

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00: Benutzerhandbuch

[iDRAC-Übersicht](#)

[iDRAC konfigurieren](#)

[Verwaltungsstation konfigurieren](#)

[Verwalteten Server konfigurieren](#)

[iDRAC mittels der Webschnittstelle konfigurieren](#)

[iDRAC mit Microsoft Active Directory verwenden](#)

[GUI-Konsolenumleitung verwenden](#)

[Virtuellen Datenträger konfigurieren und verwenden](#)

[Befehlszeilenoberfläche des lokalen RACADM verwenden](#)

[iDRAC-SM-CLP-Befehlszeilenoberfläche verwenden](#)

[Betriebssystem mittels iVM-CLI bereitstellen](#)

[iDRAC-Konfigurationshilfsprogramm verwenden](#)

[Wiederherstellung und Fehlerbehebung des verwalteten Servers](#)

[Übersicht der RACADM-Unterbefehle](#)


[Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank](#)

[RACADM- und SM-CLP-Äquivalenzen](#)

[Glossar](#)

Anmerkungen und Hinweise

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

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

Irrtümer und technische Änderungen vorbehalten.
© 2007-2008 Dell Inc. Alle Rechte vorbehalten.

Nachdrucke jeglicher Art ohne die vorherige schriftliche Genehmigung von Dell Inc. sind strengstens untersagt.

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

Copyright 1998-2006 The OpenLDAP Foundation. Alle Rechte vorbehalten. Neuverteilung und Verwendung in Quell- und Binärforn mit oder ohne Modifizierung werden nur erlaubt, wenn durch die öffentliche Lizenz von OpenLDAP autorisiert. Eine Kopie dieser Lizenz ist in der Datei LICENSE im Verzeichnis der obersten Ebene der Verteilung erhältlich oder auch unter www.OpenLDAP.org/license.html. OpenLDAP ist ein eingetragenes Markenzeichen von OpenLDAP Foundation. Individuelle Dateien und/oder beigetragene Pakete könnten durch andere Beteiligte urheberrechtlich geschützt sein und zusätzlichen Einschränkungen unterliegen. Diese Arbeit wird vom LDAP v3.3-Vertrieb der University of Michigan abgeleitet. Diese Arbeit enthält außerdem Materialien, die von öffentlichen Quellen stammen. Informationen zu OpenLDAP stehen unter www.openldap.org/ zur Verfügung. Teil-Copyright 1998-2004 Kurt D. Zellenga. Teil-Copyright 1998-2004 Net Boolean Incorporated. Teil-Copyright 2001-2004 IBM Corporation. Alle Rechte vorbehalten. Neuverteilung und Verwendung in Quell- und Binärforn mit oder ohne Modifizierung werden nur erlaubt, wenn durch die öffentliche Lizenz von OpenLDAP autorisiert. Teil-Copyright 1999-2003 Howard Y.H. Chu. Teil-Copyright 1999-2003 Symas Corporation. Teil-Copyright 1998-2003 Hallvard B. Furuseth. Alle Rechte vorbehalten. Neuverteilung und Gebrauch in Quell- und Binärforn mit oder ohne Modifizierung, werden erlaubt vorausgesetzt, dass dieser Hinweis bewahrt wird. Die Namen der Inhaber des Urheberrechts dürfen nicht verwendet werden, um von dieser Software abgeleitete Produkte ohne vorherige schriftliche Erlaubnis zu indossieren oder zu fördern. Diese Software wird ohne Mängelgewähr ohne ausdrückliche oder implizierte Garantie zur Verfügung gestellt. Teil-Copyright (c) 1992-1996 Regenten der University of Michigan. Alle Rechte vorbehalten. Neuverteilung und Gebrauch in Quell- und Binärforn werden erlaubt vorausgesetzt, dass dieser Hinweis bewahrt wird, und dass es der University of Michigan in Ann Arbor anerkannt wird. Der Name der Universität darf nicht verwendet werden, um von dieser Software abgeleitete Produkte ohne vorherige schriftliche Erlaubnis zu indossieren oder zu fördern. Diese Software wird ohne Mängelgewähr ohne ausdrückliche oder implizierte Garantie zur Verfügung gestellt. Alle anderen in dieser Dokumentation genannten Markenzeichen und Handelsbezeichnungen sind Eigentum der entsprechenden Hersteller und Firmen. Dell Inc. verzichtet auf alle Besitzrechte an Markenzeichen und Handelsbezeichnungen, die nicht ihr Eigentum sind.

März 2008 Rev. A01

[Zurück zum Inhaltsverzeichnis](#)

Übersicht der RACADM-Unterbefehle

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [help](#)
- [config](#)
- [getconfig](#)
- [getssninfo](#)
- [getsysinfo](#)
- [getractime](#)
- [setniccfg](#)
- [getniccfg](#)
- [getsvctag](#)
- [racreset](#)
- [racresetcfg](#)
- [serveraction](#)
- [getractlog](#)
- [clrraclog](#)
- [getsel](#)
- [clrsl](#)
- [getractelog](#)
- [sslcsrgen](#)
- [sslcertupload](#)
- [sslcertdownload](#)
- [sslcertview](#)
- [testemail](#)
- [testtrap](#)
- [vmdisconnect](#)

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

help

In [Tabelle A-1](#) wird der Unterbefehl **help** beschrieben.

Tabelle A-1. Befehl Help

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

Zusammenfassung

```
racadm help
```

```
racadm help <Unterbefehl>
```

Beschreibung

Der Unterbefehl **help** listet alle Unterbefehle auf, die verfügbar sind, wenn der Befehl **racadm** zusammen mit einer einzeiligen Beschreibung verwendet wird. Es kann ebenfalls ein Unterbefehl nach dem Befehl **help** eingegeben werden, um die Syntax für einen bestimmten Unterbefehl zu erhalten.

Ausgabe

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

Der Befehl **racadm help <Unterbefehl>** zeigt nur Informationen zu dem festgelegten Unterbefehl an.

Unterstützte Schnittstellen

- 1 Lokaler RACADM

config

In [Tabelle A-2](#) werden die Unterbefehle **config** und **getconfig** beschrieben.

Tabelle A-2. config/getconfig

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

Zusammenfassung

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

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

Unterstützte Schnittstellen

- 1 Lokaler RACADM

Beschreibung

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

Eingabe

In [Tabelle A-3](#) werden die Unterbefehlsoptionen für **config** beschrieben.

Tabelle A-3. config-Unterbefehlsoptionen und -Beschreibungen

Option	Beschreibung
-f	Über die Option -f <Dateiname> kann config den Inhalt der durch <Dateiname> festgelegten Datei lesen und den iDRAC konfigurieren. Die Datei muss Daten in dem Format enthalten, das unter Syntax der Konfigurationsdatei festgelegt ist.
-p	Die Option -p bzw. die Kennwortoption weist config an, die Kennworteinträge in der config-Datei -f <Dateiname> zu löschen, nachdem die Konfiguration abgeschlossen wurde.
-g	Die Option -g <Gruppenname> bzw. die Gruppenoption muss zusammen mit der Option -o verwendet werden. Der <i>Gruppenname</i> gibt die Gruppe an, in der das einzustellende Objekt enthalten ist.
-o	Die Option -o <Objektname> <Wert> bzw. Objektoption muss zusammen mit der Option -g verwendet werden. Diese Option legt den Objektnamen fest, der mit der Zeichenkette <Wert> geschrieben wird.
-i	Die Option -i <Index> bzw. die Indexoption ist nur für an einen Index gekoppelte Gruppen gültig und kann zur Festlegung einer eindeutigen Gruppe verwendet werden. Der Index wird hier durch den Indexwert angegeben und nicht durch einen "Benennungs"-Wert.
-c	Die Option -c bzw. die Überprüfungsoption wird zusammen mit dem Unterbefehl config verwendet und ermöglicht Ihnen, die .cfg -Datei zu parsen, um Syntaxfehler zu finden. Falls Fehler gefunden werden, wird die Zeilennummer zusammen mit einer kurzen Beschreibung des Fehlers angezeigt. Es kommen keine Schreibvorgänge zum iDRAC vor. Diese Option ist nur eine Kontrolle.

Ausgabe

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

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

Dieser Unterbefehl zeigt an, wie viele geschriebene Konfigurationsobjekte sich von wie vielen Gesamtobjekten in der **.cfg**-Datei befinden.


Beispiele

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

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

```
1 racadm config -f myrac.cfg
```

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

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

getconfig

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

speichern.

Eingabe

In [Tabelle A-4](#) werden die Unterbefehlsoptionen für **getconfig** beschrieben.


 **ANMERKUNG:** Die Option **-f** ohne Dateiangabe wird den Dateinhalt an den Terminal-Bildschirm ausgegeben.

Tabelle A-4. **getconfig**-Unterbefehlsoptionen

Option	Beschreibung
-f	Die Option -f <Dateiname> weist getconfig an, die gesamte iDRAC-Konfiguration in eine Konfigurationsdatei zu schreiben. Diese Datei kann dann für Batch-Konfigurationsvorgänge verwendet werden, die den Unterbefehl config anwenden. ANMERKUNG: Die Option -f erstellt keine Einträge für die Gruppen cfglpmiPet und cfglpmiPef . Sie müssen mindestens ein Trap-Ziel einstellen, um die cfglpmiPet -Gruppe zur Datei zu erfassen.
-g	Die Option -g <Gruppenname> bzw. Gruppenoption kann zur Anzeige der Konfiguration einer einzelnen Gruppe verwendet werden. Der <i>Gruppenname</i> ist der Name der Gruppe, die in den racadm.cfg -Dateien verwendet wird. Wenn es sich bei der Gruppe um eine indizierte Gruppe handelt, verwenden Sie die Option -i .
-h	Die Option -h bzw. die Hilfeoption zeigt eine Liste aller verfügbarer Konfigurationsgruppen an, die verwendet werden können. Diese Option ist nützlich, wenn die genauen Gruppennamen nicht bekannt sind.
-i	Die Option -i <Index> bzw. die Indexoption ist nur für an einen Index gekoppelte Gruppen gültig und kann zur Festlegung einer eindeutigen Gruppe verwendet werden. Wenn die Option -i <Index> nicht festgelegt ist, wird ein Wert von 1 für Gruppen angenommen, bei denen es sich um Tabellen mit mehreren Einträgen handelt. Der Index wird durch den Indexwert angegeben und nicht durch einen "Benennungs"-Wert.
-o	Die Option -o <Objektname> bzw. die Objektoption bestimmt den Objektnamen, der in der Abfrage verwendet wird. Diese Option kann mit der Option -g verwendet werden.
-u	Die Option -u <Benutzername> bzw. die Benutzernamensoption kann verwendet werden, um die Konfiguration für den festgelegten Benutzer anzuzeigen. Die Option <Benutzername> ist der Anmelde-name des Benutzers.
-v	Die Option -v bzw. die ausführliche Option zeigt zusätzlich zu den Eigenschaften weitere Details an und wird mit der Option -g verwendet.

