-11. Unterstützte Eigenschaftennamen für Netzteilsensoren

Objekt	Eigenschaft	Beschreibung
CIM_NumericSensor	SystemCreationClassName	Der Name der Systemerstellungsklasse CIM_ComputerSystem).
	SystemName	Die Service-Tag-Nummer des Systems – eine eindeutige Systemidentifikation, die in der Unternehmensumgebung vorhanden ist.
	CreationClassName	Der Name der Erstellungsklasse – CIM_PowerSupply.
	DeviceID	Die eindeutige ID des Sensors im System. pwrsupply 1...n
	TotalOutputPower	Die Gesamtleistungsausgabe, wie auf der DRAC-Benutzeroberfläche dargestellt.
	ElementName	Name des bestimmten Sensors.
	OperationalStatus	Aktueller Betriebsstatus der Netzteileinheit.
	HealthState	Der Funktionszustand der Netzteileinheit.
	EnabledState	Zeigt an, ob der Sensor aktiviert oder deaktiviert ist. 1=Aktiviert

Eigenschaftennamen für Eingriff, Batterie, Spannung und Hardwareleistungssensoren

Tabelle 13-12. Unterstützte Eigenschaftennamen für Eingriff, Batterie, Spannung und Hardwareleistungssensoren

Objekt	Eigenschaft	Beschreibung
CIM_NumericSensor	SystemCreationClassName	Der Name der Systemerstellungsklasse CIM_ComputerSystem).
	SystemName	Die Service-Tag-Nummer des Systems – eine eindeutige Systemidentifikation, die in der Unternehmensumgebung vorhanden ist.
	CreationClassName	Der Name der Erstellungsklasse – CIM_Sensor
	DeviceID	Eindeutige ID des Sensors im System. Intrusion1...n (für Eingriffssensor) Battery1...n (für Batteriesensor) Voltage1...n (für Spannungssensor) Hardware performance sensor1...n (für Hardwareleistungssensor)
	SensorType	1=Andere 3=V (für Spannungssensor)
	PossibleStates	Die möglichen Zustände des Sensors { „kein Eingriff“, „Gehäuseeingriff“, „Laufwerkschachteingriff“, „Eingriff in E/A-Kartenbereich“, „Eingriff in Prozessorbereich“, „LAN-Unterbrechung“, „unbefugtes Docking“, „Eingriff in Lüfter-Bereich“ } (für den Eingriffssensor) { „nicht vorhanden“, „niedrig“, „feherlhaft“, „gut“ } (für den Batteriesensor) { „gut“, „schlecht“, „unbekannt“ } (für den Spannungssensor) { „Normal“, „Andere“, „Thermischer Schutz“, „Kühlungskapazität verändert“, „Stromkapazität verändert“, „Benutzerkonfiguration“ } (für den Hardwareleistungssensor)
	CurrentState	Der aktuelle, vom Sensor gemeldete Zustand.
	ElementName	Der Name des Sensors.
	OtherSensorTypeDescription	Wenn die Eigenschaft sensortype einen Wert von „1“ (andere) aufweist, bietet diese Eigenschaft eine zusätzliche Beschreibung des entsprechenden Sensors. „Gehäuseeingriffsensor“ (für Eingriffssensor) „CMOS-Batteriesensor“ (für Batteriesensor)

		„Hardwareleistungssensor“ (für Hardwareleistung)
	EnabledState	Zeigt an, ob der Sensor aktiviert oder deaktiviert ist. 1=Aktiviert (für alle Sensoren)

Eigenschaftennamen für Lüfter- und Netzteilredundanz-eingestellte Sensoren

Tabelle 13-13. Unterstützte Eigenschaftennamen für Lüfter- und Netzteilredundanzsatz-Sensoren

Objekt	Eigenschaft	Beschreibung
CIM_RedundancySet	InstanceID	Instanznummer
	RedundancyStatus	Der Redundanzstatus
	TypeOfSet	3=Lastverteilt (für Lüfterredundanz) 4=Stand-by (für Netzteilredundanz)
	MinNumberNeeded	0=Unbekannt
	ElementName	Name des Sensors

Eigenschaftennamen für Gehäusesensoren

Tabelle 13-14. Unterstützte Eigenschaftennamen für Gehäusesensoren

Objekt	Eigenschaft	Beschreibung
CIM_Chassis	CreationClassName	Der Name der Erstellungsklasse – CIM_Chassis
	PackageType	Pakettyp 3=Chassis
	ChassisPackageType	Chassis package type 17=Hauptsystemgehäuse
	Hersteller	Hersteller „Dell“
	Modell	Der Modellname des Systems
	ElementName	Elementname

Eigenschaftennamen für Energieverwaltungsdienst

Tabelle 13-15. Unterstützte Eigenschaftennamen für Energieverwaltungsdienst

Objekt	Eigenschaft	Beschreibung
CIM_PowerManagementService	CreationClassName	Der Name der Erstellungsklasse – CIM_PowerManagementService
	Name	IPMI-Energiedienst
	ElementName	Energieverwaltungsdienst für Dell-Server
	powerstate	Aktueller Leistungszustand des Systems. 2=Ein 6=Aus Kann auf die folgenden Werte eingestellt werden: 2=Versorgung ein 6=Versorgung aus 5=Versorgungs-Reset 9=System aus- und einschalten

Unter Verwendung des Verbs Set können Sie den Energiezustand des Systems einstellen. Beispiel: Das System einschalten, wenn es ausgeschaltet ist:

```
set powerstate=2
```

Eigenschaftennamen für Energiekapazität

Tabelle 13-16. Unterstützte Eigenschaftennamen für Energiekapazität

Objekt	Eigenschaft	Beschreibung
CIM_PowerManagementCapabilities	InstanceID	Eindeutige Instanz-ID für die Stromkapazitäten
	PowerChangeCapabilities	3=Energiezustand einstellbar
	ElementName	Energieverwaltungsdienst für Dell-Server
	PowerStatesSupported	2=Versorgung ein 6=Versorgung aus 5=Versorgungs-Reset 9=System aus- und einschalten

---

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Überwachungs- und Warnungsverwaltung

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Dieser Abschnitt erklärt, wie DRAC 5 überwacht wird und erklärt außerdem die Verfahren zum Konfigurieren Ihres Systems und wie DRAC 5 Warnungen empfängt.

Das verwaltete System zur Erfassung des Bildschirms „Letzter Absturz" konfigurieren

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

1. Installieren Sie die Managed System-Software. Weitere Informationen über das Installieren der Managed System-Software finden Sie im *Server Administrator-Benutzerhandbuch*.

2. Führen Sie ein unterstütztes Microsoft Windows-Betriebssystem aus, bei dem die Windows-Funktion „Automatisch neustarten" in den **Windowseinstellungen unter Starten und Wiederherstellen** deaktiviert ist.

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

   Zum Aktivieren unter 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 die automatische Wiederherstellung und setzen Sie die Maßnahme **Automatische Wiederherstellung** auf **Reset**, **Herunterfahren** oder **Aus- und Einschaltzyklus**. Zum Konfigurieren des Zeitgebers für **Automatische Wiederherstellung** müssen Sie Server Administrator oder IT Assistant verwenden.

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

   Der Bildschirm Letzter Absturz ist nicht verfügbar, wenn die Maßnahme **Autom. Wiederherstellung** auf **Herunterfahren** oder **Aus- und Einschalten** eingestellt ist, während das verwaltete System ausgeschaltet ist.

Die Windows-Option „Automatischer Neustart" deaktivieren

Um sicherzustellen, dass die Funktion der Internet-basierten DRAC 5-Schnittstelle des Bildschirms Letzter Absturz korrekt funktioniert, deaktivieren Sie die Option **Automatischer Neustart** auf verwalteten Systemen, die die Betriebssysteme Microsoft Windows Server 2003 und Windows 2000 Server 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 die Registerkarte **Erweitert**.

3. Klicken Sie unter **Autostart und Wiederherstellung** auf **Einstellungen**.

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

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

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 die Registerkarte **Erweitert**.

3. Klicken Sie auf die Schaltfläche **Autostart und Wiederherstellung...**

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

Plattformereignisse konfigurieren

Die Konfiguration von Plattformereignissen bietet eine Möglichkeit, das Remote-Zugriffsgerät so zu konfigurieren, dass ausgewählte Maßnahmen beim Auftreten bestimmter Ereignismeldungen ausgeführt werden. Diese Maßnahmen umfassen Neustart, Aus-/Einschalten, Herunterfahren, Versorgungsleistungsherabsetzung und das Auslösen einer Warnung (Plattformereignis-Trap [PET] und/oder E-Mail).

Die filterbaren Plattformereignisse umfassen:

- 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
- Systemstromsondenwarnung
- Systemstromsondenfehler

Wenn ein Plattformereignis auftritt (z. B. ein Lüftersondenfehler), wird ein Systemereignis erstellt und im Systemereignisprotokoll (SEL) verzeichnet. Wenn dieses Ereignis einem Plattformereignisfilter (PEF) in der Liste der Plattformereignisfilter der webbasierten Schnittstelle entspricht und Sie diesen Filter auf die Erstellung einer Warnung (PET oder E-Mail) konfiguriert haben, dann wird eine PET- oder E-Mail-Warnung an ein konfiguriertes Ziel bzw. an mehrere konfigurierte Ziele gesendet.

Wenn derselbe Plattformereignisfilter auch zur Ausführung einer Maßnahme (wie eines Systemneustarts) konfiguriert ist, wird die Maßnahme ausgeführt.

Plattformereignisfilter (PEF) konfigurieren

Konfigurieren Sie Ihre Plattformereignisfilter, bevor Sie die Einstellungen für Plattformereignis-Traps oder E-Mail-Warnungen konfigurieren.

PEF mittels der Internet-Benutzeroberfläche konfigurieren

1. Melden Sie sich über einen unterstützten Webbrowser am Remote- System an. Siehe Auf die Internet-basierte Schnittstelle zugreifen.
2. Klicken Sie auf das Register **Warnungsverwaltung** und dann auf **Plattformereignisse**.
3. Globale Warnungen aktivieren.
   a. Klicken Sie auf **Warnungsverwaltung**, und wählen Sie **Plattformereignisse** aus.
   b. Wählen Sie das Kontrollkästchen **Plattformereignis-Filterwarnung aktivieren** aus.
4. Wählen Sie unter **Plattformereignis-Filterkonfiguration** das Kontrollkästchen **Plattformereignis-Filterwarnungen aktivieren** aus, und klicken Sie dann auf **Änderungen übernehmen**.
5. Klicken Sie unter **Plattformereignisfilterliste** auf den Filter, den Sie konfigurieren möchten.
6. Nehmen Sie auf der Seite **Plattformereignisse festlegen** die entsprechenden Auswahlen vor, und klicken Sie dann auf **Änderungen übernehmen**.

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

PEF mittels RACADM-CLI konfigurieren

1. Aktivieren Sie PEF.

   Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
   ```

   wobei 1 und 1 für den PEF-Index bzw. für die Auswahloption „aktivieren/deaktivieren" stehen.

   PEF-Index kann ein Wert von 1 bis 17 sein. Die Auswahloption „aktivieren/deaktivieren" kann auf 1 (aktiviert) oder 0 (deaktiviert) eingestellt werden.

   Beispiel: Um PEF mit dem Index 5 zu aktivieren, geben Sie den folgenden Befehl ein:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
   ```

2. Konfigurieren Sie die PEF-Maßnahmen.

   Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

   ```
   racadm config -g cfgIpmiPef -i <index> -o cfgIpmiPefAction <Maßnahme>
   ```

   wobei die *<Maßnahme>*-Wertbits wie folgt lauten:

   - *<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
   - *<Maßnahme>* Wertbit 4 – 1 = Versorgungsleistungsverminderung; 0 = keine Versorgungsleistungsverminderung

   Beispiel: Um PEF zum Systemneustart zu aktivieren, geben Sie den folgenden Befehl ein:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 2
   ```

   wobei 1 der PEF-Index ist und 2 die PEF-Maßnahme für den Neustart.

PET konfigurieren

PET mittels der Internet-Benutzeroberfläche konfigurieren

1. Melden Sie sich über einen unterstützten Internet-Browser am Remote- System an. Siehe Auf die Internet-basierte Schnittstelle zugreifen.
2. Vergewissern Sie sich, dass Sie die unter PEF mittels der Internet- Benutzeroberfläche konfigurieren beschriebenen Verfahren ausgeführt haben.
3. Konfigurieren Sie die PET-Regel.
   a. Klicken Sie im Register **Warnungsverwaltung** auf **Traps-Einstellungen**.
   b. Konfigurieren Sie unter **Ziel-Konfigurationseinstellungen** das Feld **Community-Zeichenkette** mit den entsprechenden Informationen, und klicken Sie dann auf **Änderungen übernehmen**.
4. Konfigurieren Sie Ihre PET-Ziel-IP-Adresse
   a. Klicken Sie in der Spalte **Zielnummer** auf eine Zielnummer.
   b. Stellen Sie sicher, dass das Kontrollkästchen **Ziel aktivieren** ausgewählt ist.
   c. Geben Sie in das **Ziel-IP-Adressfeld** eine gültige PET-Ziel-IP-Adresse ein.
   d. Klicken Sie auf **Änderungen übernehmen**.
   e. Klicken Sie auf **Test-Trap senden**, um die konfigurierte Warnung (falls gewünscht) zu testen.

   ANMERKUNG: Ihr Benutzerkonto muss über die Berechtigung **Testwarnungen** verfügen, um dieses Verfahren ausführen zu können. Siehe Tabelle 5-4.

   f. Wiederholen Sie die Schritte a bis 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 die Eingabetaste:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

2. Aktivieren Sie PET.

   Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, und drücken Sie nach jedem Befehl auf die Eingabetaste:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
   ```

   wobei 1 und 1 für den PET-Zielindex bzw. für die Auswahloption „aktivieren/deaktivieren" stehen.

   Der PET-Zielindex kann ein Wert von 1 bis 4 sein. Die Auswahloption „aktivieren/deaktivieren" kann auf 1 (aktiviert) oder 0 (deaktiviert) eingestellt werden.

   Beispiel: Um PET mit dem Index 4 zu aktivieren, geben Sie den folgenden Befehl ein:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 0
   ```

3. Konfigurieren Sie die PET-Regel.

   Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

   ```
   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, die die Plattformereigniswarnungen empfängt.

4. Konfigurieren Sie die Community-Namen-Zeichenkette.

   Geben Sie Folgendes in die Befehlszeile ein:

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

E-Mail-Warnungen konfigurieren

E-Mail-Warnungen mittels der Internet-Benutzeroberfläche konfigurieren

1. Melden Sie sich über einen unterstützten Internet-Browser am Remote- System an. Siehe Auf die Internet-basierte Schnittstelle zugreifen.

2. Vergewissern Sie sich, dass Sie die unter PEF mittels der Internet- Benutzeroberfläche konfigurieren beschriebenen Verfahren ausgeführt haben.

3. Konfigurieren Sie die E-Mail-Warnungseinstellungen.

   a. Klicken Sie im Register **Warnungsverwaltung** auf **E-Mail- Warnungseinstellungen**.

   b. Unter **SMTP- (E-Mail-) Serveradresseinstellungen** konfigurieren Sie das Feld **SMTP- (E-Mail-) Server-IP-Adresse** mit den entsprechenden Informationen, und klicken Sie dann auf **Änderungen übernehmen**.

4. Konfigurieren Sie das E-Mail-Warnungsziel.

   a. Klicken Sie in der Spalte **E-Mail-Warnungsnummer** auf eine E-Mail- Warnungsnummer.

   b. Stellen Sie sicher, dass das Kontrollkästchen **E-Mail-Warnung aktivieren** ausgewählt ist.

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

   d. Geben Sie in das Feld **E-Mail-Beschreibung** eine Beschreibung ein (falls erforderlich).

   e. Klicken Sie auf **Änderungen übernehmen**.

   f. Klicken Sie auf **Test-E-Mail senden**, um die konfigurierte E-Mail- Warnung (falls gewünscht) zu testen.

   ANMERKUNG: Ihr Benutzerkonto muss über die Berechtigung **Testwarnungen** verfügen, um dieses Verfahren ausführen zu können. Siehe Tabelle 5-4.

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

5. Globale Warnungen aktivieren.

   a. Klicken Sie auf **Warnungsverwaltung**, und wählen Sie **Plattformereignisse** aus.

   b. Wählen Sie das Kontrollkästchen **Plattformereignis-Filterwarnung aktivieren** aus.

E-Mail-Warnungen mittels RACADM-CLI konfigurieren

1. Aktivieren Sie die globalen Warnungen.

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

2. Aktivieren Sie E-Mail-Warnungen.

   Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, und drücken Sie nach jedem Befehl auf die Eingabetaste:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
   ```

   wobei 1 und 1 für den E-Mail-Zielindex bzw. für die Auswahloption „aktivieren/deaktivieren" stehen.

   Der E-Mail-Zielindex kann ein Wert von 1 bis 4 sein. Die Auswahloption „aktivieren/deaktivieren" kann auf 1 (aktiviert) oder 0 (deaktiviert) eingestellt werden.

   Beispiel: Um E-Mail mit dem Index 4 zu aktivieren, geben Sie den folgenden Befehl ein:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. Konfigurieren Sie Ihre E-Mail-Einstellungen.

   Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <E-Mail-Adresse>
   ```

   wobei 1 der E-Mail-Zielindex ist und *<E-Mail-Adresse>* die Ziel-E-Mail-Adresse, die die Plattformereigniswarnungen empfängt.

   Um eine kundenspezifische Meldung zu konfigurieren, geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie <Eingabe>:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <Kundenspezifische_Meldung>
   ```

   wobei 1 der E-Mail-Zielindex ist und *<Kundenspezifische_Meldung>* die kundenspezifische Meldung.

E-Mail-Warnungen testen

Mit der RAC-E-Mail-Warnungsfunktion können Benutzer E-Mail-Warnungen erhalten, wenn auf dem verwalteten System ein kritisches Ereignis auftritt. Das folgende Beispiel zeigt, wie man die E-Mail-Warnungsfunktion testet, um sicherzustellen, dass der RAC ordnungsgemäß E-Mail-Warnungen über das Netzwerk versenden kann.

```
racadm testemail -i 2
```

ANMERKUNG: Stellen Sie sicher, dass die **SMTP**- und **E-Mail-Warnung**s-Einstellungen konfiguriert sind, bevor die E-Mail-Warnungsfunktion getestet wird. Weitere Informationen finden Sie unter E-Mail-Warnungen konfigurieren.

RAC-SNMP-Trap-Warnungsfunktion testen

Die RAC-SNMP-Trap-Warnungsfunktion ermöglicht SNMP-Trap-Listener-Konfigurationen, Traps für Systemereignisse zu empfangen, die auf dem verwalteten System auftreten.

Das folgende Beispiel veranschaulicht, wie ein Benutzer die SNMP-Trap-Warnungsfunktion des RAC testen kann.

```
racadm testtrap -i 2
```

Stellen Sie vor dem Testen der RAC-SNMP-Trap-Warnungsfunktion sicher, dass die SNMP- und Trap-Einstellungen ordnungsgemäß konfiguriert sind. Anleitungen zum Konfigurieren dieser Einstellungen finden Sie in den Unterbefehlsbeschreibungen testtrap>und testemail.

Häufig gestellte Fragen

Warum wird die folgende Meldung angezeigt?

`Remote-Zugriff: SNMP-Authentifizierungsfehler`

Als Teil der Ermittlung versucht IT Assistant, die Get- und Set-Community-Namen des Geräts zu überprüfen. In IT Assistant gibt es den Get-**Community-Name = public** und den Set-**Community-Name = private**. Standardmäßig lautet der Community-Name des DRAC 5-Agenten public. Wenn IT Assistant eine Set-Aufforderung aussendet, erstellt der DRAC 5-Agent den SNMP-Authentifizierungsfehler, da 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-Namen festzulegen, verwenden Sie den folgenden Befehl:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <Community-Name>
```

Um zu verhindern, dass SNMP-Authentifizierungs-Traps erstellt werden, müssen Sie Community-Namen eingeben, die vom Agenten akzeptiert werden. Da DRAC 5 nur einen einzigen Community-Namen zulässt, müssen Sie den gleichen **Get**- und **Set**-Community-Namen für das IT Assistant-Ermittlungs-Setup eingeben.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Intelligent Platform Management Interface (IPMI) konfigurieren

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

---

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

DRAC 5 ist vollständig IPMI 2.0-konform. Die DRAC-IPMI kann mit folgenden Hilfsmitteln konfiguriert werden:

- Browser
- Open Source-Dienstprogramm, wie z. B. *ipmitool*
- Dell OpenManage-IPMI-Shell, **ipmish**
- RACADM

Weitere Informationen über die Anwendung der IPMI-Shell, ipmish, befinden sich im *Dell OpenManage BMC-Benutzerhandbuch* auf der Dell Support-Website unter **support.dell.com / manuals**.

Weitere Informationen über die Verwendung von RACADM finden Sie unter RACADM im Remote-Zugriff verwenden.

IPMI mittels der webbasierten Schnittstelle konfigurieren

1. Melden Sie sich über einen unterstützten Internet-Browser am Remote- System an. Siehe Auf die Internet-basierte Schnittstelle zugreifen.

2. Konfigurieren Sie IPMI-über-LAN.
   a. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.
   b. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Netzwerk**.
   c. Wählen Sie auf der Seite **Netzwerkkonfiguration** unter **IPMI-LAN- Einstellungen** die Option **IPMI über LAN aktivieren** aus, und klicken Sie auf **Änderungen übernehmen**.
   d. Aktualisieren Sie die IPMI-LAN-Kanalberechtigungen, falls erforderlich.

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

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

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

   ANMERKUNG: DRAC 5-IPMI unterstützt das RMCP+-Protokoll.

   Geben Sie unter **IPMI-LAN-Einstellungen** den Verschlüsselungsschlüssel in das Feld **Verschlüsselungsschlüssel** ein, und klicken Sie auf **Änderungen anwenden**.

   ANMERKUNG: Der Verschlüsselungsschlüssel muss aus einer geraden Anzahl von maximal 40 Hexadezimalzeichen bestehen.

3. IPMI Seriell über LAN (SOL) konfigurieren.
   a. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.
   b. Klicken Sie auf der Registerkarte **Konfiguration** auf **Seriell über LAN**.
   c. Auf der Seite **Seriell über LAN-Konfiguration** wählen Sie **Seriell über LAN aktivieren**.
   d. Aktualisieren Sie die IPMI-SOL-Baudrate.

   ANMERKUNG: Um die serielle Konsole über LAN umzuleiten, stellen Sie sicher, dass die SOL-Baudrate mit der Baudrate des verwalteten Systems übereinstimmt.

   e. Klicken Sie auf das Dropdown-Menü **Baudrate**, wählen die die entsprechende Baudrate aus, und klicken Sie auf **Änderungen übernehmen**.

f. Aktualisieren Sie die **erforderliche Mindestberechtigung**. Diese Eigenschaft definiert die Mindestbenutzerberechtigung, die zur Verwendung der Funktion **Seriell über LAN** erforderlich ist.

Klicken Sie auf das Dropdown-Menü **Beschränkung der Kanalberechtigungsebene**, und wählen Sie **Benutzer**, **Operator** oder **Administrator** aus.

g. Klicken Sie auf **Änderungen übernehmen**.

4. Konfigurieren Sie IPMI-Seriell.

a. Klicken Sie auf der Registerkarte **Konfiguration** auf **Seriell**.

b. Im Menü **Serielle Konfiguration** ändern Sie den IPMI-Seriell- Verbindungsmodus auf die entsprechende Einstellung.

Unter **IPMI-Seriell** klicken Sie auf das Dropdown-Menü **Verbindungsmoduseinstellung**, und wählen Sie den entsprechenden Modus aus.

c. Stellen Sie die IPMI-Seriell-Baudrate ein.

Klicken Sie auf das Dropdown-Menü **Baudrate**, wählen Sie die entsprechende Baudrate aus, und klicken Sie auf **Änderungen übernehmen**.

d. Stellen Sie die Beschränkung der Kanalberechtigungsebene ein.

Klicken Sie auf das Dropdown-Menü **Beschränkung der Kanalberechtigungsebene**, und wählen Sie **Administrator**, **Operator** oder **Benutzer** aus.

e. Klicken Sie auf **Änderungen übernehmen**.

f. Stellen Sie sicher, dass der serielle MUX im BIOS-Setup-Programm des verwalteten Systems korrekt eingestellt ist.

- Starten Sie das System neu.
- Drücken Sie während des POST <F2>, um das BIOS-Setup-Programm zu öffnen.
- Wechseln Sie zu **Serielle Kommunikation**.
- Stellen Sie im Menü **Serial Connection** (Serielle Verbindung) sicher, dass **External Serial Connector** (Externe serielle Schnittstelle) auf **Remote Access Device** (Remote-Zugriffsgerät) gesetzt ist.
- Speichern und beenden Sie das BIOS-Setup-Programm.
- Starten Sie das System neu.

Wenn sich IPMI-Seriell im Terminalmodus befindet, können Sie die folgenden zusätzlichen Einstellungen konfigurieren:

- Löschsteuerung
- Echosteuerung
- Zeilenbearbeitung
- Neue Zeilenfolgen
- Neue Zeilenfolgen eingeben

Weitere Informationen über diese Eigenschaften finden Sie in der IPMI 2.0-Spezifikation.

IPMI mittels RACADM-CLI konfigurieren

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

2. Konfigurieren Sie IPMI-über-LAN.

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

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

a. Aktualisieren Sie die IPMI-Kanalberechtigungen.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <Stufe>
```

wobei <*Stufe*> eine der folgenden Optionen ist:

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

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

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

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

ANMERKUNG: DRAC 5-IPMI unterstützt das RMCP+-Protokoll. Die IPMI 2.0-Spezifikationen enthalten weitere Informationen.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <Schlüssel>
```

wobei *<Schlüssel>* ein aus 20 Zeichen bestehender Verschlüsselungsschlüssel in einem gültigen Hexadezimal-Format darstellt.

3. IPMI Seriell über LAN (SOL) konfigurieren.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a. Aktualisieren Sie die IPMI-SOL-Mindestberechtigungsebene.

VORSICHTSHINWEIS: Die IPMI-SOL-Mindestberechtigungsstufe bestimmt die Mindestberechtigung, die zum Aktivieren von IPMI SOL erforderlich ist. Weitere Informationen enthält die IPMI 2.0-Spezifikation.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <Stufe>
```

wobei *<Stufe>* eine der folgenden Optionen ist:

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

Beispiel: Um die IPMI-Berechtigungen auf 2 (Benutzer) zu konfigurieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

b. Aktualisieren Sie die IPMI-SOL-Baudrate.

ANMERKUNG: Um die serielle Konsole über LAN umzuleiten, stellen Sie sicher, dass die SOL-Baudrate mit der Baudrate des verwalteten Systems übereinstimmt.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <Baudrate>
```

wobei *<Baudrate>* 9600, 19200, 57600 oder 115200 Bits pro Sekunde ist.

Beispiel:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. Aktivieren Sie SOL.

ANMERKUNG: SOL kann für jeden einzelnen Benutzer aktiviert oder deaktiviert werden.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <ID> 2
```

wobei *<ID>* die eindeutige Benutzer-ID ist.

4. Konfigurieren Sie IPMI-Seriell.

a. Ändern Sie den Modus der seriellen IPMI-Verbindung auf die entsprechende Einstellung.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

b. Stellen Sie die IPMI-Seriell-Baudrate ein.

Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <Baudrate>
```

wobei *<Baudrate>* 9600, 19200, 57600 oder 115200 Bits pro Sekunde ist.

Beispiel:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600
```

c. Aktivieren Sie die Hardware-Datenflusssteuerung auf der seriellen IPMI.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1
```

d. Stellen Sie die Mindestberechtigungsebene auf dem seriellen IPMI- Kanal ein.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <Ebene>
```

wobei <*Stufe*> eine der folgenden Optionen ist:

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

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

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

e. Stellen Sie sicher, dass der serielle MUX im BIOS-Setup-Programm ordnungsgemäß eingestellt ist.

- Starten Sie das System neu.
- Drücken Sie während des POST <F2>, um das BIOS-Setup-Programm zu öffnen.
- Wechseln Sie zu **Serielle Kommunikation**.
- Stellen Sie im Menü **Serial Connection** (Serielle Verbindung) sicher, dass **External Serial Connector** (Externe serielle Schnittstelle) auf **Remote Access Device** (Remote-Zugriffsgerät) gesetzt ist.
- Speichern und beenden Sie das BIOS-Setup-Programm.
- Starten Sie das System neu.

Die IPMI- Konfiguration ist abgeschlossen.

Wenn sich die serielle IPMI im Terminalmodus befindet, können Sie die folgenden zusätzlichen Einstellungen mittels der Befehle **racadm config cfgIpmiSerial** konfigurieren:

- Löschsteuerung
- Echosteuerung
- Zeilenbearbeitung
- Neue Zeilenfolgen
- Neue Zeilenfolgen eingeben

Weitere Informationen über diese Eigenschaften finden Sie in der IPMI 2.0-Spezifikation.

Serielle IPMI-Remote-Zugriffsschnittstelle verwenden

In der seriellen IPMI-Schnittstelle sind die folgenden Modi verfügbar:

- **IPMI-Terminalmodus** - Unterstützt ASCII-Befehle, die von einem seriellen Terminal gesendet werden. Der Befehlssatz ist auf eine bestimmte Anzahl von Befehlen (einschließlich der Stromsteuerung) begrenzt und unterstützt Raw-IPMI-Befehle, die als hexadezimale ASCII-Zeichen eingegeben werden.
- **Grundlegender IPMI-Modus** - Unterstützt eine binäre Schnittstelle für den Programmzugriff, wie die IPMI-Shell (IPMISH), die zusammen mit dem Baseboard-Verwaltungsdienstprogramm (BMU) enthalten ist.

So konfigurieren Sie den IPMI-Modus mittels RACADM:

1. Deaktivieren Sie die serielle RAC-Schnittstelle.

   Geben Sie Folgendes in die Befehlszeile ein:

   ```
   racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
   ```

2. Aktivieren Sie den entsprechenden IPMI-Modus.

   Beispiel: Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 oder 1>
   ```

Weitere Informationen erhalten Sie unter Gruppen- und Objektdefinitionen der DRAC 5-Eigenschaftendatenbank.

Seriell über LAN konfigurieren

ANMERKUNG: Vollständige Informationen zu Seriell über LAN finden Sie im *Benutzerhandbuch zum Dell OpenManage-Baseboard-Verwaltungs-Controller*.

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 15-1 enthält Informationen über die Einstellungen der Seite **Seriell über LAN-Konfiguration**.
4. Klicken Sie auf **Änderungen übernehmen**.
5. Konfigurieren Sie die erweiterten Einstellungen, falls erforderlich. Klicken Sie andernfalls auf die entsprechende Schaltfläche der Seite **Seriell über LAN-Konfiguration**, um fortzufahren (sehen Sie Tabelle 15-2).

   So konfigurieren Sie die erweiterten Einstellungen:

   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 15-3.

   c. Klicken Sie auf **Änderungen übernehmen**.

   d. Klicken Sie auf der Seite **Seriell über LAN-Konfiguration – Erweiterte Einstellungen** auf die entsprechende Schaltfläche, um fortzufahren. Sehen Sie Tabelle 15-4 oder die Beschreibung der Schaltflächen auf der Seite **Seriell über LAN-Konfiguration – Erweiterte Einstellungen**.

Tabelle 15-1. Einstellungen der Seite Seriell über LAN-Konfiguration

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 Kanalberechtigungsebene	Stellt die Mindestbenutzerberechtigung für IPMI-Seriell über LAN ein: **Administrator**, **Operator** oder **Benutzer**.

Tabelle 15-2. Schaltflächen der Seite Seriell über LAN-Konfiguration

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Seriell über LAN – Konfiguration** aus.
Aktualisieren	Aktualisiert die Seite **Seriell über LAN – Konfiguration**.
Erweiterte Einstellungen	Öffnet die Seite **Seriell über LAN-Konfiguration – Erweiterte Einstellungen**.
Änderungen übernehmen	Wendet die Einstellungen der Seite **Seriell über LAN – Konfiguration** an.

Tabelle 15-3. Einstellungen der Seite Seriell über LAN-Konfiguration – Erweiterte Einstellungen

Einstellung	Beschreibung
Intervall der Zeichenakkumulation	Die Zeitspanne, die BMC vor dem Übertragen eines teilweisen SOL-Zeichen-Datenpakets wartet. 1-basierte 5-ms-Schritte.
Schwellenwert der gesendeten Zeichen	BMC sendet ein SOL-Zeichen-Datenpaket mit den Zeichen, sobald diese Anzahl der Zeichen (oder eine höhere Anzahl) akzeptiert worden ist. 1-basierte Einheiten.

Tabelle 15-4. Schaltflächen der Seite Seriell über LAN-Konfiguration – Erweiterte Einstellungen

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Seriell über LAN-Konfiguration – Erweiterte Einstellungen** aus.

Aktualisieren	Aktualisiert die Seite **Seriell über LAN-Konfiguration – Erweiterte Einstellungen**.
Zurück zur Seite Seriell über LAN–Konfiguration	Kehrt zur Seite **Seriell über LAN – Konfiguration** zurück.
Änderungen übernehmen	Wendet die Einstellungen der Seite **Seriell über LAN-Konfiguration – Erweiterte Einstellungen** an.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Wiederherstellung und Fehlerbehebung beim verwalteten System

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

In diesem Abschnitt wird erklärt, wie Tasks mithilfe der Internet-basierten Schnittstelle von DRAC 5 ausgeführt werden, die mit der Wiederherstellung und Fehlerbehebung eines abgestürzten Remote-Systems in Verbindung stehen.

Erste Schritte bei der Fehlerbehebung eines Remote-Systems

Die folgenden Fragen werden häufig für die Fehlerbehebung bei Problemen auf hoher Ebene auf dem verwalteten System gestellt:

1. Ist das System ein- oder ausgeschaltet?
2. Wenn eingeschaltet, funktioniert das Betriebssystem, ist es abgestürzt oder nur blockiert?
3. Wenn ausgeschaltet, wurde der Strom unerwartet ausgeschaltet?

Überprüfen Sie bei abgestürzten Systemen den Bildschirm des letzten Absturzes (sehen Sie Bildschirm des letzten Systemabsturzes anzeigen), und verwenden Sie die Konsolenumleitung (sehen Sie Unterstützte Bildschirmauflösungs-Bildwiederholfrequenzen auf dem verwalteten System) und die Remote-Energieverwaltung (sehen Sie Versorgungsspannung auf einem Remote-System verwalten), um das System neu zu starten und das Neustartverfahren zu beobachten.

Versorgungsspannung auf einem Remote- System verwalten

DRAC 5 ermöglicht Ihnen, im Remote-Zugriff mehrere Versorgungsspannungsmaßnahmen auf dem verwalteten System auszuführen, damit Sie das System nach einem Systemausfall oder einem anderen Systemereignis wiederherstellen können.

Die Seite **Stromverwaltung** bietet Anleitungen für Folgendes:

- Durchführen eines ordentlichen Herunterfahrens durch das Betriebssystem beim Neustart und Ein- oder Ausschalten des Systems.
- Aktuellen **Versorgungsspannungsstatus** des Systems anzeigen – entweder **EIN** oder **AUS**.

Zum Zugriff auf die Seite **Stromverwaltung** von der **System** struktur aus klicken Sie auf **System** und dann auf das Register **Stromverwaltung**.

ANMERKUNG: Sie müssen über die Berechtigung **Server-Maßnahmenbefehle ausführen** verfügen, um Energieverwaltungsmaßnahmen ausführen zu können.

Spannungssteuerungsmaßnahmen über die DRAC 5-GUI auswählen

1. Wählen Sie eine der folgenden **Spannungssteuerungsmaßnahmen** aus.
   - **System einschalten** – Schaltet die Versorgung des Systems ein (entspricht dem Drücken des Netzschalters, wenn die Systemversorgung ausgeschaltet ist).
   - **System ausschalten** – Schaltet die Versorgung des Systems aus (entspricht dem Drücken des Betriebsschalters bei eingeschaltetem Systemversorgung).
   - **System zurücksetzen** – Führt einen Reset des Systems aus (entspricht dem Drücken der Reset-Taste). Die Versorgung 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 Versorgungsspannungs- Verwaltungsmaßnahme (z. B. das System zum Ein- und Ausschalten zu veranlassen) auszuführen.
3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Stromverwaltung**, um fortzufahren (siehe Tabelle 16-1).

Tabelle 16-1. Schaltflächen der Seite Stromverwaltung (oben rechts)

Schaltfläche	Maßnahme
Drucken	Druckt die Seite **Stromverwaltung**
Aktualisieren	Lädt die Seite **Stromverwaltung** neu

Spannungssteuerungsmaßnahmen über die DRAC 5-CLI auswählen

Verwenden Sie den Befehl `racadm serveraction`, um Stromverwaltungsvorgänge auf dem Hostsystem auszuführen.

`racadm serveraction <Maßnahme>`

Die Optionen für die Zeichenkette <*Maßnahme*> lauten:

- **powerdown** - Fährt das verwaltete System herunter.
- **powerup** - Fährt das verwaltete System hoch.
- **powercycle** - Löst einen Ein-/Ausschaltvorgang auf dem verwalteten System aus. Diese Maßnahme ist dem Drücken des Netzschalters an der Systemvorderseite ähnlich, um das System aus- und dann wieder einzuschalten.
- **powerstatus** - Zeigt den aktuellen Stromstatus des Servers an („EIN" oder „AUS").
- **hardreset** - Führt einen Reset (Neustart) auf dem verwalteten System durch.

Systeminformationen anzeigen

Die Seite **Systemzusammenfassung** enthält Informationen über die folgenden Systemkomponenten:

- Hauptsystemgehäuse
- Remote-Access-Controller
- Baseboard-Verwaltungs-Controller

Erweitern Sie, um auf die Systeminformationen zuzugreifen, die **System** struktur und klicken Sie auf **Eigenschaften**.

Hauptsystemgehäuse

Tabelle 16-2 und Tabelle 16-3 beschreiben die Eigenschaften des Hauptsystemgehäuses.

ANMERKUNG: Damit Sie Informationen zu **Hostname** und **BS-Name** erhalten können, müssen auf dem verwalteten System DRAC 5-Dienste installiert sein.

Tabelle 16-2. Systeminformationsfelder

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

Tabelle 16-3. Felder zur autom. Wiederherstellung

Feld	Beschreibung
Wiederherstellungs-maßnahme	Wird ein „hängendes System" festgestellt, kann DRAC so konfiguriert werden, dass eine der folgenden Maßnahmen ausgeführt wird: Keine Maßnahme, Hardware-Reset, Herunterfahren oder Aus- und Einschalten.
Anfänglicher Countdown	Die Anzahl der Sekunden nach der Feststellung eines „hängenden Systems", bis der DRAC eine Wiederherstellungsmaßnahme ausführt.
Vorhandener Countdown	Der aktuelle Wert des Countdown-Zeitgebers in Sekunden.

Tabelle 16-4. Embedded NIC-MAC-Adresse

Feld	Beschreibung
NIC1 Ethernet	Die NIC 1-Ethernet-Adresse.
NIC2 Ethernet	Die NIC 2-Ethernet-Adresse.

Remote-Access-Controller

Tabelle 16-5 beschreibt die Eigenschaften des Remote-Access-Controllers.

Tabelle 16-5. RAC-Informationsfelder

Feld	Beschreibung
Name	Kurzname.
Produktinformationen	Ausführlicher Name.
Hardwareversion	Version der Remote-Access-Controller-Karte oder „unbekannt".
Firmware-Version	Aktuelle DRAC 5-Firmware-Versionsstufe.
Aktualisierte Firmware	Datum und Uhrzeit, zu dem bzw. zu der die Firmware zuletzt aktualisiert wurde.
RAC-Uhrzeit	Systemzeit-Einstellung.

Baseboard-Verwaltungs-Controller

Tabelle 16-6 beschreibt die Eigenschaften des Baseboard-Verwaltungs-Controllers.