Ausgabe

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

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

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

Beispiele

```
1 racadm getconfig -g cfgLanNetworking
```

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

```
1 racadm getconfig -f myrac.cfg
```

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

```
1 racadm getconfig -h
```

Zeigt eine Liste der verfügbaren Konfigurationsgruppen auf dem iDRAC an.

```
1 racadm getconfig -u Wurzel
```

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

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

Zeigt die Benutzergruppeninstanz bei Index 2 mit ausführlichen Informationen zu den Eigenschaftswerten an.

Zusammenfassung

```
racadm getconfig -f <Dateiname>
```

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

```
racadm getconfig -u <Benutzername>
```

```
racadm getconfig -h
```

Unterstützte Schnittstellen

- 1 Lokaler RACADM

getssninfo

In [Tabelle A-5](#) wird der Unterbefehl `getssninfo` beschrieben.

Tabelle A-5. Unterbefehl `getssninfo`

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

Zusammenfassung

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

Beschreibung

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

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

Unterstützte Schnittstellen

- 1 Lokaler RACADM

Eingabe

In [Tabelle A-6](#) werden die Unterbefehlsoptionen für `getssninfo` beschrieben.

Tabelle A-6. `getssninfo`-Unterbefehl - Optionen

Option	Beschreibung
<code>-A</code>	Die Option <code>-A</code> verhindert die Ausgabe von Kopfzellen.
<code>-u</code>	Die Benutzernamensoption <code>-u <Benutzername></code> begrenzt die ausgedruckte Ausgabe auf detaillierte Sitzungseinträge für den angegebenen Benutzernamen. Wird als Benutzername ein Sternchensymbol (*) angegeben, werden alle Benutzer aufgeführt. Es werden keine zusammenfassenden Informationen ausgegeben, wenn diese Option angegeben wird.

Beispiele

- 1 `racadm getssninfo`

[Tabelle A-7](#) enthält ein Ausgabebeispiel des Befehls `racadm getssninfo`.

Tabelle A-7. Ausgabebeispiel für den Unterbefehl `getssninfo`

--	--	--	--

Benutzer	IP-Adresse	Typ	Konsolen
root	192.168.0.10	Telnet	Virtual KVM

```

1 racadm getssninfo -A

"root" 143.166.174.19 "Telnet" "NONE"

1 racadm getssninfo -A -u *

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

1 "bob" "143.166.174.19" "GUI" "NONE"

```

getsysinfo

[Tabelle A-8](#) beschreibt den **racadm getsysinfo** Unterbefehl.

Tabelle A-8. getsysinfo

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

Zusammenfassung

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

Beschreibung

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

Unterstützte Schnittstellen

```
1 Lokaler RACADM
```

Eingabe

In [Tabelle A-9](#) werden die Unterbefehlsoptionen für **getsysinfo** beschrieben.

Tabelle A-9. getsysinfo-Unterbefehlsoptionen

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

Ausgabe

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

Beispielausgabe

```

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

```

```

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

```

```

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

```

```

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

```

Beispiele

```

l racadm getsysinfo -A -s

"Systeminformationen:" "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "ON"

l racadm getsysinfo -w -s

```

```

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

```

```

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

```

Einschränkungen

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

getractive

In [Tabelle A-10](#) wird der Unterbefehl **getractive** beschrieben.

Tabelle A-10. getractive

Unterbefehl	Definition
getractive	Zeigt die aktuelle Uhrzeit vom Fernzugriff-Controller an.

Zusammenfassung

```
racadm getractive [-d]
```

Beschreibung

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

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

Ausgabe

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

Beispielausgabe

```
racadm getractive
Thu Dec 8 20:15:26 2005
racadm getractive -d
20071208201542.000000
```

Unterstützte Schnittstellen

- 1 Lokaler RACADM
-

setniccfg

[Tabelle A-11](#) beschreibt den Unterbefehl **setniccfg**.

Tabelle A-11. **setniccfg**

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

Zusammenfassung

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

Beschreibung

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

- 1 Die Option **-d** aktiviert DHCP für die NIC (Standardeinstellung: DHCP aktiviert).
- 1 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
```

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

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

Ausgabe

Mit dem Unterbefehl **setniccfg** wird eine angemessene Fehlermeldung angezeigt, wenn der Vorgang erfolglos ist. Wenn erfolgreich, wird eine Meldung angezeigt.

Unterstützte Schnittstellen

getniccfg

In [Tabelle A-12](#) wird der Unterbefehl **getniccfg** beschrieben.

Tabelle A-12. **getniccfg**

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

Zusammenfassung

```
racadm getniccfg
```

Beschreibung

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

Beispielausgabe

Mit dem Unterbefehl **getniccfg** wird eine entsprechende Fehlermeldung angezeigt, wenn der Vorgang nicht erfolgreich ausgeführt werden konnte. Bei erfolgreicher Ausführung wird andernfalls die Ausgabe in folgendem Format angezeigt:

```
NIC Enabled      = 1
DHCP Enabled     = 1
IP Address       = 192.168.0.1
Subnet Mask      = 255.255.255.0
Gateway          = 192.168.0.1
```

Unterstützte Schnittstellen

getsvctag

In [Tabelle A-13](#) wird der Unterbefehl **getsvctag** beschrieben.

Tabelle A-13. **getsvctag**

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

Zusammenfassung

```
racadm getsvctag
```

Beschreibung

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

Beispiel

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

```
Y76TP0G
```

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

Unterstützte Schnittstellen

- 1 Lokaler RACADM
-

racreset

In [Tabelle A-14](#) wird der Unterbefehl **racreset** beschrieben.

Tabelle A-14. racreset

Unterbefehl	Definition
racreset	Setzt den iDRAC zurück.

 **HINWEIS:** Wenn Sie einen `racreset`-Unterbefehl ausgeben, kann der iDRAC bis zu einer Minute in Anspruch nehmen, um in einen einsetzbaren Zustand zurückzukehren.

Zusammenfassung

```
racadm racreset
```

Beschreibung

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

Beispiele

- 1 `racadm racreset`

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

Unterstützte Schnittstellen

- 1 Lokaler RACADM
-

racresetcfg

In [Tabelle A-15](#) wird der Unterbefehl **racresetcfg** beschrieben.

Tabelle A-15. racresetcfg

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

Zusammenfassung

```
racadm racresetcfg
```

Unterstützte Schnittstellen

- 1 Lokaler RACADM

Beschreibung

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

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

serveraction

In [Tabelle A-16](#) wird der Unterbefehl `serveraction` beschrieben.

Tabelle A-16. `serveraction`

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

Zusammenfassung

```
racadm serveraction <Maßnahme>
```

Beschreibung

Der Unterbefehl `serveraction` ermöglicht Benutzern, Stromverwaltungsvorgänge auf dem Host-System auszuführen. [Tabelle A-17](#) beschreibt die `serveraction` Stromsteuerungsoptionen.

Tabelle A-17. `serveraction`-Unterbefehlsoptionen

Zeichenkette	Definition
<code><Maßnahme></code>	Bestimmt die Maßnahme. Die Optionen für die Zeichenkette <code><Maßnahme></code> sind: <ul style="list-style-type: none">1 <code>powerdown</code> - Fährt den verwalteten Server herunter.1 <code>powerup</code> - Fährt den verwalteten Server hoch.1 <code>powercycle</code> - Leitet einen Ein-/Ausschaltvorgang auf dem verwalteten Server ein. Diese Maßnahme ist dem Drücken des Netzschalters auf der Systemvorderseite ähnlich, um das System aus- und dann wieder einzuschalten.1 <code>powerstatus</code> - Zeigt den aktuellen Stromstatus des Servers an (EIN oder AUS).1 <code>hardreset</code> - Führt einen Reset-Vorgang (Neustartvorgang) auf dem verwalteten Server aus.

Ausgabe

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

Unterstützte Schnittstellen

- 1 Lokaler RACADM

getraclog

[Tabelle A-18](#) beschreibt den Befehl `racadm getraclog`.

Tabelle A-18. `getraclog`

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

Zusammenfassung

```
racadm getraclog-i
```

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

Beschreibung

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

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

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

Tabelle A-19. getraclog-Unterbefehloptionen

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

Ausgabe

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

Beispielausgabe

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

Unterstützte Schnittstellen

- 1 Lokaler RACADM

clrraclog

Zusammenfassung

```
racadm clrraclog
```

Beschreibung

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

getsel

In [Tabelle A-20](#) wird der Unterbefehl **getsel** beschrieben.

Tabelle A-20. getsel

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

Zusammenfassung

```
racadm getsel-i
```

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

Beschreibung

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

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

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

Tabelle A-21. Optionen des Unterbefehls getsel

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

Ausgabe

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

Beispiel:

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

Unterstützte Schnittstellen

- 1 Lokaler RACADM
-

clrsel

Zusammenfassung

```
racadm clrsel
```

Beschreibung

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

Unterstützte Schnittstellen

1 Lokaler RACADM

gettracelog

In [Tabelle A-22](#) wird der Unterbefehl `gettracelog` beschrieben.

Tabelle A-22. `gettracelog`

Befehl	Definition
<code>gettracelog -i</code>	Zeigt die Anzahl der Einträge im iDRAC-Ablaufverfolgungsprotokoll an.
<code>gettracelog</code>	Zeigt das Ablaufverfolgungsprotokoll des iDRAC an.

Zusammenfassung

```
racadm gettracelog-i
```

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

Beschreibung

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

Tabelle A-23. Optionen des `gettracelog`-Unterbefehls

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

Ausgabe

Die Standardausgabe-Anzeige enthält Datensatznummer, Zeitstempel, Schweregrad, und Beschreibung. Der Zeitstempel beginnt um Mitternacht, dem 1. Januar, und nimmt so lange zu, bis das verwaltete System startet. Nach dem Start des verwalteten Systems wird die Systemzeit des verwalteten Systems für den Zeitstempel verwendet.

Beispiel:

```
Record: 1
```

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

```
Source: ssnmgrd[175]
```

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

Unterstützte Schnittstellen

sslcsrgen

In [Tabelle A-24](#) wird der Unterbefehl **sslcsrgen** beschrieben.

Tabelle A-24. sslcsrgen

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

Zusammenfassung

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

```
racadm sslcsrgen -s
```

Beschreibung

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

Optionen

In [Tabelle A-25](#) werden die Unterbefehloptionen für **sslcsrgen** beschrieben.

Tabelle A-25. sslcsrgen-Unterbefehloptionen


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

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

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

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

- 1 CSR erfolgreich erstellt.
- 1 CSR existiert nicht.
- 1 CSR-Erstellung im Gange.

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

Beispiele

```
racadm sslcsrgen -s
```

oder

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

Unterstützte Schnittstellen

sslcertupload

In [Tabelle A-26](#) wird der Unterbefehl **sslcertupload** beschrieben.

Tabelle A-26. sslcertupload

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

Zusammenfassung

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

Optionen

In [Tabelle A-27](#) werden die Unterbefehloptionen für **sslcertupload** beschrieben.

Tabelle A-27. sslcertupload-Unterbefehloptionen

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

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

Beispiel

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

Unterstützte Schnittstellen

- 1 Lokaler RACADM
-

sslcertdownload

In [Tabelle A-28](#) wird der Unterbefehl **sslcertdownload** beschrieben.

Tabelle A-28. sslcertdownload

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

Zusammenfassung

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

Optionen

In [Tabelle A-29](#) werden die Unterbefehloptionen für **sslcertdownload** beschrieben.

Tabelle A-29. sslcertdownload-Unterbefehloptionen

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

Der Befehl **sslcertdownload** gibt bei Erfolg 0 und bei Nichterfolg einen anderen Wert als 0 zurück.

Beispiel

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

Unterstützte Schnittstellen

- 1 Lokaler RACADM

sslcertview

In [Tabelle A-30](#) wird der Unterbefehl **sslcertview** beschrieben.

Tabelle A-30. sslcertview

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

Zusammenfassung

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

Optionen

In [Tabelle A-31](#) werden die Unterbefehloptionen für **sslcertview** beschrieben.

Tabelle A-31. sslcertview-Unterbefehloptionen

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

Ausgabebeispiel

```
racadm sslcertview -t 1

Serial Number           : 00

Subject Information:
Country Code (CC)      : US
State (S)              : Texas
```

```

Locality (L)           : Round Rock
Organization (O)       : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN)       : iDRAC default certificate

```

```

Issuer Information:
Country Code (CC)     : US
State (S)             : Texas
Locality (L)         : Round Rock
Organization (O)      : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN)     : iDRAC default certificate

```

```

Valid From           : Jul 8 16:21:56 2005 GMT
Valid To             : Jul 7 16:21:56 2010 GMT

```

```
racadm sslcertview -t 1 -A
```

```

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT

```

Unterstützte Schnittstellen

- 1 Lokaler RACADM

testemail

In [Tabelle A-32](#) wird der Unterbefehl **testemail** beschrieben.

Tabelle A-32. testemail-Konfiguration

Unterbefehl	Beschreibung
testemail	Prüft die E-Mail-Warnmeldungsfunktion des iDRAC.

Zusammenfassung

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

Beschreibung

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

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

Tabelle A-33. Test-E-Mail-Konfiguration

Maßnahme	Befehl
Aktivieren Sie die Warnung	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
Stellen Sie die Ziel-E-Mail-Adresse ein	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com
Stellen Sie die kundenspezifische Meldung ein, die zur Ziel-E-Mail-Adresse gesendet wird	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "Dies ist ein Test! "
Stellen Sie sicher, dass die SNMP-IP-Adresse korrekt konfiguriert wird	racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr -i 192.168.0.152

Die aktuellen E-Mail-Warnungseinstellungen ansehen

```
racadm getconfig -g cfgEmailAlert -i <Index>
```

wo <index> ist eine Zahl zwischen 1 und 4

Optionen

In [Tabelle A-34](#) werden die Unterbefehloptionen für **testemail** beschrieben.

Tabelle A-34. Option für Unterbefehl testemail

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

Ausgabe

Keine.

Unterstützte Schnittstellen

- 1 Lokaler RACADM

testtrap

In [Tabelle A-35](#) wird der Unterbefehl **testtrap** beschrieben.

Tabelle A-35. testtrap

Unterbefehl	Beschreibung
testtrap	Prüft die SNMP-Trap-Warnmeldungsfunktion des iDRAC.

Zusammenfassung

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

Beschreibung

Mit dem Unterbefehl **testtrap** wird die SNMP-Trap-Warnmeldungsfunktion des iDRAC geprüft, indem ein Test-Trap vom iDRAC an einen festgelegten Ziel-Trap-Abhörer auf dem Netzwerk gesendet wird.

Bevor Sie den Unterbefehl **testtrap** ausführen, stellen Sie sicher, dass der festgelegte Index in der RACADM-Gruppe [cfgIpmiPet](#) korrekt konfiguriert ist.

[Tabelle A-36](#) enthält eine Liste und zugehörige Befehle für die Gruppe [cfgIpmiPet](#).

Tabelle A-36. cfg-E-Mail-Warnungsbefehle

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

Eingabe

In [Tabelle A-37](#) werden die Unterbefehloptionen für **testtrap** beschrieben.

Tabelle A-37. testtrap-Unterbefehloptionen

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

Unterstützte Schnittstellen

- 1 Lokaler RACADM
-

vmdisconnect

In [Tabelle A-38](#) wird der Unterbefehl **vmdisconnect** beschrieben.

Tabelle A-38. vmdisconnect

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

Zusammenfassung