Tabelle 16-6. BMC-Informationsfelder

Feld	Beschreibung
Name	„Baseboard-Verwaltungs-Controller".
IPMI-Version	Version der Intelligente Plattform-Verwaltungsschnittstelle (IPMI).
Anzahl von möglichen aktiven Sitzungen	Maximale Anzahl von Sitzungen, die gleichzeitig aktiv sein können.
Anzahl von aktuellen aktiven Sitzungen	Gesamtanzahl aktueller aktiver 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.

So zeigen Sie das Systemereignisprotokoll an:

1. Klicken Sie in der **System** struktur auf **System**.
2. Klicken Sie auf das Register **Protokolle** und dann auf **Systemereignisprotokoll**.

   Auf der Seite **Systemereignisprotokoll** werden der Ereignis-Schweregrad sowie weitere Informationen angezeigt; siehe Tabelle 16-7.
3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Systemereignisprotokoll**, um fortzufahren (siehe Tabelle 16-8).

Tabelle 16-7. Statusanzeigesymbole

Symbol/Kategorie	Beschreibung

	Eine grüne Markierung zeigt eine unproblematische (normale) Statusbedingung an.
	Ein gelbes Dreieck, das ein Ausrufezeichen enthält, zeigt eine (nichtkritische) Warnungs-Statusbedingung an.
	Ein rotes X zeigt eine kritische (Ausfall) Statusbedingung an.
	Ein Fragezeichen-Symbol zeigt an, dass der Status unbekannt ist.
Uhrzeit / Datum	Datum und Uhrzeit des Ereigniseintritts. Wenn das Datumsfeld leer ist, trat das Ereignis während des Systemstarts auf. Das Format lautet TT/MM/JJJJ hh:mm:ss, basierend auf dem 24-Stunden-Zeitsystem.
Beschreibung	Eine kurze Beschreibung des Ereignisses.

Tabelle 16-8. Schaltflächen der SEL-Seite

Schaltfläche	Maßnahme
Drucken	Druckt das **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 es ermöglicht, das **SEL** in einem Verzeichnis Ihrer Wahl zu speichern. **ANMERKUNG:** Wenn Sie Internet Explorer verwenden und beim Speichern auf ein Problem stoßen, laden Sie die kumulative Sicherheitsaktualisierung für Internet Explorer von der Support-Website von Microsoft unter support.microsoft.com herunter.
Aktualisieren	Lädt die Seite **SEL** hoch.

Befehlszeile zum Anzeigen des Systemprotokolls verwenden

```
racadm getsel-i
```

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

```
racadm getsel <Optionen>
```

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

ANMERKUNG: Weitere Informationen zu den verwendbaren Optionen finden Sie unter getsel.

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

```
racadm clrsel
```

Die POST- und Betriebssystemstart-Capture- Protokolle verwenden

Diese Funktion von DRAC 5 ermöglicht Ihnen, ein Stop-Motion-Video der letzten drei Instanzen des BIOS-POST und des Betriebssystemstarts abzuspielen.

So zeigen Sie die POST- und Betriebssystemstart-Capture-Protokolle an:

1. Klicken Sie in der **System** struktur auf **System**.
2. Klicken Sie auf die Registerkarte **Protokolle** und dann auf die Registerkarte **START-Capture**.
3. Wählen Sie die Protokollnummer des POST-Protokolls oder des Start- Capture-Protokolls des Betriebssystems aus.

   Das Video des Protokolls wird auf einem neuen Bildschirm abgespielt.
4. Klicken Sie auf **Stopp**, um die Wiedergabe anzuhalten.

Bildschirm des letzten Systemabsturzes anzeigen

VORSICHTSHINWEIS: Die Funktion „Bildschirm Letzter Absturz" erfordert ein verwaltetes System mit im Server Administrator konfigurierter Funktion Autom. Wiederherstellung. Stellen Sie außerdem sicher, dass die Funktion Automatisierte Systemwiederherstellung mittels DRAC

aktiviert ist. Wechseln Sie zur Seite Dienste, Registerkarte Konfiguration, 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 Systemabsturz angezeigt. Die letzten Systemausfall-Informationen werden im DRAC 5-Speicher gespeichert und sind im Remote-Zugriff zugänglich.

So zeigen Sie die Seite **Bildschirm Letzter Absturz** an:

1. Klicken Sie in der **System** struktur auf **System**.
2. Klicken Sie auf das Register **Protokolle** und dann auf **Letzter Absturz**.

Die Seite **Bildschirm Letzter Absturz** enthält die folgenden Schaltflächen (siehe Tabelle 16-9) oben rechts auf dem Bildschirm:

Tabelle 16-9. Schaltflächen der Seite „Bildschirm Letzter Absturz"

Schaltfläche	Maßnahme
Drucken	Druckt die Seite **Bildschirm Letzter Absturz**.
Speichern	Öffnet ein Popup-Fenster, das es ermöglicht, den Bildschirm Letzter Absturz in einem Verzeichnis Ihrer Wahl zu speichern.
Löschen	Löscht die Seite **Bildschirm Letzter Absturz**.
Aktualisieren	Lädt die Seite **Bildschirm Letzter Absturz** neu.

ANMERKUNG: Aufgrund von Schwankungen des Zeitgebers für automatische Wiederherstellung kann der **Bildschirm Letzter Absturz** nicht erfasst werden, wenn der System-Reset-Zeitgeber auf einen Wert unter 30 Sekunden eingestellt wird. Stellen Sie den System-Reset-Zeitgeber mit dem Server Administrator oder IT Assistant auf mindestens 30 Sekunden ein, und vergewissern Sie sich, dass die Funktionen unter **Bildschirm Letzter Absturz** ordnungsgemäß funktionieren. Weitere Informationen hierzu finden Sie unter Das verwaltete System zur Erfassung des Bildschirms „Letzter Absturz" konfigurieren.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Wiederherstellung und Störungsbehebung des DRAC 5

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

In diesem Abschnitt wird das Ausführen von Tasks beschrieben, die mit der Wiederherstellung und Fehlerbehebung eines abgestürzten DRAC 5 in Verbindung stehen.

Die Fehlerbehebung des DRAC 5 kann unter Verwendung eines der folgenden Hilfsprogramme durchgeführt werden:

- RAC-Protokoll
- Diagnosekonsole
- Ablaufverfolgungsprotokoll
- racdump
- coredump

RAC-Protokoll verwenden

Das **RAC-Protokoll** ist ein beständiges Protokoll, das in der DRAC 5-Firmware geführt wird. Das Protokoll enthält eine Liste von Benutzermaßnahmen (wie z. B. An- und Abmelden und Änderungen der Sicherheitsrichtlinie) sowie Warnungen, die vom DRAC 5 ausgegeben werden. Die ältesten Einträge werden überschrieben, wenn der Protokollspeicher erschöpft ist.

So rufen Sie das RAC-Protokoll über die DRAC 5-Benutzeroberfläche (UI) auf:

1. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Protokolle** und anschließend auf **RAC- Protokoll**.

Das **RAC-Protokoll** stellt die in Tabelle 17-1 aufgeführten Informationen zur Verfügung.

Tabelle 17-1. Informationen der RAC-Protokollseite

Feld	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit (z. B. 19. Dez. 16:55:47). Ist der DRAC 5 beim erstmaligen Start nicht in der Lage, mit dem verwalteten System zu kommunizieren, wird die entsprechende Uhrzeit als Systemstartzeit angezeigt.
Quelle	Die Schnittstelle, die das Ereignis verursacht hat.
Beschreibung	Eine kurze Beschreibung des Ereignisses und des Namens des Benutzers, der sich an DRAC 5 angemeldet hat.

Schaltflächen der RAC-Protokollseite verwenden

Die Seite **RAC-Protokoll** enthält die unter Tabelle 17-2 aufgeführten Schaltflächen.

Tabelle 17-2. Schaltflächen des RAC-Protokolls

Schaltfläche	Maßnahme
Drucken	Druckt die Seite **RAC-Protokoll** aus.
Protokoll löschen	Löscht die **RAC-Protokolleinträge**. **ANMERKUNG:** Die Schaltfläche **Protokoll löschen** wird nur angezeigt, wenn Sie über die Berechtigung **Protokolle löschen** verfügen.
Speichern unter	Öffnet ein Popup-Fenster, in dem Sie das **RAC-Protokoll** in einem Verzeichnis Ihrer Wahl speichern können.

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

Befehlszeile verwenden

Zeigen Sie die RAC-Protokolleinträge mittels des Befehls `getraclog` an.

```
racadm getraclog -i
```

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

```
racadm getraclog [Optionen]
```

ANMERKUNG: Weitere Informationen finden Sie unter getraclog.

Mithilfe des Befehls `clrraclog` können Sie alle Einträge aus dem iDRAC-Protokoll löschen.

```
racadm clrraclog
```

Diagnosekonsole verwenden

Der DRAC 5 bietet einen Standardsatz von Netzwerkdiagnose-Hilfsprogrammen (sehen Sie Tabelle 17-3), die den Microsoft Windows- oder Linux-basierten Systemen gelieferten Hilfsprogrammen ähnlich sind. Mit der Internet-basierten DRAC 5-Schnittstelle können Sie auf die Hilfsprogramme zum Netzwerk-Debuggen zugreifen.

So greifen Sie auf die Seite **Diagnosekonsole** zu:

1. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Diagnose**.

Tabelle 17-3 beschreibt die Optionen, die auf der Seite **Diagnosekonsole** verfügbar sind. Geben Sie einen Befehl ein und klicken Sie auf **Senden**. Die Debug-Ergebnisse werden auf der Seite **Diagnosekonsole** angezeigt.

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

Tabelle 17-3. Diagnosebefehle

Befehl	Beschreibung
arp	Zeigt den Inhalt der Tabelle des Adressauflösungsprotokolls (ARP) an. ARP-Einträge dürfen nicht hinzugefügt oder gelöscht werden.
ifconfig	Zeigt den Inhalt der Netzwerkschnittstellentabelle an.
netstat	Druckt den Inhalt der Routingtabelle aus. Wenn die optionale Schnittstellenzahl im Textfeld rechts neben der Option **netstat** angegeben wird, druckt netstat zusätzliche Informationen über den Verkehr auf der Schnittstelle, die Pufferauslastung und andere Informationen zur Netzwerkschnittstelle aus.
ping *<IP-Adresse>*	Überprüft, ob die Ziel-IP-Adresse von DRAC 5 aus mit dem aktuellen Routingtabelleninhalt erreichbar ist. Im Feld rechts von dieser Option muss eine Ziel-IP-Adresse eingegeben werden. Ein ICMP-Echo-Paket (Internet-Steuerungsmeldungs-protokoll) wird basierend auf dem aktuellen Inhalt der Routingtabelle zur Ziel-IP-Adresse gesendet.
gettracelog	Zeigt das DRAC 5-Ablaufverfolgungsprotokoll an. Weitere Informationen finden Sie unter gettracelog.

Ablaufverfolgungsprotokoll verwenden

Das interne DRAC 5-Ablaufverfolgungsprotokoll wird von Administratoren verwendet, um Warnmeldungen und Netzwerkprobleme von DRAC 5 zu debuggen.

So greifen Sie über die Internet-basierte DRAC 5-Schnittstelle auf das Ablaufverfolgungsprotokoll zu:

1. Klicken Sie in der **System** struktur auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Diagnose**.
3. Geben Sie den **gettracelog**-Befehl oder den **racadm gettracelog**-Befehl in das **Befehl**sfeld ein.

   ANMERKUNG: Sie können diesen Befehl auch über die Befehlszeilenoberfläche verwenden. Weitere Informationen finden Sie unter gettracelog.

Das Ablaufverfolgungsprotokoll verfolgt die folgenden Informationen:

- DHCP - Verfolgt Pakete, die an einen DHCP-Server gesendet und von ihm empfangen werden.
- IP - Verfolgt gesendete und empfangene IP-Pakete.

Das Ablaufverfolgungsprotokoll kann auch DRAC 5-Firmware-spezifische Fehlercodes enthalten, die mit der internen DRAC 5-Firmware (und nicht mit dem Betriebssystem des verwalteten Systems) in Verbindung stehen.

ANMERKUNG: DRAC 5 gibt kein Echo eines ICMP (Ping) bei einer Paketgröße von über 1500 Byte zurück.

---

racdump verwenden

Der Befehl racadm racdump bietet einen Einzelbefehl zum Abrufen von Informationen zum Abbild und Status sowie zu allgemeinen DRAC 5-Platinen-Informationen.

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

---

coredump verwenden

Mit dem Befehl racadm coredump werden detaillierte Informationen im Zusammenhang mit kritischen Problemen angezeigt, die kürzlich am RAC aufgetreten sind. Die coredump-Informationen können zur Diagnose dieser kritischen Probleme eingesetzt werden.

Wenn verfügbar, sind die Coredump-Informationen über Ein-/Ausschaltzyklen des RAC beständig und bleiben verfügbar, bis eine der folgenden Bedingungen eintritt:

- Die Coredump-Informationen werden mit dem Unterbefehl **coredumpdelete** gelöscht.
- Auf dem RAC tritt ein weiterer kritischer Zustand ein. In diesem Fall beziehen sich die coredump-Informationen auf den zuletzt aufgetretenen kritischen Fehler.

Der Befehl racadm coredumpdelete kann zum Löschen aller gegenwärtig vorhandenen, im RAC gespeicherten **Coredump**-Daten verwendet werden.

Weitere Informationen finden Sie unter dem Befehl coredump und coredumpdelete.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Sensoren

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Hardwaresensoren oder -sonden helfen Ihnen, die Systeme im Netzwerk auf effizientere Weise zu überwachen, indem Sie geeignete Maßnahmen ergreifen können, um Notfallsituationen, wie z. B. eine Instabilität oder Beschädigung des Systems, zu verhindern.

Sie können DRAC 5 zum Überwachen von Hardwaresensoren für Batterien, Lüftersensoren, Gehäuseeingriff, Netzteilen, aufgenommenen Strom, Temperatur und Spannung einsetzen.

Batteriesonden

Die Batteriesonden bieten Informationen zu Systemplatinen-CMOS und Speicher-ROMB-Batterien (RAID auf Systemplatine).

ANMERKUNG: Die Einstellungen für Speicher-ROMB-Batterien sind nur verfügbar, wenn das System einen ROMB aufweist.

Lüftersonden

Der Lüftersonden-Sensor bietet Informationen zu Folgendem:

- Lüfterredundanz - die Fähigkeit des sekundären Lüfters, den primären Lüfter zu ersetzen, wenn der primäre Lüfter nicht mehr in der Lage ist, unter einer voreingestellten Geschwindigkeit Wärme abzuleiten.
- Liste der Lüftersonden - bietet Informationen zur Lüftergeschwindigkeit aller Lüfter im System.

Gehäuseeingriffssonden

Die Gehäuseeingriffssonden geben Aufschluss über den Gehäusestatus bzw. darüber, ob das Gehäuse geöffnet oder geschlossen ist.

Netzteilsonden

Die Netzteilsonden bieten Informationen zu Folgendem:

- Status der Netzteile bzw. ob sich diese innerhalb des normalen Schwellenwertbereichs befinden oder den Schwellenwert überschritten haben.

  ANMERKUNG: Schwellenwerte können nur über den Dell OpenManage Server Administrator eingestellt werden. Weitere Informationen finden Sie im *Dell OpenManage Server Administrator-Benutzerhandbuch*.

- Netzteilredundanz bzw. die Fähigkeit des redundanten Netzteils, das primäre Netzteil zu ersetzen, falls das primäre Netzteil ausfallen sollte.

  ANMERKUNG: Sollte sich im System nur ein Netzteil befinden, wird der Abschnitt zur Netzteilredundanz nicht angezeigt.

Hardwareleistungssensoren

Der Hardwareleistungssensor gibt den Leistungsstatus des Hauptprozessors (CPU) an, ob dieser nun herabgesetzt oder normal ist. Der Status der Hardwareleistungssensoren wird herabgesetzt, wenn sich die CPU im gedrosselten Zustand befindet.

Stromüberwachungssonden

Die Stromüberwachung liefert Informationen zum Stromverbrauch in *Echtzeit*, in Watt und Ampere. Diese Informationen werden DRAC 5 über die Firmware-Sensoren des Baseboard-Verwaltungs-Controllers (BMC) zur Verfügung gestellt.

ANMERKUNG: Diese Funktion wird nur auf einer eingeschränkten Reihe von Dell PowerEdge *x*9*xx*- und *xx*0*x*-Systemen unterstützt.

DRAC 5 stellt erweiterte Energieüberwachungsfunktionen bereit. Dazu gehören:

- Grafische Darstellung der Systemleistung in Watt und des Systemstroms in Ampere über eine bestimmte Zeitspanne.

- Statistik in Diagrammform zur maximalen, minimalen und durchschnittlichen Stromaufnahme des Systems in Watt und BTU/H (British Thermal Unit per Hour) während der letzten Stunde, des letzten Tags und der letzten Woche der aktuellen DRAC-Zeit.
- Leistungsaufnahme des Systems in Watt und aufgenommener Durchschnittsstrom von jedem Netzteil in Ampere.

Diagramminformationen

Auf der Seite **Diagramminformationen** werden die Diagramme für die Systemleistungsstufe in Watt und für die Netzteile in Ampere über einen bestimmten Zeitraum dargestellt. Die Seite wird jede Minute automatisch aktualisiert.

ANMERKUNG: Die Daten werden von DRAC 5 alle fünf Minuten abgerufen und gehen verloren, nachdem ein DRAC-Reset durchgeführt, die Versorgung ein- und ausgeschaltet oder eine Firmware-Aktualisierung durchgeführt wurde.

ANMERKUNG: In den Diagrammen sind möglicherweise auch Lücken zu sehen, wenn das System entweder ausgeschaltet war oder BMC-Resets durchgeführt wurden. Der Grund hierfür liegt darin, dass in dieser Zeit die Stromsensoren nicht verfügbar sind.

Die Leistungsaufnahme in Watt zeigt die Zeitspanne an, während der die Daten über die Leistung gesammelt werden. Im Dropdown-Menü dieser Seite können Sie den Bereich auf der X-Achse auf 1 Stunde, 1 Tag oder 1 Woche einstellen. Die Zeitspanne gilt ab dem Zeitpunkt, der gegenwärtig für DRAC eingestellt ist. Auf der Y-Achse wird die Leistung (in Watt) angezeigt, die vom System aufgenommen wurde.

Die Stromaufnahme in Ampere zeigt die Zeitspanne an, in der die Daten über die Stromaufnahme gesammelt werden. Im Dropdown-Menü dieser Seite können Sie den Bereich auf der X-Achse auf 1 Stunde, 1 Tag oder 1 Woche einstellen. Die Zeitspanne gilt ab der aktuellen DRAC-Zeit. Auf der Y-Achse wird der Strom (Ampere) angezeigt, der von den Netzteilen aufgenommen wird. Wenn mehr als ein Netzteil im System vorhanden ist und die Messwerte gleich sind, können die Stromdiagramme einander überlappen.

Informationen zum Stromverbrauch

Auf der Seite **Stromverbrauchsinformationen** wird die Leistungsaufnahme des Systems (in Watt) angezeigt sowie der durchschnittliche Stromverbrauch (in Ampere) jedes Netzteils.

Auf dieser Seite werden außerdem der Status der Sensoren, der Sensorname, die Leistungsaufnahme, Mindest- und Höchstschwellenwerte für die Ausgabe von Warnungen und Ausfallalarmen, die Position des Netzteils sowie der durchschnittliche Strom jedes Netzteils (in Ampere) angezeigt.

Energiestatistik

Auf der Seite **Stromstatistik** wird die durchschnittliche Leistungsaufnahme und die Statistik zur maximalen und minimalen Leistungsaufnahme des Systems in Watt und BTU/H (British Thermal Unit per Hour) während der letzten Stunde, des letzten Tages und der letzten Woche ab der aktuellen DRAC-Zeit angezeigt. Die Daten werden von DRAC 5 abgerufen und zurückgesetzt, falls DRAC aus einem bestimmten Grund zurückgesetzt wird.

Temperatursensoren

Der Temperatursensor gibt Auskunft über die Umgebungstemperatur der Systemplatine. Die Temperatursensen zeigen an, ob sich der Status der Sensoren innerhalb des voreingestellten Warnungsschwellenwert-Bereichs und kritischen Schwellenwert-Bereichs befindet.

Spannungssonden

Bei den folgenden Sonden handelt es sich um typische Spannungssonden. Es ist möglich, dass diese und/oder andere Sonden auf Ihrem System vorhanden sind.

- CPU [n] VCORE
- Systemplatine 0,9 V PG
- Systemplatine 1,5 V ESB2 PG
- Systemplatine 1,5 V PG
- Systemplatine 1,8 V PG
- Systemplatine 3,3 V PG
- Systemplatine 5 V PG
- Systemplatine Backplane PG
- Systemplatine CPU VTT
- Systemplatine Linear PG

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Zum Einstieg mit DRAC 5

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

DRAC 5 ermöglicht Ihnen, ein Dell-System im Remote-Zugriff zu überwachen bzw. zu reparieren und auf das System Fehlerbehebungsmaßnahmen anzuwenden, selbst wenn es heruntergefahren ist. DRAC 5 bietet eine umfangreiche Auswahl an Funktionen wie Konsolenumleitung, virtueller Datenträger, virtuelle KVM, Smart Card-Authentifizierung und mehr.

Die Management Station ist das System, von dem aus ein Administrator im Remote-Zugriff ein Dell-System verwaltet, in dem eine DRAC-Karte installiert ist. Die auf diese Weise überwachten Systeme werden als verwaltete Systeme bezeichnet.

Befolgen Sie die nachstehenden Schritte, um die DRAC-Karte einsetzen zu können.

1. Installieren Sie die DRAC 5-Karte im Dell-System – DRAC 5 ist eventuell auf Ihrem System vorinstalliert oder ist andernfalls separat als Kit erhältlich.

   ANMERKUNG: Dieses Verfahren kann je nach System unterschiedlich sein. Genaue Anleitungen zum Ausführen dieses Verfahrens befinden sich im *Hardware-Benutzerhandbuch* Ihres Systems, das auf der Dell Support-Website unter **support.dell.com / manuals** zur Verfügung steht.

   Die DRAC 5-Software muss sowohl auf der Management Station als auch auf dem verwalteten System installiert werden. Ohne die Managed System-Software kann RACADM nicht lokal verwendet werden, und DRAC kann den Bildschirm des letzten Absturzes nicht erfassen.

2. Konfigurieren Sie die Eigenschaften, Netzwerkeinstellungen und Benutzer von DRAC 5 – DRAC 5 kann sowohl unter Verwendung des Dienstprogramms zur Remote-Zugriffs-Konfiguration, als auch über die Internet-basierte Schnittstelle oder RACADM konfiguriert werden.

3. Konfigurieren Sie das Microsoft Active Directory für den Zugriff auf DRAC 5, wodurch Sie die DRAC 5-Benutzerberechtigungen zu den vorhandenen Benutzern in der Active Directory-Software hinzufügen bzw. steuern können.

4. Konfigurieren Sie die Smart Card-Authentifizierung – Smart Card bietet eine zusätzliche Sicherheitsstufe für Ihr Unternehmen.

5. Konfigurieren Sie Remote-Zugriffspunkte wie Konsolenumleitung und virtueller Datenträger.

6. Konfigurieren Sie die Sicherheitseinstellungen.

7. Verwenden Sie das Serververwaltungs-Befehlszeilenprotokoll (SM-CLP) der auf Standards beruhenden Verwaltung zum Verwalten der Systeme auf dem Netzwerk.

8. Konfigurieren Sie Warnmeldungen für eine effiziente Systemverwaltung.

9. Konfigurieren Sie die DRAC 5-IPMI-Einstellungen (Intelligente Plattform-Verwaltungsschnittstelle) zum Verwenden der auf Standards beruhenden IPMI-Hilfsprogramme zum Verwalten der Systeme auf dem Netzwerk.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Grundlegende Installation von DRAC 5

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

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

Bevor Sie beginnen

Stellen Sie die folgenden Artikel aus dem Lieferumfang des Systems bereit, bevor Sie die DRAC 5-Software installieren und konfigurieren:

- DRAC 5-Hardware (gegenwärtig installiert oder im optionalen Einbausatz)
- DRAC 5-Installationsverfahren (wird in diesem Kapitel beschrieben)
- DVD *Dell Systems Management Tools and Documentation*

DRAC 5-Hardware installieren

ANMERKUNG: Die DRAC 5-Verbindung emuliert eine USB-Tastaturverbindung. Infolgedessen wird Sie das System beim Neustart nicht benachrichtigen, wenn keine Tastatur angeschlossen ist.

DRAC 5 kann im System installiert oder getrennt als Einbausatz erhältlich sein. Informationen zum Einstieg mit dem im System installierten DRAC 5 stehen unter Übersicht zu Softwareinstallation und -konfiguration zur Verfügung.

Ist im System kein DRAC 5 installiert, so finden Sie im Dokument *Remote-Zugriffskarte installieren*, das im DRAC 5-Einbausatz enthalten ist, oder im *Installations- und Fehlerbehebungshandbuch* zur Plattform entsprechende Hardware-Installationsanleitungen.

ANMERKUNG: Das mit dem System gelieferte *Installations-und Fehlerbehebungshandbuch* enthält Informationen über den Ausbau der DRAC 5-Karte. Sehen Sie sich außerdem alle mit dem ausgebauten DRAC 5 in Verbindung stehenden Microsoft Active Directory-RAC-Eigenschaften an, um sicherzustellen, dass bei der Verwendung des erweiterten Schemas die ordnungsgemäße Sicherheit gewährleistet ist.

System für die Verwendung von DRAC 5 konfigurieren

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

So führen Sie das Remote-Zugriffs-Konfigurationsdienstprogramm von Dell aus:

1. Schalten Sie das System ein oder starten Sie es neu.
2. Drücken Sie <Strg><E>, wenn Sie während des POST dazu aufgefordert werden.

   Wenn Ihr Betriebssystem zu laden beginnt, bevor Sie <Strg><E> gedrückt haben, lassen Sie das System vollständig hochfahren, starten Sie das System neu, und versuchen Sie es noch einmal.
3. Konfigurieren Sie die NIC.
   a. Markieren Sie die **NIC-Auswahl** mithilfe der Nach-unten-Taste.
   b. Wählen Sie mit der Nach-links- und Nach-rechts-Taste eine der folgenden NIC-Optionen aus:
      - **Dediziert** – Wählen Sie diese Option aus, um das Remote-Zugriffsgerät zu aktivieren und die auf dem Remote-Access-Controller (RAC) verfügbare dedizierte Netzwerkschnittstelle zu verwenden. Diese Schnittstelle wird nicht an das Host-Betriebssystem freigegeben und leitet den Verwaltungsdatenverkehr auf ein separates physisches Netzwerk um, wodurch er vom Anwendungsdatenverkehr getrennt wird. Diese Option ist nur verfügbar, wenn im System eine DRAC-Karte installiert ist.
      - **Freigegeben** – Wählen Sie diese Option aus, um die Netzwerkschnittstelle gemeinsam mit dem Host-Betriebssystem zu verwenden. Die Netzwerkschnittstelle des Remote-Zugriffsgeräts ist vollständig funktionsfähig, wenn das Host-Betriebssystem für NIC-Teaming konfiguriert ist. Das Remote-Zugriffsgerät empfängt Daten über NIC 1 und NIC 2, sendet Daten jedoch nur über NIC 1. Wenn NIC 1 fehlschlägt, ist der Zugriff auf das Remote-Zugriffsgerät nicht möglich.
      - **Failover** – Wählen Sie diese Option aus, um die Netzschnittstelle gemeinsam mit dem Host-Betriebssystem zu verwenden. Die Netzwerkschnittstelle des Remote-Zugriffsgeräts ist vollständig funktionsfähig, wenn das Host-Betriebssystem für NIC-Teaming konfiguriert ist. Das Remote-Zugriffsgerät empfängt Daten über NIC 1 und NIC 2, sendet Daten jedoch nur über NIC 1. Wenn NIC 1 ausfällt, schaltet das Remote-Zugriffsgerät für alle Datenübertragungen auf NIC 2. Das Remote-Zugriffsgerät verwendet NIC 2 weiterhin für die Datenübertragung. Wenn NIC 2 ausfällt, schaltet das Remote-Zugriffsgerät für alle Datenübertragungen zu NIC 1 zurück.

4. Konfigurieren Sie die LAN-Parameter des Netzwerk-Controllers zur Verwendung von DHCP oder einer statischen IP-Adressenquelle.
    a. Wählen Sie mit der Abwärtspfeiltaste **LAN-Parameter** aus, und drücken Sie <Eingabe>.
    b. Wählen Sie die **IP-Adressen-Quelle** mit den Pfeiltasten aus.
    c. Wählen Sie mit der Nach-rechts- und Nach-links-Taste **DHCP** oder **Statisch** aus.
    d. Wenn Sie **Statisch** ausgewählt haben, konfigurieren Sie die **Ethernet- IP-Adresse**, **Subnetzmaske** und **Standard-Gateway**-Einstellungen.
    e. Drücken Sie die <Esc>-Taste.
5. Drücken Sie die <Esc>-Taste.
6. Wählen Sie **Änderungen speichern und beenden** aus.

   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 Dell-Systeme, die mit einem einzelnen LAN auf der Hauptplatine konfiguriert sind) können für NIC-Teaming konfiguriert werden. Die Modi Freigegeben und Team arbeiten auf diesen Systemen unabhängig voneinander.

Das *Benutzerhandbuch zu den Dienstprogrammen des Dell OpenManage Baseboard-Management-Controllers enthält* weitere Informationen über das Dell Remote-Zugriffs-Konfigurationsdienstprogramm.

Übersicht zu Softwareinstallation und - konfiguration

Dieser Abschnitt beinhaltet eine Übersicht auf höchster Ebene des DRAC 5-Softwareinstallations- und Konfigurationsverfahrens. Konfigurieren Sie DRAC 5 mit der Internet-basierten Schnittstelle, RACADM-CLI oder der seriellen/Telnet/SSH-Konsole.

Weitere Informationen zu den DRAC 5-Softwarekomponenten finden Sie unter Software auf dem verwalteten System installieren.

DRAC 5-Software installieren

So installieren Sie die DRAC 5-Software:

1. Installieren Sie die Software auf dem verwalteten System. Siehe Software auf dem verwalteten System installieren.
2. Installieren Sie die Software auf der Management Station. Siehe Software auf der Management Station installieren.

DRAC 5 konfigurieren

So konfigurieren Sie DRAC 5:

1. Wählen Sie eines der folgenden Konfigurationshilfsprogramme aus:
    - Webbasierte Schnittstelle
    - RACADM-CLI
    - Serielle/Telnet/SSH-Konsole

VORSICHTSHINWEIS: Die gleichzeitige Verwendung von mehr als einem DRAC 5-Konfigurationshilfsprogramm kann zu unerwarteten Ergebnissen führen.

2. Konfigurieren Sie die DRAC 5-Netzwerkeinstellungen. Siehe DRAC 5- Eigenschaften konfigurieren.
3. Fügen Sie DRAC 5-Benutzer hinzu und konfigurieren Sie diese. Siehe DRAC 5-Benutzer hinzufügen und konfigurieren.
4. Konfigurieren Sie den Webbrowser, um auf die webbasierte Schnittstelle zuzugreifen. Siehe Konfigurieren eines unterstützten Webbrowsers.
5. Deaktivieren Sie die Windows-Option für den automatischen Neustart. Siehe Die Windows-Option Automatischer Neustart deaktivieren.
6. Aktualisieren Sie die DRAC 5-Firmware. Siehe Verbindung zum verwalteten System über die lokale serielle Schnittstelle oder die Telnet- Management Station (Kundensystem) herstellen.
7. Greifen Sie über ein Netzwerk auf den DRAC 5 zu. Siehe Verbindung zum verwalteten System über die lokale serielle Schnittstelle oder die Telnet-Management Station (Kundensystem) herstellen.

Software auf dem verwalteten System installieren

Die Installation von Software auf dem verwalteten System ist optional. Ohne die Managed System-Software kann RACADM nicht lokal verwendet werden, und DRAC kann den Bildschirm des letzten Absturzes nicht erfassen.

Installieren Sie die Managed System-Software, indem Sie die Software unter Verwendung der DVD *Dell Systems Management Tools and Documentation* auf dem verwalteten System installieren. Anleitungen zur Installation dieser Software sind im *Schnellinstallationshandbuch* enthalten.

Die Managed System-Software installiert Ihre Auswahl der entsprechenden Version von Dell OpenManage Server Administrator auf dem verwalteten System.

ANMERKUNG: Die DRAC 5-Management Station-Software und die DRAC 5-Managed System-Software dürfen nicht auf demselben System installiert sein.

VORSICHTSHINWEIS: Die neueste DRAC-Firmware unterstützt nur die aktuellste RACADM-Version. Es können Fehler auftreten, wenn Sie eine ältere RACADM-Version zum Abfragen eines DRAC mit der neuesten Firmware verwenden. Installieren Sie die RACADM-Version, die mit Ihrer neuesten Dell OpenManage-DVD bereitgestellt wurde.

Wenn Server Administrator nicht auf dem verwalteten System installiert ist, können Sie weder den Bildschirm des letzten Systemabsturzes anzeigen noch die Funktion **Autom. Wiederherstellung** verwenden.

Weitere Informationen zum Bildschirm des letzten Absturzes finden Sie unter Bildschirm des letzten Systemabsturzes anzeigen.

Software auf der Management Station installieren

Das System enthält das Dell OpenManage-Systems Management Software-Paket. Dieses Paket enthält unter anderem die DVD *Dell Systems Management Tools and Documentation*. Informationen über die Installation der Server Administrator-Software sind im *Server Administrator-Benutzerhandbuch* enthalten.

Management Station von Red Hat Enterprise Linux (Version 4) konfigurieren

Für den digitalen KVM Viewer von Dell ist eine zusätzliche Konfiguration erforderlich, damit dieser auf der Management Station von Red Hat Enterprise Linux (Version 4) ausgeführt werden kann. Führen Sie die folgenden Verfahren aus, wenn Sie das Betriebssystem Red Hat Enterprise Linux (Version 4) auf der Management Station installieren:

- Installieren Sie, wenn Sie dazu aufgefordert werden, Pakete hinzuzufügen oder zu entfernen, die optionale **Legacy-Software-Entwicklungs** software. Dieses Softwarepaket enthält die Softwarekomponenten, die zum Ausführen des digitalen KVM Viewers von Dell auf der Management Station erforderlich sind.
- Öffnen Sie die folgenden Anschlüsse der Firewall, um sicherzustellen, dass der digitale KVM Viewer von Dell ordnungsgemäß funktioniert:
  - Tastatur- und Mausanschluss (Standard: Port 5900)
  - Videoanschluss (Standard: Port 5901)

RACADM auf einer Linux-Management Station installieren und entfernen

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

ANMERKUNG: Wenn Sie **Setup** auf der DVD *Dell Systems Management Tools and Documentation* ausführen, wird das RACADM-Dienstprogramm für alle unterstützten Betriebssysteme auf der Management Station installiert.

RACADM installieren

1. Melden Sie sich als root an dem System an, auf dem Sie die Management Station-Komponenten installieren möchten.
2. Falls erforderlich, stellen Sie die DVD *Dell Systems Management Tools and Documentation* unter Verwendung des folgenden Befehls oder eines ähnlichen Befehls bereit:

   ```
   mount /media/cdrom
   ```

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

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

Um Hilfe zum RACADM-Befehl zu erhalten, geben Sie nach der Eingabe der vorherigen Befehle **racadm help** ein.

RACADM deinstallieren

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

```
rpm -e <racadm-Paketname>
```

wobei <*racadm-Paketname*> das rpm-Paket ist, das zur Installation der RAC-Software verwendet wurde.

Wenn der rpm-Paketname z. B. **srvadmin-racadm5** lautet, geben Sie Folgendes ein:

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

DRAC 5-Firmware aktualisieren

Verwenden Sie eines der folgenden Verfahren, um die DRAC 5-Firmware zu aktualisieren.

- Internet-basierte Schnittstelle
- RACADM-CLI
- Dell Aktualisierungspakete

Bevor Sie beginnen

Führen Sie die folgenden Verfahren aus, bevor Sie die DRAC 5-Firmware mittels des lokalen RACADM oder mit Hilfe von Dell Aktualisierungspaketen aktualisieren. Andernfalls schlägt die Firmware-Aktualisierung eventuell fehl.

1. Installieren und aktivieren Sie die entsprechende IPMI und die entsprechenden Treiber des verwalteten Knotens.
2. Wenn das System das Windows-Betriebssystem ausführt, aktivieren und starten Sie den **Windows Management Instrumentation**-Dienst (WMI).
3. Wenn das 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 nicht gemountet ist, bzw. dass er nicht vom Betriebssystem oder einer anderen Anwendung / einem anderen Benutzer verwendet wird.
5. Trennen Sie die Verbindung zum virtuellen Datenträger und heben Sie die Bereitstellung auf (unmount).
6. Stellen Sie sicher, dass der 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** herunter, und speichern Sie die Datei auf Ihrem lokalen System.

Die folgenden Softwarekomponenten sind in Ihrem DRAC 5-Firmware-Paket enthalten:

- Kompilierter DRAC 5-Firmware-Code und Daten
- Erweiterungs-ROM-Image
- Webbasierte Benutzerschnittstelle, JPEG und andere Benutzeroberflächendateien
- Standard-Konfigurationsdateien

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

DRAC 5-Firmware mittels der Internet-basierten Schnittstelle aktualisieren

1. Öffnen Sie die Internet-basierte Schnittstelle, und melden Sie sich am Remote-System an.

   Siehe Auf die Internet-basierte Schnittstelle zugreifen.

2. Klicken Sie in der **System**struktur auf **Remote-Zugriff** und dann auf das Register **Aktualisierung**.
3. Geben Sie auf der Seite **Firmware-Aktualisierung** in das Feld **Firmware- Image** den Pfad zum 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 Feld **Firmware-Image**.

   Beispiel:

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

   Der standardmäßige Name des Firmware-Images lautet **firmimg.d5**.

4. Klicken Sie auf **Aktualisieren**.

   Die Aktualisierung kann mehrere Minuten in Anspruch nehmen. Nach Abschluss wird ein Dialogfeld eingeblendet.

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

6. Klicken Sie nach dem DRAC 5-Reset auf **Anmelden**, um sich an DRAC 5 anzumelden.

DRAC 5-Firmware mittels racadm aktualisieren

Sie können die DRAC 5-Firmware mittels des CLI-basierten racadm-Hilfsprogramms aktualisieren. Wenn auf dem verwalteten System Server Administrator installiert ist, können Sie die Firmware mit lokalem racadm aktualisieren.

1. Laden Sie das DRAC 5-Firmware-Image von der Dell Support-Website unter **support.dell.com** auf das verwaltete System herunter.

   Beispiel:

   ```
   C:\downloads\firmimg.d5
   ```

2. Führen Sie den folgenden racadm-Befehl aus:

   ```
   racadm -pud c:\downloads\
   ```

   Sie können die Firmware auch unter Verwendung von remote racadm aktualisieren.

   Beispiel:

   racadm -r <*DRAC5-IP-Adresse*> U <*Benutzername*> -p <*Kennwort*> fwupdate -p -u -d <*Pfad*>

   wobei *Pfad* der Ort ist, an dem Sie die Datei **firmimg.d5** auf dem verwalteten System gespeichert haben.

DRAC 5-Firmware mittels Dell Aktualisierungspakete für unterstützte Windows- und Linux-Betriebssysteme aktualisieren

Die Dell Update Packages für unterstützte Windows- und Linux-Betriebssysteme können von der Dell Support-Website unter **support.dell.com** heruntergeladen und ausgeführt werden. Weitere Informationen finden Sie im *Dell Update Package-Benutzerhandbuch*.

Browser-Cache löschen

Nach der Firmware-Aktualisierung löschen Sie den Cache des Webbrowsers.

Die Online-Hilfe Ihres Webbrowsers enthält weitere Informationen.