```
racadm vmdisconnect
```

Beschreibung

Mit dem Unterbefehl **vmdisconnect** kann ein Benutzer die Sitzung des virtuellen Datenträgers eines anderen Benutzers abbrechen. Wenn die Webschnittstelle unterbrochen wurde, spiegelt sie den korrekten Verbindungsstatus wider. Dies ist nur durch die Verwendung von lokalem RACADM verfügbar.

Der Unterbefehl **vmdisconnect** ermöglicht einem iDRAC-Benutzer, alle aktiven Sitzungen des virtuellen Datenträgers abzubreaken. Die aktiven Sitzungen des virtuellen Datenträgers können auf der RAC-Webschnittstelle oder durch die Verwendung des RACADM-Unterbefehls [getsysinfo](#) angezeigt werden.

Unterstützte Schnittstellen

- 1 Lokaler RACADM
-

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Anzeigbare Zeichen](#)
- [idRacInfo](#)
- [cfgLanNetworking](#)
- [cfgUserAdmin](#)
- [cfgEmailAlert](#)
- [cfgSessionManagement](#)
- [cfgSerial](#)
- [cfgRacTuning](#)
- [ifcRacManagedNodeOs](#)
- [cfgRacSecurity](#)
- [cfgRacVirtual](#)
- [cfgActiveDirectory](#)
- [cfgStandardSchema](#)
- [cfgIpmiSol](#)
- [cfgIpmiLan](#)
- [cfgIpmiPef](#)
- [cfgIpmiPet](#)

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

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

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

Anzeigbare Zeichen

Anzeigbare Zeichen umfassen den folgenden Satz:

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

idRacInfo

Diese Gruppe enthält Anzeigeparameter, um Informationen zu den Einzelheiten des abgefragten iDRACs zu bieten.

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

idRacProductInfo (Nur-Lesen)

Zulässige Werte

Zeichenkette mit bis zu 63 ASCII-Zeichen.

Standardeinstellung

Integrierter Dell Remote Access Controller

Beschreibung

Eine Textzeichenkette, die das Produkt identifiziert.

idRacDescriptionInfo (Nur-Lese)

Zulässige Werte

Zeichenkette mit bis zu 255 ASCII-Zeichen

Standardeinstellung

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

Beschreibung

Eine Textbeschreibung des RAC-Typs.

idRacVersionInfo (Nur-Lese)

Zulässige Werte

Zeichenkette mit bis zu 63 ASCII-Zeichen.

Standardeinstellung

1.0

Beschreibung

Eine Zeichenkette, die die aktuelle Produktfirmware-Version enthält.

idRacBuildInfo (Nur-Lesen)

Zulässige Werte

Zeichenkette mit bis zu 16 ASCII-Zeichen.

Standardeinstellung

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

Beschreibung

Eine Zeichenkette mit der aktuellen Produkt-Build-Version.

idRacName (Nur-Lesen)

Zulässige Werte

Zeichenkette mit bis zu 15 ASCII-Zeichen

Standardeinstellung

iDRAC

Beschreibung

Ein vom Benutzer vergebener Name zur Identifizierung dieses Controllers.

idRacType (Nur-Lesen)

Standardeinstellung

8

Beschreibung

Identifiziert den Typ des Remote Access Controllers als iDRAC.

cfgLanNetworking

Diese Gruppe enthält Parameter zum Konfigurieren der iDRAC-NIC.

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

cfgDNSDomainNameFromDHCP (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0


Beschreibung

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

cfgDNSDomainName (Lesen/Schreiben)

Zulässige Werte

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

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

Standardeinstellung

""


Beschreibung

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

cfgDNSRacName (Lesen/Schreiben)

Zulässige Werte

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

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

Standardeinstellung

rac-Service-Tag-Nummer

Beschreibung

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

cfgDNSRegisterRac (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Registriert den iDRAC-Namen auf dem DNS-Server.

cfgDNSServersFromDHCP (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

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


cfgDNSServer1 (Lesen/Schreiben)

Zulässige Werte

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

Beschreibung

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

 **ANMERKUNG:** `cfgDNSServer1` und `cfgDNSServer2` können beim Austauschen von Adressen auf identische Werte eingestellt werden.

cfgDNSServer2 (Lesen/Schreiben)

Zulässige Werte


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

Standardeinstellung

0.0.0.0

Beschreibung

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

 **ANMERKUNG:** `cfgDNSServer1` und `cfgDNSServer2` können beim Austauschen von Adressen auf identische Werte eingestellt werden.

cfgNicEnable (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)


Standardeinstellung

0

Beschreibung

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

cfgNicIpAddress (Lesen/Schreiben)

 **ANMERKUNG:** Dieser Parameter kann nur konfiguriert werden, wenn der Parameter `cfgNicUseDhcp` auf 0 (FALSE) eingestellt ist.

Zulässige Werte

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

Standardeinstellung


192.168.0.*n*

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

Beschreibung

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

cfgNicNetmask (Lesen/Schreiben)

 **ANMERKUNG:** Dieser Parameter kann nur konfiguriert werden, wenn der Parameter `cfgNicUseDhcp` auf 0 (FALSE) eingestellt ist.

Zulässige Werte

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


Standardeinstellung

255.255.255.0

Beschreibung

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

cfgNicGateway (Lesen/Schreiben)

 **ANMERKUNG:** Dieser Parameter kann nur konfiguriert werden, wenn der Parameter `cfgNicUseDhcp` auf 0 (FALSE) eingestellt ist.

Zulässige Werte

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

Standardeinstellung

192.168.0.1

Beschreibung

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

cfgNicUseDhcp (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

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

cfgNicMacAddress (Nur-Lese)

Zulässige Werte

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

Standardeinstellung

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

Beschreibung

Die iDRAC-NIC-MAC-Adresse.

cfgUserAdmin

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

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

cfgUserAdminIpmiLanPrivilege (Lesen/Schreiben)

Zulässige Werte

- 2 (Benutzer)
- 3 (Operator)
- 4 (Administrator)
- 15 (Kein Zugriff)

Standardeinstellung

- 4 (Benutzer 2)
- 15 (Alle anderen)

Beschreibung

Die maximale Berechtigung auf dem IPMI LAN-Kanal.

cfgUserAdminPrivilege (Lesen/Schreiben)

Zulässige Werte

0x00000000 bis 0x000001ff

Standardeinstellung

0x00000000

Beschreibung

Diese Eigenschaft legt die für den Benutzer zugelassenen rollenbasierten Autoritätsberechtigungen fest. Der Wert wird als Bitmaske dargestellt, wodurch beliebige Kombinationen von Berechtigungswerten möglich werden. [Tabelle B-1](#) beschreibt die Benutzerberechtigungs-Bitwerte, die zum Erstellen von Bitmasken kombiniert werden können.

Tabelle B-1. Bit-Masken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
----------------------	------------------------

Bei iDRAC anmelden	0x0000001
iDRAC konfigurieren	0x0000002
Benutzer konfigurieren	0x0000004
Protokolle löschen	0x0000008
Serversteuerungsbefehle ausführen	0x0000010
Zugriff auf Konsolenumleitung	0x0000020
Zugriff auf Virtueller Datenträger	0x0000040
Testwarnungen	0x0000080
Debug-Befehle ausführen	0x0000100

Beispiele

[Tabelle B-2](#) enthält Beispielsberechtigungs-Bitmasken für Benutzer mit einer oder mehr Berechtigungen.

Tabelle B-2. Beispiel-Bitmasken für Benutzerberechtigungen

Benutzerberechtigung(en)	Berechtigungs-Bitmaske
Ein Benutzerzugriff auf den iDRAC ist nicht zulässig.	0x00000000
Der Benutzer hat nur die Berechtigung, sich am iDRAC anzumelden und Informationen zum iDRAC sowie zu den Serverkonfigurationen anzuzeigen.	0x00000001
Der Benutzer hat die Berechtigung, sich am iDRAC anzumelden und Konfigurationsänderungen vorzunehmen.	$0x00000001 + 0x00000002 = 0x00000003$
Der Benutzer kann sich am RAC anmelden, auf virtuelle Datenträger und auf die Konsolenumleitung zugreifen.	$0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1$

cfgUserAdminUserName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 16.

Standardeinstellung

...

Beschreibung

Der Name des Benutzers dieses Indexes. Der Benutzer-Index wird durch Schreiben einer Zeichenkette in dieses Namensfeld erzeugt, falls der Index leer ist. Das Schreiben der Zeichenkette von doppelten Notierungen (""") löscht den Benutzer an diesem Index. Der Name kann nicht geändert werden. Sie müssen löschen und dann den Namen neu erstellen. Die Zeichenkette darf keine / (Schrägstriche), \ (umgekehrten Schrägstriche), . (Punkte), @ (Klammeraffen) oder Anführungszeichen enthalten.

 **ANMERKUNG:** Dieser Eigenschaftswert muss im Vergleich zu anderen Benutzernamen eindeutig sein.

cfgUserAdminPassword (Nur Schreiben)

Zulässige Werte

Eine Zeichenkette mit bis zu 20 ASCII-Zeichen

Standardeinstellung

...

Beschreibung

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

Eigenschaft geschrieben wurde.

cfgUserAdminEnable

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert einen einzelnen Benutzer.

cfgUserAdminSolEnable

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

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

cfgEmailAlert

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

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

cfgEmailAlertIndex (Nur-Lesen)

Zulässige Werte

1-4

Standardeinstellung

Dieser Parameter wird beruhend auf vorhandenen Beispielen bestückt.

Beschreibung

Der eindeutige Index eines Warnungsbeispiels.

cfgEmailAlertEnable (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Legt die Ziel-E-Mail-Adresse für E-Mail-Warnungen fest. Beispiel: user1@company.com.

cfgEmailAlertAddress

Zulässige Werte

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

Standardeinstellung

""

Beschreibung

Die E-Mail-Adresse der Warnungsquelle.

cfgEmailAlertCustomMsg

Zulässige Werte

Zeichenkette. Maximale Länge = 32.

Standardeinstellung

""

Beschreibung

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

cfgSessionManagement

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

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

cfgSsnMgtConsRedirMaxSessions (Lesen/Schreiben)

Zulässige Werte

1 - 2

Standardeinstellung

2

Beschreibung

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

cfgSsnMgtWebserverTimeout (Lesen/Schreiben)

Zulässige Werte

60 - 1920

Standardeinstellung

300

Beschreibung

Definiert die Zeitüberschreitung des Web Servers. Diese Eigenschaft stellt die Zeit in Sekunden ein, die eine Verbindung im Leerlauf verbleiben kann (es gibt keine Benutzereingabe). Die Sitzung wird annulliert, wenn die durch diese Eigenschaft eingestellte Frist erreicht wird. Änderungen an dieser Einstellung betreffen die aktuelle Sitzung nicht. Es ist erforderlich, dass Sie sich ab- und wieder anmelden, damit die neuen Einstellungen wirksam werden können.

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

cfgSsnMgtSshIdleTimeout (Lesen/Schreiben)

Zulässige Werte

0 (Kein Zeitlimit)

60 - 1920

Standardeinstellung

300

Beschreibung

Definiert die Zeitüberschreitung für den Secure Shell-Leerlauf. Diese Eigenschaft stellt die Zeit in Sekunden ein, die eine Verbindung im Leerlauf verbleiben kann (es gibt keine Benutzereingabe). Die Sitzung wird annulliert, wenn die durch diese Eigenschaft eingestellte Frist erreicht wird. Änderungen an dieser Einstellung betreffen die aktuelle Sitzung nicht. Es ist erforderlich, dass Sie sich ab- und wieder anmelden, damit die neuen Einstellungen wirksam werden können.

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

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

(Warnung: Sitzung nicht mehr gültig, mögliche Zeitüberschreitung)

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

cfgSsnMgtTelnetIdleTimeout (Lesen/Schreiben)

Zulässige Werte

0 (Kein Zeitlimit)

60 – 1920

Standardeinstellung

300

Beschreibung

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

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

Warnung: Sitzung nicht mehr gültig, mögliche Zeitüberschreitung

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

cfgSerial

Diese Gruppe enthält Konfigurationsparameter für die iDRAC-Dienste.

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

cfgSerialSshEnable (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

1

Beschreibung

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

cfgSerialTelnetEnable (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert die Telnet-Konsolenschnittstelle auf dem iDRAC.

cfgRacTuning

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

cfgRacTuneHttpPort (Lesen/Schreiben)

Zulässige Werte

10 – 65535

Standardeinstellung

80

Beschreibung

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

cfgRacTuneHttpsPort (Lesen/Schreiben)

Zulässige Werte

10 – 65535

Standardeinstellung

443

Beschreibung

Gibt die Schnittstellennummer an, die für die HTTPS-Netzwerkcommunication mit dem iDRAC zu verwenden ist.

cfgRacTuneIpRangeEnable

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

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

cfgRacTuneIpRangeAddr

Zulässige Werte

Zeichenkette, formatierte IP-Adresse. Beispiel: 192.168.0.44.

Standardeinstellung

192.168.1.1

Beschreibung

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

cfgRacTuneIpRangeMask

Zulässige Werte

Normale IP-Maskenwerte mit linksbündigen Bits

Standardeinstellung

255.255.255.0

Beschreibung

Zeichenkette, formatierte IP-Adresse. Beispiel: 255.255.255.0.

cfgRacTuneIpBlkEnable

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

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

cfgRacTuneIpBlkFailCount

Zulässige Werte

2 – 16

Standardeinstellung

5

Beschreibung

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

cfgRacTuneIpBlkFailWindow

Zulässige Werte

10 – 65535

Standardeinstellung

60

Beschreibung

Definiert die Zeitspanne in Sekunden, während der die fehlerhaften Versuche gezählt werden. Wenn Fehlversuche diese Grenze überschreiten, werden sie von der Zählung ausgeschlossen.

cfgRacTuneIpBlkPenaltyTime

Zulässige Werte

10 – 65535

Standardeinstellung

300

Beschreibung

Definiert die Zeitspanne in Sekunden, während der Sitzungsaufforderungen von einer IP-Adresse mit übermäßigen Fehlversuchen zurückgewiesen werden.

cfgRacTuneSshPort (Lesen/Schreiben)

Zulässige Werte

1 – 65535

Standardeinstellung

22

Beschreibung

Gibt die für die iDRAC-SSH-Schnittstelle verwendete Schnittstellenummer an.

cfgRacTuneTelnetPort (Lesen/Schreiben)

Zulässige Werte

1 – 65535

Standardeinstellung

23

Beschreibung

Gibt die für die iDRAC-Telnet-Schnittstelle verwendete Schnittstellenummer an.

cfgRacTuneConRedirEncryptEnable (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

1

Beschreibung

Chiffriert das Video in einer Konsolenumleitungssitzung.

cfgRacTuneConRedirPort (Lesen/Schreiben)

Zulässige Werte

1 – 65535

Standardeinstellung

5900

Beschreibung

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

cfgRacTuneConRedirVideoPort (Lesen/Schreiben)


Zulässige Werte

Standardeinstellung

5901

Beschreibung

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

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

cfgRacTuneAsrEnable (Lesen/Schreiben)

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

0

Beschreibung

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

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

cfgRacTuneWebserverEnable (Lesen/Schreiben)

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

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

cfgRacTuneLocalServerVideo (Lesen/Schreiben)

Zulässige Werte

1 (Wahr)

0 (Deaktivieren)

Standardeinstellung

1

Beschreibung

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

ifcRacManagedNodeOs

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

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

ifcRacMnOsHostname (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

""

Beschreibung

Der Host-Name des verwalteten Servers.

ifcRacMnOsOsName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

""

Beschreibung

Der Betriebssystemname des verwalteten Servers.

cfgRacSecurity

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

Unter dem RACADM [sslcsrgen](#)-Unterbefehl finden Sie weitere Informationen über das Erstellen von Zertifikatsignierungsanforderungen.

cfgSecCsrCommonName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Allgemeinen Namen (CN) an.

cfgSecCsrOrganizationName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Organisationsnamen (O) an.

cfgSecCsrOrganizationUnit (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt die CSR-Organisationseinheit (OU) an.

cfgSecCsrLocalityName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Ort (L) an.

cfgSecCsrStateName (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Gibt den CSR-Zustandsnamen (S) an.

cfgSecCsrCountryCode (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 2.

Standardeinstellung

""

Beschreibung

Gibt die CSR-Landescodes (CC) an

cfgSecCsrEmailAddr (Lesen/Schreiben)

Zulässige Werte

Zeichenkette. Maximale Länge = 254.

Standardeinstellung

""

Beschreibung

Legt die CSR-E-Mail-Adresse fest.

cfgSecCsrKeySize (Lesen/Schreiben)

Zulässige Werte

1024

2048

4096

Standardeinstellung

1024

Beschreibung

Gibt die asymmetrische SSL-Schlüsselgröße für den CSR an.

cfgRacVirtual

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

cfgVirMediaAttached (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

1

Beschreibung

Dieses Objekt wird verwendet, um virtuellen Geräte über den USB-Bus mit dem System zu verbinden. Wenn die Geräte angeschlossen sind, erkennt der Server gültige, am System angeschlossene USB-Massenspeichergeräte. Dies entspricht dem Anschließen eines lokalen USB-CDROM-/Disketten-Laufwerks am USB-Anschluss eines Systems. Wenn die Geräte angeschlossen sind, können Sie im Remote-Zugriff über die iDRAC-Webschnittstelle oder die CLI eine Verbindung zu den virtuellen Geräten herstellen. Durch die Einstellung dieses Objekts auf 0 werden die Geräte veranlasst, sich vom USB-Bus zu trennen.

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

cfgVirAtapiSrvPort (Lesen/Schreiben)

Zulässige Werte

1 - 65535

Standardeinstellung

3668

Beschreibung

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

cfgVirAtapiSrvPortSsl (Lesen/Schreiben)

Zulässige Werte

Jede unbenutzte Schnittstelle zwischen 0 und 65535 dezimal.

Standardeinstellung

3670

Beschreibung

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

cfgVirMediaBootOnce (Lesen/Schreiben)

Zulässige Werte

1 (Aktiviert)

0 (Deaktiviert)

Standardeinstellung

0

Beschreibung

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

cfgFloppyEmulation (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)

Standardeinstellung

0

Beschreibung

Wenn auf 0 eingestellt, wird das virtuelle Diskettenlaufwerk von Windows-Betriebssystemen als Wechselplatte erkannt. Windows-Betriebssysteme werden den Laufwerksbuchstaben C: oder höher während der Aufzählung zuweisen. Wenn auf 1 eingestellt, wird das virtuelle Diskettenlaufwerk als ein Diskettenlaufwerk von Windows-Betriebssystemen erkannt. Windows-Betriebssysteme werden die Laufwerksbuchstaben A: oder B: zuweisen.

cfgActiveDirectory

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

cfgADracDomain (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

""

Beschreibung

Active Directory-Domäne, in der sich der DRAC befindet

cfgAD RacName (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

""

Beschreibung

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

cfgAD Enable (Lesen/Schreiben)

Zulässige Werte

1 (WAHR)

0 (FALSCH)


Standardeinstellung

0

Beschreibung

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

cfgAD AuthTimeout (Lesen/Schreiben)

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

Zulässige Werte

15 – 300

Standardeinstellung

120

Beschreibung

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

cfgADRootDomain (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

""

Beschreibung

Root-Domäne des Domänen-Waldes.

cfgADSpecifyServerEnable (Lesen/Schreiben)

Zulässige Werte

1 oder 0 (Wahr oder Falsch)

Standardeinstellung

0

Beschreibung

1 (Wahr) ermöglicht Ihnen, ein LDAP oder einen Server des globalen Katalogs festzulegen. 0 (Falsch) deaktiviert diese Option.

cfgADDomainController (Lesen/Schreiben)

Gültige IP-Adresse oder ein vollqualifizierter Domänenname (FQDN)

Standardeinstellung

Kein Standardwert

Beschreibung

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

cfgADGlobalCatalog (Lesen/Schreiben)

Zulässige Werte

Gültige IP-Adresse oder vollqualifizierter Domänenname (FQDN)

Standardeinstellung

Kein Standardwert

Beschreibung

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

cfgFloppyEmulation (Lesen/Schreiben)

Zulässige Werte

1 = Aktiviert Active Directory mit dem erweiterten Schema.

2 = Aktiviert Active Directory mit dem Standardschema.

Standardeinstellung

1 = Erweitertes Schema

Beschreibung

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

cfgStandardSchema

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

cfgSSADRoleGroupIndex (Nur-Lesen)

Zulässige Werte

Ganze Zahl von 1 bis 5.

Beschreibung

Index der Rollengruppe, wie im Active Directory registriert.

cfgSSADRoleGroupName (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

(Vordruck)

Beschreibung

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

cfgSSADRoleGroupDomain (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

(Vordruck)

Beschreibung

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

cfgSSADRoleGroupPrivilege (Lesen/Schreiben)

Zulässige Werte

0x00000000 bis 0x000001ff

Standardeinstellung

(Vordruck)

Beschreibung

Verwenden Sie die Bitmaskenwerte [Tabelle B-3](#), um rollenbasierte Autoritätsberechtigungen für eine Rollengruppe einzustellen.

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

Berechtigung der Rollengruppe	Bit-Maske
Bei iDRAC anmelden	0x00000001
iDRAC konfigurieren	0x00000002
Benutzer konfigurieren	0x00000004
Protokolle löschen	0x00000008