Konfigurieren eines unterstützten Webbrowsers

Die folgenden Abschnitte enthalten Anweisungen zur Konfiguration von unterstützten Webbrowsern. *Eine Liste der unterstützten Webbrowser finden Sie in der* Dell Systems Software Support Matrix auf der Dell Support-Website unter **support.dell.com/manuals**.

Konfigurieren des Internet-Browsers, um eine Verbindung zur Internet-basierten Schnittstelle herzustellen

Wenn Sie von einer Management Station, die über einen Proxy-Server an das Internet angeschlossen ist, eine Verbindung zur Internet-basierten DRAC 5-Schnittstelle herstellen, muss der Internet-Browser so konfiguriert werden, dass er von diesem Server aus auf das Internet zugreifen kann.

So konfigurieren Sie Internet Explorer, um auf einen Proxy-Server zuzugreifen:

1. Öffnen Sie ein Webbrowser-Fenster.

2. Klicken Sie auf **Extras** und dann auf **Internetoptionen**.

3. Klicken Sie im Fenster **Internetoptionen** auf das Register **Verbindungen**.

4. Klicken Sie unter **LAN-Einstellungen (Lokales Netzwerk)** auf **LAN- Einstellungen**.

5. Wenn das Kästchen **Proxy-Server verwenden** markiert ist, wählen Sie das Kästchen **Proxy-Server für lokale Adressen deaktivieren** aus.

6. Klicken Sie zweimal auf **OK**.

Liste vertrauenswürdiger Domänen

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

32-Bit- und 64-Bit-Webbrowser

Die Internet-basierte DRAC 5-Schnittstelle wird auf 64-Bit-Internet-Browsern nicht unterstützt. Wenn Sie einen 64-Bit-Browser öffnen, auf die Konsolenumleitungsseite zugreifen und versuchen, das Plug-in zu installieren, schlägt das Installationsverfahren fehl. Wenn dieser Fehler nicht bestätigt wurde und Sie dieses Verfahren wiederholen, wird die Konsolenumleitungsseite geladen, obwohl die Plug-in-Installation während des ersten Versuchs fehlgeschlagen ist. Dieses Problem tritt auf, weil der Webbrowser die Plug-in-Informationen im Profilverzeichnis speichert, obwohl das Plug-in-Installationsverfahren fehlgeschlagen ist. Sie können dieses Problem lösen, indem Sie einen unterstützten 32-Bit-Internet-Browser installieren, diesen ausführen und sich an DRAC 5 anmelden.

Lokalisierte Versionen der webbasierten Schnittstelle anzeigen

Windows

Die Internet-basierte DRAC 5-Schnittstelle wird für die folgenden Windows-Betriebssystemsprachen unterstützt:

- Englisch
- Französisch
- Deutsch
- Spanisch
- Japanisch
- Chinesisch (vereinfacht)

So zeigen Sie eine lokalisierte Version der Internet-basierten DRAC 5-Schnittstelle in Internet Explorer an:

1. Klicken Sie auf das Menü **Extras** und wählen Sie **Internetoptionen** aus.

2. Klicken Sie im Fenster **Internetoptionen** auf **Sprachen**.

3. Klicken Sie im **Fenster Spracheinstellung** auf **Hinzufügen**.

4. Wählen Sie im Fenster **Sprache hinzufügen** eine unterstützte Sprache aus.

   Um mehr als eine Sprache auszuwählen, drücken Sie <Strg>.

5. Wählen Sie Ihre bevorzugte Sprache aus, und klicken Sie auf **Nach oben**, um die Sprache an die Spitze der Liste zu verschieben.

6. Klicken Sie auf **OK**.

7. Klicken Sie im Fenster **Spracheinstellung** auf **OK**.

Linux

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

1. Öffnen Sie ein Terminal.

2. Geben Sie „locale" ein und drücken Sie die Eingabetaste. Die folgende Ausgabe wird eingeblendet.

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
```

```
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3. Wenn die Werte „zh_CN.UTF-8" einschließen, sind keine Änderungen erforderlich. Wenn die Werte „zh_CN.UTF-8" nicht einschließen, fahren Sie mit Schritt 4 fort.

4. Wechseln Sie zur Datei /etc/sysconfig/i18n.

5. Wenden Sie in der Datei folgende Änderungen an:

   Aktueller Eintrag:

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

   Aktualisierter Eintrag:

   ```
   LANG="zh_CN.UTF-8"
   SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
   ```

6. Melden Sie sich vom Betriebssystem ab und anschließend wieder an.

7. Starten Sie DRAC 5 neu.

Wenn Sie von einer beliebigen anderen Sprache zu vereinfachtem Chinesisch wechseln, müssen Sie sicherstellen, dass die Korrektur noch gültig ist. Ist dies nicht der Fall, wiederholen Sie das Verfahren.

Informationen zu erweiterten DRAC 5-Konfigurationen finden Sie unter Erweiterte Konfiguration des DRAC 5.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Erweiterte Konfiguration des DRAC 5

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Dieser Abschnitt enthält Informationen zur erweiterten DRAC 5-Konfiguration und wird Benutzern mit fortgeschrittenen Kenntnissen im Bereich System-Management empfohlen, die die DRAC-Umgebung ihren speziellen Bedürfnissen anpassen möchten.

Bevor Sie beginnen

Die grundlegende Installation bzw. das grundlegende Setup der DRAC 5-Hardware und -Software sollte zu diesem Zeitpunkt bereits abgeschlossen sein. Weitere Informationen finden Sie unter Grundlegende Installation von DRAC 5.

DRAC 5-Eigenschaften konfigurieren

Sie können die DRAC 5-Eigenschaften (Netzwerk, Benutzer usw.) entweder über die Internet-basierte Schnittstelle oder mittels RACADM konfigurieren.

DRAC 5 bietet eine Internet-basierte Schnittstelle und RACADM (eine Befehlszeilen-Schnittstelle), mit denen Sie die DRAC 5-Eigenschaften und -Benutzer konfigurieren, Remote-Verwaltungs-Tasks ausführen und Probleme an einem Remote (verwalteten) System beheben können. Verwenden Sie für die tägliche Systemverwaltung die Internet-basierte DRAC 5-Schnittstelle. Dieses Kapitel gibt Informationen an zur Ausführung von allgemeinen Systemverwaltungs-Tasks mit Hilfe der Internet-basierten DRAC 5-Schnittstelle und Links zu in Beziehung stehenden Informationen.

Alle Internet-basierten Schnittstellenkonfigurations-Tasks können auch mit RACADM ausgeführt werden.

DRAC 5 mittels Internet-Benutzeroberfläche konfigurieren

Die DRAC 5-Online-Hilfe enthält kontextabhängige Informationen über jede Seite der Internet-basierten Schnittstelle.

Auf die Internet-basierte Schnittstelle zugreifen

So greifen Sie auf die DRAC 5-Internet-basierte Schnittstelle zu:

1. Öffnen Sie einen unterstützten Webbrowser.

   Eine Liste der unterstützten Webbrowser finden Sie in der Dell Systems Software Support Matrix auf der Dell Support-Website unter **support.dell.com / manuals**.

2. Geben Sie in das Feld **Adresse** Folgendes ein, und drücken Sie die Eingabetaste.

   `https://<IP-Adresse>`

   Wurde die Standard-HTTPS-Portnummer (443) geändert, geben Sie Folgendes ein:

   `https://<IP-Adresse>:<Anschlussnummer>`

   wobei *IP-Adresse* die IP-Adresse des DRAC 5 ist und *Port-Nummer* die HTTPS-Port-Nummer.

   Das DRAC 5-Fenster **Anmelden** wird angezeigt.

ANMERKUNG: Wenn Sie Internet Explorer Version 6 SP2 oder Version 7 verwenden, um sich an der DRAC 5-Internet-GUI anzumelden und sich der Client auf einem privaten Netzwerk befindet, jedoch keinen Zugriff auf das Internet hat, kann sich eine Verzögerung von bis zu 30 Sekunden ergeben. So lösen Sie das Problem:

1. Deaktivieren Sie den Phishing-Filter.

https://phishingfilter.microsoft.com/faq.aspx.

2. CRL-Fetching deaktivieren:

   a. Klicken Sie auf **Extras**→ **Optionen**→ Register **Erweitert**→ **Sicherheit**.

   b. Heben Sie die Markierung von **Auf gesperrte Zertifikate von Herausgebern überprüfen** auf.

Anmeldung

Sie können sich entweder als DRAC 5-Benutzer oder als Microsoft Active Directory-Benutzer anmelden. Der Standardbenutzername und das Standardkennwort lauten **root** bzw. **calvin**.

Stellen Sie sicher, bevor Sie sich bei DRAC 5 anmelden, dass Sie über die Berechtigung **Am DRAC 5 anmelden** verfügen. Sprechen Sie mit dem DRAC- oder Netzwerk-Administrator Ihrer Organisation, um Ihre Zugriffsberechtigungen zu sicherzustellen.

So melden Sie sich an:

1. Geben Sie eine der folgenden Eingaben in das Feld **Benutzername** ein:
   - Ihren DRAC 5-Benutzernamen.

     Beispiel: <*Benutzername*>

     Beim DRAC 5-Benutzernamen für lokale Benutzer ist Groß- und Kleinschreibung zu beachten.
   - 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**.

     Beim Active Directory-Benutzernamen ist keine Groß- und Kleinschreibung zu beachten.

2. Geben Sie in das Feld **Kennwort** Ihr DRAC 5-Benutzerkennwort oder Active Directory-Benutzerkennwort ein.

   Dieses Feld unterscheidet Groß- und Kleinschreibung.

3. Klicken Sie auf **OK** oder drücken Sie die Taste <Eingabe>.

Abmeldung

1. Klicken Sie in der rechten oberen Ecke des Fensters der Internet-basierten DRAC 5-Schnittstelle auf **Abmelden**, um die Sitzung zu schließen.
2. Schließen Sie das Browser-Fenster.

ANMERKUNG: Die Schaltfläche **Abmelden** wird erst angezeigt, wenn Sie sich anmelden.

ANMERKUNG: Das Schließen des Browsers ohne ordnungsgemäße Abmeldung führt dazu, dass die Sitzung so lange geöffnet bleibt, bis eine Zeitüberschreitung eintritt. Es wird empfohlen, dass Sie zum Beenden der Sitzung auf die Schaltfläche Abmelden klicken; ansonsten bleibt die Sitzung aktiv, bis die Sitzungszeitüberschreitung erreicht wird.

ANMERKUNG: Das Schließen der DRAC 5-Internet-basierten Schnittstelle in Microsoft Internet Explorer mithilfe der Schließen-Schaltfläche („x") in der oberen rechten Ecke des Fensters führt eventuell zu einem Anwendungsfehler. Laden Sie, um dieses Problem zu beheben, von der Microsoft Support-Website unter **support.microsoft.com** die neueste kumulative Sicherheitsaktualisierung für den Internet Explorer herunter.

Das Managed System aktivieren und konfigurieren, um eine serielle oder Telnet-Konsole zu verwenden

Die folgenden Unterabschnitte enthalten Informationen darüber, wie man eine serielle/Telnet/SSH-Konsole auf dem verwalteten System aktiviert und konfiguriert.

Verwenden des seriellen Befehls connect com2

Stellen Sie bei der Verwendung des seriellen Befehls **connect com2** sicher, dass Folgendes korrekt konfiguriert ist:

- Die Einstellung **Serielle Datenübertragung**→ **Serielle Schnittstelle** im **BIOS-Setup**-Programm.
- Die DRAC-Konfigurationseinstellungen.

Wird eine Telnet-Sitzung zum DRAC 5 aufgebaut und sind diese Einstellungen falsch, kann **connect com2** einen leeren Bildschirm anzeigen.

BIOS-Setup-Programm für eine serielle Verbindung auf dem verwalteten System konfigurieren

Führen Sie die folgenden Schritte aus, um das **BIOS-Setup**-Programm so zu konfigurieren, dass es die Ausgabe zu einer seriellen Schnittstelle umleitet.

ANMERKUNG: Das **System-Setup**-Programm muss in Verbindung mit dem Befehl **connect com2** konfiguriert werden.

1. Schalten Sie das System ein oder starten Sie es neu.
2. Drücken Sie die Taste <F2> umgehend, wenn folgende Meldung angezeigt wird:

   `<F2> = System Setup` (System-Setup)

3. Scrollen Sie nach unten, und wählen Sie durch Drücken der Eingabetaste **Serielle Datenübertragung** aus.
4. Stellen Sie den Bildschirm **Serial Communication** folgendermaßen ein:

   Externer serieller Anschluss – **Remote-Zugriffsgerät**

   Umleitung nach Start – **Deaktiviert**

5. Drücken Sie auf <Esc>, um das **System-Setup**-Programm zu beenden und die Konfiguration des **System-Setup**-Programms abzuschließen.

Serielle Remote-Zugriffs-Schnittstelle verwenden

Wenn eine serielle Verbindung mit dem RAC-Gerät aufgebaut wird, sind die folgenden Schnittstellen verfügbar:

- Serielle IPMI-Schnittstelle Siehe Serielle IPMI-Remote-Zugriffsschnittstelle verwenden.
- Serielle RAC-Schnittstelle

Serielle RAC-Schnittstelle

RAC unterstützt auch eine serielle Konsolenschnittstelle (oder *serielle RAC-Konsole*), die über eine RAC-CLI verfügt, die nicht durch IPMI definiert wird. Enthält Ihr System eine RAC-Karte mit aktivierter **serieller Konsole**, überschreibt die RAC-Karte die seriellen IPMI-Einstellungen und zeigt die serielle RAC-CLI-Schnittstelle an.

Setzen Sie zum Aktivieren der seriellen RAC-Terminalschnittstelle die Eigenschaft **cfgSerialConsoleEnable** auf **1** (TRUE).

Beispiel:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

Weitere Informationen finden Sie unter cfgSerialConsoleEnable (Lesen/Schreiben).

Tabelle 4-1 enthält die Einstellungen der seriellen Schnittstelle.

Tabelle 4-1. Einstellungen der seriellen Schnittstelle

IPMI-Modus	Serielle RAC-Konsole	Schnittstelle
Grundlegend	Deaktiviert	Grundlegender Modus
Grundlegend	Aktiviert	RAC-CLI
Terminal	Deaktiviert	IPMI-Terminalmodus
Terminal	Aktiviert	RAC-CLI

Linux während des Starts für die Umleitung der seriellen Konsole konfigurieren

Die folgenden Schritte beziehen sich speziell auf den Linux Grand Unified Bootloader (GRUB). Ähnliche Änderungen sind bei der Verwendung eines anderen Bootloaders erforderlich.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine korrekte Textanzeige sicherzustellen; andernfalls werden einige Textanzeigen möglicherweise unleserlich dargestellt.

Bearbeiten Sie die Datei **/etc/grub.conf** wie folgt:

1. Suchen Sie in der Datei die Abschnitte zur allgemeinen Einstellung und fügen Sie die folgenden zwei Zeilen hinzu:

   ```
   serial -unit=1 -speed=57600
   terminal -timeout=10 serial
   ```

2. Hängen Sie zwei Optionen an die Kernel-Zeile an:

   ```
   kernel ..... console=ttyS1,57600
   ```

3. Wenn **/etc/grub.conf** eine splashimage-Direktive enthält, kommentieren Sie sie aus.

Tabelle 4-2 enthält ein Beispiel einer **/etc/grub.conf**-Datei, die die in diesem Verfahren beschriebenen Änderungen zeigt.

Tabelle 4-2. Beispieldatei: /etc/grub.conf

```
# grub.conf generated by anaconda

#

# Note that you do not have to rerun grub after making changes

# to this file

# NOTICE: You do not have a /boot partition. This means that

# all kernel and initrd paths are relative to /, e.g.

# root (hd0,0)

# kernel /boot/vmlinuz-version ro root= /dev/sdal

# initrd /boot/initrd-version.img

#

#boot=/dev/sda

default=0

timeout=10

#splashimage=(hd0,2)/grub/splash.xpm.gz

serial -unit=1 -speed=57600
terminal -timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0 console=ttyS1,57600
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

Verwenden Sie bei der Verarbeitung der Datei **/etc/grub.conf** die folgenden Richtlinien:

1. Deaktivieren Sie die grafische GRUB-Schnittstelle und verwenden Sie die textbasierte Schnittstelle; andernfalls wird der GRUB-Bildschirm nicht in der RAC-Konsolenumleitung angezeigt. Zum Deaktivieren der grafischen Schnittstelle kommentieren Sie die Zeile aus, die mit splashimage beginnt.

2. Um GRUB-Optionen das Starten mehrerer Konsolensitzungen über die serielle RAC-Verbindung zu ermöglichen, fügen Sie die folgende Zeile zu allen Optionen hinzu:

   ```
   console=ttyS1,57600
   ```

   Tabelle 4-2 zeigt `console=ttyS1,57600` nur zur ersten Option hinzugefügt.

Anmeldung zur Konsole nach dem Start aktivieren

Bearbeiten Sie die Datei **/etc/inittab** wie folgt:

Fügen Sie eine neue Zeile hinzu, um agetty auf der seriellen COM2-Schnittstelle zu konfigurieren:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

Tabelle 4-3 zeigt eine Beispieldatei mit der neuen Zeile.

Tabelle 4-3. Beispieldatei: /etc/innitab

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

#          the system in a certain run-level.
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:

# 0 - halt (Do NOT set initdefault to this) # 1 - Single user mode

# 2 - Multiuser, without NFS (The same as 3, if n:
#   0 - Halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have

#       networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
```

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Bearbeiten Sie die Datei **/etc/securetty** wie folgt:

Fügen Sie eine neue Zeile mit dem Namen des seriellen tty für COM2 hinzu:

```
ttyS1
```

Tabelle 4-4 zeigt eine Beispieldatei mit der neuen Zeile.

Tabelle 4-4. 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-serielle / Telnet / SSH-Konsole aktivieren

Die serielle/Telnet/SSH-Konsole kann lokal oder im Remote-Zugriff aktiviert werden.

Serielle / Telnet / SSH-Konsole lokal aktivieren

ANMERKUNG: Zum Durchführen der Anweisungen in diesem Abschnitt benötigt der betreffende Benutzer die Berechtigung zum Konfigurieren von DRAC 5.

Geben Sie die folgenden lokalen RACADM-Befehle über eine Eingabeaufforderung ein, um die serielle/Telnet/SSH-Konsole vom verwalteten System aus zu aktivieren:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1

racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Serielle / Telnet / SSH-Konsole im Remote-Zugriff aktivieren

Geben Sie die folgenden Remote-**RACADM**-Befehle über eine Eingabeaufforderung ein, um die serielle/Telnet/SSH-Konsole im Remote-Zugriff zu aktivieren:

```
racadm -u <Benutzername> -p <Kennwort> -r <DRAC 5-IP-Adresse> config -g cfgSerial -o cfgSerialConsoleEnable 1

racadm -u <Benutzername> -p <Kennwort> -r <DRAC 5-IP-Adresse> config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm -u <Benutzername> -p <Kennwort> -r <DRAC 5-IP-Adresse> config -g cfgSerial -o cfgSerialSshEnable 1
```

ANMERKUNG: Wenn Sie den Internet Explorer Version 6 SP2 oder Version 7 verwenden, um sich am verwalteten System eines privaten Netzwerks anzumelden, jedoch keinen Zugriff auf das Internet haben, kann sich während der Verwendung von dezentralen RACADM-Befehlen eine Verzögerung von bis zu 30 Sekunden ergeben.

RACADM-Befehl für die Konfiguration der Einstellungen der seriellen und Telnet-Konsole verwenden

Dieser Unterabschnitt enthält Anweisungsschritte zum Konfigurieren der Standard-Konfigurationseinstellungen für die serielle und Telnet/SSH-Konsolenumleitung.

Geben Sie, um die Einstellungen zu konfigurieren, den RACADM-Befehl **config** mit der entsprechenden Gruppe, der entsprechenden Eigenschaft sowie den entsprechenden Eigenschaftswerten für die Einstellung, die Sie konfigurieren möchten, ein.

Sie können RACADM-Befehle lokal oder im Remote-Zugriff eingeben. Wenn Sie RACADM-Befehle im Remote-Zugriff verwenden, müssen Sie den Benutzernamen, das Kennwort sowie die DRAC 5-IP-Adresse des verwalteten Systems mit eingeben.

RACADM lokal verwenden

Geben Sie zur lokalen Eingabe von RACADM-Befehlen den folgenden Befehl über eine Eingabeaufforderung auf dem verwalteten System ein:

```
racadm config -g <Gruppe> -o <Eigenschaft> <Wert>
```

Geben Sie, um eine Liste der Eigenschaften anzuzeigen, den folgenden Befehl über eine Eingabeaufforderung auf dem verwalteten System ein:

```
racadm getconfig -g <Gruppe>
```

RACADM im Remote-Zugriff verwenden

Geben Sie, um RACADM-Befehle im Remote-Zugriff zu verwenden, den folgenden Befehl über eine Eingabeaufforderung auf einer Management Station ein:

```
racadm -u <Benutzername> -p <Kennwort> -r <DRAC 5-IP-Adresse> config -g <Gruppe> -o <Eigenschaft> <Wert>
```

Stellen Sie sicher, dass Ihr Web-Server mit einer DRAC 5-Karte konfiguriert ist, bevor Sie RACADM im Remote-Zugriff verwenden. Andernfalls überschreitet RACADM das Zeitlimit, und die folgende Meldung wird angezeigt:

```
Unable to connect to RAC at specified IP address. (Verbindung zu RAC konnte unter angegebener IP-Adresse nicht hergestellt werden.)
```

Geben Sie zum Aktivieren des Web-Servers mittels Secure Shell (SSH), Telnet oder lokalem RACADM den folgenden Befehl über eine Eingabeaufforderung auf einer Management Station ein:

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

Konfigurationseinstellungen anzeigen

Tabelle 4-5 enthält die Maßnahmen und die entsprechenden Befehle für die Anzeige der Konfigurationseinstellungen. Öffnen Sie zum Ausführen der Befehle auf dem verwalteten System eine Eingabeaufforderung. Geben Sie den Befehl ein, und drücken Sie die Eingabetaste.

Tabelle 4-5. Konfigurationseinstellungen anzeigen

Maßnahme	Befehl
Verfügbare Gruppen auflisten	racadm getconfig -h
Aktuelle Einstellungen für eine bestimmte Gruppe anzeigen	racadm getconfig -g *<Gruppe>* Beispiel: Geben Sie den folgenden Befehl ein, um eine Liste aller **cfgSerial**-Gruppeneinstellungen anzuzeigen: racadm getconfig-g cfgSerial
Zeigt die aktuellen Einstellungen für eine bestimmte Gruppe im Remote-Zugriff an	racadm -u *<Benutzer>* -p *<Kennwort>* -r *<DRAC 5-IP -Adresse>* getconfig -g cfgSerial Beispiel: Geben Sie Folgendes ein, um eine Liste aller Einstellungen für die **cfgSerial**-Gruppe im Remote-Zugriff anzuzeigen: racadm -u root -p calvin -r 192.168.0.1 getconfig -g cfgSerial

Telnet-Port-Nummer konfigurieren

Geben Sie den folgenden Befehl ein, um die Telnet-Port-Nummer für DRAC 5 zu ändern.

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <neue Anschlussnummer>
```

Verwenden einer seriellen Konsole oder Telnet- Konsole

Sie können die seriellen Befehle in Tabelle 4-19 im Remote-Zugriff mittels RACADM ausführen oder über die Eingabeaufforderung der seriellen/Telnet/SSH-Konsole.

An DRAC 5 anmelden

Melden Sie sich, unter Ausführung der folgenden Schritte, an DRAC 5 an, nachdem Sie Ihre Management Station-Terminalemulator-Software und das BIOS des verwalteten Knotens konfiguriert haben:

1. Stellen Sie unter Verwendung der Terminalemulations-Software der Management Station eine Verbindung zu DRAC 5 her.
2. Geben Sie Ihren DRAC 5-Benutzernamen ein, und drücken Sie auf die Eingabetaste.

   Sie sind jetzt an DRAC 5 angemeldet.

Textkonsole starten

Nachdem Sie sich über die Management Station-Terminal-Software mittels Telnet oder SSH an DRAC 5 angemeldet haben, können Sie die Textkonsole des verwalteten Systems umleiten, indem Sie den Telnet-/SSH-Befehl **connect com2** verwenden. Es wird nur jeweils ein einzelner **connect com2**-Client unterstützt.

Öffnen Sie, um eine Verbindung zur Textkonsole des verwalteten Systems herzustellen, eine DRAC 5-Eingabeaufforderung (wird über eine Telnet- oder SSH-Sitzung angezeigt), und geben Sie Folgendes ein:

```
connect com2
```

In einer seriellen Sitzung können Sie zur seriellen Konsole des verwalteten Systems eine Verbindung herstellen, indem Sie <Esc><Umsch><Q> drücken, wodurch die serielle Schnittstelle des verwalteten Systems direkt mit der COM2-Schnittstelle des Servers verbunden und DRAC 5 umgangen wird. Drücken Sie, um DRAC 5 wieder mit der seriellen Schnittstelle zu verbinden, <Esc><Umsch><9>. Die Baudraten der COM2-Schnittstelle des verwalteten Knotens und der seriellen DRAC 5-Schnittstelle müssen identisch sein.

Der Befehl `connect -h com2` zeigt den Inhalt des seriellen Verlaufspuffers an, bevor dieser auf Tastatureingaben oder neue Zeichen von der seriellen Schnittstelle wartet.

ANMERKUNG: Wird die Option **-h** verwendet wird, müssen der Client- und Server-Terminalemulationstyp (ANSI oder VT100) identisch sein, andernfalls könnte die Ausgabe entstellt sein. Setzen Sie außerdem die Client-Terminalzeilenanzahl auf **25**.

Die Standardgröße (bzw. maximale Größe) des Verlaufspuffers beträgt 8192 Zeichen. Sie können diese Zahl auf einen kleineren Wert einstellen, indem Sie den folgenden Befehl verwenden:

```
racadm config -g cfgSerial -o cfgSerialHistorySize <Zahl>
```

Seriellen Modus und Terminalmodus konfigurieren

IPMI und seriellen RAC konfigurieren

1. Erweitern Sie die **System** struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Seriell**.
3. Konfigurieren Sie die seriellen IPMI-Einstellungen.

   Eine Beschreibung der seriellen IPMI-Einstellungen ist unter Tabelle 4-6 verfügbar.
4. Konfigurieren Sie die seriellen RAC-Einstellungen.

   Eine Beschreibung der seriellen RAC-Einstellungen ist unter Tabelle 4-7 verfügbar.
5. Klicken Sie auf **Änderungen übernehmen**.
6. Klicken Sie auf der Seite **Serielle Konfiguration** auf die entsprechende Schaltfläche, um fortzufahren. Eine Beschreibung der Einstellungen für die Seite der seriellen Konfiguration ist unter Tabelle 4-8 verfügbar.

Tabelle 4-6. Serielle IPMI-Einstellungen

Einstellung	Beschreibung
Verbindungs-moduseinstellung	• Direktverbindung, grundlegender Modus - grundlegender serieller IPMI-Modus • Direktverbindung, Terminalmodus - serieller IPMI-Terminalmodus
Baudrate	Legt die Datengeschwindigkeit fest. Wählen Sie **9600 Bit/s**, **19,2 kBit/s**, **57,6 kBit/s** oder **115,2 kBit/s** aus.
Flusskontrolle	• Keine - Hardware-Datenflusssteuerung Aus • RTS/CTS – Hardware-Datenflusssteuerung Ein
Beschränkung der Kanalberechtigungs-ebene	• Administrator • Operator • Benutzer

Tabelle 4-7. Serielle RAC-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert die serielle RAC-Konsole. Markiert=Aktiviert; Unmarkiert=Deaktiviert
Maximale Sitzungen	Die maximale Anzahl gleichzeitiger Sitzungen, die für dieses System zulässig sind.

Zeitüberschreitung	Die maximale Leerlaufzeit (in Sekunden), bevor die Leitung getrennt wird. Der Bereich beträgt 60 bis 1920 Sekunden. Die Standardeinstellung beträgt 300 Sekunden. Wählen Sie 0 Sekunden, um die Zeitüberschreitungsfunktion zu deaktivieren.
Umleitung aktiviert	Aktiviert oder deaktiviert die Konsolenumleitung. Markiert=Aktiviert; Unmarkiert=Deaktiviert
Baudrate	Die Datengeschwindigkeit auf dem externen seriellen Anschluss. Die Werte betragen **9600 Bit/s**, **28,8 KBit/s**, **57,6 KBit/s** und **115,2 KBit/s**. Die Standardeinstellung ist **57,6 kBit/s**.
Escape-Taste	Gibt die <Esc>-Taste an. Die Standardeinstellung sind die Zeichen ^ \.
Größe Verlaufspuffer	Die Größe des seriellen Verlaufspuffers, der die letzten in die Konsole geschriebenen Zeichen enthält. Maximum und Standard = 8192 Zeichen.
Anmeldungsbefehl	Die auf die gültige Anmeldung hin auszuführende DRAC-Befehlszeile.

Tabelle 4-8. Einstellungen der Seite "Serielle Konfiguration"

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Serielle Konfiguration** aus.
Aktualisieren	Aktualisiert die Seite **Serielle Konfiguration**.
Änderungen übernehmen	Wendet die IPMI- und seriellen RAC-Änderungen an.
Terminalmodus-Einstellungen	Öffnet die Seite **Terminalmodus-Einstellungen**.

Terminalmodus konfigurieren

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Seriell**.
3. Klicken Sie auf der Seite **Serielle Konfiguration** auf **Terminalmodus- Einstellungen**.
4. Konfigurieren Sie die Terminalmodus-Einstellungen.

   Eine Beschreibung der Terminalmodus-Einstellungen finden Sie unter Tabelle 4-9.
5. Klicken Sie auf **Änderungen übernehmen**.
6. Klicken Sie auf der Seite **Terminalmodus-Einstellungen** auf die entsprechende Schaltfläche, um fortzufahren. Eine Beschreibung der Schaltflächen der Seite „Terminalmodus-Einstellungen" finden Sie unter Tabelle 4-10.

Tabelle 4-9. Terminalmodus-Einstellungen

Einstellung	Beschreibung
Zeilenbearbeitung	Aktiviert oder deaktiviert die Zeilenbearbeitung.
Löschsteuerung	Wählen Sie eine der folgenden Optionen: • **BMC gibt ein <Rückt><Leer><Rückt>-Zeichen aus, wenn <Rückt> oder <Entf> empfangen wird.** • **BMC gibt ein <Entf>-Zeichen aus, wenn <Rückt> oder <Entf> empfangen wird.**
Echo-Steuerung	Aktiviert oder deaktiviert Echo.
Handshaking-Steuerung	Aktiviert oder deaktiviert Handshaking.
Neue Zeilenreihenfolge	Wählen Sie **None**, **<CR-LF>**, **<NULL>**, **<CR>**, **<LF-CR>** oder **<LF>** aus.
Neue Zeilenreihenfolge eingeben	Wählen Sie **<CR>** oder **<NULL>** aus.

Tabelle 4-10. Schaltflächen der Seite Terminalmodus-Einstellungen

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Terminalmodus-Einstellungen** aus.
Aktualisieren	Aktualisiert die Seite **Terminalmodus-Einstellungen**.
Zurück zur Konfiguration der seriellen Schnittstelle	Kehrt zur Seite **Konfiguration des seriellen Anschlusses** zurück.
Änderungen übernehmen	Übernimmt die Änderungen der Terminalmodus-Einstellungen.

Verbindung zum verwalteten System über die lokale serielle Schnittstelle oder die Telnet- Management Station (Kundensystem) herstellen

Das verwaltete System ermöglicht eine Verbindung zwischen DRAC 5 und der seriellen Schnittstelle des Systems, damit Sie das verwaltete System einschalten, ausschalten oder zurücksetzen können und einen Zugriff auf Protokolle haben.

Die serielle Konsole ist über DRAC 5 am externen seriellen Anschluss des verwalteten Systems zugänglich. Es darf jeweils nur ein serielles Client-System (Management Station) aktiv sein. Die Telnet- und SSH-Konsolen sind an DRAC 5 über die DRAC-Modi verfügbar (siehe DRAC-Modi). Zu einem beliebigen Zeitpunkt können bis zu vier Telnet-Client-Systeme und vier SSH-Clients angeschlossen werden. Die Verbindung der Management Station zur seriellen Konsole oder Telnet-Konsole des verwalteten Systems erfordert die Terminalemulations-Software der Management Station. Weitere Informationen finden Sie unter Terminalemulationssoftware der Management Station konfigurieren.

Die folgenden Unterabschnitte beschreiben die Verbindung zwischen Management Station verwaltetem System mittels der folgenden Verfahren.

- Verwendung einer externen seriellen Schnittstelle des verwalteten Systems, der Terminal-Software und eines DB-9- oder Null-Modemkabels
- Verwendung der Telnet-Verbindung, der Terminal-Software über die DRAC 5-NIC des verwalteten Systems oder der freigegebenen Team-NIC

DB-9- oder Nullmodemkabel für die serielle Konsole anschließen

Um mit einer seriellen Textkonsole auf das verwaltete System zuzugreifen, schließen Sie ein DB-9-Nullmodemkabel an den COM-Anschluss auf dem verwalteten System an. Nicht alle DB-9-Kabel führen die Stiftbelegung/Signale, die für diese Verbindung erforderlich sind. Das DB-9-Kabel für diese Verbindung muss der in Tabelle 4-11 dargestellten Spezifikation entsprechen.

ANMERKUNG: Das DB-9-Kabel kann auch für die BIOS-Textkonsolenumleitung verwendet werden.

Tabelle 4-11. Erforderliche Stiftbelegung für das DB-9-Nullmodemkabel

Signalname	DB-9-Stift (Server-Stift)	DB-9-Stift (Workstation-Stift)
FG (Gehäusemasse)	-	-
TD (Daten senden)	3	2
RD (Daten empfangen)	2	3
RTS (Anforderung zu senden)	7	8
CTS (Sendebereitschaft)	8	7
SG (Betriebserde)	5	5
DSR (Datensatz bereit)	6	4
CD (Trägersignalerkennung)	1	4
DTR (Datenterminal bereit)	4	1 und 6

Terminalemulationssoftware der Management Station konfigurieren

DRAC 5 unterstützt eine serielle Konsole oder eine Telnet-Textkonsole einer Management Station, auf der eine der folgenden Arten von Terminalemulations-Software ausgeführt wird:

- Linux Minicom in einem Xterm
- Hilgraeve HyperTerminal Private Edition (Version 6.3)
- Linux Telnet in einem Xterm
- Microsoft Telnet

Um Ihre Art der Terminalsoftware zu konfigurieren, führen Sie die folgenden Schritte aus. Wenn Sie Microsoft Telnet verwenden, ist keine Konfiguration erforderlich.

Linux Minicom für die serielle Konsolenemulation konfigurieren

Minicom ist das Zugriffsdienstprogramm des seriellen Anschlusses für Linux. Die folgenden Schritte beziehen sich auf die Konfiguration der Minicom-Version 2.0. Andere Versionen von Minicom können geringfügig abweichen, erfordern jedoch die selben grundlegenden Einstellungen. Verwenden Sie die Informationen in Erforderliche Minicom-Einstellungen für die Emulation der seriellen Konsole zur Konfiguration anderer Minicom-Versionen.

Minicom Version 2.0 für die Emulation der seriellen Konsole konfigurieren

ANMERKUNG: Um sicherzustellen, dass der Text ordnungsgemäß angezeigt wird, empfiehlt Dell, dass Sie ein Xterm-Fenster zur Anzeige der Telnet-Konsole verwenden, statt der in der Linux-Installation enthaltenen Standardkonsole.

1. Um eine neue Xterm-Sitzung zu starten, geben Sie bei der Eingabeaufforderung `xterm &` ein.
2. Bewegen Sie im Xterm-Fenster den Mauspfeil in die untere rechte Ecke des Fensters, und ändern Sie die Größe des Fensters auf 80 x 25.
3. Wenn Sie keine Minicom-Konfigurationsdatei haben, fahren Sie mit dem nächsten Schritt fort.

   Wenn Sie eine Minicom-Konfigurationsdatei haben, geben Sie `minicom <Minicom Konfigurationsdateiname>` ein, und fahren Sie mit Schritt 17 fort.
4. Geben Sie an der Xterm-Eingabeaufforderung `minicom -s` ein.
5. Wählen Sie die Option **Seriellen Anschluss einrichten** aus und drücken Sie die Taste <Eingabe>.
6. Drücken Sie <a> und wählen Sie das entsprechende serielle Gerät (z. B. **/dev/ttyS0**) aus.
7. Drücken Sie <e>, und stellen Sie die Option **Bps/Par/Bits** auf **57600 8N1** ein.
8. Drücken Sie <f>, und stellen Sie die **Hardware-Datenflusssteuerung** auf **Ja** und die **Software-Datenflusssteuerung** auf **Nein** ein.
9. Um das Menü **Seriellen Anschluss einrichten** zu beenden, drücken Sie die Taste <Eingabe>.
10. Wählen Sie **Modem und Wählen** aus und drücken Sie die Taste <Eingabe>.
11. Drücken Sie im Menü **Modem-Wählen und Parameter-Setup** die <Rücktaste>, um die Einstellungen **init**, **reset**, **connect** und **hangup** zu löschen, sodass sie leer sind.
12. Drücken Sie die Eingabetaste, um jeden leeren Wert zu speichern.
13. Wenn alle angegebenen Felder gelöscht sind, drücken Sie die Taste <Eingabe>, um das Menü **Modem-Wählen und Parameter-Setup** zu beenden.
14. Wählen Sie **Setup als config_name speichern** aus und drücken Sie die Taste <Eingabe>.
15. Wählen Sie **Minicom beenden** aus und drücken Sie die Taste <Eingabe>.
16. Geben Sie bei der Befehls-/Shell-Eingabeaufforderung `minicom <Minicom Konfigurationsdateiname>` ein.
17. Um das Minicom-Fenster auf 80 x 25 zu erweitern, ziehen Sie an der Ecke des Fensters.
18. Drücken Sie <Strg+a>, <z>, <x>, um Minicom zu beenden.

ANMERKUNG: Wenn Sie Minicom für die serielle Textkonsolenumleitung verwenden, um das BIOS des verwalteten Systems zu konfigurieren, wird empfohlen, in Minicom die Farbeinstellung einzuschalten. Geben Sie zum Einschalten der Farbe den folgenden Befehl ein: minicom -c on<

Stellen Sie sicher, dass das Minicom-Fenster eine Eingabeaufforderung wie z. B. `[DRAC 5\root]#` anzeigt. Wenn die Eingabeaufforderung angezeigt wird, wurde Ihre Verbindung erfolgreich hergestellt, und Sie können jetzt mithilfe des seriellen Befehls **connect** eine Verbindung zur Konsole des verwalteten Systems herstellen.

Erforderliche Minicom-Einstellungen für die Emulation der seriellen Konsole

Verwenden Sie Tabelle 4-12 zum Konfigurieren einer beliebigen Minicom-Version.

Tabelle 4-12. Minicom-Einstellungen für die Emulation der seriellen Konsole

Beschreibung der Einstellung	Erforderliche Einstellung
Bit/s/Par/Bit	57600 8N1
Hardware-Datenflusssteuerung	Ja
Software-Datenflusssteuerung	Nein
Terminalemulation	ANSI
Einwahl per Modem und Parameter-Einstellungen	Löschen Sie die Einstellungen **init**, **reset**, **connect** und **hangup**, sodass sie leer sind
Fenstergröße	80 x 25 (um die Größe zu ändern, ziehen Sie die Ecke des Fensters)

HyperTerminal für die serielle Konsolenumleitung konfigurieren

HyperTerminal ist das Zugriffsdienstprogramm des seriellen Anschlusses von Microsoft Windows. Um die Größe Ihres Konsolenbildschirms angemessen einzustellen, verwenden Sie Hilgraeve HyperTerminal Private Edition, Version 6.3.

So konfigurieren Sie HyperTerminal für die serielle Konsolenumleitung:

1. Starten Sie das HyperTerminal-Programm.
2. Geben Sie einen Namen für die neue Verbindung ein und klicken Sie auf **OK**.
3. Wählen Sie neben **Verbindung herstellen mit:** den COM-Anschluss auf der Management Station (z. B. COM2) aus, an dem Sie das DB-9-Nullmodemkabel angeschlossen haben, und klicken Sie auf **OK**.
4. Konfigurieren Sie die Einstellungen des COM-Anschlusses wie unter Tabelle 4-13 gezeigt.
5. Klicken Sie auf **OK**.
6. Klicken Sie auf **Datei→ Eigenschaften** und dann auf das Register **Einstellungen**.
7. Stellen Sie die **Telnet-Terminal-ID:** auf **ANSI**.
8. Klicken Sie auf **Terminal-Setup** und stellen Sie die **Bildschirmzeilen** auf **26**.
9. Stellen Sie die **Spalten** auf **80** und klicken Sie auf **OK**.

Tabelle 4-13. Einstellungen des COM-Anschlusses der Management Station

Beschreibung der Einstellung	Erforderliche Einstellung
Bits pro Sekunde	57600
Datenbits	8
Parität	NONE
Stoppbits	1
Datenflusssteuerung	Hardware

Das HyperTerminal-Fenster zeigt eine Eingabeaufforderung wie z. B. `[DRAC 5\root]#` an. Ihre Verbindung wurde erfolgreich hergestellt, wenn die Eingabeaufforderung angezeigt wird, und Sie können jetzt mithilfe des seriellen Befehls **connect com2** eine Verbindung zur Konsole des verwalteten Systems herstellen.

Linux XTerm für die Umleitung der Telnet-Konsole konfigurieren

Verwenden Sie die folgenden Richtlinien, wenn Sie die Schritte in diesem Abschnitt ausführen:

- Stellen Sie, wenn Sie den Befehl **connect com2** zur Anzeige der System-Setup-Bildschirme über eine Telnet-Konsole verwenden, den Terminal-Typ im System-Setup und für die Telnet-Sitzung auf **ANSI** ein.
- Um sicherzustellen, dass der Text ordnungsgemäß angezeigt wird, empfiehlt Dell, dass Sie ein Xterm-Fenster zur Anzeige der Telnet-Konsole verwenden, statt der in der Linux-Installation enthaltenen Standardkonsole.

So führen Sie Telnet mit Linux aus:

1. Starten Sie eine neue Xterm-Sitzung.

   Geben Sie auf der Eingabeaufforderung `xterm &` ein.

2. Klicken Sie auf die untere rechte Ecke des XTerm-Fensters, und stellen Sie das Fenster auf 80 x 25 ein.
3. Stellen Sie zu DRAC 5 im verwalteten System eine Verbindung her.

   Geben Sie auf der Xterm-Eingabeaufforderung `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 auf ANSI-Modus ändern. Um dieses Verfahren im BIOS-Setup-Menü auszuführen, wählen Sie **Konsolenumleitung→ Remote-**

Terminaltyp→ ANSI aus.

1. Aktivieren Sie **Telnet** in den **Windows-Komponentendiensten**.
2. Stellen Sie auf der Management Station eine Verbindung zu DRAC 5 her.

   Öffnen Sie eine Eingabeaufforderung, geben Sie folgenden Befehl ein, und drücken Sie die Eingabetaste:

   `telnet <IP-Adresse>:<Anschlussnummer>`

   wobei *IP-Adresse* die IP-Adresse für den DRAC 5 ist und *Port-Nummer* die Telnet-Port-Nummer (wenn Sie ein neues Port verwenden).

Die Rücktaste für die Telnet-Sitzung konfigurieren

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

So konfigurieren Sie Microsoft-Telnet-Clients zur Verwendung der Rücktaste:

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

   `telnet`

   Drücken Sie, wenn eine Telnet-Sitzung ausgeführt wird, <Strg><]>.
3. Geben Sie in der Eingabeaufforderung Folgendes ein:

   `set bsasdel`

   Die folgende Meldung wird eingeblendet:

   Backspace will be sent as delete. (Rücktaste wird als Löschen gesendet.)

So konfigurieren Sie eine Linux-Telnet-Sitzung zur Verwendung der Rücktaste:

1. Öffnen Sie eine Eingabeaufforderung und geben Sie Folgendes ein:

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

   `telnet`

Verwenden einer seriellen Konsole oder Telnet- Konsole

Serielle Befehle, **Telnet**-Befehle und RACADM-CLI können auf einer seriellen Konsole oder Telnet-Konsole eingegeben und auf dem Server lokal oder im Remote-Zugriff ausgeführt werden. Die lokale RACADM-CLI wird für die ausschließliche Verwendung durch einen Root-Benutzer installiert.

Telnet mittels Windows XP oder Windows 2003 ausführen

Wenn Ihre Management Station 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 im Microsoft Knowledge Base-Artikel 824810.

Telnet mittels Windows 2000 ausführen

Wenn Ihre Management Station Windows 2000 ausführt, können Sie nicht mit der Taste <F2> auf das BIOS-Setup zugreifen. Verwenden Sie zum Beheben dieses Problems den Telnet-Client, der mit den Windows-Diensten für UNIX 3.5 geliefert wurde (empfohlener Gratis-Download von Microsoft). Rufen Sie **www.microsoft.com/downloads/** auf und suchen Sie nach *Windows-Dienste für UNIX 3.5*.

Secure Shell (SSH) verwenden

Es ist wichtig, dass die Geräte und die Geräteverwaltung des Systems sicher sind. Integrierte angeschlossene Geräte bilden den Kern vieler

Geschäftsprozesse. Werden diese Geräte gefährdet, kann dies gleichzeitig auch eine Gefährdung Ihres Geschäfts bedeuten, was neue Sicherheitsanforderungen an die Geräte-Verwaltungssoftware der Befehlszeilenoberfläche (CLI) stellt.

Secure Shell (SSH) ist eine Befehlszeilensitzung, die dieselben Fähigkeiten wie eine Telnet-Sitzung aufweist, jedoch mit verbesserter Sicherheit. DRAC 5 unterstützt SSH-Version 2 mit Kennwortauthentifizierung. SSH wird auf DRAC 5 aktiviert, wenn Sie Ihre DRAC 5-Firmware installieren oder aktualisieren.

Sie können entweder PuTTY oder OpenSSH auf der Management Station verwenden, um eine Verbindung zu DRAC 5 des verwalteten Systems# herzustellen. Wenn während des Anmeldungsverfahrens ein Fehler auftritt, gibt der Secure Shell-Client eine Fehlermeldung aus. Der Meldungstext ist vom Client abhängig und wird nicht von DRAC 5 gesteuert.

ANMERKUNG: OpenSSH sollte unter Windows von einem VT100 oder ANSI-Terminalemulator ausgeführt werden. Das Ausführen von OpenSSH mit der Windows-Eingabeaufforderung ergibt nicht die volle Funktionalität (einige Tasten reagieren nicht und es werden keine Grafiken angezeigt).

Es werden nur vier SSH-Sitzungen gleichzeitig unterstützt. Die Sitzungszeitüberschreitung wird durch die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert, wie unter Gruppen- und Objektdefinitionen der DRAC 5-Eigenschaftendatenbank beschrieben.

Geben Sie zum Aktivieren von SSH unter DRAC 5 Folgendes ein:

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Geben Sie zum Ändern des SSH-Anschlusses Folgendes ein:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <Schnittstellennummer>
```

Weitere Informationen zu den Eigenschaften `cfgSerialSshEnable` und `cfgRacTuneSshPort` finden Sie unter Gruppen- und Objektdefinitionen der DRAC 5-Eigenschaftendatenbank.

Die DRAC 5-SSH-Umsetzung unterstützt mehrfache Verschlüsselungs-Schemata, wie in Tabelle 4-14 dargestellt.

Tabelle 4-14. Verschlüsselungsschemata

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

ANMERKUNG: SSHv1 wird nicht unterstützt.

DRAC 5-Netzwerkeinstellungen konfigurieren

VORSICHTSHINWEIS: Durch Änderungen der DRAC 5-Netzwerkeinstellungen kann die aktuelle Netzwerkverbindung getrennt werden.

Konfigurieren Sie die DRAC 5-Netzwerkeinstellungen mithilfe eines der folgenden Hilfsprogramme:

- Webbasierte Schnittstelle – Siehe DRAC 5-NIC konfigurieren
- RACADM-CLI - siehe cfgLanNetworking
- Konfigurationsdienstprogramm zum Dell-Remote-Zugriff – sehen Sie System für die Verwendung von DRAC 5 konfigurieren

ANMERKUNG: Wird DRAC 5 in einer Linux-Umgebung eingesetzt, finden Sie entsprechende Informationen unter RACADM installieren.

Über ein Netzwerk auf DRAC 5 zugreifen

Nach der Konfiguration von DRAC können Sie im Remote-Zugriff mittels einer der folgenden Schnittstellen auf das verwaltete System zugreifen:

- Webbasierte Schnittstelle

- RACADM
- Telnet-Konsole
- SSH
- IPMI

Tabelle 4-15 beschreibt die einzelnen DRAC 5-Schnittstellen.

Tabelle 4-15. DRAC 5-Schnittstellen

Schnittstelle	Beschreibung
Webbasierte Schnittstelle	Ermöglicht den Remote-Zugriff auf DRAC 5 über eine graphische Benutzeroberfläche. Die Internet-basierte Schnittstelle ist in die DRAC 5-Firmware integriert. Der Zugriff erfolgt über die NIC-Schnittstelle von einem unterstützten Internet-Browser auf der Management Station aus. *Eine Liste der unterstützten Webbrowser finden Sie in der* Dell Systems Software Support Matrix auf der Dell Support-Website unter **support.dell.com / manuals**.

RACADM	Ermöglicht den Remote-Zugriff auf DRAC 5 mittels einer Befehlszeilenoberfläche. RACADM verwendet die IP-Adresse des verwalteten Systems, um RACADM-Befehle (racadm-Remote-Kapazitätsoption [-r]) auszuführen.
	
	ANMERKUNG: Die racadm-Remote-Kapazität wird nur auf Management Stations unterstützt.
	
	ANMERKUNG: Wenn Sie die racadm-Remote-Funktion verwenden, müssen Sie über Schreibberechtigung für die Ordner verfügen, in denen Sie **racadm**-Unterbefehle anwenden, die sich auf Dateivorgänge beziehen, wie z. B.:
	
	`racadm getconfig -f <Dateiname>`
	
	oder:
	
	`racadm sslcertupload -t 1 -f c:\cert\cert.txt Unterbefehle`

Telnet-Konsole	Ermöglicht den Zugriff auf DRAC 5 mittels des Server-RAC-Ports und Hardwareverwaltungs-Schnittstellen über die DRAC 5-NIC und bietet Unterstützung für serielle Befehle und RACADM-Befehle, einschließlich **powerdown**, **powerup**, **powercycle** und **hardreset**. **ANMERKUNG:** Telnet ist ein ungesichertes Protokoll, das alle Daten, einschließlich Kennwörtern, als unformatierten Text überträgt. Verwenden Sie bei Übertragung vertraulicher Informationen die SSH-Schnittstelle.
SSH-Schnittstelle	Bietet dieselben Fähigkeiten wie die Telnet-Konsole und verwendet eine verschlüsselte Transportschicht für höhere Sicherheit.
IPMI-Schnittstelle	Ermöglicht den Zugriff über DRAC 5 auf die grundlegenden Verwaltungsfunktionen des Remote-Systems. Die Schnittstelle umfasst IPMI-über-LAN, IPMI-über-Seriell und Seriell-über-LAN. Weitere Informationen finden Sie im *Benutzerhandbuch zum Dell OpenManage-Baseboard-Verwaltungs-Controller*.

ANMERKUNG: Der DRAC 5-Standardbenutzername lautet `root`, und das Standardkennwort `calvin`.

Sie können auf die Internet-basierte DRAC 5-Schnittstelle über den DRAC 5-NIC mittels eines unterstützten Internet-Browsers oder über Server Administrator oder IT Assistant zugreifen.

Eine Liste der unterstützten Webbrowser finden Sie in der Dell Systems Software Support Matrix auf der Dell Support-Website unter **support.dell.com / manuals**.

Starten Sie den Server Administrator für den Zugriff auf die DRAC 5-Remote-Zugriffs-Schnittstelle über den Server Administrator. Von der Systemstruktur im linken Fensterbereich der Server Administrator-Startseite klicken Sie auf **System**→ **Hauptsystemgehäuse**→ **Remote-Access-Controller**. Weitere Informationen finden Sie im Server Administrator-Benutzerhandbuch.

DRAC 5-NIC konfigurieren

Netzwerk- und IPMI-LAN-Einstellungen konfigurieren

ANMERKUNG: Zur Ausführung der folgenden Schritte müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

ANMERKUNG: Für die meisten DHCP-Server ist ein Server zum Speichern eines Client-Bezeichner-Tokens in der Reservierungstabelle erforderlich. Der Client (z. B. DRAC 5) muss dieses Token während der DHCP-Verhandlung zur Verfügung stellen. Für RACs stellt DRAC 5 die Client-Bezeichner-Option als eine Ein-Byte-Schnittstellennummer (0), gefolgt von einer Sechs-Byte-MAC-Adresse, zur Verfügung.

ANMERKUNG: Wurde DRAC auf dem verwalteten System für den Modus **Freigegeben** oder **Freigegeben mit Failover** konfiguriert und ist DRAC bei aktiviertem Spanning Tree Protocol (STP) an einen Schalter angeschlossen, werden Netzwerk-Clients eine 20 bis 30 Sekunden dauernde Verzögerung in der Konnektivität feststellen, wenn sich der LOM-Verknüpfungsstatus der Management Station während der STP-Konvergenz ändert.

1. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.

2. Klicken Sie auf die Registerkarte **Konfiguration**, und klicken Sie auf **Netzwerk**.

3. Konfigurieren Sie die DRAC 5-NIC-Einstellungen auf der Seite **Netzwerkkonfiguration**.

   Tabelle 4-16 und Tabelle 4-17 beschreibt die **Netzwerkeinstellungen** und **IPMI-Einstellungen** auf der Seite **Netzwerkkonfiguration**.

4. Wenn dies abgeschlossen ist, klicken Sie auf **Änderungen übernehmen**.

5. Klicken Sie auf der Seite **Netzwerkkonfiguration** auf die entsprechende Schaltfläche, um fortzufahren. Siehe Tabelle 4-18.

Tabelle 4-16. Netzwerkeinstellungen

Einstellung	Beschreibung
NIC-Auswahl	Zeigt den ausgewählten NIC-Modus an: (**Dediziert**, **Freigegeben mit Failover** oder **Freigegeben**). Die Standardeinstellung lautet **Dediziert**.
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 lautet **Aktiviert**.
DHCP verwenden (für die NIC-IP-Adresse)	Aktiviert den 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 Gateways** und der **statischen Subnetzmaske**. Die Standardeinstellung lautet **Deaktiviert**.
Statische IP-Adresse	Bestimmt oder bearbeitet die statische IP-Adresse für die DRAC 5-NIC. Entfernen Sie, um diese Einstellung zu ändern, die Markierung im Kontrollkästchen **DHCP (für NIC-IP-Adresse) verwenden**.
Statisches Gateway	Bestimmt oder bearbeitet den statischen Gateway für die DRAC 5-NIC. Entfernen Sie, um diese Einstellung zu ändern, die Markierung im Kontrollkästchen **DHCP (für NIC-IP-Adresse) verwenden**.
Statische Subnetzmaske	Bestimmt oder bearbeitet die statische Subnetzmaske für die DRAC 5-NIC. Entfernen Sie, um diese Einstellung zu ändern, die Markierung im Kontrollkästchen **DHCP (für NIC-IP-Adresse) verwenden**.
DHCP zum Abrufen von DNS-Serveradressen verwenden	Ruft die primären und sekundären DNS-Serveradressen vom DHCP-Server anstatt von den statischen Einstellungen ab. Die Standardeinstellung lautet **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 nur, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden nicht ausgewählt** ist. Sie können die IP-Adresse 0.0.0.0 eingeben, wenn Ihnen kein anderer DNS-Server zur Verfügung steht.
DRAC auf DNS registrieren	Registriert den DRAC 5-Namen auf dem DNS-Server. Die Standardeinstellung lautet **Deaktiviert**.
DNS-DRAC-Name	Zeigt den DRAC 5-Namen nur an, 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-Domänen-namen verwenden	Verwendet den Standard-DNS-Domänennamen. Ist das Kästchen nicht ausgewählt und wird die Option **DRAC 5 auf DNS registrieren** ausgewählt, können Sie den **DNS-Domänennamen** im Feld DNS-Domänenname ändern. Die Standardeinstellung lautet **Deaktiviert**.
DNS-Domänenname	Die Standardeinstellung des DNS-Domänennamens lautet **MYDOMAIN**. Ist das Kontrollkästchen **DHCP für DNS-Domänennamen verwenden** ausgewählt, können Sie dieses Feld nicht ändern, da es grau unterlegt ist.
Automatische Verhandlung	Bestimmt, ob DRAC 5 den **Duplexmodus** und die **Netzwerkgeschwindigkeit** durch Kommunikation mit dem am nächsten gelegenen Router oder Hub automatisch einstellt (**Ein**) oder Ihnen ermöglicht, den **Duplexmodus** und die **Netzwerkgeschwindigkeit** manuell einzustellen (**Aus**).
Netzwerkge-schwindigkeit	Stellt die Netzwerkgeschwindigkeit entsprechend der Netzwerkumgebung auf 100 MBit oder 10 MBit ein. Diese Option ist nicht verfügbar, wenn **Automatische Verhandlung** auf **Ein** eingestellt ist.
Duplexmodus	Stellt den Duplexmodus, entsprechend der Netzwerkumgebung, auf Voll oder Halb ein. Diese Option ist nicht verfügbar, wenn **Automatische Verhandlung** auf **Ein** eingestellt ist.

Tabelle 4-17. IPMI LAN-Einstellungen

Einstellung	Beschreibung
IPMI-über-LAN aktivieren	Aktiviert den IPMI-LAN-Kanal.
Beschränkung der Kanalberechtigungsebene	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.
Verschlüsselungs-schlüssel	Bestimmt das Verschlüsselungsschlüssel-Zeichenformat: 0 bis 20 Hexadezimalzeichen (keine Leerstellen erlaubt).

	Die Standardeinstellung lautet **0000000000000000000**.
VLAN-ID aktivieren	Aktiviert die VLAN-ID. Bei Aktivierung wird nur abgestimmter VLAN-ID-Verkehr akzeptiert.
VLAN-ID	Das VLAN-ID-Feld der 802.1g-Felder.
Priorität	Das Prioritätsfeld der 802.1g-Felder.

Tabelle 4-18. Schaltflächen der Seite „Netzwerkkonfiguration"

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Netzwerkkonfiguration** aus.
Aktualisieren	Lädt die Seite **Netzwerkkonfiguration** neu.
Erweiterte Einstellungen	Zeigt die Seite **Netzwerksicherheit** an.
Änderungen übernehmen	Speichert die an der Netzwerkkonfiguration vorgenommenen Änderungen. **ANMERKUNG:** Bei Änderungen der NIC-IP-Adresseneinstellungen werden alle Benutzersitzungen geschlossen, und Benutzer müssen mit den aktualisierten IP-Adresseneinstellungen eine neue Verbindung zur Internet-basierten DRAC 5-Schnittstelle aufbauen. Alle anderen Änderungen erfordern, dass die NIC zurückgesetzt wird, was einen kurzzeitigen Verlust der Konnektivität verursachen kann.

Weitere Informationen finden Sie unter Netzwerksicherheitseinstellungen mittels DRAC 5-GUI vornehmen.

RACADM im Remote-Zugriff verwenden

ANMERKUNG: Konfigurieren Sie die IP-Adresse Ihres DRAC 5, bevor Sie die racadm-Remote-Funktion verwenden. Weitere Informationen zum Setup von DRAC 5 sowie eine Liste diesbezüglicher Dokumente finden Sie unter Grundlegende Installation von DRAC 5.

RACADM bietet eine Remote-Funktionsoption (**-r**), mit der eine Verbindung zum verwalteten System hergestellt werden kann und **racadm**-Unterbefehle von einer Remote-Konsole oder einer Management Station aus ausgeführt werden können. Zur Anwendung der Remote-Funktion benötigen Sie einen gültigen Benutzernamen (Option **-u**) und ein gültiges Kennwort (Option **-p**) sowie die DRAC 5-IP-Adresse.

ANMERKUNG: Verfügt das System, von dem aus Sie auf das Remote-System zugreifen, über kein DRAC-Zertifikat in seinem standardmäßigen Zertifikatspeicher, wird beim Eingeben eines racadm-Befehls eine Meldung eingeblendet.

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors.
```

(Sicherheitswarnung: Zertifikat ist ungültig - Name auf Zertifikat ist ungültig oder stimmt nicht mit Standortnamen überein

Ausführung wird fortgesetzt. Verwenden Sie die Option -S für racadm, um die Ausführung bei zertifikatbezogenen Fehlern anzuhalten.)

racadm setzt die Ausführung des Befehls fort. Wenn Sie jedoch die Option –S verwenden, hält racadm die Ausführung des Befehls an und blendet die folgende Meldung ein:

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Racadm not continuing execution of the command.

EORROR: Unable to connect to RAC at specified IP address
```

(Sicherheitswarnung: Zertifikat ist ungültig - Name auf Zertifikat ist ungültig oder stimmt nicht mit Standortnamen überein

Racadm setzt die Ausführung des Befehls nicht fort.

FEHLER: Verbindung zu RAC konnte unter angegebener IP-Adresse nicht hergestellt werden.)

ANMERKUNG: Die racadm-Remote-Kapazität wird nur auf Management Stations unterstützt. Weitere Informationen befinden sich auf der Support-Matrix der Dell-Systemsoftware auf der Dell Support-Website unter support.dell.com/manuals.

ANMERKUNG: Wenn Sie die racadm-Remote-Fähigkeit verwenden, müssen Sie über Schreibberechtigungen für die Ordner verfügen, in denen Sie die racadm-Unterbefehle anwenden, die sich auf Dateivorgänge beziehen, wie z. B.:

```
racadm getconfig -f <Dateiname>

oder

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

RACADM Übersicht

```
racadm -r <RAC-IP-Adresse> -u <Benutzername> -p <Kennwort> <Unterbefehl> <Unterbefehl-Optionen>

racadm -i -r <RAC-IP-Adresse> <Unterbefehl> <Unterbefehl-Optionen>
```

Beispiel:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo

racadm -i -r 192.168.0.120 getsysinfo
```

Die folgende Syntax muss verwendet werden, wenn die HTTPS-Port-Nummer von RAC auf ein von dem Standard-Port (443) abweichendes anwendungsspezifisches Port geändert wird:

```
racadm -r <RAC IP Address>:<port> -u <username> -p <password> <subcommand> <subcommand options>

racadm -i -r <RAC IP Address>:<port> <subcommand> <subcommand options>
```

RACADM-Optionen

Tabelle 4-19 führt die Optionen für den **racadm**-Befehl auf.

Tabelle 4-19. racadm-Befehlsoptionen

Option	Beschreibung
-r <RAC-IP-Adr> **-r <RAC-IP-Adr>:<Anschlussnummer>**	Bestimmt die Remote-IP-Adresse des Controllers. Verwenden Sie *:<Port-Nummer>*, wenn die DRAC 5-Port-Nummer nicht die des Standard-Ports (443) ist.
-i	Weist **racadm** an, den Benutzer interaktiv nach dem Benutzernamen und dem Kennwort zu fragen.
-u <Benutzername>	Gibt den Benutzernamen an, der verwendet wird, um die Befehlstransaktion zu authentifizieren. Wenn die Option **-u** verwendet wird, muss auch die Option **-p** verwendet werden, wobei die Option **-i** (interaktiv) nicht zulässig ist.
-p <Kennwort>	Gibt das Kennwort an, das zur Authentifizierung der Befehlstransaktion verwendet wird. Wenn die Option **-p** verwendet wird, ist die Option **-i** nicht erlaubt.
-S	Legt fest, dass **racadm** auf ungültige Zertifikatfehler prüfen soll. **racadm** hält die Ausführung des Befehls unter Ausgabe einer Fehlermeldung an, wenn ein ungültiges Zertifikat ermittelt wird.

Die RACADM-Remote-Funktion aktivieren und deaktivieren

ANMERKUNG: Es wird empfohlen, diese Befehle auf Ihrem lokalen System auszuführen.

Die RACADM-Remote-Funktion ist standardmäßig aktiviert. Wenn deaktiviert, geben Sie den folgenden 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 4-20 enthält eine Beschreibung der einzelnen **racadm**-Unterbefehle, die Sie in RACADM ausführen können. Für eine ausführliche Auflistung von **RACADM**-Unterbefehlen einschließlich der Syntax und gültiger Einträge siehe Übersicht der RACADM-Unterbefehle.

Bei der Eingabe eines RACADM-Unterbefehls muss dem Befehl das Präfix `racadm` vorausgestellt werden. Beispiel:

```
racadm help
```

Tabelle 4-20. RACADM-Unterbefehle

Befehl	Beschreibung
Hilfe	Führt die DRAC 5-Unterbefehle auf.
Hilfe *<Unterbefehl>*	Listet die Verwendung für den angegebenen Unterbefehl auf.

arp	Zeigt den Inhalt der ARP-Tabelle an. Es dürfen keine ARP-Tabelleneinträge hinzugefügt oder gelöscht werden.
clearasrscreen	Löscht den letzten ASR-Bildschirm (Absturz, letzter blauer Bildschirm).
clrraclog	Löscht das 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, oder zeigt den Status der DRAC 5-Firmware-Aktualisierungen an.
getssninfo	Zeigt Informationen über aktive Sitzungen an.
getsysinfo	Zeigt allgemeine Informationen von DRAC 5 und des Systems an.
getractime	Zeigt die DRAC 5-Uhrzeit an.
ifconfig	Zeigt die aktuelle RAC-IP-Konfiguration an.
netstat	Zeigt die Routingtabelle und die aktuellen Verbindungen an.
ping	Überprüft, ob die Ziel-IP-Adresse von DRAC 5 aus mit dem aktuellen Routingtabelleninhalt 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	Gibt den DRAC 5-Status sowie Zustandsinformationen für das Debuggen aus.
racreset	Setzt DRAC 5 zurück.
racresetcfg	Setzt DRAC 5 auf die Standardkonfiguration zurück.
serveraction	Führt Energieverwaltungsvorgänge auf dem verwalteten System aus.
getraclog	Zeigt das RAC-Protokoll an.
clrsel	Löscht die Einträge des Systemereignisprotokolls.
gettracelog	Zeigt das DRAC 5-Ablaufverfolgungsprotokoll an. Bei Verwendung von -i zeigt der Befehl die Anzahl von Einträgen im DRAC 5-Ablaufverfolgungsprotokoll an.
sslcsrgen	Erstellt die SSL-CSR und lädt sie herunter.
sslcertupload	Lädt ein CA-Zertifikat oder Serverzertifikat zu DRAC 5 hoch.
sslcertdownload	Lädt ein Zertifizierungsstellenzertifikat (CA) herunter.
sslcertview	Zeigt ein CA-Zertifikat oder Serverzertifikat in DRAC 5 an.
sslresetcfg	Stellt das Webserverzertifikat mit den Werkseinstellungen wieder her und startet den Webbrowser neu.
testemail	Zwingt DRAC 5, eine Test-E-Mail über den DRAC 5-NIC zu senden, um die E-Mail-Konfiguration zu überprüfen.
testtrap	Zwingt DRAC 5, eine Test-SNMP-Trap über den DRAC 5-NIC zu senden, um die Trap-Konfiguration zu überprüfen.
vmdisconnect	Erzwingt das Schließen einer Verbindung des virtuellen Datenträgers.
vmkey	Setzt die virtuelle Flash-Größe auf die Standardgröße (16 MB) zurück.

Häufig gestellte Fragen zu RACADM-Fehlermeldungen

Nachdem (unter Verwendung des Befehls racadm racreset) ein DRAC 5-Reset ausgeführt wurde, gebe ich einen Befehl ein, worauf die folgende Meldung angezeigt 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 eingeben.

Wenn ich die racadm-Befehle und -Unterbefehle verwende, erhalte ich Fehlermeldungen, die ich nicht verstehe.

Bei der Verwendung von **racadm**-Befehlen und -Unterbefehlen können ein oder mehrere der folgenden Fehler auftreten:

- Lokale racadm-Fehlermeldungen – Probleme wie Syntax, typografische Fehler und falsche Namen.
- Fehlermeldungen zu Remote racadm – Probleme wie falsche IP-Adresse, falscher Benutzername oder falsches Kennwort.

Wenn ich die DRAC-IP-Adresse von meinem System aus pinge und meine DRAC 5-Karte dann während der Ping-Antwort zwischen den Modi Dediziert und Freigegeben umschaltet, erhalte ich keine Antwort.

Löschen Sie die ARP-Tabelle auf dem System.

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 auf eine

DRAC 5-Karte oder zu 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 z. B. die statische IP-Adresse), die vor dem Export der Datei auf anderen DRAC 5-Karten geändert werden müssen.

Führen Sie die folgenden Verfahren zur Konfiguration mehrerer DRAC 5-Karten aus:

1. Verwenden Sie RACADM, um den Ziel-DRAC 5 abzufragen, der die entsprechende Konfiguration enthält.

   ANMERKUNG: Die erstellte **.cfg**-Datei enthält keine Benutzerkennwörter.

   Öffnen Sie eine Eingabeaufforderung und geben Sie Folgendes ein:

   ```
   racadm getconfig-f myfile.cfg
   ```

   ANMERKUNG: Die Umleitung der RAC-Konfiguration in eine Datei unter Verwendung von **getconfig -f** wird nur bei den lokalen und Remote-RACADM-Schnittstellen unterstützt.

2. Ändern Sie die Konfigurationsdatei mit einem einfachen Texteditor (optional).

3. Verwenden Sie die neue Konfigurationsdatei, um einen Ziel-RAC zu ändern.

   Geben Sie bei der Eingabeaufforderung Folgendes ein:

   ```
   racadm config -f myfile.cfg
   ```

4. Setzen Sie den Ziel-RAC zurück, der konfiguriert wurde.

   Geben Sie bei der Eingabeaufforderung Folgendes ein:

   ```
   racadm reset
   ```

Der Unterbefehl **getconfig -f racadm.cfg** fordert die DRAC 5-Konfiguration an und erstellt die **racadm.cfg**-Datei. Die Datei kann, falls erforderlich, mit einem anderen Namen konfiguriert werden.

Sie können den Befehl **getconfig** dazu verwenden, die folgenden Maßnahmen auszuführen:

- Alle Konfigurationseigenschaften in einer Gruppe anzeigen (nach Gruppenname und -index)
- Alle Konfigurationseigenschaften für einen Benutzer nach Benutzernamen anzeigen

Mit dem Unterbefehl **config** werden die Informationen in andere DRAC 5 geladen. Verwenden Sie **config** zum Synchronisieren der Benutzer- und Kennwortdatenbank mit Server Administrator.

Die ursprüngliche Konfigurationsdatei, **racadm.cfg**, wird durch den Benutzer benannt. Im folgenden Beispiel trägt die Konfigurationsdatei den Namen **myfile.cfg**. Um diese Datei zu erstellen, geben Sie bei der Eingabeaufforderung Folgendes ein:

```
racadm getconfig-f myfile.cfg
```

VORSICHTSHINWEIS: Es wird empfohlen, diese Datei mit einem einfachen Texteditor zu bearbeiten. Das racadm-Dienstprogramm verwendet einen ASCII- Textparser, der keine Formatierungen erkennt und die RACADM-Datenbank beschädigen kann.

DRAC 5-Konfigurationsdatei erstellen

Die DRAC 5-Konfigurationsdatei **<***Dateiname***>.cfg** wird mit dem Befehl `racadm config -f <Dateiname>.cfg` verwendet. Sie können die Konfigurationsdatei zum Erstellen einer Konfigurationsdatei (ähnlich einer **.ini**-Date) verwenden und DRAC 5 mit dieser Datei konfigurieren. Sie können einen beliebigen Dateinamen verwenden und die Dateierweiterung **.cfg** ist nicht erforderlich (obwohl in diesem Teilabschnitt mit dieser Erweiterung auf die Datei Bezug genommen wird).

Die **CFG**-Datei kann:

- erstellt werden
- über den Befehl `racadm getconfig -f <Dateiname>.cfg` abgerufen werden
- über den Befehl `racadm getconfig -f <Dateiname>.cfg` abgerufen und dann bearbeitet werden

ANMERKUNG: Informationen zum Befehl **getconfig** finden Sie unter getconfig.

Die **CFG**-Datei wird zunächst geparst, um zu prüfen, ob gültige Gruppen und Objektnamen vorhanden sind und ob einige einfache Syntaxregeln befolgt werden. Fehler werden mit der Zeilennummer markiert, in der der Fehler erkannt wurde, und eine einfache Meldung beschreibt das Problem. Die vollständige Datei wird auf Richtigkeit geparst und alle Fehler werden angezeigt. Schreibbefehle werden nicht an DRAC 5 übertragen, wenn in der Datei **.cfg** ein Fehler festgestellt wird. Der Benutzer muss *alle* Fehler beheben, bevor eine Konfiguration vorgenommen werden kann. Die Option **-c** kann für den Unterbefehl **config** verwendet werden, wodurch nur die Syntax überprüft wird, jedoch *keine* Schreibvorgänge zu DRAC 5 vorgenommen werden.

Verwenden Sie die folgenden Richtlinien zum Erstellen einer **.cfg**-Datei:

- Wenn der Parser auf eine indizierte Gruppe trifft, ist der Wert des verankerten Objekts für die Unterscheidung der einzelnen Indizes ausschlaggebend.

Der Parser liest alle Indizes von DRAC 5 für diese Gruppe. Alle Objekte innerhalb dieser Gruppe sind einfache Änderungen, wenn DRAC 5 konfiguriert wird. Wenn ein geändertes Objekt einen neuen Index darstellt, wird der Index während der Konfiguration in DRAC 5 erstellt.

- In einer **.cfg**-Datei können Sie keinen Index Ihrer Wahl angeben.

  Indizes können erstellt und gelöscht werden, sodass die Gruppe im Laufe der Zeit über Fragmente verwendeter und nicht verwendeter Indizes verfügen kann. Wenn ein Index vorhanden ist, wird er modifiziert. Wenn kein Index vorhanden ist, wird der erste verfügbare Index verwendet. Diese Methode sorgt für Flexibilität, wenn indizierte Einträge hinzugefügt werden, wobei der Benutzer keine genauen Index-Übereinstimmungen zwischen allen verwalteten RACs vorzunehmen muss. Neue Benutzer werden dem ersten verfügbaren Index hinzugefügt. Eine **.cfg**-Datei, die unter DRAC 5 richtig geparst und ausgeführt wird, kann auf einem anderen möglicherweise nicht richtig ausgeführt werden, falls alle Indizes belegt sind und ein neuer Benutzer hinzugefügt werden muss.

- Verwenden Sie den Unterbefehl **racresetcfg**, um alle DRAC 5-Karten mit identischen Eigenschaften zu konfigurieren.

  Verwenden Sie den Unterbefehl **racresetcfg**, um DRAC 5 auf die ursprünglichen Standardeinstellungen zurückzusetzen, und führen Sie dann den Befehl `racadm config -f <Dateiname>.cfg` aus. Stellen Sie sicher, dass die **.cfg**-Datei alle erforderlichen Objekte, Benutzer, Indizes und anderen Parameter enthält.

VORSICHTSHINWEIS: 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 verfügbar ist, werden die Einstellungen anderer Benutzer ebenfalls auf die Standardeinstellungen zurückgesetzt.

Parsing-Regeln

- Alle Zeilen, die mit „#" beginnen, werden als Kommentare behandelt.

  Eine Kommentarzeile *muss* in Spalte 1 beginnen. Das Zeichen „#" in einer anderen Spalte wird als „#"-Zeichen behandelt.

  Einige Modemparameter können „#"-Zeichen in der Zeichenkette enthalten. Ein Escape-Zeichen ist nicht erforderlich. Sie können z. B. eine **.cfg**-Datei über einen `racadm getconfig -f <Dateiname>.cfg`-Befehl erstellen und dann einen `racadm config -f <Dateiname>.cfg`-Befehl auf einen anderen DRAC 5 anwenden, ohne Escape-Zeichen hinzuzufügen.

  Beispiel:

  ```
  #

  # Dies ist eine Anmerkung

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<Modem init # Dies ist kein Kommentar>
  ```

- Alle Gruppeneinträge müssen in **„[„** und **"]"**-Zeichen eingeschlossen sein.

  Das **„["**-Startzeichen, das einen Gruppennamen angibt, *muss* in Spalte 1 beginnen. Der Gruppenname *muss* vor allen anderen Objekten in dieser Gruppe angegeben werden. Objekte, die keinen zugewiesenen Gruppennamen enthalten, erzeugen Fehler. Die Konfigurationsdaten werden in Gruppen organisiert, wie unter Gruppen- und Objektdefinitionen der DRAC 5-Eigenschaftendatenbank definiert.

  Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objekts an.

  Beispiel:

  ```
  [cfgLanNetworking] -{Gruppenname}

  cfgNicIpAddress=143.154.133.121 {Objektname}
  ```

- Alle Parameter werden als „Objekt=Wert"-Paare ohne Leerzeichen zwischen „Objekt", „=" und „Wert" angegeben.

  Leerzeichen nach dem Wert werden ignoriert. Ein Leerzeichen innerhalb einer Wertezeichenkette bleibt unverändert. Jedes Zeichen rechts von '=' wird als solches betrachtet (zum Beispiel, ein zweites '=' oder ein '#', '[', ']' und so weiter). Bei diesen Zeichen handelt es sich um gültige Modemchat-Skriptzeichen.

  Siehe Beispiel unter vorherigem Punkt.

- Der **.cfg**-Parser ignoriert einen Index-Objekt-Eintrag.

  Benutzer können *nicht* angeben, welcher Index verwendet werden soll. Ist der Index bereits vorhanden, 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: Sie können eine indizierte Gruppe manuell mit folgendem Befehl erstellen: `racadm config-g <Gruppenname>-o <verankertes Objekt>-i <Index 1-16> <eindeutiger Ankername>`

- Die Zeile für eine indizierte Gruppe kann *nicht* aus einer **.cfg**-Datei gelöscht werden.

  Benutzer müssen ein indiziertes Objekt manuell mit folgendem Befehl entfernen:

  ```
  racadm config -g <Gruppenname> -o <Objektname> -i <Index 1-16> ""
  ```

  ANMERKUNG: Eine NULL-Zeichenkette (an zwei ""-Zeichen erkennbar) weist DRAC 5 an, den Index für die angegebene Gruppe zu löschen.

Um den Inhalt einer indizierten Gruppe anzuzeigen, verwenden Sie den folgenden Befehl:

```
racadm getconfig -g <Gruppenname> -i <Index 1-16>
```

- Für indizierte Gruppen *muss* es sich bei dem Objektanker um das erste Objekt nach dem „[ ]"-Paar handeln. Im Folgenden finden Sie Beispiele für aktuelle indizierte Gruppen:

```
[cfgUserAdmin]

cfgUserAdminUserName=<BENUTZERNAME>
```

Wenn Sie `racadm getconfig -f <MeinBeispiel>.cfg` eingeben, erstellt der Befehl eine **.cfg**-Datei für die aktuelle DRAC 5-Konfiguration. Diese Konfigurationsdatei kann als Beispiel und als Ausgangspunkt für Ihre eindeutige **.cfg**-Datei verwendet werden.

DRAC 5-IP-Adresse ändern

Wenn Sie die DRAC 5-IP-Adresse in der Konfigurationsdatei ändern, so entfernen Sie auch alle unnötigen **<***Variable***>**=**Wert**-Einträge. Es verbleibt lediglich die tatsächliche Bezeichnung der variablen Gruppe mit "[" und "]" zusammen mit den beiden **<***Variable***>**=**Wert**-Einträgen, die sich auf die IP-Adressenänderung beziehen.