Serversteuerungsbefehle ausführen	0x00000010
Zugriff auf Konsolenumleitung	0x00000020
Zugriff auf Virtueller Datenträger	0x00000040
Testwarnungen	0x00000080
Debug-Befehle ausführen	0x00000100

cfgIpmiSol

Diese Gruppe wird zur Konfiguration der SOL-Fähigkeiten (Seriell über LAN) des Systems verwendet.

cfgIpmiSolEnable (Lesen/Schreiben)

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert SOL.

cfgIpmiSolBaudRate (Lesen/Schreiben)

Zulässige Werte

19200, 57600, 115200

Standardeinstellung

115200

Beschreibung

Die Baudrate für die serielle Kommunikation über LAN.

cfgIpmiSolMinPrivilege (Lesen/Schreiben)

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

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

cfgIpmiSolAccumulateInterval (Lesen/Schreiben)

Zulässige Werte

1 - 255.

Standardeinstellung

10

Beschreibung

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

cfgIpmiSolSendThreshold (Lesen/Schreiben)

Zulässige Werte

1 - 255

Standardeinstellung

255

Beschreibung

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

cfgIpmiLan

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

cfgIpmiLanEnable (Lesen/Schreiben)

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

0

Beschreibung

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

cfgIpmiLanPrivLimit (Lesen/Schreiben)

Zulässige Werte

2 (Benutzer)

3 (Operator)

4 (Administrator)

Standardeinstellung

4

Beschreibung

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

cfgIpmiLanAlertEnable (Lesen/Schreiben)

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

0

Beschreibung

Aktiviert oder deaktiviert globale E-Mail-Warmmeldungen. Diese Eigenschaft setzt alle individuellen Aktivierungs-/Deaktivierungseigenschaften für E-Mail-Warmmeldungen außer Kraft.

cfgIpmiEncryptionKey (Lesen/Schreiben)

Zulässige Werte

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

Standardeinstellung

00000000000000000000

Beschreibung

IPMI-Verschlüsselungstaste.

cfgIpmiPetCommunityName (Lesen/Schreiben)

Zulässige Werte

Eine Zeichenkette bis zu 18 Zeichen.

Standardeinstellung

public

Beschreibung

Der SNMP-Community-Name für Traps.

cfgIpmiPef

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

Die Ereignisfilter können zur Kontrolle von Regeln verwendet werden, die mit Maßnahmen in Beziehung stehen, die beim Auftreten kritischer Ereignisse auf dem verwalteten System ausgelöst werden.

cfgIpmiPefName (Nur-Lesen)

Zulässige Werte

Zeichenkette. Maximale Länge = 255.

Standardeinstellung

Der Name des Index-Filters.

Beschreibung

Gibt den Namen des Plattformereignisfilters an.

cfgIpmiPefIndex (Nur-Lesen)

Zulässige Werte

1 – 17

Standardeinstellung

Der Indexwert eines Plattformereignisfilterobjekts.

Beschreibung

Gibt den Index eines spezifischen Plattformereignisfilters an.

cfgIpmiPefAction (Lesen/Schreiben)

Zulässige Werte

0 (Keine)

1 (Herunterfahren)

2 (Reset)

3 (Aus-/Einschaltzyklus)

Standardeinstellung

0

Beschreibung

Legt die Maßnahme fest, die bei Auslösung der Warnung auf dem verwalteten Server ausgeführt wird.

cfgIpmiPefEnable (Lesen/Schreiben)

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert einen spezifischen Plattformereignisfilter.

cfgIpmiPet

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

cfgIpmiPetIndex (Lesen/Schreiben)

Zulässige Werte

1 – 4

Standardeinstellung

Der entsprechende Indexwert.

Beschreibung

Eindeutiger Bezeichner für den Index, der dem Trap entspricht.

cfgIpmiPetAlertDestIpAddr (Lesen/Schreiben)

Zulässige Werte

Eine gültige IP-Adresse darstellende Zeichenkette. Beispiel: 192.168.0.67.

Standardeinstellung

0.0.0.0

Beschreibung

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

cfgIpmiPetAlertEnable (Lesen/Schreiben)

Zulässige Werte

0 (FALSCH)

1 (WAHR)

Standardeinstellung

1

Beschreibung

Aktiviert oder deaktiviert einen spezifischen Trap.

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

RACADM- und SM-CLP-Äquivalenzen

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

[Tabelle C-1](#) führt die RACADM-Gruppen und -Objekte auf und ggf. SM-SLP-äquivalente Speicherorte im SM-CLP-MAP.

Tabelle C-1. RACADM- und SM-CLP-Äquivalenzen

RACADM-Gruppe	SM-CLP	Beschreibung
idRacInfo		
idRacName		Zeichenkette mit bis zu 15 ASCII-Zeichen Standardeinstellung: iDRAC .
idRacProductInfo		Zeichenkette mit bis zu 63 ASCII-Zeichen. Standard: Integrated Dell Remote Access Controller .
idRacDescriptionInfo		Zeichenkette mit bis zu 255 ASCII-Zeichen Standard: Diese Systemkomponente bietet einen vollständigen Satz von Remote-Verwaltungsfunktionen für Dell PowerEdge-Server.
idRacVersionInfo		Zeichenkette mit bis zu 63 ASCII-Zeichen. Standardeinstellung: 1
idRacBuildInfo		Zeichenkette mit bis zu 16 ASCII-Zeichen.
idRacType		Standardeinstellung: 8
cfgActiveDirectory		
	/system1/sp1/oemdelld_adservice1	
cfgADEnable	enablestate	0 zum Deaktivieren, 1 zum Aktivieren. Standardeinstellung: 0
cfgADName	oemdelld_adracname	Zeichenkette von bis zu 254 Zeichen.
cfgADDomain	oemdelld_adracdomain	Zeichenkette von bis zu 254 Zeichen.
cfgADRootDomain	oemdelld_adrootdomain	Zeichenkette von bis zu 254 Zeichen.
cfgADAuthTimeout	oemdelld_timeout	15 bis 300 Sekunden. Standardeinstellung: 120
cfgADType	oemdelld_schematype	1 für Standardschema, 2 für erweitertes Schema. Standardeinstellung: 1
cfgStandardSchema		
cfgSSADRoleGroupIndex		RACADM - Gruppenindex-ID (1-5).
	/system1/sp1/group1 bis /system1/sp1/group5	SM-CLP - ausgewählt mit Adressenpfad.
cfgSSADRoleGroupName	oemdelld_groupname	Zeichenkette von bis zu 254 Zeichen.
cfgSSADRoleGroupDomain	oemdelld_groupdomain	Zeichenkette von bis zu 254 Zeichen.
cfgSSADRoleGroupPrivilege	oemdelld_groupprivilege	Bitmaske mit Werten zwischen 0x00000000 und 0x000001ff.
cfgLanNetworking		
	/system1/sp1/enetport1	
cfgNicMacAddress	macaddress	Die MAC-Adresse der Schnittstelle. Kann nicht bearbeitet werden.
	/system1/sp1/enetport1/lanendpt1/ipendpt1	
cfgNicEnable	oemdelld_nicenable	0 zum Deaktivieren der NIC, 1 zum Aktivieren der NIC. Standardeinstellung: 0
cfgNicUseDHCP	oemdelld_usedhcp	0 zur Konfiguration statischer Netzwerkadressen, 1 zur Verwendung von DHCP. Standardeinstellung: 0
cfgNicIpAddress	ipaddress	Die iDRAC-IP-Adresse. Standard: 192.168.0.120 plus die Serversteckplatznummer.
cfgNicNetmask	subnetmask	Subnetzmaske für das iDRAC-Netzwerk. Standardeinstellung: 255.255.255.0
	committed	Wenn sich Gruppenwerte ändern, wird committed auf 0 eingestellt, um darauf hinzuweisen, dass die neuen Werte nicht gespeichert wurden. Stellen Sie den Wert auf 1 ein, um die neue Konfiguration zu speichern. Standardeinstellung: 1
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1	
cfgDNSDomainName	oemdelld_dnsdomainname	Zeichenkette mit bis zu 254 ASCII-Zeichen Mindestens ein Zeichen muss alphabetisch sein.
cfgDNSDomainNameFromDHCP	oemdelld_domainnamefromdhcp	Auf 1 einstellen, um Domänenname von DHCP abzurufen. Standardeinstellung: 0
cfgDNSRacName	oemdelld_dnsracname	Zeichenkette mit bis zu 63 ASCII-Zeichen. Mindestens ein Zeichen muss

		alphabetisch sein. Standard: iDRAC plus die Dell Service-Tag-Nummer.
cfgDNSRegisterRac	oemdelldnsregisterrac	Auf 1 einstellen, um iDRAC-Name in DNS zu registrieren. Standardeinstellung: 0
cfgDNSServersFromDHCP	oemdelldnsserversfromdhcp	Auf 1 einstellen, um DNS-Server-Adressen von DHCP abzurufen. Standardeinstellung: 0
	/server1/sp1/enetport1/lanendpt1 /ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer1	dnsserveraddresses1	Eine Zeichenkette, die die IP-Adresse eines DNS-Servers repräsentiert.
	/server1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer2	dnsserveraddresses2	Eine Zeichenkette, die die IP-Adresse eines DNS-Servers repräsentiert.
	/server1/sp1/enetport1/lanendpt1/ ipendpt1/remotesap1	
cfgNicGateway	defaultgatewayaddress	Eine Zeichenkette, die die IP-Adresse des Standard-Gateways repräsentiert. Standardeinstellung: 192.168.0.1
cfgRacVirtual	/server1/sp1/oemdelldnsvmservice1	
cfgFloppyEmulation	oemdelldfloppyemulation	Auf 1 einstellen, um Diskettenemulation zu aktivieren. Standardeinstellung: 0
cfgVirMediaAttached	enabledstate	Auf 1 (RACADM)/VMEDIA_ATTACH (SM-CLP)einstellen, um Datenträger anzuschließen. Standardeinstellung: 1 (RACADM)/VMEDIA_ATTACH (SM-CLP)
cfgVirMediaBootOnce	oemdelldsingleboot	Auf 1 einstellen, um nächsten Start von ausgewähltem Datenträger aus durchzuführen. Standardeinstellung 0 .
	/server1/sp1/oemdelldnsvmservice1/ tcpendpt1	
	oemdelldsslenabled	Auf 1 einstellen, wenn SSL für das erste virtuelle Datenträgergerät aktiviert ist, auf 0 einstellen, wenn nicht. Kann nicht bearbeitet werden.
cfgVirAtapiSvrPort	portnumber	Für das erste virtuelle Datenträgergerät zu verwendende Schnittstelle. Standardeinstellung: 3668
	/server1/sp1/oemdelldnsvmservice1/ tcpendpt2	
	oemdelldsslenabled	Auf 1 einstellen, wenn SSL für das zweite virtuelle Datenträgergerät aktiviert ist, auf 0 einstellen, wenn nicht. Kann nicht bearbeitet werden.
cfgVirAtapiSvrPortSsl	portnumber	Für das zweite virtuelle Datenträgergerät zu verwendende Schnittstelle. Standardeinstellung: 3670
cfgUserAdmin	/server1/sp1/oemdelldnsvmservice1/ tcpendpt2	
cfgUserAdminEnable	enabledstate	Auf 1 einstellen, um Benutzer zu aktivieren. Standardeinstellung: 0
cfgUserAdminIndex	userid	Benutzerindex, von 1 bis 16.
cfgUserAdminIpmiLanPrivilege	oemdelldipmilanprivileges	2 (Benutzer), 3 (Operator), 4 (Administrator) oder 15 (Kein Zugriff). Standardeinstellung: 4
cfgUserAdminPassword	Kennwort	Eine Zeichenkette mit bis zu 20 ASCII-Zeichen
cfgUserAdminPrivilege	oemdelldextendedprivileges	Bitmaskenwert zwischen 0x00000000 und 0x000001ff. Standardeinstellung: 0x00000000
cfgUserAdminSolEnable	solenabled	Auf 1 einstellen, um Benutzer die Verwendung von Seriell über LAN zu gestatten. Standardeinstellung: 0
cfgUserAdminUserName	username	Zeichenkette von bis zu 16 Zeichen.
cfgEmailAlert		
cfgEmailAlertAddress		E-Mail-Zieladresse, bis zu 64 Zeichen.
cfgEmailAlertCustomMsg		In E-Mail zu sendende Nachricht, bis zu 32 Zeichen.
cfgEmailAlertEnable		Auf 1 einstellen, um die E-Mail-Warnung zu aktivieren. Standardeinstellung: 0
cfgEmailAlertIndex		Index der E-Mail-Warnungsinstanz. Zahl von 1 bis 4.
cfgSessionManagement		
cfgSsnMgtConsRedirMaxSessions		Anzahl gleichzeitig zugelassener Konsolenumleitungssitzungen (1 oder 2). Standardeinstellung: 2
cfgSsnMgtSshIdleTimeout		Anzahl der Sekunden im Leerlauf, bevor für die SSH-Sitzung eine Zeitüberschreitung eintritt. 0 zum Deaktivieren der Zeitüberschreitung oder 60-1920 Sekunden. Standardeinstellung: 300

cfgSsnMgtTelnetIdleTimeout		Anzahl der Sekunden im Leerlauf, bevor für eine Telnet-Sitzung eine Zeitüberschreitung eintritt. 0 zum Deaktivieren der Zeitüberschreitung oder 60-1920 Sekunden. Standardeinstellung: 300
cfgSsnMgtWebserverTimeout		Anzahl der Sekunden im Leerlauf, bevor für die Webschnittstellensitzung eine Zeitüberschreitung eintritt. 60-1920 Sekunden. Standardeinstellung: 300
cfgRacTuning		
cfgRacTuneConRedirEnable		Auf 1 einstellen, um Konsolenumleitung zu aktivieren, auf 0 einstellen, um sie zu deaktivieren. Standardeinstellung: 1
cfgRacTuneConRedirEncryptEnable		Auf 1 einstellen, um Verschlüsselung des Konsolenumleitungs-Netzwerkdatenverkehrs zu aktivieren, auf 0 einstellen, um sie zu deaktivieren. Standardeinstellung: 1