Beispiel:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Die Datei wird wie folgt aktualisiert:

```
#

# 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 aktualisiert die entsprechenden Einträge. Außerdem kann derselbe **getconfig**-Befehl (siehe vorheriges Beispiel) zur Bestätigung der Aktualisierung verwendet werden.

Mit dieser Datei können Sie unternehmensweite Änderungen herunterladen oder neue Systeme über das Netzwerk konfigurieren.

ANMERKUNG: „Anchor" ist ein interner Ausdruck und darf nicht in der Datei verwendet werden.

DRAC 5-Netzwerkeigenschaften konfigurieren

Geben Sie Folgendes ein, um eine Liste verfügbarer Netzwerkeigenschaften zu erstellen:

```
racadm getconfig -g cfgLanNetworking
```

Wenn DHCP zur Ermittlung einer IP-Adresse verwendet werden soll, kann der folgende Befehl zum Schreiben des Objekts **cfgNicUseDhcp** und zum Aktivieren dieser Funktion verwendet werden:

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

Die Befehle bieten dieselbe Konfigurationsfunktionalität wie die Option ROM beim Systemstart, wenn Sie die Aufforderung erhalten, <Strg><e> zu drücken. Weitere Informationen zum Konfigurieren von 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: Wird **cfgNicEnable** auf **0** gesetzt, ist das DRAC 5-LAN selbst dann deaktiviert, wenn DHCP aktiviert ist.

DRAC-Modi

DRAC 5 kann für einen von drei Modi konfiguriert werden:

- Dediziert
- Freigegeben
- Freigegeben mit Failover

Tabelle 4-21 bietet eine Beschreibung der einzelnen Modi.

Tabelle 4-21. DRAC 5-NIC-Konfigurationen

Modus	Beschreibung
Dediziert	DRAC verwendet einen eigenen NIC (RJ-45-Anschluss) und die BMC-MAC-Adresse für den Netzwerkverkehr.
Freigegeben	DRAC verwendet Broadcom LOM1 auf dem Planar.
Freigegeben mit Failover	Der DRAC verwendet Broadcom LOM1 und LOM2 als Team für das Failover. Das Team verwendet die BMC-MAC- Adresse.

Häufig gestellte Fragen

Wenn ich auf die Internet-basierte DRAC 5-Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die besagt, dass der Host-Name des SSL-Zertifikats nicht mit dem Host-Namen von DRAC 5 übereinstimmt.

DRAC 5 enthält ein Standard-DRAC 5-Serverzertifikat zur Sicherung der Netzwerksicherheit für die Internet-basierte Schnittstelle und die Remote-racadm-Funktionen. Wird dieses Zertifikat verwendet, zeigt der Internet-Browser eine Sicherheitswarnung an, weil das Standardzertifikat an das **DRAC5-Standardzertifikat** ausgegeben wird, das nicht mit dem Host-Namen von DRAC 5 (z. B. der IP-Adresse) übereinstimmt.

Diese Sicherheitsbedenken können ausgeräumt werden, indem Sie ein an die IP-Adresse von DRAC 5 ausgegebenes DRAC 5-Serverzertifikat hochladen. Stellen Sie sicher, wenn Sie die zur Ausgabe des Zertifikats zu verwendende Zertifikatsignierungsanforderung (CSR) erstellen, dass der allgemeine Name (CN) der CSR der IP-Adresse von DRAC 5 (z. B. 192.168.0.120) oder dem eingetragenen DNS-DRAC-Namen entspricht.

So stellen Sie sicher, dass die CSR dem eingetragenen DNS-DRAC-Namen entspricht.

1. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.
2. Klicken Sie auf die Registerkarte **Konfiguration**, und klicken Sie auf **Netzwerk**.
3. Auf der Seite **Netzwerkeinstellungen**:
   a. Wählen Sie das Kontrollkästchen **DRAC auf DNS registrieren** aus.
   b. Geben Sie den DRAC-Namen in das Feld **DNS-DRAC-Name** ein.
4. Klicken Sie auf **Änderungen übernehmen**.

Weitere Informationen über die Erstellung von CSRs und über die Ausgabe von Zertifikaten finden Sie unter DRAC 5-Kommunikationen mit SSL- und digitalen Zertifikaten sichern.

Warum sind die Remote-RACADM- und Internet-basierten Dienste nach einer Eigenschaftsänderung nicht verfügbar?

Es kann eine Weile dauern, bis die Remote-RACADM-Dienste und die Internet-basierte Schnittstelle nach einem Reset des DRAC 5-Web Servers verfügbar sind.

Der DRAC 5-Web Server führt einen Reset nach den folgenden Ereignissen durch:

- Wenn die Netzwerkkonfiguration oder Netzwerk-Sicherheitseigenschaften mittels der DRAC 5-Internet-Benutzeroberfläche geändert werden
- Wenn die Eigenschaft **cfgRacTuneHttpsPort** geändert wird (einschließlich der Änderung durch eine config -f-<*Konfigurationsdatei*>)
- Wenn **racresetcfg** verwendet wird
- Wenn DRAC 5 zurückgesetzt wird
- Wenn ein neues SSL-Serverzertifikat hochgeladen wird

Warum registriert mein DNS-Server DRAC 5 nicht?

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

Wenn ich auf die DRAC 5-Internet-basierte Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die besagt, dass das SSL-Zertifikat durch eine nicht vertrauenswürdige Zertifizierungsstelle (CA) ausgegeben wurde.

DRAC 5 enthält ein Standard-DRAC 5-Serverzertifikat zur Sicherung der Netzwerksicherheit für die Internet-basierte Schnittstelle und die Remote-RACADM-Funktionen. Dieses Zertifikat wurde durch eine nicht zuverlässige CA ausgegeben. Diese Sicherheitsbedenken können ausgeräumt werden, indem Sie ein von einer vertrauenswürdigen CA (z. B. Thawte oder Verisign) ausgegebenes DRAC 5-Serverzertifikat hochladen. Weitere Informationen über die Ausgabe von Zertifikaten finden Sie unter DRAC 5-Kommunikationen mit SSL- und digitalen Zertifikaten sichern.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5-Benutzer hinzufügen und konfigurieren

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

RACADM-Dienstprogramm zur Konfiguration von DRAC 5-Benutzern verwenden

Erstellen Sie zur Verwaltung des Systems mit DRAC 5 und zur Aufrechterhaltung der Systemsicherheit eindeutige Benutzer mit spezifischen Verwaltungsberechtigungen (oder *rollenbasierter Autorität*). Für zusätzliche Sicherheit können Sie auch Warnungen konfigurieren, die spezifischen Benutzern per E-Mail geschickt werden, wenn ein bestimmtes Systemereignis vorkommt.

DRAC 5-Benutzer hinzufügen und konfigurieren:

ANMERKUNG: Zum Ausführen der folgenden Schritte müssen Sie über die Berechtigung zur Konfiguration von DRAC 5 verfügen.

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 die folgenden Informationen zu jedem Benutzer enthält: **Status**, **Benutzername, RAC-Berechtigung**, **IPMI-LAN-Berechtigung**, **serielle IPMI-Berechtigung** und **Seriell über LAN**.

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

4. Auf der Seite **Benutzerhauptmenü** können Sie Benutzer konfigurieren, ein Benutzerzertifikat hochladen, ein vorhandenes Benutzerzertifikat anzeigen, ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (CA) hochladen oder ein Zertifikat einer vertrauenswürdigen CA anzeigen.

   Wenn Sie **Benutzer konfigurieren** auswählen und auf **Weiter** klicken, wird die Seite Benutzerkonfiguration angezeigt. Weitere Informationen finden Sie unter Schritt 5.

   Sehen Sie Tabelle 5-1 für die Auswahl der Optionen unter dem Abschnitt **Smart Card-Konfiguration**.

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

   Tabelle 5-2 beschreibt die **Allgemeinen** Einstellungen zur Konfiguration eines neuen oder bestehenden DRAC-Benutzernamens und -Kennworts.

   Tabelle 5-3 beschreibt die **IPMI-Benutzerberechtigungen** zum Konfigurieren der LAN-Berechtigungen des Benutzers.

   Tabelle 5-4 beschreibt die **Benutzergruppen-Berechtigungen** für die Einstellungen der **IPMI-Benutzerberechtigungen** und der **DRAC-Benutzerberechtigungen**.

   Tabelle 5-5 beschreibt die **DRAC-Gruppen**berechtigungen. Wenn Sie für den Administrator, Hauptbenutzer oder Gastbenutzer eine DRAC-Benutzerberechtigung hinzufügen, wird die **DRAC-Gruppe** in eine **benutzerdefinierte** Gruppe geändert.

6. Wenn dies abgeschlossen ist, klicken Sie auf **Änderungen übernehmen**.

7. Klicken Sie auf der Seite **Benutzerkonfiguration** auf die entsprechende Schaltfläche, um fortzufahren. Siehe Tabelle 5-6.

Tabelle 5-1. Optionen im Abschnitt Smart Card-Konfiguration

Option	Beschreibung
Benutzerzertifikat hochladen	Ermöglicht Ihnen, das Benutzerzertifikat zu DRAC hochzuladen und es in das Benutzerprofil zu importieren.
Benutzerzertifikat anzeigen	Zeigt die Seite des Benutzerzertifikats an, die zu DRAC hochgeladen wurde.
Zertifikat der vertrauenswürdigen CA hochladen	Ermöglicht Ihnen, das Zertifikat der vertrauenswürdigen CA zu DRAC hochzuladen und dieses in das Benutzerprofil zu importieren.
Zertifikat der vertrauenswürdigen Zertifizierungsstelle anzeigen	Zeigt das Zertifikat der vertrauenswürdigen CA an, das zu DRAC hochgeladen wurde. Das Zertifikat der vertrauenswürdigen Zertifizierungsstelle wird von der Zertifizierungsstelle ausgestellt, die autorisiert ist, Zertifikate für Benutzer auszustellen.

Tabelle 5-2. 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 DRAC 5 zuzugreifen. Ist diese Option nicht markiert, kann der Benutzername nicht geändert werden.

Benutzername	Spezifiziert einen DRAC 5-Benutzernamen mit bis zu 16 Zeichen. Jeder Benutzer muss einen eindeutigen Benutzernamen besitzen. **ANMERKUNG:** Benutzernamen auf dem lokalen DRAC 5 dürfen die Zeichen **@ (at-Zeichen), \ (umgekehrter Schrägstrich), " (Anführungszeichen), /** (Schrägstrich) oder . (Punkt) nicht enthalten. **ANMERKUNG:** Wenn der Benutzername geändert wird, erscheint der neue Name erst bei der nächsten Benutzeranmeldung in der Benutzeroberfläche.
Kennwort ändern	Aktiviert die Felder **Neues Kennwort** und **Neues Kennwort bestätigen**. Wenn diese Option nicht markiert ist, kann das **Kennwort** des Benutzers nicht geändert werden.
Neues Kennwort	Legt das DRAC 5-Benutzerkennwort fest oder bearbeitet es.
Neues Kennwort bestätigen	Es ist erforderlich, dass Sie das Kennwort des DRAC 5-Benutzers nochmals eingeben, um es zu bestätigen.

Tabelle 5-3. IPMI-Benutzerberechtigungen

Eigenschaft	Beschreibung
Maximale LAN-Benutzerberechtigung gewährt	Legt die maximale Berechtigung des Benutzers auf dem IPMI-LAN-Kanal auf eine der folgenden Benutzergruppen fest: **Administrator**, **Operator**, **Benutzer** oder **Keine**.
Maximale serielle Schnittstellen-benutzerberechtigung gewährt	Legt die maximale Berechtigung des Benutzers auf dem seriellen IPMI-Kanal auf eine der folgenden Benutzergruppen fest: **Administrator**, **Operator**, **Benutzer** oder **Keine**.
Seriell über LAN aktivieren	Erlaubt dem Benutzer, IPMI Seriell über LAN zu verwenden. Mit einer Markierung versehen ist diese Berechtigung aktiviert.

Tabelle 5-4. DRAC-Benutzerberechtigungen

Eigenschaft	Beschreibung
DRAC-Gruppe	Legt die maximale Benutzerberechtigung als DRAC-Benutzer auf eine der folgenden Benutzergruppen fest: **Administrator**, **Hauptbenutzer**, **Gastbenutzer**, **Keine** oder **Benutzerdefiniert**. Informationen zu **DRAC-Gruppe**nberechtigungen finden Sie unter Tabelle 5-5.
Anmeldung an DRAC	Ermöglicht dem Benutzer, sich an DRAC anzumelden.
DRAC konfigurieren	Ermöglicht dem Benutzer die Konfiguration von DRAC.
Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern den Zugriff auf das System zu erlauben.
Protokolle löschen	Ermöglicht dem Benutzer das Löschen von DRAC-Protokollen.
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer die Ausführung von racadm-Befehlen.
Auf die Konsolenumleitung zugreifen	Ermöglicht dem Benutzer, die Konsolenumleitung auszuführen.
Zugriff auf virtuelle Datenträger	Ermöglicht dem Benutzer, virtuelle Datenträger auszuführen und zu verwenden.
Testwarnungen	Ermöglicht dem Benutzer, einem bestimmten Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Tabelle 5-5. DRAC-Gruppenberechtigungen

Benutzergruppe	Gewährte Berechtigungen
Administrator	**Anmeldung an DRAC**, **DRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Server-Steuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf virtuelle Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**.
Hauptbenutzer	**Anmeldung an DRAC**, **Protokolle löschen**, **Server-Steuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf virtuelle Datenträger**, **Testwarnungen**.
Gastbenutzer	Anmeldung an DRAC.
Custom (Benutzerdefiniert)	Auswahl einer beliebigen Kombination der folgenden Berechtigungen: **Anmeldung an DRAC**, **DRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Server-Maßnahmenbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf virtuelle Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**.
NONE	Keine zugewiesenen Berechtigungen.

Tabelle 5-6. Schaltflächen der Seite „Benutzerkonfiguration"

Schaltfläche	Maßnahme
Drucken	Druckt die Seite **Benutzerkonfiguration** aus.
Aktualisieren	Lädt die Seite **Benutzerkonfiguration** neu.
Zurück zur Benutzerseite	Wechselt zur **Benutzerseite** zurück.
Änderungen übernehmen	Speichert die an der Netzwerkkonfiguration vorgenommenen Änderungen.

RACADM-Dienstprogramm zur Konfiguration von DRAC 5-Benutzern verwenden

ANMERKUNG: Sie müssen als Benutzer **root** angemeldet sein, um RACADM-Befehle auf einem Remote-Linux-System ausführen zu können.

Die Internet-basierte DRAC 5-Schnittstelle bietet die schnellste Möglichkeit zur Konfiguration von DRAC 5. Wenn Sie Befehlszeilen- oder Skript-Konfigurationen bevorzugen oder mehrere DRAC 5 konfigurieren müssen, verwenden Sie RACADM, das mit den DRAC 5-Agents auf dem verwalteten System installiert ist.

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 Übersicht der RACADM-Unterbefehle beschrieben, und führen Sie unter Verwendung derselben Konfigurationsdatei den Unterbefehl **racadm config** auf den einzelnen verwalteten Systemen aus.

Bevor Sie beginnen

Sie können in der DRAC 5-Eigenschaften-Datenbank bis zu 16 Benutzer konfigurieren. Prüfen Sie, ob aktuelle Benutzer vorhanden sind, bevor Sie einen DRAC 5-Benutzer manuell aktivieren. Wenn Sie einen neuen DRAC 5 konfigurieren oder nach der Ausführung des Befehls **racadm racresetcfg** ist der einzige aktuelle Benutzer root mit dem Kennwort calvin. Der Unterbefehl **racresetcfg** setzt DRAC 5 auf die ursprünglichen Standardwerte zurück.

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

ANMERKUNG: Benutzer können im Laufe der Zeit aktiviert und deaktiviert werden. Infolgedessen kann ein Benutzer auf jedem DRAC 5 eine unterschiedliche Indexnummer besitzen.

Um nachzuprüfen, ob ein Benutzer existiert, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
racadm getconfig -u <Benutzername>
```

ODER

geben Sie den folgenden Befehl einmal für jeden Index von 1 - 16 ein:

```
racadm getconfig -g cfgUserAdmin -i <Index>
```

ANMERKUNG: Sie können auch racadm getconfig -f <myfile.cfg> eingeben und die Datei **myfile.cfg** anzeigen oder bearbeiten, die alle DRAC 5-Konfigurationsparameter enthält.

Mehrere Parameter und Objekt-IDs werden mit ihren aktuellen Werten angezeigt. Zwei Objekte von Bedeutung sind:

```
# cfgUserAdminIndex=XX

cfgUserAdminUserName=
```

Wenn das Objekt **cfgUserAdminUserName** keinen Wert besitzt, steht diese Indexnummer, die durch das Objekt **cfgUserAdminIndex** angezeigt wird, zur Verfügung. Wenn hinter dem "=" ein Name steht, wird dieser Index von diesem Benutzernamen verwendet.

ANMERKUNG: Wenn Sie einen Benutzer mit dem Unterbefehl **racadm config** manuell aktivieren oder deaktivieren, *muss* der Index mit der Option **-i** angegeben werden. Beachten Sie, dass das im vorherigen Beispiel gezeigte Objekt **cfgUserAdminIndex** ein „#"-Zeichen enthält. Wenn der Befehl **racadm config -f racadm.cfg** ferner zur Angabe einer beliebigen Anzahl von zu schreibenden Gruppen/Objekten verwendet wird, kann der Index nicht angegeben werden. Ein neuer Benutzer wird zum ersten verfügbaren Index hinzugefügt. Dieses Verhalten ermöglicht eine höhere Flexibilität bei der Konfiguration mehrerer DRAC 5 mit gleichen Einstellungen.

DRAC 5-Benutzer hinzufügen

Um der RAC-Konfiguration einen neuen Benutzer hinzuzufügen, können einige grundlegende Befehle verwendet werden. Führen Sie im Allgemeinen die folgenden Verfahren aus:

1. Legen Sie den Benutzernamen fest.
2. Legen Sie das Kennwort fest.
3. Legen Sie die Benutzerberechtigungen fest.

4. Aktivieren Sie den Benutzer.

Beispiel

Im folgenden Beispiel wird beschrieben, wie man einen neuen Benutzer namens „John" mit dem Kennwort „123456" und ANMELDE-Berechtigungen am RAC hinzufügt.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -i 2 -o cfgUserPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

Verwenden Sie zur Überprüfung einen der folgenden Befehle:

```
racadm getconfig -u john

racadm getconfig –g cfgUserAdmin –i 2
```

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 Befehlssyntax gezeigt, die zum Löschen eines RAC-Benutzers verwendet werden kann:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <Index> ""
```

Eine Null-Zeichenkette mit doppelten Anführungszeichen("") weist DRAC 5 an, die Benutzerkonfiguration am angegebenen Index zu entfernen und die Benutzerkonfiguration auf die ursprünglichen werksseitigen Standardeinstellungen zurückzusetzen.

E-Mail-Warnungen testen

Mit der RAC-E-Mail-Warnungsfunktion können Benutzer E-Mail-Warnungen erhalten, wenn auf dem verwalteten System ein kritisches Ereignis auftritt. Das folgende Beispiel zeigt, wie man die E-Mail-Warnungsfunktion testet, um sicherzustellen, dass der RAC ordnungsgemäß E-Mail-Warnungen über das Netzwerk versenden kann.

```
racadm testemail -i 2
```

ANMERKUNG: Stellen Sie sicher, dass die **SMTP**- und **E-Mail-Warnung**s-Einstellungen konfiguriert sind, bevor die E-Mail-Warnungsfunktion getestet wird. Weitere Informationen finden Sie unter E-Mail-Warnungen konfigurieren.

RAC-SNMP-Trap-Warnungsfunktion testen

Die RAC-SNMP-Trap-Warnungsfunktion ermöglicht SNMP-Trap-Listener-Konfigurationen, Traps für Systemereignisse zu empfangen, die auf dem verwalteten System auftreten.

Das folgende Beispiel veranschaulicht, wie ein Benutzer die SNMP-Trap-Warnungsfunktion des RAC testen kann.

```
racadm testtrap -i 2
```

Stellen Sie vor dem Testen der RAC-SNMP-Trap-Warnungsfunktion sicher, dass die SNMP- und Trap-Einstellungen ordnungsgemäß konfiguriert sind. Anleitungen zum Konfigurieren dieser Einstellungen finden Sie in den Unterbefehlsbeschreibungen **testtrap** und **testemail**.

DRAC 5-Benutzer mit Berechtigungen aktivieren

Um einen Benutzer mit spezifischen administrativen Berechtigungen (rollenbasierte Autorität) zu aktivieren, machen Sie zuerst einen verfügbaren Benutzer-Index ausfindig, indem Sie die Schritte unter Bevor Sie beginnen ausführen. Geben Sie dann die folgenden Befehlszeilen mit dem neuen Benutzernamen und dem neuen Kennwort ein:

ANMERKUNG: Unter Tabelle B-2 ist eine Liste gültiger Bitmaskenwerte für bestimmte Benutzerberechtigungen verfügbar. Der Standard-Berechtigungswert ist 0, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <Index> <Benutzerberechtigungs-Bitmaskenwert>
```

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

DRAC 5 mit Microsoft Active Directory verwenden

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Ein Verzeichnisdienst wird verwendet, um eine allgemeine Datenbank aller Informationen aufrechtzuerhalten, die erforderlich sind, um Benutzer, Computer, Drucker usw. auf einem Netzwerk zu steuern. Wenn Ihre Firma die Microsoft Active Directory Service-Software bereits verwendet, kann diese dahingehend konfiguriert werden, dass Sie Zugang zu DRAC 5 erhalten, wodurch Sie bestehenden Benutzern in der Active Directory-Software DRAC 5-Benutzerberechtigungen zuteilen und diese steuern können.

ANMERKUNG: Die Verwendung der Active Directory-Software zum Erkennen von iDRAC5-Benutzern wird von den Betriebssystemen Microsoft Windows 2000, Windows Server 2003 und Windows Server 2008 unterstützt.

Voraussetzungen für das Aktivieren von Active Directory-Authentifizierung für DRAC 5

Um die Active Directory-Authentifizierungsfunktion auf DRAC 5 verwenden zu können, müssen Sie bereits eine Active Directory-Infrastruktur bereitgestellt haben. Die DRAC 5-Active Directory-Authentifizierung unterstützt die Authentifizierung über verschiedene Strukturen einer einzelnen Gesamtstruktur hinweg. Informationen zur unterstützten Active Directory-Konfiguration in Hinblick auf Domänenfunktionsebene, Gruppen, Objekte usw. finden Sie unter Unterstützte Active Directory-Konfiguration.

Die Microsoft-Website enthält Informationen zum Einrichten einer Active Directory-Infrastruktur, falls Sie diese nicht schon haben.

DRAC 5 verwendet die standardmäßige PKI-Methode (Public Key Infrastructure - Infrastruktur des öffentlichen Schlüssels), um eine sichere Authentifizierung in das Active Directory herzustellen. Sie benötigen daher auch eine integrierte PKI für die Active Directory-Infrastruktur.

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

Um eine korrekte Authentifizierung zu allen Domänen-Controllern vornehmen zu können, müssen Sie auch die SSL-Verschlüsselung auf sämtlichen Domänen-Controllern aktivieren. Nähere Informationen finden Sie unter SSL auf einem Domänen-Controller aktivieren.

Unterstützte Active Directory- Authentifizierungsmechanismen

Sie können Active Directory anhand von zwei Verfahren zum Definieren des Benutzerzugriffs auf DRAC 5 verwenden: Sie können eine *Standardschema*-Lösung wählen, die nur Objekte der Active Directory-Gruppe verwendet, oder Sie können die Lösung des *erweiterten Schemas* verwenden, die Dell individuell eingerichtet hat, um von Dell definierte Active Directory-Objekte hinzuzufügen. Weitere Informationen zu diesen Lösungen sind in den nachfolgenden Abschnitten enthalten.

Wenn Sie das Active Directory verwenden, um den Zugriff auf DRAC 5 zu konfigurieren, müssen Sie entweder die Lösung des erweiterten Schemas oder des Standardschemas auswählen.

Die Vorteile bei der Verwendung der Standardschema-Lösung:

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

Die Vorteile bei der Verwendung des erweiterten Schemas sind:

- Alle Zugriffssteuerungsobjekte werden im Active Directory verwahrt.
- Maximale Flexibilität bei der Konfiguration des Benutzerzugriffs auf verschiedene DRAC 5-Karten mit unterschiedlichen Zugriffsstufen.

Übersicht des Standardschema-Active Directory

Wie in Abbildung 6-1 dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration sowohl von Active Directory als auch von DRAC 5. Auf der Seite des Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer mit DRAC 5-Zugriffsberechtigung ist ein Mitglied der Rollengruppe. Damit diesem Benutzer der Zugriff auf eine bestimmte DRAC 5-Karte erteilt werden kann, müssen der Rollengruppenname und sein Domänenname auf der bestimmten DRAC 5-Karte konfiguriert werden. Anders als bei der Lösung des erweiterten Schemas werden die Rolle und die Zugriffsstufe auf jeder einzelnen DRAC 5-Karte definiert und nicht im Active Directory. In jedem DRAC 5 können bis zu fünf Rollengruppen konfiguriert und definiert werden. Tabelle 6-12 zeigt die Zugriffsebene der Rollengruppen und Tabelle 6-1 die standardmäßigen Einstellungen der Rollengruppen.

Abbildung 6-1. Konfiguration von DRAC 5 mit Microsoft Active Directory und Standardschema

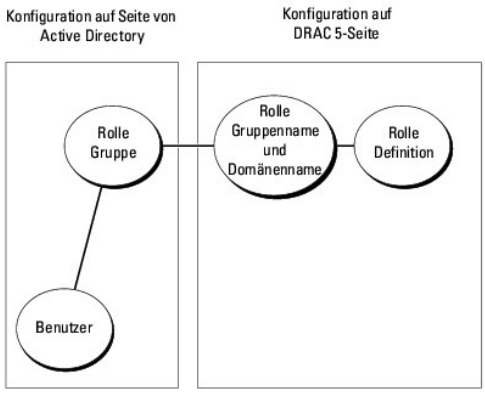


Tabelle 6-1. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppen	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
Rollengruppe 1	Administrator	Anmeldung an DRAC, DRAC konfigurieren, Benutzer konfigurieren, Protokolle löschen, Server-Steuerungsbefehle ausführen, Zugriff auf Konsolenumleitung, Zugriff auf Virtueller Datenträger, Testwarnungen, Diagnosebefehle ausführen	0x000001ff
Rollengruppe 2	Hauptbenutzer	Anmeldung an DRAC, Protokolle löschen, Server-Steuerungsbefehle ausführen, Zugriff auf Konsolenumleitung, Zugriff auf Virtueller Datenträger, Testwarnungen	0x000000f9
Rollengruppe 3	Gastbenutzer	Anmeldung an DRAC	0x00000001
Rollengruppe 4	NONE	Keine zugewiesenen Berechtigungen	0x00000000
Rollengruppe 5	NONE	Keine zugewiesenen Berechtigungen	0x00000000

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

Das Standardschema-Active Directory kann auf zwei Arten aktiviert werden:

- Mit der Internet-basierten DRAC 5-Benutzeroberfläche. Siehe Konfiguration von DRAC 5 mit dem Standardschema Active Directory und Internet-basierter Schnittstelle.
- Mit dem RACADM-CLI-Hilfsprogramm. Siehe Konfiguration von DRAC 5 mit Standardschema-Active Directory und RACADM.

Standardschema des Active Directory zum Zugriff auf DRAC 5 konfigurieren

Bevor ein Active Directory-Benutzer auf DRAC 5 zugreifen kann, müssen Sie die folgenden Schritte zum Konfigurieren des Active Directory ausführen:

1. Öffnen Sie auf einem Active Directory-Server (Domänen-Controller) das Active Directory-Benutzer- und -Computer-Snap-In.
2. Erstellen Sie eine Gruppe oder wählen Sie eine bestehende Gruppe aus. Der Name der Gruppe und der Name dieser Domäne müssen entweder über die Internet-basierte Schnittstelle oder mit RACADM auf DRAC 5 konfiguriert werden (sehen Sie Konfiguration von DRAC 5 mit dem Standardschema Active Directory und Internet-basierter Schnittstelle oder Konfiguration von DRAC 5 mit Standardschema-Active Directory und RACADM).
3. Fügen Sie den Active Directory-Benutzer als Mitglied der Active Directory-Gruppe hinzu, um den Zugriff auf DRAC 5 zu ermöglichen.

Konfiguration von DRAC 5 mit dem Standardschema Active Directory und Internet-basierter Schnittstelle

1. Öffnen Sie einen unterstützten Webbrowser.
2. Melden Sie sich bei der DRAC 5 Web-basierten Schnittstelle an.
3. Erweitern Sie die **System** struktur und klicken Sie auf **Remote-Zugriff**.
4. Klicken Sie auf das Register **Konfiguration**, und wählen Sie **Active Directory** aus.
5. Wählen Sie auf der Seite **Active Directory-Hauptmenü** die Option **Active Directory konfigurieren** aus, und klicken Sie auf **Weiter**.

6. Im Abschnitt Allgemeine Einstellungen:
   a. Wählen Sie das Kontrollkästchen **Active Directory aktivieren** aus.
   b. Geben Sie den **Root-Domänennamen** ein. Der **Root-Domänenname** ist der vollständig qualifizierte Root-Domänenname der Gesamtstruktur.
   c. Geben Sie die **Zeitüberschreitung** in Sekunden ein.
7. Klicken Sie im Abschnitt Active Directory-Schemaauswahl auf **Standardschema verwenden**.
8. Klicken Sie auf **Anwenden**, um die Active Directory-Einstellungen zu speichern.
9. Klicken Sie in der Spalte **Rollengruppen** des Abschnitts Standardschemaeinstellungen auf eine **Rollengruppe**.

   Die Seite **Rollengruppe konfigurieren** wird eingeblendet, die den **Gruppennamen**, die **Gruppendomäne** sowie die **Rollengruppenberechtigungen** einer Rollengruppe enthält.
10. Geben Sie den **Gruppennamen** ein. Der Gruppenname identifiziert die Rollengruppe im Active Directory, das mit der DRAC 5-Karte in Verbindung steht.
11. Geben Sie die **Gruppendomäne** ein. Die **Gruppendomäne** ist der vollständig qualifizierte root-Domänenname der Gesamtstruktur.
12. Richten Sie auf der Seite **Rollengruppenberechtigungen** die Gruppenberechtigungen ein.

    Tabelle 6-12 beschreibt die **Rollengruppenberechtigungen**.

    Tabelle 6-13 beschreibt die **Rollengruppenbefugnisse**. Wenn Sie eine Berechtigung modifizieren, wird die vorhandene **Rollengruppenberechtigung** (Administrator, Hauptbenutzer oder Gastbenutzer) auf Grundlage der modifizierten Berechtigungen entweder in eine benutzerdefinierte Gruppe oder in eine entsprechende Rollengruppenberechtigung geändert.
13. Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern.
14. Klicken Sie auf **Zurück zur Active Directory-Konfiguration und - Verwaltung**.
15. Klicken Sie auf **Zurück zum Active Directory Hauptmenü**.
16. Laden Sie das Stamm-CA-Zertifizierungsstellenzertifikat Ihrer Domäne in den DRAC 5 hoch.
    a. Wählen Sie das Kontrollkästchen **Active Directory- Zertifizierungsstellenzertifikat hochladen** aus, und klicken Sie dann auf **Weiter**.
    b. Geben Sie auf der Seite **Zertifikat hochladen** den Dateipfad des Zertifikats ein oder durchsuchen Sie die Zertifikatsdatei.

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

    Die SSL-Zertifikate der Domänen-Controller hätten von der Stamm-CA signiert worden sein sollen. Stellen Sie sicher, dass das Root-CA-Zertifikat auf der Management Station, die auf DRAC 5 zugreift, verfügbar ist (sehen Sie Stamm-CA-Zertifikat des Domänen-Controllers zu DRAC 5 exportieren).
    c. Klicken Sie auf **Anwenden**.

    Der DRAC 5-Web Server startet automatisch neu, nachdem Sie auf **Anwenden** klicken.
17. Melden Sie sich ab und dann bei DRAC 5 an, um die DRAC 5 Active Directory-Funktionskonfiguration abzuschließen.
18. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.
19. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**.

    Die Seite **Netzwerkkonfiguration** wird angezeigt.
20. Wenn **DHCP verwenden** (für NIC-IP-Adresse) unter **Netzwerkeinstellungen** ausgewählt ist, wählen Sie **DHCP zum Abrufen der DNS-Serveradresse verwenden** aus.

    Wählen Sie, um die IP-Adresse eines DNS-Servers manuell einzugeben, **DHCP zum Abrufen der DNS-Serveradressen verwenden** ab, und geben Sie die primäre und alternative IP-Adresse des DNS-Servers ein.
21. Klicken Sie auf **Änderungen übernehmen**.

    Die Konfiguration der Standardschema-Active Directory-Funktion von DRAC 5 wurde durchgeführt.

Konfiguration von DRAC 5 mit Standardschema-Active Directory und RACADM

Verwenden Sie die folgenden Befehle zur Konfiguration der Active Directory-Funktion von DRAC 5 mit Standardschema unter Verwendung der RACADM-CLI statt der Internet-basierten Schnittstelle.

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

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

   racadm config -g cfgActiveDirectory -o cfgADType 2

   racadm config -g cfgActiveDirectory -o cfgADRootDomain <vollständig qualifizierter root-Domänenname>

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

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

   racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupPrivilege <Bitmaskennummer für bestimmte Benutzerberechtigungen>

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

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

   ANMERKUNG: Sehen Sie Tabelle B-4 für Bitmasken-Zahlenwerte.

2. Geben Sie die folgenden racadm-Befehle ein, wenn DHCP auf DRAC 5 aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten:

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

3. Geben Sie die folgenden racadm-Befehle ein, wenn DHCP auf DRAC 5 deaktiviert ist oder Sie Ihre DNS-IP-Adresse manuell eingeben möchten:

   ```
   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>
   ```

Sie können an Stelle von DRAC 5, der nach Active Directory-Servern sucht, die Server angeben, mit denen DRAC 5 verbunden sein muss, um den Benutzer zu authentifizieren. Unter Server für Active Directory-Konfiguration angeben erhalten Sie Informationen zu RACADM-Befehlen zur Angabe von Servern.

Übersicht des Active Directory mit erweitertem Schema

Das Active Directory mit erweitertem Schema kann auf zwei Arten aktiviert werden:

- Mit der Internet-basierten DRAC 5-Benutzeroberfläche. Siehe Konfiguration von DRAC 5 über Active Directory mit erweitertem Schema und Internet-basierter Schnittstelle.
- Mit dem RACADM-CLI-Hilfsprogramm. Siehe Konfiguration von DRAC 5 über Active Directory mit erweitertem Schema und RACADM.

Active Directory-Schemaerweiterungen

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

Jedes Attribut bzw. jede Klasse, das/die zu einem vorhandenen Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert werden. Um branchenweit eindeutige IDs zu gewährleisten, unterhält Microsoft eine Datenbank von Active Directory-Objektbezeichnern (OIDs). Wenn also Unternehmen das Schema erweitern, sind diese Erweiterungen eindeutig und ergeben keine Konflikte. Um das Schema im Active Directory von Microsoft zu erweitern, erhielt Dell eindeutige OIDs, eindeutige Namenserweiterungen und eindeutig verlinkte Attribut-IDs für die Attribute und Klassen, die dem Verzeichnisdienst hinzugefügt werden.

Die Dell-Dateierweiterung lautet: dell

Die Dell Basis-OID lautet: 1.2.840.113556.1.8000.1280

Der RAC-LinkID-Bereich ist: 12070 bis 12079

Die von Microsoft aufrechterhaltene Active Directory-OID-Datenbank kann unter **http://msdn.microsoft.com/certification/ADAcctInfo.asp** eingesehen werden, indem Sie die Erweiterung Dell eingeben.

Übersicht der RAC-Schema-Erweiterungen

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

Geräten im Netzwerk, ohne zu viel Komplexität hinzuzufügen.

Active Directory - Objektübersicht

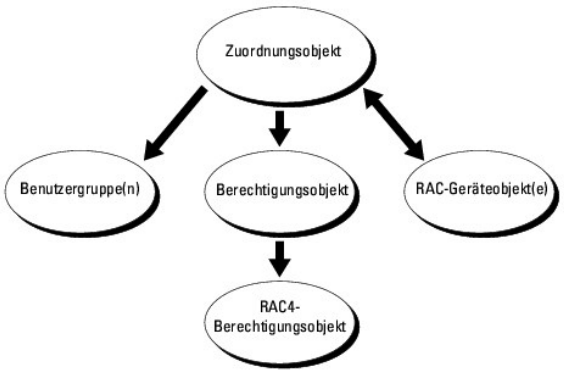
Für jedes der physischen RACs auf dem Netzwerk, das Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein RAC-Geräteobjekt erstellen. Sie können verschiedene Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt mit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

Jedoch kann jedes Zuordnungsobjekt nur mit einem Berechtigungsobjekt verknüpft werden bzw. darf jedes Benutzer-, Benutzergruppen- oder RAC-Geräteobjekt-Zuordnungsobjekt nur mit einem Berechtigungsobjekt verknüpft werden. Dieses Beispiel ermöglicht dem Administrator, die Berechtigungen jedes Benutzers für bestimmte RACs zu steuern.

Das RAC-Geräteobjekt ist die Verknüpfung zur RAC-Firmware für die Active Directory-Abfrage zur Authentifizierung und Autorisierung. Wird ein RAC zu einem Netzwerk hinzugefügt, muss der Administrator den RAC und sein Geräteobjekt mit seinem Active Directory-Namen konfigurieren, damit Benutzer mit dem Active Directory Authentifizierungen und Autorisierungen durchführen können. Der Administrator muss außerdem auch mindestens einen RAC zum Zuordnungsobjekt hinzufügen, damit Benutzer Authentifizierungen vornehmen können.

Abbildung 6-2 zeigt, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für die gesamte Authentifizierung und Autorisierung erforderlich ist.

Abbildung 6-2. Typisches Setup für Active Directory-Objekte



ANMERKUNG: Das RAC-Berechtigungsobjekt gilt für DRAC 4 und DRAC 5.

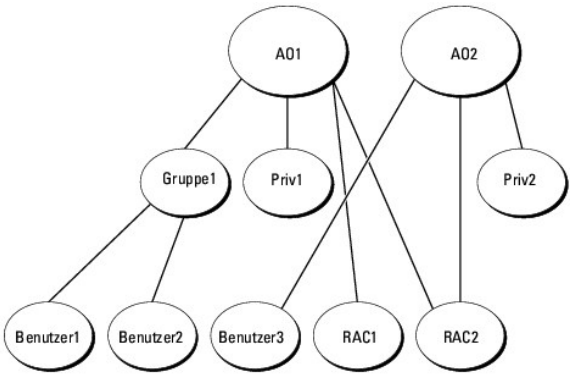
Sie können je nach Bedarf eine beliebige Anzahl von Zuordnungsobjekten erstellen. Jedoch müssen Sie mindestens ein Zuordnungsobjekt erstellen, und Sie müssen ein RAC-Geräteobjekt für jeden RAC (DRAC 5) im Netzwerk haben, das Sie mit Active Directory für die Authentifizierung und Autorisierung mit dem RAC (DRAC 5) integrieren möchten.

Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer und/oder Gruppen sowie RAC-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die „Benutzer", die „Berechtigungen" auf den RACs (DRAC 5s) haben.

Außerdem können Sie Active Directory-Objekte für eine einzelne Domäne oder in mehreren Domänen konfigurieren. Sie haben z. B. zwei DRAC 5-Karten (RAC1 und RAC2) und drei vorhandene Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Sie möchten Benutzer1 und Benutzer2 das Administratorrecht für beide DRAC 5-Karten erteilen und Benutzer3 eine Berechtigung für die Anmeldung an der RAC2-Karte. Abbildung 6-3 zeigt, wie Sie die Active Directory-Objekte in diesem Szenario einrichten können.

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

Abbildung 6-3. Active Directory-Objekte in einer einzelnen Domäne einrichten



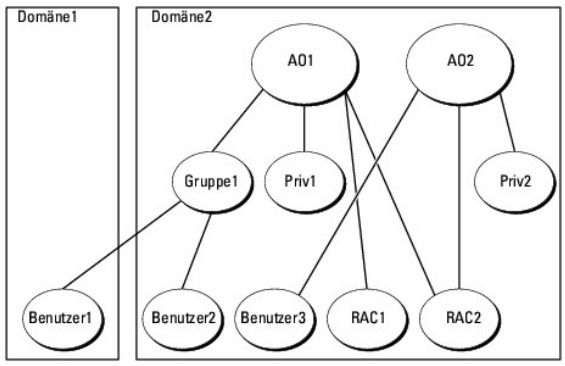
Führen Sie die folgenden Verfahren aus, um die Objekte für das Einzeldomänen-Szenario zu konfigurieren:

1. Erstellen Sie zwei Zuordnungsobjekte.
2. Erstellen Sie die beiden RAC-Geräteobjekte RAC1 und RAC2, die die zwei DRAC 5-Karten darstellen.
3. Erstellen Sie die beiden Berechtigungsobjekte Priv1 und Priv2, wobei Priv1 alle Berechtigungen (Administrator) und Priv2 Anmeldungsberechtigung besitzt.
4. Gruppieren Sie Benutzer1 und Benutzer2 in Gruppe1.
5. Fügen Sie Gruppe1 als Mitglieder in Zuordnungsobjekt 1 (AO1), Priv1 als Berechtigungsobjekte in AO1 und RAC1 und RAC2 als RAC-Geräte in AO1 hinzu.
6. Fügen Sie Benutzer3 als Mitglieder im Zuordnungsobjekt 2 (AO2), Priv2 als Berechtigungsobjekte in AO2 und RAC2 als RAC-Geräte in AO2 hinzu.

Detaillierte Anleitungen hierzu finden Sie unter DRAC 5-Benutzer und -Berechtigungen zum Active Directory hinzufügen.

Abbildung 6-4 enthält ein Beispiel von Active Directory-Objekten in mehreren Domänen. In diesem Fallbeispiel haben Sie zwei DRAC 5-Karten (RAC1 und RAC2) und drei vorhandene 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 Administratorrechten für beide DRAC 5-Karten und Benutzer3 mit der Berechtigung für die Anmeldung an der RAC2-Karte.

Abbildung 6-4. Active Directory-Objekte in mehreren Domänen einrichten



Führen Sie folgende Verfahren aus, um die Objekte für das Fallbeispiel mit mehreren Domänen zu konfigurieren:

1. Stellen Sie sicher, dass sich die Gesamtstrukturfunktion der Domäne im systemeigenen oder im Windows 2003-Modus befindet.
2. Erstellen Sie die beiden Zuordnungsobjekte AO1 (mit der Reichweite Universell) und AO2 in jeder Domäne.

   Abbildung 6-4 zeigt die Objekte in Domäne2.
3. Erstellen Sie die beiden RAC-Geräteobjekte RAC1 und RAC2, die die zwei DRAC 5-Karten darstellen.
4. Erstellen Sie die beiden Berechtigungsobjekte Priv1 und Priv2, wobei Priv1 alle Berechtigungen (Administrator) und Priv2 Anmeldungsberechtigung besitzt.
5. Gruppieren Sie Benutzer1 und Benutzer2 in Gruppe1. Die Gruppenreichweite von Gruppe1 muss universell sein.

6. Fügen Sie Gruppe1 als Mitglieder in Zuordnungsobjekt 1 (AO1), Priv1 als Berechtigungsobjekte in AO1 und RAC1 und RAC2 als RAC-Geräte in AO1 hinzu.

7. Fügen Sie Benutzer3 als Mitglieder im Zuordnungsobjekt 2 (AO2), Priv2 als Berechtigungsobjekte in AO2 und RAC2 als RAC-Geräte in AO2 hinzu.

Active Directory mit erweitertem Schema zum Zugriff auf DRAC 5 konfigurieren

Konfigurieren Sie die Active Directory-Software und den DRAC 5, indem Sie die folgenden Schritte der Reihenfolge nach ausführen, bevor Sie Active Directory verwenden, um auf DRAC 5 zuzugreifen:

1. Erweitern Sie das Active Directory-Schema (siehe Erweitern des Active Directory-Schemas).

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

3. Fügen Sie dem Active Directory die DRAC 5-Benutzer und ihre Berechtigungen hinzu (sehen Sie DRAC 5-Benutzer und -Berechtigungen zum Active Directory hinzufügen).

4. Aktivieren Sie SSL auf allen Domänen-Controllern (siehe SSL auf einem Domänen-Controller aktivieren).

5. Konfigurieren Sie die DRAC 5-Active Directory-Eigenschaften entweder unter Verwendung der Internet-basierten DRAC 5-Schnittstelle oder unter Verwendung von RACADM (sehen Sie Konfiguration von DRAC 5 über Active Directory mit erweitertem Schema und Internet-basierter Schnittstelle oder Konfiguration von DRAC 5 über Active Directory mit erweitertem Schema und RACADM).

Erweitern des Active Directory-Schemas

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

Sie können das Schema mit einer der folgenden Methoden erweitern:

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

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

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

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

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Files**. Zur Verwendung des Dell Schema Extender für Erweiterungen des Active Directory-Schemas siehe Dell Schema Extender verwenden.

Sie können Schema Extender oder die LDIF-Dateien an einem beliebigen Standort kopieren und ausführen.

Dell Schema Extender verwenden

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

1. Klicken Sie auf dem **Begrüßungsbildschirm** auf **Weiter**.

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

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

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

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

   Das Schema wird erweitert. Um die Schemaerweiterung zu überprüfen, verwenden Sie die Microsoft-Verwaltungskonsole (MMC) und das Active Directory-Schema-Snap-In, um das Vorhandensein folgender Elemente zu überprüfen:

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

Die Microsoft-Dokumentation enthält weitere Informationen über die Aktivierung und Anwendung des Active Directory Schema-Snap-In im MMC.

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

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabelle 6-3. dellRacDevice Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.1**
Beschreibung	Repräsentiert das Dell RAC-Gerät. Das RAC-Gerät muss als dellRacDevice im Active Directory konfiguriert werden. Mit dieser Konfiguration kann der DRAC 5 LDAP(Lightweight Directory Access Protocol)-Anfragen an das Active Directory senden.
Klassentyp	Strukturklasse
SuperClasses	dellProduct
Attribute	**dellSchemaVersion** **dellRacType**

Tabelle 6-4. dellAssociationObject Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.2**
Beschreibung	Repräsentiert das Dell-Zuordnungsobjekt. Das Zuordungsobjekt ist die Verbindung zwischen Benutzern und Geräten.
Klassentyp	Strukturklasse
SuperClasses	Gruppe
Attribute	**dellProductMembers** **dellPrivilegeMember**

Tabelle 6-5. dellRAC4Privileges Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
Beschreibung	Wird verwendet, um die Berechtigungen (Autorisierungsrechte) für das DRAC 5-Gerät zu definieren.
Klassentyp	Erweiterungsklasse
SuperClasses	NONE
Attribute	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Tabelle 6-6. dellPrivileges Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.4**
Beschreibung	Wird als Container-Klasse für die Dell-Berechtigungen (Autorisierungsrechte) verwendet.
Klassentyp	Strukturklasse
SuperClasses	Benutzer
Attribute	**dellRAC4Privileges**

Tabelle 6-7. dellProduct Class

OID	**1.2.840.113556.1.8000.1280.1.1.1.5**
Beschreibung	Die Hauptklasse, von der alle Dell-Produkte abgeleitet werden.
Klassentyp	Strukturklasse
SuperClasses	Computer
Attribute	**dellAssociationMembers**

Tabelle 6-8. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden

Attributname / Beschreibung	Zugewiesener OID / Syntax-Objektkennzeichner	Einzelbewertung
dellPrivilegeMember Die Liste von dellPrivilege-Objekten, die zu diesem Attribut gehören.	1.2.840.113556.1.8000.1280.1.1.2.1 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Die Liste von dellRacDevices-Objekten, die zu dieser Funktion gehören. Dieses Attribut ist die Vorwärtsverbindung zur dellAssociationMembers-Rückwärtsverbindung. Link-ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE, wenn der Benutzer Anmeldungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.3 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.4 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.5 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE, wenn der Benutzer Protokolllöschungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.7 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE, wenn der Benutzer Konsolenumleitungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.8 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE, wenn der Benutzer Rechte für den virtuellen Datenträger auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE, wenn der Benutzer Testwarnungsbenutzerrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.10 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE, wenn der Benutzer Debug-Befehl-Admin-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion Die aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren.	1.2.840.113556.1.8000.1280.1.1.2.12 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType	1.2.840.113556.1.8000.1280.1.1.2.13	TRUE

Dieses Attribut ist der Aktuelle RAC-Typ für das dellRacDevice-Objekt und die Rückwärtsverknüpfung zur dellAssociationObjectMembers-Vorwärtsverknüpfung.	Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
dellAssociationMembers Liste der dellAssociationObject Members, die diesem Produkt angehören. Dieses Attribut ist die Rückwärtsverknüpfung zum Attribut dellProductMembers. Link-ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch die Active Directory-Benutzer und das Computer-Snap-In erweitern, damit der Administrator RAC(DRAC 5)-Geräte, Benutzer und Benutzergruppen, RAC-Zuordnungen und RAC-Berechtigungen verwalten kann.

Wenn Sie die Systems Management-Software mit der DVD *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsverfahrens die Option **Dell-Erweiterung zum Snap-In von Active Directory-Benutzern und -Computern** auswählen. Das *Schnellinstallationshandbuch zu Dell OpenManage-Software* enthält zusätzliche Anleitungen zur Installation von Systemverwaltungssoftware.

Weitere Informationen über Active Directory-Benutzer und das Computer-Snap-In finden Sie in der Microsoft-Dokumentation.

Administratorpaket installieren

Sie müssen das Administratorpaket auf jedem System installieren, das Active Directory-DRAC 5-Objekte verwaltet. Wenn Sie das Administratorpaket nicht installieren, können Sie das Dell-RAC-Objekt nicht im Container anzeigen.

Weitere Informationen finden Sie unter Öffnen des Active Directory-Benutzer- und -Computer-Snap-In.

Öffnen des Active Directory-Benutzer- und -Computer-Snap-In

So öffnen Sie das Snap-In von Active Directory-Benutzern und -Computern:

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

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

   Die Microsoft-Verwaltungskonsole (MMC) wird eingeblendet.

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

3. Klicken Sie auf **Add/Remove Snap-in** (Snap-In hinzufügen/entfernen).

4. Wählen Sie das Snap-In von **Active Directory Users and Computers** (Active Directory-Benutzern und -Computern) und klicken Sie auf **Add** (Hinzufügen).

5. Klicken Sie auf **Schließen** und anschließend 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 die einzelnen Objekttypen hinzuzufügen, führen Sie folgende Verfahren durch:

- RAC-Geräteobjekt erstellen
- Erstellen eines Berechtigungsobjekts
- Erstellen eines Zuordnungsobjekts
- Einem Zuordnungsobjekt Objekte hinzufügen

RAC-Geräteobjekt erstellen

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

2. Wählen Sie **Neu→ Dell RAC-Objekt** aus.

   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 in Schritt a von Konfiguration von DRAC 5 über Active Directory mit erweitertem Schema und Internet-basierter Schnittstelle eingeben.

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

5. Klicken Sie auf **OK**.

Erstellen von Berechtigungsobjekten

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

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

2. Wählen Sie **Neu→ Dell RAC-Objekt** aus.

   Das Fenster **Neues Objekt** wird geöffnet.

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

4. Wählen Sie **Berechtigungsobjekt** aus.

5. Klicken Sie auf **OK**.

6. Klicken Sie mit der rechten Maustaste auf das Berechtigungsobjekt, das Sie erstellt haben, und wählen Sie **Eigenschaften** aus.

7. Klicken Sie auf das Register **RAC-Berechtigungen**, und wählen Sie die Berechtigungen aus, die der Benutzer erhalten soll (weitere Informationen finden Sie unter Tabelle 5-4).

Erstellen von Zuordnungsobjekten

Das Zuordnungsobjekt wird von einer Gruppe abgeleitet und muss einen Gruppentyp enthalten. Die Zuordnungsreichweite legt den Sicherheitsgruppentyp für das Zuordnungsobjekt fest. Wenn Sie ein Zuordnungsobjekt erstellen, müssen Sie die Zuordnungsreichweite wählen, die sich auf den Typ der Objekte bezieht, die hinzugefügt werden sollen.

Wird z. B. **Universal** ausgewählt, bedeutet dies, dass Zuordnungsobjekte nur verfügbar sind, wenn die Active Directory-Domäne im systemspezifischen Modus oder einem höheren Modus funktioniert.

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

2. Wählen Sie **Neu→ Dell RAC-Objekt** aus.

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

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

4. Wählen Sie **Zuordnungsobjekt**.

5. Wählen Sie den Wirkungsbereich für das **Zuordnungsobjekt**.

6. Klicken Sie auf **OK**.

Hinzufügen von Objekten zu einem Zuordnungsobjekt

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und RAC-Geräte oder RAC-Gerätegruppen zuordnen. Wenn das System Windows 2000 oder höher ausführt, müssen Sie Universal-Gruppen verwenden, damit sich Benutzer- oder RAC-Objekte über Domänen erstrecken.

Sie können Gruppen von Benutzern und RAC-Geräte hinzufügen. Die Verfahren zum Erstellen von Dell-bezogenen Gruppen und nicht-Dell-bezogenen Gruppen sind identisch.

Benutzer oder Benutzergruppen hinzufügen

1. Klicken Sie mit der rechten Maustaste auf das **Zuordnungsobjekt** und wählen Sie **Eigenschaften** aus.

2. Wählen Sie das Register **Benutzer** und klicken Sie auf **Hinzufügen**.

3. Geben Sie den Namen des Benutzers oder der Benutzergruppe ein und klicken Sie auf **OK**.

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

Berechtigungen hinzufügen

1. Wählen Sie das Register **Berechtigungsobjekt** und klicken Sie auf **Hinzufügen**.

2. Geben Sie den Berechtigungsobjektnamen ein und klicken Sie auf **OK**.

Klicken Sie auf das Register **Produkte**, um der Zuordnung ein oder mehrere RAC-Geräte hinzuzufügen. Die zugeordneten Geräte geben die an das Netzwerk angeschlossenen RAC-Geräte an, die für die festgelegten Benutzer oder Benutzergruppen verfügbar sind. Einem Zuordnungsobjekt können mehrere RAC-Geräte hinzugefügt werden.

RAC-Geräte oder RAC-Gerätegruppen hinzufügen

Um RAC-Geräte oder RAC-Gerätegruppen hinzufügen:

1. Wählen Sie das Register **Benutzer** und klicken Sie auf **Hinzufügen**.

2. Geben Sie den Namen des RAC-Geräts oder der RAC-Gerätegruppe ein und klicken Sie auf **OK**.

3. Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.

Konfiguration von DRAC 5 über Active Directory mit erweitertem Schema und Internet-basierter Schnittstelle

1. Öffnen Sie einen unterstützten Webbrowser.

2. Melden Sie sich bei der DRAC 5 Web-basierten Schnittstelle an.

3. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.

4. Klicken Sie auf das Register **Konfiguration**, und wählen Sie **Active Directory** aus.

5. Wählen Sie auf der Seite **Active Directory-Hauptmenü** die Option **Active Directory konfigurieren** aus, und klicken Sie auf **Weiter**.

6. Im Abschnitt Allgemeine Einstellungen:

   a. Wählen Sie das Kontrollkästchen **Active Directory aktivieren** aus.

   b. Geben Sie den **Root-Domänennamen** ein. Der **Root-Domänenname** ist der vollständig qualifizierte Root-Domänenname der Gesamtstruktur.

   c. Geben Sie die **Zeitüberschreitung** in Sekunden ein.

7. Klicken Sie im Abschnitt zur Auswahl des Active Directory-Schemas auf **Erweitertes Schema verwenden**.

8. Im Abschnitt Erweiterte Schemaeinstellungen:

   a. Geben Sie den **DRAC-Namen** ein. Dieser Name muss derselbe Name wie der allgemeine Name des neuen RAC-Objekts sein, das sie im Domänen-Controller erstellt haben (sehen Sie Schritt 3 von RAC- Geräteobiekt erstellen).

   b. Geben Sie den **DRAC-Domänennamen** ein (z. B. `drac5.com`). Verwenden Sie nicht den NetBIOS-Namen. Der **DRAC- Domänenname** ist der vollständig qualifizierte Domänenname der untergeordneten Domäne, in der sich das RAC-Geräteobjekt befindet.

9. Klicken Sie auf **Anwenden**, um die Active Directory-Einstellungen zu speichern.

10. Klicken Sie auf **Zurück zum Active Directory Hauptmenü**.

11. Laden Sie das Stamm-CA-Zertifizierungsstellenzertifikat Ihrer Domäne in den DRAC 5 hoch.

    a. Wählen Sie das Kontrollkästchen **Active Directory- Zertifizierungsstellenzertifikat hochladen** aus, und klicken Sie dann auf **Weiter**.

    b. Geben Sie auf der Seite **Zertifikat hochladen** den Dateipfad des Zertifikats ein oder durchsuchen Sie die Zertifikatsdatei.

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

Die SSL-Zertifikate der Domänen-Controller hätten von der Stamm-CA signiert worden sein sollen. Halten Sie das Stamm-CA-Zertifikat auf der Management Station, die auf den DRAC 5 zugreift, bereit (sehen Sie Stamm-CA-Zertifikat des Domänen-Controllers zu DRAC 5 exportieren).

c. Klicken Sie auf **Anwenden**.

Der DRAC 5-Web Server startet automatisch neu, nachdem Sie auf **Anwenden** klicken.

12. Melden Sie sich ab und dann bei DRAC 5 an, um die DRAC 5 Active Directory-Funktionskonfiguration abzuschließen.

13. Klicken Sie in der **System**struktur auf **Remote-Zugriff**.

14. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**.

Die Seite **Netzwerkkonfiguration** wird angezeigt.

15. Wenn **DHCP verwenden (für NIC-IP-Adresse) u**nter **Netzwerkeinstellungen** ausgewählt ist, wählen Sie **DHCP zum Abrufen der DNS-Serveradresse verwenden** aus.

Wählen Sie, um die IP-Adresse eines DNS-Servers manuell einzugeben, **DHCP zum Abrufen der DNS-Serveradressen verwenden** ab, und geben Sie die primäre und alternative IP-Adresse des DNS-Servers ein.

16. Klicken Sie auf **Änderungen übernehmen**.

Die Konfiguration der Funktion des DRAC 5-Active Directory mit erweitertem Schema wurde durchgeführt.

Konfiguration von DRAC 5 über Active Directory mit erweitertem Schema und RACADM

Verwenden Sie die folgenden Befehle zum Konfigurieren der Active Directory-Funktion von DRAC 5 mit erweitertem Schema unter Verwendung des RACADM-CLI-Dienstprogramms statt der Internet-basierten Schnittstelle.

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

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

racadm config -g cfgActiveDirectory -o cfgADType 1

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

      racadm config -g cfgActiveDirectory -o cfgADRootDomain <vollständig qualifizierter root-Domänenname>

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

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

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

2. Ist DHCP auf DRAC 5 aktiviert und möchten Sie den vom DHCP-Server bereitgestellten DNS verwenden, so geben Sie den folgenden racadm- Befehl ein:

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

3. Ist DHCP auf DRAC 5 deaktiviert oder möchten Sie Ihre DNS-IP-Adresse eingeben, so 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>
```

Drücken Sie auf **Eingabe**, um die DRAC 5-Active Directory-Funktionskonfiguration abzuschließen.

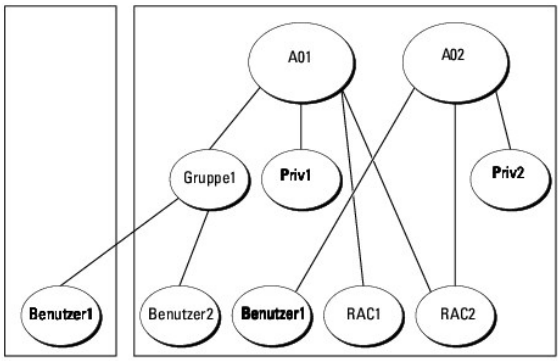
Sie können an Stelle von DRAC 5, der nach Active Directory-Servern sucht, die Server angeben, mit denen DRAC 5 verbunden sein muss, um den Benutzer zu authentifizieren. Unter Server für Active Directory-Konfiguration angeben erhalten Sie Informationen zu RACADM-Befehlen zur Angabe von Servern.

Unter Verwendung des erweiterten Schemas Berechtigungen ansammeln

Die Methode zur Authentifizierung des erweiterten Schemas unterstützt das Ansammeln von Berechtigungen über unterschiedliche Berechtigungsobjekte, die mit demselben Benutzer über verschiedene Zuordnungsobjekte in Verbindung stehen. Mit anderen Worten sammelt die Authentifizierung des erweiterten Schemas Berechtigungen an, um dem Benutzer den Supersatz aller zugewiesener Berechtigungen zu ermöglichen, die den verschiedenen, demselben Benutzer zugeordneten Berechtigungsobjekten entsprechen.

Abbildung 6-5 bietet ein Beispiel des Ansammelns von Berechtigungen unter Verwendung des erweiterten Schemas.

Abbildung 6-5. Ansammeln von Berechtigungen für einen Benutzer



Die Abbildung stellt zwei Zuordnungsobjekte dar – A01 und A02. Diese Zuordnungsobjekte können derselben Domäne oder unterschiedlichen Domänen zugehören. Benutzer1 wird über beide Zuordnungsobjekte mit RAC1 und RAC2 assoziiert. Benutzer1 hat daher Berechtigungen angesammelt, die sich aus der Kombination der für die Objekte Priv1 und Priv2 eingerichteten Berechtigungen zusammensetzen.

Beispiel: Priv1 hat die Berechtigungen Anmeldung, Virtueller Datenträger und Protokolle löschen, und Privr2 hat die Berechtigungen Anmeldung, DRAC konfigurieren und Testwarnmeldungen. Benutzer1 verfügt jetzt über den folgenden Berechtigungssatz: Anmeldung, Virtueller Datenträger, Protokolle löschen, DRAC konfigurieren und Testwarnmeldungen, was den kombinierten Berechtigungssatz von Priv1 und Priv2 darstellt.

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

Server für Active Directory-Konfiguration angeben

Wenn Sie ein LDAP, einen Server für den globalen Katalog oder eine Zuordnungsobjekt-Domäne (gilt nur für erweitertes Schema) angeben möchten, anstatt die Server zu verwenden, die vom DNS-Server zurückgegeben wurden, um nach einem Benutzernamen zu suchen, geben Sie den folgenden Befehl ein, um die Option **Server angeben** zu aktivieren:

```
racadm config -g cfgActive Directory -o cfgADSpecifyServer Enable 1
```

ANMERKUNG: Wenn Sie diese Option verwenden, wird der Hostname im CA-Zertifikat nicht mit dem Namen des angegebenen Servers verglichen. Dies ist besonders hilfreich, wenn Sie ein DRAC-Administrator sind, da Ihnen ermöglicht wird, sowohl einen Hostnamen als auch eine IP-Adresse einzugeben.

Nachdem Sie die Option **Server angeben** aktiviert haben, können Sie einen LDAP-Server oder einen Server für den globalen Katalog mit einer IP-Adresse oder einem vollständig qualifizierten Domänennamen (FQDN) des Servers angeben. Der FQDN besteht aus dem Hostnamen und dem Domänennamen des Servers.

ANMERKUNG: Wenn Sie die Active Directory-Authentifizierung auf Grundlage von Kerberos verwenden, geben Sie nur den FQDN des Servers an. Das Angeben der IP-Adresse wird nicht unterstützt. Weitere Informationen finden Sie unter Kerberos-Authentifizierung aktivieren.

Geben Sie zum Bestimmen eines LDAP-Servers unter Verwendung der Befehlszeilenschnittstelle (CLI) Folgendes ein:

```
racadm config -g cfgActive Directory -o cfgADDomainController <vollständig qualifizierter Domänenname oder IP-Adresse>
```

Geben Sie zum Bestimmen eines Servers für den globalen Katalog unter Verwendung der Befehlszeilenschnittstelle (CLI) Folgendes ein:

```
racadm config -g cfgActive Directory -o cfgGlobalCatalog <vollständig qualifizierter Domänenname oder IP-Adresse>
```

Um eine Zuordnungsobjektdomäne (gilt nur für erweitertes Schema) unter Verwendung der CLI festzulegen, geben Sie Folgendes ein:

```
racadm config -g cfgActive Directory -o cfgAODomain <Domain>:<vollständig qualifizierter Domänenname oder IP-Adresse>
```

wobei <Domäne> die Domäne ist, in der sich das Zuordnungsobjekt befindet und IP/FQDN die IP-Adresse oder der FQDN des bestimmten Hosts (Domänen-Controller der Domäne), zu DRAC 5 eine Verbindung herstellt.

Stellen Sie bei der Angabe des Zuordnungsobjekts sicher, dass Sie auch die IP-Adresse oder den FQDN für den globalen Katalog angeben.

ANMERKUNG: Wenn Sie als IP-Adresse 0.0.0.0 angeben, wird DRAC 5 nicht nach einem Server suchen.

Sie können eine Liste von LDAPs, Servern für den globalen Katalog oder Zuordnungsobjekte angeben, indem Sie ein Kommatrennungsformat anwenden. Mit DRAC 5 können Sie bis zu vier IP -Adressen oder Hostnamen angeben.

Wenn LDAPS nicht für alle Domänen und Anwendungen korrekt konfiguriert ist, kann seine Aktivierung während des Funktionierens der vorhandenen Anwendungen/Domänen zu unerwarteten Ergebnissen führen.

Für das erweiterte Schema können Sie entweder den Domänen-Controller oder den globalen Katalog mit Zuordnungsobjekt angeben. Nur den globalen Katalog oder nur das Zuordnungsobjekt anzugeben, ist für das erweiterte Schema nicht möglich. Wenn Sie nur den Domänen-Controller angeben, müssen sich alle Objekte (einschließlich Benutzer, Gruppe, RAC, Berechtigung und Zuordnung) in der gleichen Domäne befinden. Verwenden Sie die Option für den globalen Katalog mit der Option des Zuordnungsobjekts, wenn sich eines dieser Objekte in einer anderen Domäne befinden sollte. Es können bis zu vier Domänen-Controller angegeben werden. Alle diese Einträge müssen auf die gleiche Domäne verweisen. Es können bis zu vier Server für den globalen Katalog angegeben werden. Es können bis zu vier Zuordnungsobjektserver angegeben werden. Alle diese Einträge müssen auf die gleiche Domäne verweisen. Falls

Sie die Zuordnungsobjektoption verwenden, müssen Sie auch die Option für den globalen Katalog konfigurieren, damit eine Anmeldung möglich ist. Geben Sie den Namen des Domänen-Controllers ein, bei dem Sie den Benutzer erstellt haben. Es kann hier eine IP oder FQDN angegeben werden.

Geben Sie für das Standardschema nur den Domänen-Controller und den globalen Katalog an. Die Angabe eines Zuordnungsobjekts ist beim Standardschema nicht möglich. Sie können den Domänen-Controller angeben, auf dem die Benutzerrollengruppen erstellt werden. Geben Sie entweder die IP oder den FQDN an. Es können bis zu vier Domänen-Controller angegeben werden. Alle diese Einträge müssen auf die gleiche Domäne verweisen. Wenn Sie nur den Domänen-Controller angeben, müssen sich der Benutzer und die Gruppe in der gleichen Domäne befinden. Wenn sich die Rollengruppen in unterschiedlichen Domänen befinden, müssen Sie auch den Server für den globalen Katalog angeben. Es können bis zu vier Server für den globalen Katalog angegeben werden. Hier kann die IP oder der FQDN angegeben werden. Sie können außerdem nur die Server für den globalen Katalog angeben.

Active Directory-Zertifikate konfigurieren und verwalten

Zugriff auf das Active Directory-Hauptmenü:

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 6-9 führt die Optionen der Seite **Active Directory-Hauptmenü** auf.

Tabelle 6-9. Optionen der Hauptmenüseite des Active Directory

Feld	Beschreibung
Active Directory konfigurieren	Konfiguriert den DRAC-Namen, den ROOT-Domänennamen, den DRAC-Domänennamen, die Active Directory-Authentifizierungs-Zeitüberschreitung, die Active Directory-Schemaauswahl und die Rollengruppeneinstellungen des Active Directory.
Active Directory-CA-Zertifikat hochladen	Lädt ein Active Directory-Zertifikat zu DRAC hoch.
DRAC-Serverzertifikat herunterladen	Der Windows-Download-Manager ermöglicht, ein DRAC-Serverzertifikat auf das System herunterzuladen.
Active Directory-CA-Zertifikat anzeigen	Zeigt das Active Directory-Zertifikat an, das zu DRAC hochgeladen wurde.

Active Directory konfigurieren (Standardschema und erweitertes Schema)

1. Wählen Sie auf der Seite **Active Directory-Hauptmenü** die Option **Active Directory konfigurieren** aus, und klicken Sie auf **Weiter**.
2. Geben Sie auf der Seite **Active Directory-Konfiguration und -Verwaltung** die Active Directory-Einstellungen ein.

   Tabelle 6-10 beschreibt die Einstellungen der Seite **Active Directory-Konfiguration und -Verwaltung**.
3. Auf **Anwenden klicken**, um die Einstellungen zu speichern.
4. Klicken Sie auf die entsprechende Schaltfläche der Seite **Active Directory- Konfiguration**, um fortzufahren. Siehe Tabelle 6-11.
5. Klicken Sie zur Konfiguration der Rollengruppen für das Active Directory- Standardschema auf die individuelle Rollengruppe (1 - 5). Siehe Tabelle 6-12 und Tabelle 6-13.

   ANMERKUNG: Um die Einstellungen der Seite **Active Directory-Konfiguration und -Verwaltung** speichern zu können, müssen Sie auf **Anwenden** klicken, bevor Sie mit der Seite **Benutzerdefinierte Rollengruppe** fortfahren.

Tabelle 6-10. Einstellungen der Seite Active Directory-Konfiguration und -Verwaltung

Einstellung	Beschreibung
Active Directory aktivieren	Aktiviert Active Directory. Markiert=Aktiviert; Unmarkiert=Deaktiviert.
ROOT-Domänenname	Der ROOT-Domänenname des Active Directory. Dieser Wert lautet standardmäßig **NULL**. Der Name muss ein gültiger Domänenname sein und aus *x.y* bestehen, wobei *x* eine ASCII-Zeichenkette mit 1 - 254 Zeichen, ohne Leerstellen, und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net oder org ist.
Zeitüberschreitung	Die Wartezeit in Sekunden, bis die Active Directory-Abfragen beendet sind. Der Mindestwert ist gleich oder größer als 15 Sekunden. Der Standardwert beträgt 120 Sekunden.
Standardschema verwenden	Verwendet das Standardschema mit Active Directory
Erweitertes Schema verwenden	Verwendet das erweiterte Schema mit Active Directory

DRAC-Name	Der Name, der die DRAC 5-Karte in Active Directory eindeutig identifiziert. Dieser Wert lautet standardmäßig **NULL**. Der Name muss eine ASCII-Zeichenkette mit 1 - 254 Zeichen, ohne Leerstellen, sein.
DRAC-Domänenname	Der DNS-Name (Zeichenkette) der Domäne, wo sich das Active Directory-DRAC 5-Objekt befindet. Dieser Wert lautet standardmäßig **NULL**. Der Name muss ein gültiger Domänenname sein und aus *x.y* bestehen, wobei *x* eine ASCII-Zeichenkette mit 1 - 254 Zeichen, ohne Leerstellen, und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net oder org ist.
Rollengruppen	Die Liste der Rollengruppen, die mit der DRAC 5-Karte in Verbindung stehen. Klicken Sie zum Ändern der Einstellungen für eine Rollengruppe in der Rollengruppenliste auf eine Rollengruppennummer. Das Fenster **Rollengruppe konfigurieren** wird angezeigt. **ANMERKUNG:** Wenn Sie auf den Rollengruppen-Link klicken, bevor Sie die Einstellungen der Seite **Active Directory-Konfiguration und -Verwaltung** übernommen haben, verlieren Sie diese Einstellungen.
Gruppenname	Der Name, der die Rollengruppe im Active Directory identifiziert, das mit der DRAC 5-Karte in Verbindung steht.
Gruppendomäne	Die Domäne, in der sich die Gruppe befindet.
Gruppenberechtigung	Die Zugriffsstufe für die Gruppe.

Tabelle 6-11. Schaltflächen der Seite „Active Directory-Konfiguration und Verwaltung"

Schaltfläche	Beschreibung
Drucken	Druckt die Seite **Active Directory-Konfiguration und -Verwaltung** aus.
Anwenden	Speichert die Änderungen, die auf der Seite **Active Directory-Konfiguration und -Verwaltung** vorgenommen wurden.
Zurück zum Active Directory-Hauptmenü	Wechselt zur Seite **Active Directory Hauptmenü** zurück.

Tabelle 6-12. Rollengruppenberechtigungen

Einstellung	Beschreibung
Zugriffsstufe der Rollengruppe	Legt die maximale DRAC-Benutzerberechtigung des Benutzers auf eine der folgenden Möglichkeiten fest: Administrator, Hauptbenutzer, Gastbenutzer, Keine oder Benutzerdefiniert. Sehen Sie Tabelle 6-13 zu **Rollengruppen**-Berechtigungen.
Anmeldung an DRAC	Ermöglicht dem Benutzer, sich an DRAC anzumelden.
DRAC konfigurieren	Ermöglicht dem Benutzer die Konfiguration von DRAC.
Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern den Zugriff auf das System zu erlauben.
Protokolle löschen	Ermöglicht dem Benutzer das Löschen von DRAC-Protokollen.
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer die Ausführung von racadm-Befehlen.
Auf die Konsolenumleitung zugreifen	Ermöglicht dem Benutzer, die Konsolenumleitung auszuführen.
Zugriff auf virtuelle Datenträger	Ermöglicht dem Benutzer, virtuelle Datenträger auszuführen und zu verwenden.
Testwarnungen	Ermöglicht dem Benutzer, einem bestimmten Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Tabelle 6-13. Rollengruppenberechtigungen

Eigenschaft	Beschreibung
Administrator	**Anmeldung an DRAC**, **DRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Server-Steuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
Hauptbenutzer	**Anmeldung an DRAC**, **Protokolle löschen**, **Server-Steuerungsbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**
Gastbenutzer	Anmeldung an DRAC
Custom (Benutzerdefiniert)	Auswahl einer beliebigen Kombination der folgenden Berechtigungen: **Anmeldung an DRAC**, **DRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen**, **Server-Maßnahmenbefehle ausführen**, **Zugriff auf Konsolenumleitung**, **Zugriff auf Virtueller Datenträger**, **Testwarnungen**, **Diagnosebefehle ausführen**
NONE	Keine zugewiesenen Berechtigungen

Active Directory-CA-Zertifikat hochladen

1. Wählen Sie auf der Seite **Active Directory-Hauptmenü** die Option **Active Directory-CA-Zertifikat hochladen** aus, und klicken Sie auf **Weiter**.
2. Geben Sie auf der Seite **Zertifikat hochladen** in das Feld **Dateipfad** den Dateipfad des Zertifikats ein, oder klicken Sie auf **Durchsuchen**, um zu der Zertifikatsdatei zu wechseln.

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

3. Klicken Sie auf **Anwenden**.
4. Klicken Sie auf die entsprechende Schaltfläche der Seite **Zertifikat hochladen**, um fortzufahren. Siehe Tabelle 6-11.

DRAC-Server-Zertifikat herunterladen

1. Wählen Sie auf der Seite **Active Directory-Hauptmenü** die Option **DRAC-Serverzertifikat herunterladen** aus, und klicken Sie auf **Weiter**.
2. Klicken Sie im Fenster **Datei herunterladen** auf **Speichern**, und speichern Sie die Datei in einem Verzeichnis auf Ihrem System.
3. Klicken Sie im Fenster **Herunterladen abgeschlossen** auf **Schließen**.

Active Directory-CA-Zertifikat anzeigen

Verwenden Sie die Seite **Active Directory Hauptmenü**, um ein CA-Serverzertifikat für DRAC 5 anzuzeigen.

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

   Tabelle 6-14 erläutert die Felder und zugehörigen Beschreibungen, die im Fenster **Zertifikat** aufgeführt werden.

2. Klicken Sie auf die entsprechende Schaltfläche der Seite **Active Directory- CA-Zertifikat**, um fortzufahren. Siehe Tabelle 6-11.

Tabelle 6-14. Informationen zum Active Directory-CA-Zertifikat

Feld	Beschreibung
Seriennummer	Seriennummer des Zertifikats
Informationen des Antragstellers	Vom Bewerber eingegebene Zertifikatsattribute
Ausstellerinformationen	Vom Aussteller zurückgegebene Zertifikatsattribute.
Gültig von	Datum der Zertifikatsausstellung.
Gültig bis	Verfalldatum des Zertifikats.

SSL auf einem Domänen-Controller aktivieren

Werden Benutzer durch DRAC 5 mittels eines Active Directory-Domänen-Controller authentifiziert, wird eine SSL-Sitzung mit dem Domänen-Controller gestartet. Der Domänen-Controller sollte jetzt ein von der Zertifizierungsstelle (CA) signiertes Zertifikat veröffentlichen – das Stammzertifikat, das auch in DRAC 5 hochgeladen wird. Damit, anders ausgedrückt, die DRAC 5-Authentifizierung auf einen *beliebigen* Domänen-Controller möglich ist – gleich, ob es sich um den Stamm-Domänen-Controller oder den untergeordneten Domänen-Controller handelt – muss dieser Domänen-Controller ein SSL-aktiviertes, von der CA der Domäne signiertes Zertifikat besitzen.

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

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

Stamm-CA-Zertifikat des Domänen-Controllers zu DRAC 5 exportieren

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

1. Machen Sie den Domänen-Controller ausfindig, der den Microsoft Enterprise-CA-Dienst ausführt.
2. Wählen Sie **Start**→ **Ausführen**.
3. Geben Sie `MMC` in das Feld **Ausführen** ein und klicken Sie auf **OK**.
4. Klicken Sie im Fenster **Konsole 1** (MMC) auf **Datei** (oder auf **Konsole** bei Windows 2000-Computern), und wählen Sie **Snap-In hinzufügen/entfernen** aus.
5. Klicken Sie im Fenster **Snap-In hinzufügen/entfernen** auf **Hinzufügen**.
6. Wählen Sie im Fenster **Eigenständiges Snap-In** die Option **Zertifikate** aus und klicken Sie auf **Hinzufügen**.
7. Wählen Sie **Computer**-Konto und klicken Sie auf **Weiter**.
8. Wählen Sie **Lokaler Computer** und klicken Sie auf **Fertig stellen**.
9. Klicken Sie auf **OK**.
10. Erweitern Sie im Fenster **Konsole 1** den Ordner **Zertifikate**, erweitern Sie den Ordner **Persönlich** und klicken Sie auf den Ordner **Zertifikate**.
11. Suchen Sie das Stamm-CA-Zertifikat, klicken Sie mit der rechten Maustaste darauf, wählen Sie **Alle Aufgaben** aus, und klicken Sie auf **Exportieren...**.
12. Klicken Sie im **Zertifikate exportieren-Assistenten** auf **Weiter** und wählen Sie **Privaten Schlüssel nicht exportieren** aus.
13. Klicken Sie auf **Weiter** und wählen Sie **Base-64-kodiert X.509 (.cer)** als Format.
14. Klicken Sie auf **Weiter**, um das Zertifikat in einem Verzeichnis auf dem System zu speichern.
15. Laden Sie das in Schritt 14 gespeicherte Zertifikat zu DRAC 5 hoch.

    Informationen zum Hochladen des Zertifikats unter Verwendung von RACADM finden Sie unter Konfiguration von DRAC 5 über Active Directory mit erweitertem Schema und Internet-basierter Schnittstelle.

    Um das Zertifikat mittels der Internet-basierten Schnittstelle hochzuladen, führen Sie das folgende Verfahren aus:

    a. Öffnen Sie einen unterstützten Webbrowser.
    b. Melden Sie sich bei der DRAC 5 Web-basierten 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. Wählen Sie auf der Seite **Sicherheitszertifikat Hauptseite** die Option **Serverzertifikat hochladen** aus, und klicken Sie auf **Weiter**.
    f. Führen Sie auf dem Bildschirm **Zertifikat hochladen** eines der folgenden Verfahren aus:
        - Klicken Sie auf **Durchsuchen**, und wählen Sie das Zertifikat aus.
        - Geben Sie den Pfad zum Zertifikat in das Feld **Wert** ein.
    g. Klicken Sie auf **Anwenden**.

SSL-Zertifikat der DRAC 5-Firmware importieren

ANMERKUNG: Ist der Active Directory-Server so eingestellt, dass der Client während der Initialisierungsphase einer SSL-Sitzung authentifiziert wird, muss das DRAC 5-Serverzertifikat auch zum Active Directory-Domänen-Controller hochgeladen werden. Dieser zusätzliche Schritt ist nicht erforderlich, wenn das Active Directory während der Initialisierungsphase einer SSL-Sitzung keine Client-Authentifizierung ausführt.

Wenden Sie das folgende Verfahren an, um das DRAC 5-Firmware-SSL-Zertifikat in alle 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-Web Server verwendet wird. Alle DRAC 5-Controller werden mit einem selbstsignierten Standardzertifikat versendet.

Wählen Sie, um über die DRAC 5-Internet-basierte Schnittstelle auf das Zertifikat zuzugreifen, **Konfiguration→ Active Directory→ DRAC 5-Serverzertifikat herunterladen** aus.

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

   Wenn Sie Ihr eigenes Zertifikat installiert haben, stellen Sie sicher, dass die Zertifizierungsstelle, die das Zertifikat signiert hat, in der Liste **Vertrauenswürdige Stammzertifizierungsstellen** aufgeführt ist. Wenn die Zertifizierungsstelle nicht in der Liste enthalten ist, muss diese auf allen Domänen-Controllern installiert werden.
5. Klicken Sie auf **Weiter** und wählen Sie aus, ob Windows den Zertifikatspeicher automatisch aufgrund des Zertifikattyps auswählen soll, oder suchen Sie selbst nach einem Speicher.
6. Klicken Sie auf **Fertig stellen** und dann auf **OK**.

SSL-Uhrzeit auf DRAC 5 einstellen

Wenn DRAC 5 einen Active Directory-Benutzer authentifiziert, überprüft DRAC 5 auch das vom Active Directory-Server veröffentlichte Zertifikat, damit sichergestellt werden kann, dass DRAC mit einem autorisierten Active Directory-Server kommuniziert.

Bei dieser Prüfung wird auch darauf geachtet, dass der Gültigkeitszeitraum des Zertifikats innerhalb des von DRAC 5 festgelegten Zeitbereichs liegt. Es ist jedoch möglich, dass die auf dem Zertifikat angegeben Zeitzonen nicht mit denen auf DRAC 5 übereinstimmen. Dies könnte passieren, wenn die Uhrzeit auf DRAC 5 die lokale Ortszeit wiedergibt und die Uhrzeit für das Zertifikat in mittlerer Greenwich-Zeit angegeben wird.

Um sicherzustellen, dass DRAC 5 die mittlere Greenwich-Zeit zum Vergleich mit der Zertifikat-Uhrzeit verwendet, muss das Zeitzonen-Offset-Objekt eingestellt werden.