cfgRacTuneConRedirPort		Für die Konsolenumleitung zu verwendende Schnittstelle. Standardeinstellung: 5900
cfgRacTuneConRedirVideoPort		Für die Konsolenvideoumleitung zu verwendende Schnittstelle. Standardeinstellung: 5901
cfgRacTuneHttpPort		Die für Webschnittstellen-HTTP zu verwendende Schnittstelle. Standardeinstellung: 80
cfgRacTuneHttpsPort		Die für sicheres Webschnittstellen-HTTPS zu verwendende Schnittstelle. Standardeinstellung: 443
cfgRacTuneIpBlkEnable		Auf 1 einstellen, um IP-Blockierung zu aktivieren. Standardeinstellung: 0
cfgRacTuneIpBlkFailCount		Anzahl der fehlgeschlagenen, zu zählenden Anmeldeversuche, bevor IP blockiert wird (2 bis 16). Standardeinstellung: 5
cfgRacTuneIpBlkFailWindow		Zeitspanne in Sekunden, während der die fehlgeschlagenen Anmeldeversuche gezählt werden (10 bis 65535). Standardeinstellung: 60
cfgRacTuneIpBlkPenaltyTime		Zeitspanne in Sekunden, während der eine blockierte IP blockiert bleibt (10 bis 65535). Standardeinstellung: 300
cfgRacTuneIpRangeAddr		Basis-IP-Adresse für IP-Bereichsfilter. Standardeinstellung: 192.168.0.1
cfgRacTuneIpRangeEnable		Auf 1 einstellen, um IP-Bereichsfilterung zuzulassen. Standardeinstellung: 0
cfgRacTuneIpRangeMask		Bitmaske zur Auswahl gültiger IP-Adressen auf Basisadresse angewendet. Standardeinstellung: 255.255.255.0
cfgRacTuneLocalServerVideo		Auf 1 einstellen, um lokale iKVM-Konsole zu aktivieren. Standardeinstellung: 1
cfgRacTuneSshPort		Für den SSH-Dienst zu verwendende Schnittstelle. Standardeinstellung: 22
cfgRacTuneTelnetPort		Für den Telnet-Dienst zu verwendende Schnittstelle. Standardeinstellung: 23
cfgRacTuneWebserverEnable		Auf 1 einstellen, um die iDRAC-Webschnittstelle zu aktivieren. Standardeinstellung: 1
ifcRacManagedNodeOS		
ifcRacMnOsHostname		Host-Name des verwalteten Servers. Zeichenkette von bis zu 255 Zeichen.
ifcRacMnOsOsName		Name des Betriebssystems des verwalteten Servers. Eine Zeichenkette von bis zu 255 Zeichen.
cfgRacSecurity /system1/sp1/oemdel_l_racsecurity1		
cfgRacSecCsrCommonName	commonname	Allgemeiner Name des Active Directory. Zeichenkette von bis zu 254 Zeichen.
cfgRacSecCsrCountryCode	oemdel_l_countrycode	Active Directory, Landesvorwahl. 2 Zeichen.
cfgRacSecCsrEmailAddr	oemdel_l_emailaddress	Die für die Zertifikatsignierungsanforderung zu verwendende E-Mail-Adresse. Zeichenkette von bis zu 254 Zeichen.
cfgRacSecCsrKeySize	oemdel_l_keysize	Länge des Verschlüsselungsschlüssels (512, 1024 oder 2048). Standardeinstellung: 1024 .
cfgRacSecCsrLocalityName	oemdel_l_localityname	Name des Active Directory-Speicherorts. Zeichenkette von bis zu 254 Zeichen.
cfgRacSecCsrOrganizationName	organizationname	Name der Active Directory-Organisation. Zeichenkette von bis zu 254 Zeichen.
cfgRacSecCsrOrganizationUnit	oemdel_l_organizationunit	Name der Active Directory-Organisationseinheit. Zeichenkette von bis zu 254 Zeichen.
cfgRacSecCsrStateName	oemdel_l_statename	Active Directory, Name des Staats. Zeichenkette von bis zu 254 Zeichen.
cfgIpmiSol		
cfgIpmiSolAccumulateInterval		Höchstanzahl der abzuwartenden Millisekunden, bevor ein teilweises Seriell über LAN-Paket gesendet wird (1 bis 255). Standardeinstellung: 10
cfgIpmiSolBaudRate		Die für Seriell über LAN zu verwendende Baudrate (19200, 57600, 115200). Standardeinstellung: 115200
cfgIpmiSolEnable		Auf 1 einstellen, um die Seriell über LAN-Funktion zu aktivieren. Standardeinstellung: 0
cfgIpmiSolSendThreshold		Maximale Anzahl der zu erfassenden Zeichen, bevor SOL-Daten gesendet werden (1 bis 255). Standardeinstellung: 255
cfgIpmiSolMinPrivilege		Erforderliche Mindestberechtigung für die Verwendung von SOL. 2 (Benutzer), 3 (Operator) oder 4 (Administrator). Standardeinstellung: 4

cfglpmiLan		
cfglpmiEncryptionKey		Eine aus 0 bis 40 Hexadezimalzahlen bestehende Zeichenkette. Standardeinstellung: 00
cfglpmiLanAlertEnable		Auf 1 einstellen, um IPMI LAN-Warnungen zu aktivieren. Standardeinstellung: 0
cfglpmiLanEnable		Auf 1 einstellen, um die IPMI über LAN-Schnittstelle zu aktivieren. Standardeinstellung: 0
cfglpmiPetCommunityName		Eine Zeichenkette von bis zu 18 Zeichen. Standardeinstellung: öffentlich
cfglpmiPef		
cfglpmiPefAction		Die zu treffende Maßnahme bei Feststellung eines Ereignisses. 0 (keine), 1 (Herunterfahren), 2 (Reset), 3 (Aus- und einschalten). Standardeinstellung: 0
cfglpmiPefEnable		Auf 1 einstellen, um Plattformereignisfilterung zu aktivieren. Standardeinstellung: 0
cfglpmiPefIndex		Die Indexnummer des Plattformereignisfilters. (1 - 17)
cfglpmiPefName		Der Name des Plattformereignisses, eine aus bis zu 254 Zeichen bestehende Zeichenkette. Kann nicht bearbeitet werden.
cfglpmiPet		
cfglpmiPetAlertDestIpAddr		IP-Adresse des Plattformereignis-Trap-Empfängers. Standardeinstellung: 0.0.0.0
cfglpmiPetAlertEnable		Auf 1 einstellen, um den Plattformereignis-Trap zu aktivieren. Standardeinstellung: 1
cfglpmiPetIndex		Indexnummer (1-4) des Plattformereignis-Traps.

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

iDRAC-Übersicht

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [iDRAC-Verwaltungsfunktionen](#)
- [iDRAC-Sicherheitsfunktionen](#)
- [Unterstützte Plattformen](#)
- [Unterstützte Betriebssysteme](#)
- [Unterstützte Internebrowser](#)
- [Unterstützte Remote-Zugriffsverbindungen](#)
- [iDRAC-Schnittstellen](#)
- [Weitere nützliche Dokumente](#)

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

Der iDRAC verwendet einen integrierten System-auf-Chip-Mikroprozessor für das Remote-Überwachungs-/Steuerungssystem. Der iDRAC und der verwaltete PowerEdge-Server koexistieren auf der Systemplatine. Das Serverbetriebssystem, bei dem es sich um ein Microsoft® Windows®- oder Linux-Betriebssystem handeln kann, ist zuständig für das Ausführen von Anwendungen; der iDRAC ist zuständig für das Überwachen und Verwalten der Umgebung und des Zustands des Servers außerhalb des Betriebssystems.

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

Verwaltete Server werden in einem Dell M1000-e-Systemgehäuse mit modularen Netzteilen, Kühlungsblöcken und einem Chassis Management Controller (CMC) installiert. Der CMC überwacht und verwaltet alle im Gehäuse installierten Komponenten. Redundante CMCs können für den Fall eines Ausfalls des primären CMCs hinzugefügt werden, um Hot-Failover zu bieten. Das Gehäuse bietet über seine LCD-Anzeige, Verbindungen der lokalen Konsole sowie seine Webschnittstelle Zugriff auf die iDRACs.

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

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

iDRAC-Verwaltungsfunktionen

Der iDRAC bietet die folgenden Verwaltungsfunktionen:


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

iDRAC-Sicherheitsfunktionen

Der iDRAC bietet die folgenden Sicherheitsfunktionen:

- 1 Benutzerauthentifizierung durch Microsoft Active Directory (optional) oder durch Hardware-gespeicherte Benutzer-ID und Kennwörter
- 1 Rollenbasierte Autorität, die einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren
- 1 Benutzer-ID- und Kennwort-Konfiguration über die Webschnittstelle oder SM-CLP

- 1 SM-CLP und Webschnittstellen, die 128-Bit-SSL-Verschlüsselung und 40-Bit-SSL-Verschlüsselung unterstützen (für Länder, in denen 128 Bit nicht verwendet werden können)
- 1 Konfiguration der Sitzungszeitüberschreitung (in Sekunden) über die Webschnittstelle oder SM-CLP
- 1 Konfigurierbare IP-Schnittstellen (wo anwendbar)

 **ANMERKUNG:** Telnet unterstützt SSL-Verschlüsselung nicht.

- 1 Secure Shell (SSH), die eine verschlüsselte Übertragungsschicht zum Zweck höherer Sicherheit verwendet
- 1 Beschränkung der Anmeldemisserfolge pro IP-Adresse, mit Anmeldeblockierung der IP-Adresse bei Überschreitung der Grenze
- 1 Eingeschränkter IP-Adressenbereich für Clients, die eine Verbindung zum iDRAC herstellen

Unterstützte Plattformen

Der iDRAC unterstützt die folgenden PowerEdge-Systeme im Dell PowerEdge M1000-e-Systemgehäuse:

- 1 PowerEdge M600
- 1 PowerEdge M605

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

Unterstützte Betriebssysteme


[Tabelle 1-1](#) führt die Betriebssysteme auf, die den iDRAC unterstützen.

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

Tabelle 1-1. Unterstützte Betriebssysteme

Betriebssystem-Familie	Betriebssystem
Microsoft Windows	<p>Microsoft® Windows Server® 2003 R2 Standard und Enterprise Editions (32-Bit x 86) mit SP2</p> <p>Microsoft Windows Server 2003 Web, Standard und Enterprise (32-Bit x 86) Editions mit SP2</p> <p>Microsoft Windows Server 2003 Standard und Enterprise (x64) Editions mit SP2</p> <p>Microsoft Windows Storage Server 2003 R2 Express, Workgroup, Standard und Enterprise x64 Editions</p> <p>Microsoft Windows Vista® Gold Business und Enterprise Editions</p> <p>Microsoft Windows Server 2008 Web, Standard und Enterprise (32-Bit x 86) Editions</p> <p>Microsoft Windows Server 2008 Web, Standard, Enterprise und Datacenter (x64) Editions</p> <p>ANMERKUNG: Wenn Sie Windows Server 2003 mit dem Service Pack 1 installieren, seien Sie sich bewusst, dass die Sicherheitseinstellungen von DCOM geändert werden. Weitere Informationen finden Sie in Artikel 903220 auf der Microsoft Support-Website unter support.microsoft.com/kb/903220.</p>
Red Hat® Linux®	<p>Enterprise Linux WS, ES und AS (Version 3) (x86 und x86_64)</p> <p>Enterprise Linux WS, ES und AS (Version 4) (x86 und x86_64)</p> <p>Enterprise Linux 5 (x86 und x86_64)</p>
SUSE® Linux	<p>Enterprise Server 9 mit Aktualisierung 2 und Aktualisierung 3 (x86_64)</p> <p>Enterprise Server 10 (Gold) (x86_64)</p>

Unterstützte Internetbrowser

 **HINWEIS:** Konsolenumleitung und Virtueller Datenträger unterstützen nur 32-Bit-Internetbrowser. Das Verwenden von 64-Bit-Webbrowsern führt zu unerwarteten Ergebnissen oder Fehlern.

[Tabelle 1-2](#) führt die als iDRAC-Clients unterstützten Webbrowser auf.

Neueste Informationen befinden sich in der iDRAC-Infodatei und dem *Kompatibilitätshandbuch zu Dell OpenManage Server Administrator*, das sich auf Dells

Support-Website unter support.dell.com befindet.

Tabelle 1-2. Unterstützte Internetbrowser

Betriebssystem	Unterstützter Internetbrowser
Windows	Internet Explorer 6.0 (32-Bit) mit Service Pack 2 (SP2), nur für Windows XP und Windows 2003 R2 SP2
	Internet Explorer 7.0, nur für Windows Vista, Windows XP und Windows 2003 R2 SP2
Linux	Mozilla Firefox 1.5 (32-Bit), nur auf SUSE Linux (Version 10)
	Mozilla Firefox 2.0 (32-Bit)

Unterstützte Remote-Zugriffsverbindungen

[Tabelle 1-3](#) führt die Verbindungsfunktionen auf.

Tabelle 1-3. Unterstützte Remote-Zugriffsverbindungen

Verbindung	Funktionen
iDRAC-NIC	<ul style="list-style-type: none"> 10Mbps/100Mbs/1Gbps Ethernet über CMC Gb Ethernet-Schnittstelle DHCP-Unterstützung SNMP-Traps und E-Mail-Ereignis-Benachrichtigung Unterstützung für SM-CLP-Befehlsshell (Telnet oder SSH), für Verfahren wie iDRAC-Konfigurations-, Systemstart-, Reset-, Einschalt- und Herunterfahren-Befehle Unterstützung für IPMI-Dienstprogramme, wie z. B. ipmitool und ipmishell

iDRAC-Schnittstellen

[Tabelle 1-4](#) führt die Schnittstellen auf, an denen iDRAC nach Verbindungen abhört. [Tabelle 1-5](#) kennzeichnet die Schnittstellen, die der iDRAC als Client verwendet. Diese Informationen sind erforderlich, wenn Firewalls für den Remote-Zugriff auf einen iDRAC geöffnet werden.