```
racadm config -g cfgRacTuning -o cfgRacTuneTimeZoneOffset <Offset-Wert>
```

Weitere Details finden Sie unter cfgRacTuneTimezoneOffset (Lesen/Schreiben).

Unterstützte Active Directory-Konfiguration

Der Abfragealgorithmus des Active Directory auf DRAC 5 unterstützt mehrere Strukturen in einer einzelnen Gesamtstruktur.

DRAC 5-Active Directory-Authentifizierung unterstützt den gemischten Modus (d. h. die Domänen-Controller in der Struktur führen unterschiedliche Betriebssysteme aus, wie z. B Microsoft Windows NT 4.0, Windows 2000 oder Windows Server 2003). Alle durch das DRAC 5-Abfrageverfahren verwendeten Objekte (unter Benutzer, RAC-Geräteobjekt und Zuordnungsobjekt) müssen sich jedoch in derselben Domäne befinden. Das Dell-erweiterte Active Directory-Benutzer- und Computer-Snap-In überprüft den Modus und beschränkt Benutzer, um Objekte über Domänen hinweg zu erstellen (wenn im Mischmodus).

Das Active Directory von DRAC 5 unterstützt verschiedene Domänenumgebungen unter der Voraussetzung, dass die Funktionsebene der Domänenstruktur der Modus Systemeigen oder der Modus Windows 2003 ist. Außerdem müssen die Gruppen unter Zuordnungsobjekt, RAC-Benutzerobjekten und RAC-Geräteobjekten (einschließlich Zuordnungsobjekt) universelle Gruppen sein.

ANMERKUNG: Das Zuordnungsobjekt und das Berechtigungsobjekt müssen sich in derselben Domäne befinden. Das Dell-erweiterte Active Directory-Benutzer- und -Computers-Snap-In zwingt Sie, diese beiden Objekte in derselben Domäne zu erstellen. Andere Objekte können sich in verschiedenen Domänen befinden.

Active Directory zum Anmelden an DRAC 5 verwenden

Sie können Active Directory verwenden, um sich an DRAC 5 anzumelden. Verwenden Sie dazu eines der folgenden Verfahren:

- Webbasierte Schnittstelle
- Remote-RACADM
- Serielle oder Telnet-Konsole.

Die Anmeldungssyntax ist für alle drei Methoden gleich:

<*Benutzername@Domäne*>

oder

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

wobei *Benutzername* eine ASCII-Zeichenkette mit 1-256 Zeichen ist.

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

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

Sie können sich auch unter Verwendung der Smart Card an DRAC 5 anmelden. Weitere Informationen finden Sie unter Anmeldung an DRAC 5 über die Smart Card.

Active Directory für die Einmalanmeldung verwenden

Sie können DRAC 5 zum Verwenden von Kerberos – einem Netzwerk-Authentifizierungsprotokoll – verwenden, um die einfache Anmeldung zu aktivieren und sich an DRAC 5 anzumelden. Weitere Informationen zum Setup von DRAC 5 zur Verwendung der Funktion der einfachen Anmeldung über Active Directory finden Sie unter Kerberos-Authentifizierung aktivieren.

DRAC 5 zur Verwendung der einfachen Anmeldung konfigurieren

1. Wechseln Sie zu **Remote-Zugriff**→ Register **Konfiguration**→ Unterregister **Active Directory**→, und wählen Sie **Active Directory konfigurieren** aus.
2. Wählen Sie auf der Seite **Active Directory-Konfiguration und -Verwaltung** die Option **Einfache Anmeldung** aus.

   Diese Option ermöglicht Ihnen, sich direkt nach dem Anmelden an der Workstation an DRAC 5 anzumelden.

Anmelden an DRAC 5 unter Verwendung der einfachen Anmeldung

1. Melden Sie sich unter Verwendung Ihres Netzwerkkontos an der Workstation an.
2. Greifen Sie unter Verwendung von https auf die DRAC-Webseite zu.

   `https://<IP-Adresse>`

   Wurde die Standard-HTTPS-Portnummer (443) geändert, geben Sie Folgendes ein:

   `https://<IP-Adresse>:<Anschlussnummer>`

   wobei *IP-Adresse* die IP-Adresse des DRAC 5 ist und *Port-Nummer* die HTTPS-Port-Nummer.

   Die DRAC 5-Seite zur einfachen Anmeldung wird angezeigt.
3. Klicken Sie auf **Anmelden**.

   DRAC 5 meldet Sie an und verwendet dabei die Anmeldeinformationen, die im Betriebssystem zwischengespeichert wurden, als Sie sich unter Verwendung Ihres gültigen Active Directory-Kontos angemeldet haben.

Häufig gestellte Fragen

Gibt es Beschränkungen der Domänen-Controller SSL-Konfiguration?

Ja. Die SSL-Zertifikate aller Active Directory-Server in der Struktur müssen von der gleichen Stammzertifizierungsstelle signiert werden, da DRAC 5 nur das Hochladen eines einzigen CA-SSL-Zertifikats zulässt.

Ich habe ein neues RAC-Zertifikat erstellt und hochgeladen, und jetzt startet die Internet-basierte Schnittstelle nicht.

Wenn Sie zum Erstellen des RAC-Zertifikats Microsoft Certificate Services verwenden, ist eine mögliche Ursache, dass Sie bei der Erstellung des Zertifikats versehentlich **Benutzerzertifikat** statt **Internetzertifikat** ausgewählt haben.

Erstellen Sie zur Wiederherstellung eine CSR, und erstellen Sie dann ein neues Internet-Zertifikat über die Microsoft Certificate Services. Laden Sie das Zertifikat unter Verwendung der 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 an DRAC 5 anmelden kann? Wie kann ich das Problem beheben?

1. Stellen Sie sicher, dass Sie während einer Anmeldung den korrekten Benutzerdomänennamen und nicht den NetBIOS-Namen verwenden.
2. Wenn Sie ein lokales DRAC-Benutzerkonto haben, melden Sie sich mit Ihren lokalen Anmeldeinformationen an DRAC 5 an.

   Wenn Sie angemeldet sind:

a. Stellen Sie sicher, dass Sie das Kästchen **Active Directory aktivieren** auf der Konfigurationsseite des DRAC 5-Active Directory markiert haben.

b. Stellen Sie sicher, dass die DNS-Einstellung auf der Konfigurationsseite des DRAC 5-Netzwerkbetriebs korrekt ist.

c. Stellen Sie sicher, dass Sie das Active Directory-Zertifikat von Ihrer Active Directory-Stammzertifizierungsstelle zu DRAC 5 hochgeladen haben.

d. Überprüfen Sie die Domänen-Controller SSL-Zertifikate, um sicherzustellen, dass sie nicht abgelaufen sind.

e. Stellen Sie sicher, dass der **DRAC-Name**, **Stammdomänenname** und **DRAC-Domänenname** mit der Active Directory- Umgebungskonfiguration übereinstimmen.

f. Stellen Sie sicher, dass das DRAC 5-Kennwort maximal 127 Zeichen lang ist. Während DRAC 5 Kennwörter von bis zu 256 Zeichen unterstützt, unterstützt Active Directory nur Kennwörter, die maximal 127 Zeichen lang sind.

SSO-Anmeldung schlägt bei Active Directory-Benutzern auf dem Windows 7 Betriebssystem fehl. Was muss ich tun, um dieses Problem zu beheben?

Sie müssen die Verschlüsselungstypen für Windows 7 aktivieren. Aktivieren der Verschlüsselungstypen (für Standard- und erweitertes Schema):

1. Melden Sie sich als Administrator oder als Benutzer mit Administratorrechten an.
2. Wechseln Sie zu **Start** und führen Sie **gpedit.msc** aus.

   Das Fenster **Editor für lokale Gruppenrichtlinien** wird angezeigt.
3. Navigieren Sie zu **Einstellungen des lokalen Computers**→ **Windows- Einstellungen**→ **Sicherheitseinstellungen**→ **Lokale Richtlinien**→ **Sicherheitsoptionen**.
4. Klicken Sie mit der rechten Maustaste auf **Netzwerksicherheit: Für Kerberos genehmigte Verschlüsselungstypen konfigurieren** und wählen Sie **Eigenschaften** aus.
5. Aktivieren Sie alle Optionen und klicken Sie auf **OK**.

   Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.
6. Navigieren Sie im Fenster **Editor für lokale Gruppenrichtlinien** zu **Einstellungen des lokalen Computers**→ **Windows-Einstellungen**→ **Sicherheitseinstellungen**→ **Lokale Richtlinien**→ **Sicherheitsoptionen**.
7. Klicken Sie mit der rechten Maustaste auf **Netzwerksicherheit: NTLM einschränken: Ausgehender NTLM-Verkehr zu Remote-Server** und wählen Sie **Eigenschaften** aus.
8. Wählen Sie **Alle zulassen**, klicken Sie auf **OK** und schließen Sie dann das Fenster **Editor für lokale Gruppenrichtlinien**.
9. Wechseln Sie zu **Start** und führen Sie **cmd** aus.

   Das **Befehlszeilen**fenster wird angezeigt.
10. Führen Sie den Befehl `gpupdate /force` aus.

    Die Gruppenrichtlinien werden aktualisiert.
11. Schließen Sie das **Befehlszeilen**fenster.

Führen Sie die folgenden zusätzlichen Einstellungen für das erweiterte Schema aus:

1. Wechseln Sie zu **Start** und führen Sie **regedit** aus.

   Das Fenster **Registrierungseditor** wird angezeigt.
2. Navigieren Sie zu **HKEY_LOCAL_MACHINE**→ **System**→ **CurrentControlSet**→ **Control**→ **LSA**.
3. Klicken Sie mit der rechten Maustaste in den rechten Fensterbereich und wählen Sie **Neu**→ **DWORD (32-Bit) Wert** aus.
4. Geben Sie dem neuen Schlüssel den Namen **SuppressExtendedProtection**.
5. Klicken Sie mit der rechten Maustaste auf **SuppressExtendedProtection** und klicken Sie dann auf **Ändern**.
6. Geben Sie in das Feld **Wertdaten** die Zahl **1** ein und klicken Sie auf **OK**.
7. Schließen Sie das Fenster **Registrierungseditor**.

   Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Kerberos-Authentifizierung aktivieren

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Kerberos ist ein Netzwerk-Authentifizierungsprotokoll, das Systemen ermöglicht, auf sichere Weise über ein ungesichertes Netzwerk zu kommunizieren. Dazu wird den Systemen erlaubt, ihre Authentizität zu beweisen.

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista und Windows Server 2008 verwenden Kerberos standardmäßig als Authentifizierungsmethode.

Beginnend mit DRAC 5 Version 1.40 verwendet der DRAC 5 Kerberos zum Unterstützen zweier Typen von Authentifizierungsmechanismen – Einfache Anmeldung und Active Directory-Smart Card-Anmeldung. Bei der einfachen Anmeldung verwendet DRAC 5 die im Betriebssystem zwischengespeicherten Anmeldeinformationen des Benutzers, nachdem sich der Benutzer unter Verwendung eines gültigen Active Directory-Kontos angemeldet hat.

Beginnend mit DRAC 5 Version 1.40 verwendet Active Directory-Authentifizierung die auf der Smart Card basierende Zweifaktorauthentifizierung (TFA) zusätzlich zur Benutzername-Kennwort-Kombination als gültige Anmeldeinformationen.

Voraussetzungen zum Einrichten von Kerberos- Authentifizierung

- Konfigurieren Sie DRAC 5 für die Active Directory-Anmeldung. Weitere Informationen finden Sie unter Active Directory zum Anmelden an DRAC 5 verwenden.
- Für Active Directory-Benutzer, für die Sie Kerberos-Authentifizierung bereitstellen möchten, müssen Sie die folgenden Eigenschaften festlegen:
  - DES-Verschlüsselungstypen für dieses Konto verwenden
  - Keine Kerberos-Vorauthentifizierung vorschreiben
- Registrieren Sie DRAC 5 als Computer in der Active Directory-Root-Domäne.

  a. Wechseln Sie zu **Remote-Zugriff**→ Register **Konfiguration**→ Unterregister **Netzwerk**→ **Netzwerkeinstellungen**.

  b. Geben Sie eine gültige IP-Adresse für **Bevorzugter/Statischer DNS- Server** an. Dieser Wert ist die IP-Adresse des DNS als Teil der Root-Domäne, welche die Active Directory-Konten der Benutzer authentifiziert.

  c. Wählen Sie **DRAC auf DNS registrieren** aus.

  d. Geben Sie einen gültigen **DNS-Domänennamen an**.

  ANMERKUNG: Stellen Sie sicher, dass der DNS-Name durch den DNS-Server aufgelöst wird.

  Weitere Informationen finden Sie in der *DRAC 5-Online-Hilfe*.

- Synchronisieren Sie die DRAC 5-Zeiteinstellungen mit denen des Active Directory-Domänen-Controllers. Die Kerberos-Authentifizierung bei DRAC 5 schlägt fehl, wenn die DRAC-Zeit von der Zeit des Domänen-Controllers abweicht. Es ist ein maximaler Unterschied von 5 Minuten zulässig. Um die erfolgreiche Authentifizierung zu ermöglichen, synchronisieren Sie die Serverzeit mit der Zeit des Domänen-Controllers und führen dann einen **Reset** der DRAC-Zeit durch.

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

  ```
  racadm config -g cfgRacTuning -o

  cfgRacTuneTimeZoneOffset Offset-Wert
  ```

  Offset-Wert ist die Verzögerungszeit in Minuten.

- Installieren Sie Microsoft Visual C++ 2005 Redistributable Package auf dem Client-System.
- Führen Sie das Dienstprogramm **ktpass** auf dem Active Directory-Server aus.

  DRAC 5 ist ein Gerät mit einem Nicht-Windows-Betriebssystem. Deshalb müssen Sie das Dienstprogramm **ktpass** (Teil von Microsoft Windows) auf dem Domänen-Controller (Active Directory-Server) ausführen, wo Sie DRAC 5 einem Benutzerkonto in Active Directory zuordnen möchten. Führen Sie dazu folgende Schritte durch:

  a. Starten Sie das Active Directory Management-Tool.

  b. Klicken Sie mit der rechten Maustaste auf den Ordner **Benutzer**, wählen Sie **Neu**, und klicken Sie anschließend auf **Benutzer**.

  c. Geben Sie den Namen des DRAC5-Hosts ein, für den Sie Kerberos- Unterstützung hinzufügen wollen.

  d. Speichern Sie den Benutzer.

  e. Starten Sie eine Eingabeaufforderung und geben Sie anschließend den folgenden Befehl ein:

  ```
  C:\>ktpass -princ HOST/dracname.domain-name.com@DOMAIN-NAME.COM -mapuser account -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass password -out c:\krbkeytab
  ```

  wobei

  - dracname ist der DNS-Name des DRAC 5.

- `domain-name` ist der Active Directory Domänenname, mit dem Sie sich authentifizieren wollen. Er sollte durch den tatsächlichen Domänennamen ersetzt werden (in Großbuchstaben).
- `Konto` ist der Benutzername, ein gültiges Benutzerkonto, das Sie in Schritt n und Schritt c in Active Directory erstellt haben. Der Benutzername muss im Format *Domänennamen.com/Benutzername* angegeben werden.
- `Kennwort` ist das Kennwort für das Benutzerkonto.
- `DES-CBC-MD5` ist der Verschlüsselungstyp, den DRAC 5 für die Kerberos-Authentifizierung verwendet.
- `KRB5_NT_PRINCIPAL` ist der Prinzipaltyp.

f. Laden Sie die resultierende Keytab-Datei auf den DRAC 5-Host hoch.

ANMERKUNG: Es wird empfohlen, das neueste **ktpass**-Dienstprogramm zum Erstellen der Keytab-Datei zu verwenden.

Dieses Verfahren erstellt eine Keytab-Datei, die Sie zu DRAC 5 5 hochladen müssen.

ANMERKUNG: Das Keytab enthält einen Verschlüsselungsschlüssel und muss an einem sicheren Ort aufbewahrt werden.

Weitere Informationen zum Dienstprogramm **ktpass** finden Sie auf der Microsoft-Website unter:
http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true

---

DRAC 5 für Kerberos-Authentifizierung konfigurieren

Laden Sie Keytab von der Active Directory-Root-Domäne zu DRAC 5 hoch:

1. Wechseln Sie zu **Remote-Zugriff**→ Register **Konfiguration**→ Unterregister **Active Directory**.
2. Wählen Sie **Kerberos-Keytab hochladen** aus und klicken Sie auf **Weiter**.
3. Wählen Sie auf der Seite **Kerberos-Keytab-Upload** die hochzuladende Keytab-Datei aus, und klicken Sie auf **Anwenden**.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Einfache Anmeldung aktivieren

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Mit einer einfachen Anmeldung können Sie sich ohne Angabe der Anmeldeinformationen beim DRAC anmelden, nachdem Sie sich mit einem Active Directory-Konto beim Betriebssystem angemeldet haben. DRAC verwendet in diesem Fall die im Betriebssystem zwischengespeicherten Anmeldeinformationen. DRAC verwendet Kerberos, ein Netzwerk-Authentifizierungsprotokoll, für die einfache Anmeldung.

Voraussetzungen zum Einrichten der einfachen Anmeldung

- Konfigurieren Sie DRAC 5 für die Active Directory-Anmeldung. Weitere Informationen finden Sie unter Active Directory zum Anmelden an DRAC 5 verwenden.
- Einrichten der Kerberos-Authentifizierung für DRAC 5. Weitere Informationen finden Sie unter Kerberos-Authentifizierung aktivieren.

DRAC 5 zur Verwendung der einfachen Anmeldung konfigurieren

1. Wechseln Sie zu **Remote-Zugriff**→ Register **Konfiguration**→ Unterregister **Active Directory**→ und wählen Sie **Active Directory konfigurieren** aus.
2. Wählen Sie auf der Seite **Active Directory-Konfiguration und -Verwaltung** die Option **Einfache Anmeldung** aus.

   Diese Option ermöglicht es Ihnen, sich direkt nach dem Anmelden an der Workstation an DRAC 5 anzumelden.

Anmelden an DRAC 5 unter Verwendung der einfachen Anmeldung

ANMERKUNG: Stellen Sie beim Anmelden an DRAC 5 sicher, dass Sie über die neuesten Laufzeit-Komponenten der Microsoft Visual C++ 2005-Bibliotheken verfügen. Weitere Informationen finden Sie auf der Microsoft-Website.

1. Melden Sie sich unter Verwendung eines gültigen Active Directory-Kontos am System an.
2. Geben Sie die Internetadresse von DRAC 5 in die Adresszeile Ihres Browsers ein.

   ANMERKUNG: Abhängig von Ihren Browser-Einstellungen werden Sie eventuell aufgefordert, das Einfache Anmeldung-ActiveX-Plug-In herunterzuladen und zu installieren, wenn Sie diese Funktion zum ersten Mal verwenden.

   Sie sind jetzt an DRAC 5 angemeldet.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Smart Card-Authentifizierung konfigurieren

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Der Dell Remote Access Controller 5 (DRAC 5), Version 1.30 und höher unterstützt die *Zweifaktor-Authentifizierung* bei der Anmeldung an der DRAC 5-Internet-Schnittstelle. Diese Unterstützung wird über die Funktion der **Smart Card-Anmeldung** von DRAC 5 zur Verfügung gestellt.

Für herkömmliche Authentifizierungsschemata werden der Benutzername und das Kennwort zum Authentifizieren von Benutzern verwendet. Diese Option bietet minimale Sicherheit.

Bei der Zweifaktor-Authentifizierung wird andererseits eine höhere Sicherheitsstufe geboten, indem Benutzer aufgefordert werden, ein Kennwort oder eine PIN sowie einen privaten Schlüssel für ein Digitalzertifikat anzugeben.

Für die Zweifaktor-Authentifizierung ist es erforderlich, dass Benutzer ihre Identität durch die Angabe *beider* Faktoren bestätigen.

Smart Card-Anmeldung an DRAC 5 konfigurieren

Aktivieren Sie die Smart Card-Anmeldungsfunktion für DRAC 5 über **Remote-Zugriff**→ **Konfiguration**→ **Smart Card**.

Wenn Sie:

- Wenn Sie die Smart Card-Konfiguration **deaktivieren**, werden zur Eingabe eines Benutzernamens und eines Kennworts für die Microsoft Active Directory oder die lokale Anmeldung aufgefordert.
- Wenn Sie **Aktivieren** oder **Mit Remote-RACADM aktivieren** auswählen, werden Sie bei allen nachfolgenden Anmeldungsversuchen über die GUI zu einer Smart Card-Anmeldung aufgefordert.

  Wenn Sie **Aktivieren** auswählen, werden alle bandexternen CLI-Schnittstellen (Befehlszeilenschnittstelle) wie z. B. Telnet, ssh, seriell, Remote-RACADM und IPMI über LAN deaktiviert. Der Grund hierfür ist, dass diese Dienste nur Einzelfaktor-Authentifizierung unterstützen.

  Wenn Sie **Mit Remote-RACADM aktivieren** auswählen, werden alle bandexternen CLI-Schnittstellen, außer Remote-RACADM, deaktiviert.

  ANMERKUNG: Dell empfiehlt DRAC 5-Administratoren, die Einstellung **Mit Remote-RACADM aktivieren** nur zu verwenden, um zur Ausführung von Scripts über Remote-RACADM-Befehle auf die DRAC 5-Benutzeroberfläche zuzugreifen. Ist es für einen Administrator nicht erforderlich ist, Remote-RACADM zu verwenden, empfiehlt Dell, die Einstellung **Aktiviert** für die Smart Card-Anmeldung zu wählen. Vergewissern Sie sich vor der Aktivierung der **Smart Card-Anmeldung** ebenfalls, dass die Konfiguration des lokalen DRAC 5-Benutzers bzw. des Active Directory abgeschlossen ist.

- **CRL-Prüfung für Smart Card-Anmeldung aktivieren**, das DRAC-Zertifikat des Benutzers, das vom CRL-Verteilungsserver (Certificate Revocation List, Zertifikatsperrliste) heruntergeladen wird, wird in der CRL auf Widerrufung überprüft.

  ANMERKUNG: Die CRL-Verteilungsserver werden in den Smart Card-Zertifikaten der Benutzer aufgeführt.

Konfigurieren von lokalen DRAC 5-Benutzern für die Smart Card-Anmeldung

Sie können die lokalen DRAC 5-Benutzer so konfigurieren, dass die Anmeldung an DRAC 5 über die Smart Card erfolgen muss. Wechseln Sie zu **Remote-Zugriff**→ **Konfiguration**→ **Benutzer**.

Bevor sich der Benutzer jedoch mittels der Smart Card an DRAC 5 anmelden kann, muss das Smart Card-Zertifikat sowie das Zertifikat der vertrauenswürdigen Zertifizierungsstelle (CA) des Benutzers zu DRAC 5 hochgeladen werden.

Smart Card-Zertifikat exportieren

Das Zertifikat des Benutzers kann abgerufen werden, indem Sie das Smart Card-Zertifikat mittels der Kartenverwaltungssoftware (CMS) von der Smart Card in eine Datei mit Base64-kodiertem Format exportieren. Die CMS ist normalerweise vom Anbieter der Smart Card erhältlich. Diese kodierte Datei muss als Benutzerzertifikat zu DRAC 5 hochgeladen werden. Die vertrauenswürdige Zertifizierungsstelle, welche die Smart Card-Benutzerzertifikate ausstellt, sollte auch das CA-Zertifikat in eine Datei in Base64-kodiertem Format exportieren. Laden Sie diese Datei als Datei der vertrauenswürdigen CA für den Benutzer hoch. Konfigurieren Sie den Benutzer mit dem Benutzernamen, der den Benutzerprinzipalnamen (UPN) des Benutzers im Smart Card-Zertifikat bildet.

ANMERKUNG: Achten Sie bei der Anmeldung an DRAC 5 darauf, dass der im DRAC 5 konfigurierte Benutzername in Bezug auf Groß- bzw. Kleinschreibung von Buchstaben identisch mit dem Benutzerprinzipalnamen (UPN) im Smart Card-Zertifikat ist.

Beispiel: Wenn das Smart Card-Zertifikat an den Benutzer ausgegeben wurde, muss der Benutzername „Beispielbenutzer@Domäne.com" als „Beispielbenutzer" konfiguriert werden.

Konfigurieren von Active Directory-Benutzern für die Smart Card-Anmeldung

Um Active Directory-Benutzer so zu konfigurieren, dass sie sich mittels Smart Card an DRAC 5 anmelden müssen, muss DRAC 5-Administrator den DNS-Server konfigurieren, das Active Directory-CA-Zertifikat zu DRAC 5 hochladen und die Active Directory-Anmeldung aktivieren. Weitere Informationen zum Einrichten von Active Directory-Benutzern finden Sie unter DRAC 5 mit Microsoft Active Directory verwenden.

Sie müssen Active Directory und Kerberos für die Smart Card Active Directory-Anmeldung konfigurieren. Informationen zur jeweiligen Konfiguration erhalten Sie unter DRAC 5 mit Microsoft Active Directory verwenden und Kerberos-Authentifizierung aktivieren.

Sie sind bei DRAC mit den entsprechenden Berechtigungen angemeldet, wenn Sie ein lokaler DRAC-Benutzer sind.

Sie sind bei DRAC mit den entsprechenden Microsoft Active Directory-Berechtigungen angemeldet, wenn:

- Sie ein Microsoft Active Directory-Benutzer sind,
- Sie in DRAC für die Active Directory-Anmeldung konfiguriert sind,
- DRAC für die Kerberos Active Directory-Authentifizierung freigeschaltet ist.

Smart Card konfigurieren

ANMERKUNG: Zur Änderung dieser Einstellungen müssen Sie über die Berechtigung **DRAC 5 konfigurieren** verfügen.

1. Erweitern Sie die **System**struktur und klicken Sie auf **Remote-Zugriff**.
2. Klicken Sie auf das Register **Konfiguration** und dann auf **Smart Card**.
3. Konfigurieren Sie die Einstellungen für die Smart Card-Anmeldung.

   Tabelle 9-1 enthält Informationen über die Einstellungen der Seite **Smart Card**.
4. Klicken Sie auf **Änderungen übernehmen**.

Tabelle 9-1. Smart Card-Einstellungen

Einstellung	Beschreibung
Smart Card-Anmeldung konfigurieren	• Deaktiviert - Deaktiviert die Smart Card-Anmeldung. Bei nachfolgenden Anmeldungen über die grafische Benutzeroberfläche (GUI) wird die reguläre Anmeldungsseite angezeigt. Alle bandexternen Befehlszeilenoberflächen einschließlich Secure Shell (SSH), Telnet, Seriell- und Remote-RACADM sind auf ihre Standardeinstellungen gesetzt. • Aktiviert – Aktiviert die Smart Card-Anmeldung. Geben Sie nach dem Übernehmen der Änderungen, dem Abmelden und dem Einsetzen der Smart Card Ihre Smart Card-PIN ein, und klicken Sie dann auf **Login**, um sich beim DRAC anzumelden. Durch die Aktivierung der Smart Card-Anmeldung werden alle bandexternen CLI-Schnittstellen, einschließlich SSH, Telnet, Seriell, Remote-RACADM und IPMI über LAN deaktiviert. • Mit Remote-Racadm aktiviert - Aktiviert die Smart Card-Anmeldung zusammen mit Remote-RACADM. Alle anderen bandexternen CLI-Schnittstellen werden deaktiviert. **ANMERKUNG:** Für die Smart Card-Anmeldung ist die Konfiguration der lokalen DRAC 5-Benutzer mit den entsprechenden Zertifikaten erforderlich. Wenn die Smart Card-Anmeldung zur Anmeldung eines Microsoft Active Directory-Benutzers verwendet wird, ist sicherzustellen, dass das Active Directory-Benutzerzertifikat für diesen Benutzer konfiguriert wird. Das Benutzerzertifikat kann auf der Seite **Benutzer**→ **Benutzerhauptmenü** konfiguriert werden.
CRL-Prüfung für Smart Card-Anmeldung aktivieren	Diese Prüfung ist nur für lokale Smart Card-Benutzer verfügbar. Wählen Sie diese Option aus, wenn DRAC die Zertifikatsperrliste (CRL) zum Widerrufen des Smart Card-Zertifikats des Benutzers prüfen soll. Damit die CRL-Funktion funktioniert, muss DRAC über eine gültige DNS-IP-Adresse verfügen, die als Teil der Netzwerkkonfiguration konfiguriert ist. Sie können die DNS-IP-Adresse in DRAC unter **Remote-Zugriff**→ **Konfiguration**→ **Netzwerk** konfigurieren. Der Benutzer wird nicht in der Lage sein, sich anzumelden, wenn eine der folgenden Bedingungen erfüllt ist: • Das Benutzerzertifikat wird in der CRL-Datei als widerrufen aufgeführt. • DRAC ist nicht in der Lage, mit dem CRL-Verteilungsserver zu kommunizieren. • DRAC ist nicht in der Lage, die CRL herunterzuladen. **ANMERKUNG:** Damit diese Prüfung erfolgreich ausgeführt werden kann, müssen Sie die IP-Adresse des DNS-Servers auf der Seite **Konfiguration**→ **Netzwerk** korrekt konfigurieren.

Anmeldung an DRAC 5 über die Smart Card

Die DRAC 5-Internet-Schnittstelle zeigt die Smart Card-Anmeldeseite an, wenn Sie die Smart Card-Anmeldefunktion aktiviert haben.

ANMERKUNG: Vergewissern Sie sich vor der Aktivierung der Smart Card-Anmeldung für den Benutzer, dass die Konfiguration des lokalen DRAC 5-Benutzers bzw. des Active Directory abgeschlossen wurde.

ANMERKUNG: Abhängig von den Browser-Einstellungen können Sie eventuell aufgefordert werden, das Smart-Card-Reader-ActiveX-Plug-In herunterzuladen und zu installieren, wenn Sie diese Funktion zum ersten Mal anwenden.

1. Greifen Sie unter Verwendung von https auf die DRAC 5-Webseite zu.

   `https://<IP-Adresse>`

   Wurde die Standard-HTTPS-Portnummer (443) geändert, geben Sie Folgendes ein:

   `https://<IP-Adresse>:<Anschlussnummer>`

   wobei *IP-Adresse* die IP-Adresse des DRAC 5 ist und *Port-Nummer* die HTTPS-Port-Nummer.

   Die DRAC 5-**Anmeldungsseite** wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

2. Legen Sie die Smart Card in das Lesegerät ein, und geben Sie Ihre Smart Card-PIN ein.

3. Klicken Sie auf **Anmelden**.

ANMERKUNG: Wenn Sie ein Active Directory-Benutzer sind, für den die Option **CRL-Prüfung für Smart Card-Anmeldung aktivieren** ausgewählt wurde, versucht DRAC 5, die CRL herunterzuladen und sucht in der CRL nach dem Benutzerzertifikat. Die Anmeldung durch das Active Directory schlägt fehl, wenn das Zertifikat als widerrufen aufgeführt ist, oder wenn die CRL aus einem bestimmten Grund nicht heruntergeladen werden kann. Die Smart Card-Anmeldung wird nur vom Microsoft Internet Explorer unterstützt.

Unter Verwendung der Active Directory-Smart Card-Authentifizierung an DRAC 5 anmelden

1. Melden Sie sich unter Verwendung von https an DRAC 5 an.

   `https://<IP-Adresse>`

   Wurde die Standard-HTTPS-Portnummer (443) geändert, geben Sie Folgendes ein:

   `https://<IP-Adresse>:<Anschlussnummer>`

   wobei *IP-Adresse* die IP-Adresse des DRAC 5 ist und *Port-Nummer* die HTTPS-Port-Nummer.

   Die DRAC 5-Anmeldeseite wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

2. Legen Sie die Smart Card in das Lesegerät ein, und geben Sie Ihre Smart Card-PIN ein.

3. Klicken Sie auf **Anmelden**.

   Sie sind jetzt über Ihre im Active Directory festgelegten Anmeldeinformationen an DRAC 5 angemeldet. Weitere Informationen finden Sie unter Kerberos-Authentifizierung aktivieren.

Fehlerbehebung bei der Smart Card-Anmeldung an DRAC 5

Wenden Sie die folgenden Tipps an, die beim Debuggen einer Smart Card, auf die nicht zugegriffen werden kann, behilflich sein können.

Das ActiveX-Plugin kann das Smart Card-Laufwerk nicht erkennen

Stellen Sie sicher, dass die Smart Card auf dem Microsoft Windows-Betriebssystem unterstützt wird. Windows unterstützt eine beschränkte Anzahl von Cryptographic Service Providers (CSP) für die Smart Card.

Tipp: Sie können generell überprüfen, ob die Smart Card-CSPs auf einem bestimmten Client vorhanden sind, indem Sie die Smart Card beim Windows-Anmeldebildschirm (Strg-Alt-Entf) in das Laufwerk einlegen, um zu sehen, ob Windows die Smart Card erkennt und das PIN-Dialogfeld einblendet.

Falsche Smart Card-PIN

Prüfen Sie, ob die Smart Card aufgrund übermäßiger Versuche mit einer falschen PIN gesperrt wurde. In solchen Fällen kann Ihnen der Aussteller der Smart Card in der Organisation helfen, eine neue Smart Card zu beschaffen.

Anmeldung am lokalen DRAC 5 nicht möglich

Wenn ein lokaler DRAC 5-Benutzer nicht in der Lage ist, sich anzumelden, prüfen Sie, ob der Benutzername und das zu DRAC 5 hochgeladene Benutzerzertifikat abgelaufen sind. Die DRAC 5-Ablaufverfolgungsprotokolle können wichtige Protokollmeldungen anzeigen, die sich auf die Fehler beziehen. Hierbei ist jedoch zu beachten, dass Fehlermeldungen aus Sicherheitsgründen manchmal absichtlich unklar formuliert werden.

Anmeldung an DRAC 5 als Active Directory-Benutzer nicht möglich

Wenn Sie sich als Active Directory-Benutzer nicht an DRAC 5 anmelden können, versuchen Sie, sich an DRAC 5 anzumelden, ohne die Smart Card-Anmeldung zu aktivieren. Wenn Sie die CRL-Prüfung aktiviert haben, versuchen Sie die Active Directory-Anmeldung ohne Aktivierung der CRL-Prüfung. Das DRAC 5-Ablaufverfolgungsprotokoll sollte im Falle eines CRL-Fehlers wichtige Meldungen enthalten.

Sie haben auch die Möglichkeit, die Smart Card-Anmeldung über den lokalen racadm zu deaktivieren, indem Sie den folgenden Befehl verwenden:

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

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

GUI-Konsolenumleitung verwenden

Dell Remote Access Controller 5 Firmware-Version 1.60 Benutzerhandbuch

Dieser Abschnitt enthält Informationen über die Verwendung der DRAC 5-Konsolenumleitungsfunktion.

Übersicht

Mit der DRAC 5-Konsolenumleitungsfunktion können Sie im Remote-Zugriff im grafischen Modus oder Textmodus auf die lokale Konsole zugreifen. Mittels Konsolenumleitung können Sie ein DRAC 5-aktiviertes System bzw. mehrere DRAC 5-aktivierte Systeme von einem Standort aus steuern.

Bei all den Netzwerk- und Internet-Möglichkeiten braucht man heutzutage zur Ausführung von Routinearbeiten nicht vor jedem Server zu sitzen. Server können von einer anderen Stadt oder sogar von der anderen Seite der Welt von einem Desktop oder Laptop verwaltet werden. 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 die Verwaltung des Remote-Systems durch die Verwendung von Tastatur, Video und Maus auf der lokalen Management Station zum Steuern der entsprechenden Geräte auf einem im Remote-Zugriff verwalteten System. Diese Funktion kann in Verbindung mit der Funktion Virtueller Datenträger verwendet werden, um Remote-Software-Installationen auszuführen.

Die folgenden Regeln gelten für eine Konsolenumleitungssitzung:

- Es werden nur vier Konsolenumleitungssitzungen gleichzeitig unterstützt.
- Konsolenumleitungssitzungen können nur mit einem einzigen Remote-Zielsystem verbunden werden.
- Konsolenumleitungssitzungen können nicht auf dem lokalen System konfiguriert werden.
- Die erforderliche verfügbare Netzwerk-Mindestbandbreite beträgt 1 MB/s.

Unterstützte Bildschirmauflösungs-Bildwiederholfrequenzen auf dem verwalteten System

Tabelle 10-1 führt die unterstützten Bildschirmauflösungen und entsprechenden Bildwiederholfrequenzen für eine Konsolenumleitungssitzung auf, die auf dem verwalteten System ausgeführt wird.

Tabelle 10-1. Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

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

Management Station konfigurieren

Zur Verwendung der Konsolenumleitung auf der Management Station führen Sie die folgenden Maßnahmen durch:

1. Installieren und konfigurieren Sie einen unterstützten Internet-Browser. *Eine Liste der unterstützten Webbrowser finden Sie in der* Dell Systems Software Support Matrix auf der Dell Support-Website unter **support.dell.com/manuals**.

   VORSICHTSHINWEIS: Konsolenumleitung und Virtueller Datenträger unterstützen nur 32-Bit-Webbrowser. Das Verwenden von 64-Bit-Internet- Browsern kann zu unerwarteten Ergebnissen oder einem Fehlschlagen von Vorgängen führen.

- Konfigurieren eines unterstützten Webbrowsers

2. Konfigurieren Sie die Auflösung der Bildschirmanzeige auf mindestens 1280 x 1024 Pixel bei 60 Hz mit 128 Farben. Andernfalls können Sie die Konsole eventuell nicht im **Vollbildmodus** sehen.

3. Wenn Sie zum Herstellen der Verbindung das Java-Plug-In verwenden, muss sichergestellt werden, dass auf dem System Java Virtual Machine (JVM) Version 1.6 Update 21 oder höher installiert ist.

Konsolenumleitung konfigurieren

1. Öffnen Sie auf der Management Station einen unterstützten Internet- Browser, und melden Sie sich an DRAC 5 an. Weitere Informationen finden Sie unter Auf die Internet-basierte Schnittstelle zugreifen.

2. Klicken Sie in der **System**struktur auf **System**.

3. Klicken Sie auf das Register **Konsole** und dann auf **Konfiguration**.

4. Verwenden Sie auf der Seite **Konsolenumleitungskonfiguration** die Informationen aus Tabelle 10-2 zum Konfigurieren der Konsolenumleitungssitzung.

5. In DRAC 5, Versionen 1.40 und höher, können Sie das Plug-In des Typs **Systemeigen** oder **Java** auswählen, das Sie installieren möchten.

6. Auf **Änderungen übernehmen** klicken, um die Einstellungen zu speichern.

ANMERKUNG: Jede Änderung der Konfiguration der virtuellen Konsole beeinträchtigt bzw. trennt jegliche vorhandenen virtuellen Benutzer-Konsolensitzungen.

Tabelle 10-2. Informationen zur Seite Konsolenumleitungskonfiguration

Information (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
Videoanschlussnummer	Standardeinstellung = 5901
Videoverschlüsselung aktiviert	Markiert=Aktiviert, unmarkiert=Deaktiviert
Lokales Servervideo aktiviert	Markiert=Aktiviert, unmarkiert=Deaktiviert
Plugin-Typ	Ermöglicht Ihnen, das **systemeigene** (ActiveX für Windows und XPI-Plug-In für Linux) oder das **Java**-Plug-In auszuwählen. **ANMERKUNG:** Wenn Sie das Java-Plug-In auswählen, muss sichergestellt werden, dass auf dem System bereits Java Virtual Machine (JVM) Version 1.6 Update 21 oder höher installiert ist.
Standardzugang für Konsolenfreigabe	Wählen Sie den Zugangsstandardtyp der Konsolenfreigabe, der der Konsolenfreigabeanforderung des zweiten Benutzers angeboten wird, wenn der erste Benutzer mit der Konsole verbunden ist. Die Zugangsberechtigungen sind: • **Kein Zugang** – Gewährt dem zweiten Benutzer keinen Zugang. • **Schreibgeschützter Zugang** – Gewährt dem zweiten Benutzer nur schreibgeschützten Zugang. • **Voller Zugang** – Gewährt dem zweiten Benutzer den vollen Zugang.

Die Schaltflächen in Tabelle 10-3 sind auf der Seite **Konsolenumleitungskonfiguration** verfügbar.

Tabelle 10-3. Schaltflächen der Seite Konsolenumleitungskonfiguration

Eigenschaft	Beschreibung
Drucken	Druckt die Seite **Konsolenumleitungskonfiguration** aus.
Aktualisieren	Lädt die Seite **Konsolenumleitungskonfiguration** neu.
Änderungen übernehmen	Speichert Ihre Konfigurationseinstellungen.

ANMERKUNG: Mit DRAC 5,Version 1.30 und höher können Sie die Konsolenumleitung für einen Remote-Benutzer deaktivieren. Weitere Informationen finden Sie unter Virtuelle DRAC 5-Remote-KVM deaktivieren.

Konsolenumleitungssitzung öffnen

Wenn Sie eine Konsolenumleitungssitzung öffnen, startet die Dell Virtual KVM Viewer-Anwendung, und der Desktop des Remote-Systems wird im Viewer eingeblendet. Mit der Anwendung Virtual KVM Viewer können die Maus- und Tastatur-Funktionen des Systems von einer lokalen oder Remote-Management Station aus gesteuert werden.

So öffnen Sie eine Konsolenumleitungssitzung:

1. Öffnen Sie auf der Management Station einen unterstützten Internet- Browser, und melden Sie sich an DRAC 5 an. Weitere Informationen finden Sie unter Auf die Internet-basierte Schnittstelle zugreifen.

2. Klicken Sie in der **System** struktur auf **System** und dann auf dem Register **Konsole** auf **Konsolenumleitung**.

ANMERKUNG: Wenn Sie eine Sicherheitswarnung erhalten, die Sie auffordert, das Konsolenumleitungs-Plug-In zu installieren und auszuführen, überprüfen Sie die Authentizität des Plug-Ins, und klicken Sie dann auf **Ja**, um das Plug-In zu installieren und auszuführen. Wenn Sie Firefox ausführen, starten Sie den Browser neu, und wechseln Sie dann zu Schritt 1.

3. Verwenden Sie auf der Seite **Konsolenumleitung** die Informationen unter Tabelle 10-4, um sicherzustellen, dass eine Konsolenumleitungssitzung verfügbar ist.

Tabelle 10-4. Informationen zur Seite Konsolenumleitung

Eigenschaft	Beschreibung
Konsolenumleitung aktiviert	Ja/Nein
Videoverschlüsselung aktiviert	Ja/Nein
Lokales Servervideo aktiviert	Ja/Nein
Status	Verbunden oder unterbrochen
Max. Sitzungen	Die maximale Anzahl unterstützter Konsolenumleitungssitzungen.
Aktive Sitzungen	Die aktuelle Anzahl aktiver Konsolenumleitungssitzungen.
Plugin-Typ	Der Typ des Plug-Ins, das Sie auf der Seite **Konsolenumleitungskonfiguration** ausgewählt haben.
Standardzugang für Konsolenfreigabe	Der Zugangsstandardtyp der Konsolenfreigabe, der der Aanforderung des zweiten Benutzers angeboten wird, wenn der erste Benutzer mit der Konsole verbunden ist. Die Zugangsberechtigungen sind: • **Kein Zugang** – Zeigt an, dass dem zweiten Benutzer der Zugang verwehrt wird. • **Schreibgeschützter Zugang** – Gewährt dem zweiten Benutzer nur schreibgeschützten Zugang. • **Voller Zugang** – Gewährt dem zweiten Benutzer den vollen Zugang.

Die Schaltflächen in Tabelle 10-5 sind auf der Seite **Konsolenumleitungskonfiguration** verfügbar.

Tabelle 10-5. Schaltflächen der Seite Konsolenumleitung

Schaltfläche	Definition
Aktualisieren	Lädt die Seite **Konsolenumleitungskonfiguration** neu
Verbindung herstellen	Öffnet eine Konsolenumleitungssitzung auf dem Remote-Zielsystem.
Drucken	Druckt die Seite **Konsolenumleitungskonfiguration** aus

4. klicken Sie, um eine neue Konsole zu öffnen, auf **Verbinden**.

ANMERKUNG: DRAC 5 unterstützt vier gleichzeitige Konsolenumleitungen. Falls Sie eine Sitzung geöffnet ist und ein anderer Benutzer versucht, eine weitere Sitzung im gleichen verwalteten System zu öffnen, erhalten Sie eine Aufforderung zur Gewährung der Berechtigung für den Benutzer. Sie können Zugriff gewähren oder ablehnen. Falls Sie die Berechtigung nicht innerhalb von 30 Sekunden gewähren, wird die Aufforderung deaktiviert.

Wenn Sie einen Firefox-Browser verwenden, werden Sie aufgefordert, eine JNLP-Datei zu öffnen oder zu speichern. Sie können diese mit dem *Java Web Start Launcher* öffnen. Wenn Sie sich dafür entscheiden, die JNLP-Datei zu speichern, öffnen Sie diese manuell, bevor Sie die Sitzung abbrechen. Nachdem Sie die Sitzung abgebrochen haben, kann die gespeicherte JNLP-Datei nicht validiert werden. Wenn Sie den Internet Explorer verwenden, speichert dieser die JNLP-Datei im Ordner *Temporäre Internetdateien* und diese wird automatisch mit dem *Java Web Start Launcher* ausgeführt.

ANMERKUNG: Wenn in den folgenden Schritten ein oder mehrere Fenster zur **Sicherheitswarnung** eingeblendet werden, lesen Sie die Informationen im jeweiligen Fenster und klicken Sie auf **Ja**, um fortzufahren.

Klicken Sie, wenn Sie mit der Nutzung der Konsole fertig sind und sich abgemeldet haben (mittels des Abmeldeverfahrens des Remote-Systems), auf der Konsolenumleitungsseite auf **Verbindung trennen**, oder schließen Sie den Viewer.

Die Management Station wird mit DRAC 5 verbunden, und der Desktop des Remote-Systems wird in der digitalen KVM Viewer-Anwendung von Dell angezeigt.

5. Wenn auf dem Desktop des Remote-Systems zwei Mauszeiger angezeigt werden, synchronisieren Sie die Mauszeiger auf der Management Station und dem Remote-System. Siehe Synchronisieren der Mauszeiger.

Lokales Video deaktivieren oder aktivieren

Führen Sie zum Deaktivieren oder Aktivieren des lokalen Videos das folgende Verfahren aus:

1. Öffnen Sie auf der Management Station einen unterstützten Internet- Browser, und melden Sie sich an DRAC 5 an. Weitere Informationen finden Sie unter Auf die Internet-basierte Schnittstelle zugreifen.
2. Klicken Sie in der **System**struktur auf **System**.
3. Klicken Sie auf das Register **Konsole** und dann auf **Konfiguration**.
4. Wenn Sie auf dem Server das lokale Video aktivieren (Einschalten) möchten, wählen Sie auf der Seite **Konsolenumleitungskonfiguration** das Kontrollkästchen **Lokales Servervideo aktiviert** aus, und klicken Sie dann auf **Änderungen übernehmen**. Der Standardwert lautet EIN.
5. Wenn Sie das lokale Video auf dem Server deaktivieren (Ausschalten) möchten, heben Sie auf der Seite **Konsolenumleitungskonfiguration** die Markierung des Kontrollkästchens **Lokales Servervideo aktiviert** auf, und klicken Sie dann auf **Änderungen übernehmen**.

Die Seite **Konsolenumleitung** zeigt den Status des lokalen Servervideos an.

ANMERKUNG: Die Funktion „Video des lokalen Servers aktiviert" wird auf allen x9xx-PowerEdge-Systemen, außer PowerEdge SC1435 und 6950, unterstützt.

ANMERKUNG: Wenn Sie das lokale Video auf dem Server deaktivieren (Ausschalten), wird nur der an den lokalen Server angeschlossene Monitor deaktiviert.

ANMERKUNG: Mit DRAC 5,Version 1.30 und höher können Sie die Konsolenumleitung für einen Remote-Benutzer deaktivieren. Weitere Informationen finden Sie unter Virtuelle DRAC 5-Remote-KVM deaktivieren.

Verwendung des Video Viewer

Der Video Viewer enthält eine Benutzeroberfläche zwischen der Management Station und dem Remote-System, wodurch der Desktop des Remote-Systems sichtbar wird und die Maus-und Tastaturfunktionen von der Management Station aus gesteuert werden können. Wenn Sie eine Verbindung zum Remote-System herstellen, wird der Video Viewer in einem separaten 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 anzupassen, um das Remote-System ordnungsgemäß anzeigen 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 den Cursor im Desktop-Fenster des Viewers zur Mitte des oberen Rands.

Die Menüleiste kann außerdem aktiviert werden, indem Sie die Standard-Funktionstaste <F9> drücken. So weisen Sie diese Funktionstaste einer neuen Funktion zu:

1. Drücken Sie auf <F9>, oder bewegen Sie den Maus-Cursor zum oberen Ende des Video Viewers.
2. Drücken Sie auf den „Reißnagel", um die Viewer-Menüleiste zu sperren.
3. Klicken Sie in der Viewer-Menüleiste auf **Extras**, und wählen Sie **Sitzungsoptionen** aus.
4. Klicken Sie im Fenster **Sitzungsoptionen** auf das Register **Allgemein**.
5. Klicken Sie im Fenster des Registers **Allgemein** im Feld **Menüaktivierungs-Tastenanschlag** auf das Drop-Down-Menü, und wählen Sie eine andere Funktionstaste aus.

6. Klicken Sie auf **Anwenden** und dann auf **OK**.

Tabelle 10-6 enthält die Hauptfunktionen, die in der Viewer-Menüleiste verfügbar sind.

Tabelle 10-6. Auswahlmöglichkeiten auf der Viewer-Menüleiste

Menüelement	Element	Beschreibung
Datei	In Datei erfassen	Zeichnet den aktuellen Remote-Systembildschirm in einer **.bmp**-Datei (Windows) oder einer **.png**-Datei (Linux) auf dem lokalen System auf. Ein Dialogfeld wird angezeigt, in dem Sie die Datei zu einem angegebenen Standort speichern können.
	Beenden	Beendet die Seite **Konsolenumleitung**.
Ansicht	Aktualisieren	Aktualisiert den gesamten Viewport des Remote-Systembildschirms.
	Vollbildschirm	Erweitert den Sitzungsbildschirm von einem Fenster zum Vollbildschirm.
Makros	Verschiedene Tastenkombinationen	Führt eine Tastenanschlag-Kombination auf dem Remote-System aus. So verbinden Sie die Tastatur der Management Station mit dem Remote-System und führen ein Makro aus: 1. Klicken Sie auf **Extras**. 2. Klicken Sie im Fenster **Sitzungsoptionen** auf das Register **Allgemein**. 3. Wählen Sie **Alle Tastenanschläge an Ziel weitergeben** aus. 4. Klicken Sie auf **OK**. 5. Klicken Sie auf **Makros**. 6. Klicken Sie im **Makros**-Menü auf eine Tastenanschlag-Kombination zur Ausführung auf dem Zielsystem.
Extras	Automatische Bildregulierung	Kalibriert die Session Viewer-Videoausgabe neu.
	Manuelle Bildregulierung	Enthält einzelne Steuerungen zur manuellen Einstellung der Videoausgabe des Session Viewers. **ANMERKUNG:** Wird die horizontale Position außermittig eingestellt, führt dies zu einer Desynchronisation der Mauszeiger.
	Sitzungsoptionen	Enthält zusätzliche Session Viewer-Steuerungseinstellungen. Das Register **Maus** ermöglicht Ihnen, das Mausverhalten abhängig vom Betriebssystem zu optimieren. Wählen Sie im Dropdown-Menü einen Beendigungstastenanschlag zum Beenden des Ein-Cursor-Modus aus. Die Option **Beendigungstastenanschlag** ist verfügbar, wenn der Plug-In-Typ **Java** ist. Das Register **Allgemein** enthält die folgenden Optionen: ▪ **Tastatur-Durchschleifmodus –** Wählen Sie **Alle Tastenanschläge ans Ziel weitergeben** aus, um die Tastenanschläge der Management Station an das Remote-System weiterzugeben. ▪ **Menüaktivierungs-Tastenanschlag** – Wählt die Funktionstaste aus, mit der die Viewer-Menüleiste aktiviert wird. Im Listenfeld **Symbolleistenausblendungsverzögerung** können Sie das Intervall zwischen dem Entfernen des Mauszeigers und dem Ausblenden der Menüleiste einstellen, wenn nicht auf die Reißnagel-Schaltfläche der Menüleiste geklickt wird. Diese Option ist verfügbar, wenn der Plug-In-Typ **systemeigen** ist.
Hilfe	-	Aktiviert das **Hilfe**-Menü.

Einstellung der Videoqualität

Der Video Viewer enthält Bildregulierungen, mit denen Sie das Video auf die bestmögliche Ansicht optimieren können. Klicken Sie auf **Hilfe**, um weitere Informationen zu erhalten.

So nehmen Sie eine automatische Regulierung der Videoqualität vor:

1. Rufen Sie die Viewer-Menüleiste auf. Siehe Zugriff auf die Viewer- Menüleiste.

2. Klicken Sie auf **Extras**, und wählen Sie **Automatische Bildregulierung** aus (für **systemeigenes** Plug-In) oder **Bildeinstellungen** (für **Java**-Plug-In), um die Bildqualität des Viewer-Fensters automatisch anzupassen.

So nehmen Sie eine manuelle Regulierung der Videoqualität vor:

1. Rufen Sie die Viewer-Menüleiste auf. Siehe Zugriff auf die Viewer- Menüleiste.

2. Klicken Sie auf **Extras**, und wählen Sie **Manuelle Bildregulierung** (für **systemeigenes** Plug-In) oder **Bildeinstellungen** (für **Java**-Plug-In) aus.

3. Klicken Sie im Fenster **Manuelle Bildregulierung** auf die einzelnen Bildregulierungsschaltflächen, und stellen Sie die Regler nach Bedarf ein.

4. Klicken Sie, wenn Sie fertig sind, auf **Schließen**, um das Dialogfeld **Manuelle Bildregulierung** zu verlassen.

Die folgenden Richtlinien sind zu beachten, wenn Sie die Bildqualität von Hand einstellen:

- Um zu verhindern, dass die Mauszeiger desynchronisiert werden, passen Sie die horizontale Einstellung so an, dass sich der Desktop des Remote-Systems im Mittelpunkt des Sitzungsfensters befindet.
- Wird das Pixel/Störungs-Verhältnis auf Null eingestellt, führt dies zu mehrfachen Bildwiederholungsbefehlen, die im Video Viewer-Fenster einen übermäßigen Netzwerkverkehr und ein flackerndes Bild verursachen. Dell empfiehlt, dass Sie die Einstellung des Pixel/Störungs-Verhältnisses auf eine Stufe setzen, die optimale Systemleistung und Pixel-Verfeinerung bei minimalem Netzwerkaufkommen bietet.

Synchronisieren der Mauszeiger

Wird eine Verbindung zu einem Remote-System von Dell mittels Konsolenumleitung hergestellt, ist die Mausbeschleunigungs-Geschwindigkeit auf dem Remote System eventuell nicht synchron mit dem Mauszeiger auf der Management Station, was dazu führt, dass zwei Mauszeiger im Video Viewer-Fenster erscheinen.

So synchronisieren Sie die Mauszeiger:

1. Rufen Sie die Viewer-Menüleiste auf. Siehe Zugriff auf die Viewer- Menüleiste.
2. Klicken Sie auf **Extras**, und wählen Sie **Sitzungsoptionen** aus.
3. Klicken Sie auf das Register **Maus**, wählen Sie das Betriebssystem der Management Station aus, und klicken Sie auf **OK**.
4. Klicken Sie auf **Extras**, und wählen Sie **Manuelle Bildregulierung** aus.
5. Regulieren Sie die horizontalen Regler so, dass sich der Desktop des Remote-Systems im Mittelpunkt des Sitzungsfensters befindet.
6. Klicken Sie auf **OK**.

Wenn Sie Linux (Red Hat oder Novell) verwenden, werden die standardmäßigen Mauseinstellungen des Betriebssystems verwendet, um den Maus-Pfeil auf dem DRAC 5-Konsolenumleitungsbildschirm zu steuern.

ANMERKUNG: Für Linux-Systeme (Red Hat oder Novell) sind Probleme mit der Synchronisation des Mauspfeils bekannt. Stellen Sie, um Synchronisationsprobleme der Maus auf ein Minimum zu halten, sicher, dass alle Benutzer die standardmäßigen Mauseinstellungen verwenden.

Informationen zum Deaktivieren der Konsolenumleitung finden Sie unter Virtuelle DRAC 5-Remote-KVM deaktivieren.

Verwenden der Spannungssteuerungsoption

Die Spannungssteuerungsoption ermöglicht Folgendes auf dem verwalteten System:

- Einschalten des Systems
- Ausschalten des Systems
- Reset des Systems
- Ausschalten und wieder einschalten des Systems

Spannungssteuerung auf dem verwalteten System:

1. Rufen Sie die Viewer-Menüleiste auf. Siehe Zugriff auf die Viewer- Menüleiste.
2. Klicken Sie auf **Extras** und dann auf **Stromsteuerung**.
3. Klicken Sie auf eine beliebige Option:
   - Schaltet das System ein.
   - Schaltet das System aus.
   - Führt einen Reset des Systems durch. Startet das System neu, ohne es auszuschalten.
   - Schaltet das System aus und wieder ein. Schaltet das System aus und startet es neu.

   Es wird ein Popup-Fenster angezeigt.
4. Klicken Sie auf **Ja** und dann auf **OK**.

Häufig gestellte Fragen

Kann eine neue Remote-Konsolen-Videositzung gestartet werden, wenn das lokale Video auf dem Server ausgeschaltet ist?

Ja.

Warum dauert es 15 Sekunden, das lokale Video auf dem Server auszuschalten, nachdem eine Aufforderung zum Ausschalten des lokalen Videos gegeben wurde?

Hierdurch wird dem lokalen Benutzer die Gelegenheit gegeben, vor dem Ausschalten des Videos eine Maßnahme zu ergreifen.

Gibt es beim Einschalten des lokalen Videos eine Zeitverzögerung?

Nein, wenn DRAC 5 eine Aufforderung zum Einschalten eines lokalen Videos empfangen hat, wird das Video sofort Eingeschaltet.

Kann der lokale Benutzer das Video auch Ausschalten?

Ja, ein lokaler Benutzer kann das Video mithilfe der racadm-CLI (lokal) Ausschalten.

Kann der lokale Benutzer das Video auch Einschalten?

Ja, die racadm-CLI sollte auf dem Server des Benutzers installiert sein und nur wenn der Benutzer über eine RDP-Verbindung, wie z. B. Terminaldienste, Telnet oder SSH auf den Server zugreifen kann. Der Benutzer kann sich dann am Server anmelden und kann racadm (lokal) ausführen, um das Video einzuschalten.

Mein lokales Video ist ausgeschaltet, und ich kann aus einem bestimmten Grund nicht im Remote-Verfahren auf DRAC 5 zugreifen, und ich kann über RDP, Telnet oder SSH nicht auf den Server zugreifen. Wie stelle ich das lokale Video wieder her?

Die einzige Möglichkeit, das lokale Video wiederherzustellen, besteht in diesem Fall darin, das Netzkabel vom Server abzuziehen, den flüchtigen Serverstrom abfließen zu lassen und das Netzkabel wieder anzuschließen. Durch dieses Verfahren wird das lokale Video auf dem Servermonitor wiederhergestellt. Außerdem ändert sich die DRAC 5-Konfiguration in Lokales Video EIN (Standardeinstellung). DRAC 5 muss neu konfiguriert werden, wenn das lokale Video erneut ausgeschaltet werden muss.

Werden durch das Ausschalten des lokalen Videos auch die lokale Tastatur und die lokale Maus ausgeschaltet?

Nein, durch das Ausschalten des lokalen Videos wird nur das Video ausgeschaltet, das vom Monitorausgabeanschluss des Servers abgeht. Die Tastatur und die Maus, die lokal mit dem Server verbunden sind, werden hierdurch *nicht* ausgeschaltet.

Wird durch das Ausschalten des lokalen Servervideos das Video der Remote-vKVM-Sitzung ausgeschaltet?

Nein, das Ein- oder Ausschalten des lokalen Videos ist von der Remote-Konsolensitzung unabhängig.

Welche Berechtigungen muss ein DRAC 5-Benutzer haben, um das lokale Servervideo ein- oder ausschalten zu können?

Jeder Benutzer mit DRAC 5-Konfigurationsberechtigungen kann das lokale Servervideo ein- oder ausschalten.

Wie kann ich den aktuellen Status des lokalen Servervideos abrufen?

Der Status wird auf der Seite **Konsolenumleitungskonfiguration** der Internet-basierten DRAC 5-Schnittstelle angezeigt. Der racadm CLI-Befehl `racadm getconfig -g cfgRacTuning` zeigt den Status im Objekt cfgRacTuneLocalServerVideo an. Der Status ist auch für den lokalen Benutzer auf dem Server-LCD-Bildschirm als „Video AUS" oder „Video AUS in 15" ersichtlich.

Warum passiert es, dass ich den Status „Video AUS" oder „Video AUS in 15" manchmal nicht auf dem Server-LCD-Bildschirm sehe?

Der Status des lokalen Videos ist eine Meldung niedriger Priorität und wird beim Eintreten eines Serverereignisses hoher Priorität maskiert. Die LCD-Meldungen basieren auf einem Prioritätsprinzip. LCD-Meldungen mit hoher Priorität müssen als Erstes geklärt werden, und sobald ein entsprechendes Ereignis gelöscht oder geklärt wurde, wird die nächste Meldung niedrigerer Priorität angezeigt. Die Servervideomeldung auf dem LCD-Bildschirm soll Ihnen zur Information dienen.

Wo kann ich weitere Informationen zur Funktion des lokalen Servervideos erhalten?

In einem Weißbuch, das auf der Dell Support-Website unter **support.dell.com/manuals** zur Verfügung steht, wird diese Funktion erläutert.

Ich sehe Bildverfälschungen auf meinem Bildschirm. Wie kann ich dieses Problem beheben?

Klicken Sie im Fenster **Konsolenumleitung** auf **Aktualisieren**, um den Bildschirm zu aktualisieren.

ANMERKUNG: Es ist eventuell erforderlich, mehrmals auf **Aktualisieren** zu klicken, um die Videostörung zu korrigieren.

Während der Konsolenumleitung sind Tastatur und Maus nach der Rückkehr aus dem Ruhezustand auf einem Windows 2000-System gesperrt. Wodurch wurde dies verursacht?

Um dieses Problem zu lösen, müssen Sie einen Reset von DRAC 5 durchführen, indem Sie den Befehl **racadm racreset** ausführen.

Ich kann vom Fenster Konsolenumleitung den unteren Teil des Systembildschirms nicht sehen.

Stellen Sie sicher, dass die Bildschirmauflösung der Management Station auf 1280x1024 eingestellt ist.

Während der Konsolenumleitung ist die Maus nach der Rückkehr aus dem Ruhezustand auf einem Windows Server 2003-System gesperrt. Warum geschah dies?

Um dieses Problem zu lösen, wählen Sie aus dem Pulldown-Menü des Fensters der virtuellen KVM (vKVM) ein anderes Betriebssystem als Windows für die Mausbeschleunigung aus. Warten Sie 5 bis 10 Sekunden, und wählen Sie Windows dann erneut aus. Wenn das Problem noch immer nicht behoben ist, müssen Sie einen Reset von DRAC 5 durchführen, indem Sie den Befehl **racadm racreset** ausführen.

Wenn das Problem noch immer nicht behoben ist, müssen Sie einen Reset des DRAC 5 durchführen, indem Sie den Befehl **racadm racreset hard** ausführen.

Warum funktionieren die vKVM-Tastatur und der Maus-Mechanismus nicht?

Sie müssen den USB-Controller in den BIOS-Einstellungen des verwalteten Systems auf **Ein mit BIOS-Unterstützung** einstellen. Starten Sie das verwaltete System neu, und drücken Sie auf <F2>, um das Setup einzugeben. Wählen Sie **Integrierte Geräte** aus und dann **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 verfügt nicht über den richtigen ATI-Videotreiber. Der Videotreiber muss mit der DVD *Dell Systems Management Tools and Documentation* aktualisiert werden.

Warum erhalte ich nach Beendigung einer Windows 2000-Installation einen leeren Bildschirm auf der Remote-Konsole?

Das verwaltete System verfügt nicht über den richtigen ATI-Videotreiber. Die DRAC 5-Konsolenumleitung läuft nicht ordnungsgemäß mit einem SVGA-Videotreiber von der Windows 2000-Vertriebs-CD. Es ist erforderlich, Windows 2000 mit der DVD *Dell Systems Management Tools and Documentation* zu installieren, damit sichergestellt werden kann, dass Sie über die neuesten unterstützten Treiber für das verwaltete System verfügen.

Warum erhalte ich beim Laden des Windows 2000-Betriebssystems einen leeren Bildschirm auf dem verwalteten System?

Das verwaltete System verfügt nicht über den richtigen ATI-Videotreiber. Der Videotreiber muss unter Verwendung der DVD *Dell Systems Management Tools and Documentation* aktualisiert werden.

Warum erhalte ich im Windows-Vollbild-DOS-Fenster einen leeren Bildschirm auf dem verwalteten System?

Das verwaltete System verfügt nicht über den richtigen ATI-Videotreiber. Der Videotreiber muss unter Verwendung der DVD *Dell Systems Management Tools and Documentation* aktualisiert werden.

Warum kann ich das BIOS-Setup nicht aufrufen, indem ich die Taste <F2> drücke?

Dieses Verhalten ist in einer Windows-Umgebung typisch. Klicken Sie mit der Maus auf einen Bereich des Konsolenumleitungsfensters, um den Fokus zu regulieren. Bewegen Sie den Fokus mithilfe der Maus zur unteren Menüleiste des Konsolenumleitungsfensters. Klicken Sie auf der unteren Menüleiste auf eines der Objekte.

Warum lässt sich die vKVM-Maus nicht synchronisieren, wenn ich die DVD *Dell Systems Management Tools and Documentation* verwende, um das Betriebssystem im Remote-Zugriff zu installieren?

Konfigurieren Sie die Konsolenumleitung für das Betriebssystem, das auf dem Zielsystem ausgeführt wird.

1. Klicken Sie im vKVM-Symbolleisten-Menü auf **Extras**, und wählen Sie **Sitzungsoptionen** aus.
2. Klicken Sie im Fenster **Sitzungsoptionen** auf das Register **Maus**.
3. Wählen Sie im Feld **Mausbeschleunigung** das Betriebssystem aus, das auf dem Zielsystem ausgeführt wird, und klicken Sie auf **OK**.

Warum synchronisiert die vKVM-Maus nicht, nachdem sie auf einem Windows-System aus dem Ruhezustand zurückkehrt?

Wählen Sie für die Mausbeschleunigung ein anderes Betriebssystem aus dem Pulldown-Menü des vKVM-Fensters aus. Kehren Sie dann zum ursprünglichen Betriebssystem zurück, um die USB-Mauskomponente zu initialisieren.

1. Klicken Sie in der vKVM-Symbolleiste auf **Extras**, und wählen Sie **Sitzungsoptionen** aus.
2. Klicken Sie im Fenster **Sitzungsoptionen** auf das Register **Maus**.
3. Wählen Sie im Feld **Mausbeschleunigung** ein anderes Betriebssystem aus, und klicken Sie auf **OK**.
4. Initialisieren Sie die USB-Maus.

Warum synchronisiert die Maus nicht in DOS, wenn die Konsolenumleitung ausgeführt wird?

Das Dell-BIOS emuliert den Maustreiber als PS/2-Maus. Die PS/2-Maus ist so konzipiert, dass für den Mauszeiger die Relativposition verwendet wird, was die Verzögerung der Synchronisation verursacht. DRAC 5 verfügt über einen USB-Maustreiber, wodurch eine absolute Position und ein genaueres Verfolgen des Mauszeigers ermöglicht werden. Selbst wenn DRAC 5 die absolute USB-Mausposition an das Dell-BIOS überträgt, würde die BIOS-Emulation die Position auf die Relativposition zurückstellen und das Verhalten beibehalten.

Warum synchronisiert die Maus nicht unter der Linux-Textkonsole?

Die virtuelle KVM erfordert den USB-Maustreiber, doch der USB-Maustreiber ist nur unter dem X-Window-Betriebssystem verfügbar.

Ich habe immer noch Probleme mit der Maussynchronisierung.

Stellen Sie sicher, dass sich der Zielsystem-Desktop in der Mitte des Konsolenumleitungsfensters befindet.

1. Klicken Sie in der vKVM-Symbolleiste auf **Extras**, und wählen Sie **Manuelle Bildregulierung** aus.
2. Regulieren Sie die horizontalen und vertikalen Steuerungen wie erforderlich, um den Desktop im Konsolenumleitungsfenster auszurichten.
3. Klicken Sie auf **Close** (Schließen).
4. Bewegen Sie den Maus-Cursor des Zielsystems in die obere linke Ecke des Konsolenumleitungsfensters und dann zurück in die Mitte des Fensters.
5. Wiederholen Sie Schritt 2 bis Schritt 4, bis beide Cursors synchronisiert sind.

Warum funktionieren die vKVM-Maus und -Tastatur nicht, wenn die Mausbeschleunigung für verschiedene Betriebssysteme geändert wird?

Die USB-vKVM-Tastatur und -Maus werden 5 bis 10 Sekunden nach dem Ändern der Mausbeschleunigung inaktiv. Die Netzwerklast kann manchmal dazu führen, dass dieser Vorgang länger als gewöhnlich dauert (mehr als 10 Sekunden).

Warum kann ich vom vKVM-Fenster aus den unteren Bereich des Serverbildschirms nicht sehen?

Stellen Sie sicher, dass die Bildschirmauflösung des Servers auf 1280 x 1024 Pixel bei 60 Hz mit 128 Farben eingestellt ist.

Warum kann ich keine Tastatur oder Maus verwenden, während ich ein Microsoft-Betriebssystem mithilfe einer iDRAC5-Konsolenumleitung im Remote-Zugriff installiere?

Wenn Sie im Remote-Zugriff ein unterstütztes Microsoft-Betriebssystem auf einem System installieren, auf dem im BIOS die Konsolenumleitung aktiviert ist, wird eine EMS-Verbindungs-Meldung eingeblendet, die Sie auffordert, vor dem Fortsetzen des Vorgangs **OK** auszuwählen. Sie können nicht die Maus verwenden, um **OK** im Remote-Zugriff auszuwählen. Sie müssen entweder auf dem lokalen System **OK** auswählen oder das im Remote-Zugriff verwaltete System neu starten. Führen Sie dann eine Neuinstallation aus, und schalten Sie die Konsolenumleitung im BIOS aus.

Diese Nachricht wird durch Microsoft erstellt, um den Benutzer darauf hinzuweisen, dass die Konsolenumleitung aktiviert ist. Um sicherzustellen, dass diese Meldung nicht eingeblendet wird, schalten Sie die Konsolenumleitung im BIOS immer aus, bevor Sie ein Betriebssystem im Remote-Zugriff installieren.

Warum zeigt die Konsolenumleitung das Startmenü des Betriebssystems nicht in der chinesischen, japanischen und koreanischen Version von Microsoft Windows 2000 an?

Ändern Sie das standardmäßige Startbetriebssystem auf Windows 2000-Systemen, die mehrere Betriebssysteme starten können, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz**, und wählen Sie **Eigenschaften** aus.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Klicken Sie auf **Autostart und Wiederherstellung**.
4. Wählen Sie das neue Standardbetriebssystem aus der **Autostart**-Liste aus.
5. Geben Sie in das Feld **Anzeigen** die Anzahl der Sekunden ein, während denen die Auswahlliste angezeigt werden soll, bevor das Standardbetriebssystem automatisch gebootet wird.

Warum zeigt die Num-Tasten-Anzeige auf meiner Management Station nicht den Status der Num-Taste auf dem Remote-Server an?

Wenn über DRAC 5 zugegriffen wird, stimmt die Num-Tasten-Anzeige auf der Management Station nicht unbedingt mit dem Zustand der Num-Taste auf dem Remote-Server überein. Der Zustand der Num-Taste hängt von der Einstellung auf dem Remote-Server ab, wenn die Remote-Sitzung verbunden wird, unabhängig vom Zustand der Num-Taste auf der Management Station.

Warum werden mehrere Session Viewer-Fenster eingeblendet, wenn ich eine Konsolenumleitungssitzung aufbaue?

Sie konfigurieren eine Konsolenumleitungssitzung für das lokale System. Konfigurieren Sie die Sitzung für ein 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 benötige ich, um eine Konsolenumleitungssitzung auszuführen?

Zum Erzielen guter Leistung empfiehlt Dell eine 5 MB/s-Verbindung. Eine 1 MB/s-Verbindung ist zum Erzielen der Mindestleistung erforderlich.

Was sind die Mindestsystemanforderungen für meine Management Station zum Ausführen der Konsolenumleitung?

Die Management Station erfordert einen Intel Pentium III 500-MHz-Prozessor mit mindestens 256 MB RAM.

Wie viele Konsolenumleitungssitzungen kann ich maximal auf einem Remote-System ausführen?

DRAC 5 unterstützt bis zu zwei gleichzeitige Konsolenumleitungssitzungen.

Warum habe ich Probleme mit dem Synchronisieren der Maus?

Für Linux-Systeme (Red Hat oder Novell) sind Probleme mit der Synchronisation des Mauspfeils bekannt. Stellen Sie, um Synchronisationsprobleme der Maus auf ein Minimum zu halten, sicher, dass alle Benutzer die standardmäßigen Mauseinstellungen verwenden.

Wie kann ich einen Internet-Browser auf meiner Management Station installieren, auf der sich ein schreibgeschütztes Dateisystem befindet?

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

△ **VORSICHTSHINWEIS: In einer schreibgeschützten Client-Umgebung wird das installierte VM-Plug-In betriebsunfähig, wenn die DRAC 5-Firmware auf eine neuere Version des Plug-Ins aktualisiert wird. Dies ist der Fall, weil früheren Plug-In-Funktionen nicht erlaubt wird, zu funktionieren, wenn die Firmware eine neuere Plug-In-Version enthält. In diesem Fall werden Sie zur Plug-In-Installation aufgefordert. Da das Dateisystem schreibgeschützt ist, schlägt die Installation fehl, und die Plug-In-Funktionen sind nicht verfügbar.**

So erhalten Sie das Plug-In-Installationspaket:

1. Melden Sie sich an einem vorhandenen DRAC 5 an.
2. Ändern Sie die URL in der Adresszeile des Browsers von

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

in

```
https://<RAC_IP>/Plug-Ins/ # Achten Sie darauf, auch den abschließenden Schrägstrich 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 unter...** aus.

4. Wählen Sie einen Speicherort für die Datei des Plug-In- Installationspakets aus.

So installieren Sie das Plug-In-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 auf der Browser-Adresszeile den Dateipfad zum Plug-In- Installationspaket ein. Beispiel:

   Datei:///tmp/rac5vm.xpi

4. Der Browser führt den Benutzer durch die Plug-In-Installation.

Wenn die Installation einmal durchgeführt wurde, fordert der Browser diese Plug-In-Installation nicht erneut an, solange die Ziel-DRAC5-Firmware keine neuere Version des Plug-Ins enthält.

Warum wird die Konsolenumleitungssitzung beendet, wenn ich meinen Terminal neu starte?

befindet sich die DRAC 5-NIC-Einstellungen im „freigegebenen" oder „mit Failover freigegebenen" Modus, verursacht ein System-Reset das Zurücksetzen der LAN-On-Hauptplatine (LOM). Auf Netzwerken mit Schaltern, deren Spanning Tree Protocol (STP) aktiviert ist, verursacht dies, dass die Verbindung zwischen der Management Station und dem Client nach etwa 10 bis 15 Sekunden neu hergestellt wird. Es ergibt sich daraus, dass die Konnektivität mit dem Remote-System verloren geht, und dass auf der Konsolenumleitung und auf den Clients des virtuellen Datenträgers eine Verbindungsabbruch-Fehlermeldung angezeigt wird. Wenn Sie zu diesem Zeitpunkt auf die DRAC-GUI zugreifen, wird die Fehlermeldung „Seite nicht gefunden" angezeigt.

So umgehen Sie das Problem:

- Verwenden Sie den DRAC 5-dedizierten NIC für die Verbindung über das Netzwerk.
- Deaktivieren Sie STP auf den Netzwerkschaltern.

Zurück zum Inhaltsverzeichnis