Tabelle 1-4. Abhörschnittstellen des iDRAC-Servers

Schnittstellenummer	Funktion
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP +
3668*, 3669*	Dienst des virtuellen Datenträgers
3770*, 3771*	Virtueller Datenträger Secure Service
5900*	Konsolenumleitungstastatur/Maus
5901*	Konsolenumleitungsvideo
* Konfigurierbare Schnittstelle	

Tabelle 1-5. iDRAC-Client-Schnittstellen

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

Weitere nützliche Dokumente

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

- 1 Die iDRAC-Onlinehilfe bietet Informationen über die Verwendung der Webschnittstelle.
- 1 Das *Benutzerhandbuch zu Dell CMC Firmware, Version 1.0* bietet Informationen zur Verwendung des Controllers, der alle Module im Gehäuse verwaltet, in dem sich der PowerEdge-Server befindet.
- 1 Das *Dell OpenManage It Assistant-Benutzerhandbuch* und das *Dell OpenManage IT Assistant-Referenzhandbuch* enthalten Informationen über den IT Assistant.
- 1 Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen zur Installation und Verwendung von Server Administrator.
- 1 Das *Dell Update Packages Benutzerhandbuch* enthält Informationen über Beschaffung und Anwendung von Dell Update-Paketen als ein Teil Ihrer Systemaktualisierungsstrategie.

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

- 1 Das *Produktinformationshandbuch* enthält wichtige Sicherheits- und Durchführungsinformationen. Garantie-Informationen können innerhalb dieses Dokumentes oder als ein getrenntes Dokument beigelegt sein.
- 1 Das *Rack-Installationshandbuch* und die *Rack-Installationsanleitungen*, die Ihrer Rack-Lösung beiliegen, beschreiben, wie das System in einem Rack eingebaut wird.
- 1 Das *Handbuch zum Einstieg* enthält eine Übersicht über die Systemfunktionen, Einrichtung des Systems und technische Daten.
- 1 *Hardwarebenutzerhandbuch* gibt Auskunft über die Systemfunktionen und beschreibt die Fehlerbehebung am System sowie die Installation oder den Austausch von Systemkomponenten.
- 1 Die Dokumentation zur Systems Management Software beschreibt die Funktionen, Anforderungen, Installation und grundlegenden Betrieb der Software.
- 1 Die Betriebssystem-Dokumentation beschreibt wie man (falls erforderlich) die Betriebssystem-Software installiert, konfiguriert und verwendet.
- 1 Die Dokumentation für Komponenten, die Sie getrennt gekauft haben, bietet Informationen, um diese Optionen zu konfigurieren und installieren.
- 1 Aktualisierungen sind manchmal im System enthalten, um Änderungen am System, an der Software, und/oder Dokumentation zu beschreiben.



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

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

[Zurück zum Inhaltsverzeichnis](#)

iDRAC konfigurieren

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00: Benutzerhandbuch

- [Bevor Sie Beginnen](#)
- [Schnittstellen zur Konfiguration des iDRAC](#)
- [Konfigurations-Tasks](#)
- [Netzwerkbetrieb mittels der CMC-Webschnittstelle konfigurieren](#)
- [iDRAC-Firmware aktualisieren](#)

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

Bevor Sie Beginnen

Legen Sie vor der Konfiguration des iDRAC folgende Artikel zurecht:

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

Schnittstellen zur Konfiguration des iDRAC

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

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

Tabelle 2-1. Konfigurationsschnittstellen


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

	<p>vorhandenen Berichterstattungs- und Verwaltungshilfsprogrammen erleichtert wird.</p> <p>Ein Vergleich zwischen den RACADM- und SM-CLP-Befehlen ist unter RACADM- und SM-CLP-Äquivalenzen dargestellt.</p>
IPMI	<p>IPMI definiert einen Standard für integrierte Verwaltungssysteme wie den iDRAC, um mit anderen integrierten Systemen und Verwaltungsanwendungen zu kommunizieren.</p> <p>Sie können die iDRAC-Webschnittstellen-, SM-CLP- oder RACADM-Befehle zur Konfiguration von IPMI-Plattformereignisfiltern (PEFs) und Plattformereignis-Traps (PETs) verwenden.</p> <p>PEFs bewirken, dass der iDRAC auswählbare Maßnahmen ausführt (z. B. den Neustart des verwalteten Servers), wenn er einen entsprechenden Zustand feststellt. PETs weisen den iDRAC an, E-Mail- oder IPMI-Warnungen zu senden, wenn er bestimmte Ereignisse oder Zustände feststellt.</p> <p>Sie können auch standardmäßige IPMI-Hilfsprogramme wie ipmitool und ipmishell bei iDRAC verwenden, wenn Sie IPMI über LAN aktivieren.</p>

Konfigurations-Tasks

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

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

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


Verwaltungsstation konfigurieren


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


- 1 Siehe [Verwaltungsstation konfigurieren](#)

iDRAC-Netzwerkbetrieb konfigurieren

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

 **ANMERKUNG:** Durch das Ändern der iDRAC-Netzwerkeinstellungen werden alle aktuellen Netzwerkverbindungen zum iDRAC abgebrochen.

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

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

- 1 LCD-Bedienfeld des Gehäuses - siehe *Benutzerhandbuch zum Dell Chassis Management Controller*.
- 1 iDRAC-Konfigurationshilfsprogramm - siehe [LAN](#)
- 1 CMC-Webschnittstelle - siehe [Netzwerkbetrieb mittels der CMC-Webschnittstelle konfigurieren](#)
- 1 RACADM - siehe [cfgLanNetworking](#)

iDRAC-Benutzer konfigurieren

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

- 1 iDRAC-Konfigurationshilfsprogramm (konfiguriert nur den Benutzer auf Administratorebene) - siehe [LAN-Benutzerkonfiguration](#)
- 1 iDRAC-Webschnittstelle - siehe [iDRAC-Benutzer hinzufügen und konfigurieren](#)
- 1 RACADM - siehe [iDRAC-Benutzer hinzufügen](#)

Active Directory konfigurieren

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

- 1 Siehe [iDRAC mit Microsoft Active Directory verwenden](#)

IP-Filterung und IP-Blockierung konfigurieren

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

- 1 IDRAC-Webschnittstelle - siehe [IP-Filterung und IP-Blockierung konfigurieren](#)
- 1 RACADM - siehe [IP-Filterung konfigurieren \(IpBereich\)](#), [IP-Blockierung konfigurieren](#)

Plattformereignisse konfigurieren

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

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

- 1 IDRAC-Webschnittstelle - siehe [Plattformereignisfilter \(PEF\) konfigurieren](#)
- 1 RACADM - siehe [PEF konfigurieren](#)

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

- 1 IDRAC-Webschnittstelle - siehe [Plattformereignis-Traps \(PET\) konfigurieren](#)
- 1 RACADM - [PET konfigurieren](#)

Seriell über LAN konfigurieren

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

- 1 IDRAC-Webschnittstelle - siehe [Seriell über LAN konfigurieren](#)
- 1 Siehe auch [GUI-Konsolenumleitung verwenden](#)

iDRAC-Dienste konfigurieren

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

- 1 IDRAC-Webschnittstelle - siehe [iDRAC-Dienste konfigurieren](#)
- 1 RACADM - siehe [iDRAC-Telnet- und SSH-Dienste mittels lokalem RACADM konfigurieren](#)

SSL konfigurieren

Konfigurieren Sie SSL für den iDRAC-Web Server.

- 1 IDRAC-Webschnittstelle - siehe [SSL](#)
- 1 RACADM - siehe [cfgRacSecurity](#), [sslcsrgen](#), [sslcertupload](#), [sslcertdownload](#), [sslcertview](#)

Virtuellen Datenträger konfigurieren

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

- 1 IDRAC-Webschnittstelle - siehe [Virtuellen Datenträger konfigurieren und verwenden](#)
- 1 IDRAC-Konfigurationshilfsprogramm - siehe [Virtueller Datenträger](#)

Managed Server-Software installieren

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


- 1 Konsolenumleitung - siehe [Softwareinstallation auf dem verwalteten Server](#)
- 1 iVM-CLI - siehe [Befehlszeilenoberfläche-Dienstprogramm des Virtuellen Datenträgers verwenden](#)


Verwalteten Server für die Funktion Bildschirm Letzter Absturz konfigurieren


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

1. Verwalteter Server - siehe [Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz](#), [Die Windows-Option Automatischer Neustart deaktivieren](#)

Netzwerkbetrieb mittels der CMC-Webschnittstelle konfigurieren

 **ANMERKUNG:** Um vom CMC aus iDRAC-Netzwerkeinstellungen vornehmen zu können, müssen Sie über die entsprechenden Administratorrechte zur Gehäusekonfiguration verfügen.

 **ANMERKUNG:** Der Standard-CMC-Benutzer lautet **root**, und das Standardkennwort **calvin**.

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

1. Melden Sie sich über Ihren Webbrowser bei der CMC-Webbenutzeroberfläche an, indem Sie eine Internetadresse des Formats `https://<CMC-IP-Adresse>` oder `https://<CMC-DNS-Name>` verwenden.
2. Geben Sie den Benutzernamen und das Kennwort für den CMC ein, und klicken Sie auf **OK**.
3. Klicken Sie neben **Gehäuse** in der linken Spalte auf das Plus-Symbol (+) und dann auf **Server**.
4. Klicken Sie auf **Setup** → **Bereitstellen**.
5. Aktivieren Sie das LAN für den Server durch Markieren des Kontrollkästchens neben dem Server unterhalb der Überschrift **LAN aktivieren**.
6. Aktivieren oder deaktivieren Sie IPMI über LAN, indem Sie das Kontrollkästchen neben dem Server unterhalb der Überschrift **IPMI -über-LAN aktivieren** markieren oder seine Markierung aufheben.
7. Aktivieren oder deaktivieren Sie DHCP für den Server, indem Sie das Kontrollkästchen neben dem Server unterhalb der Überschrift **DHCP aktiviert** markieren oder seine Markierung aufheben.
8. Ist das DHCP deaktiviert, geben Sie die statische IP-Adresse, die Netzmaske und das Standard-Gateway für den Server ein.
9. Klicken Sie unten auf der Seite auf **Anwenden**.

iDRAC-Firmware aktualisieren

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

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

Firmware-Paket oder Update Package herunterladen


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


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

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

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

Firmware-Aktualisierung ausführen

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

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

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

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

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

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

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

DOS-Aktualisierungsdienstprogramm verwenden

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

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


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

Die Optionen sind folgende:

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

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

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

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

DigitalSignatur überprüfen


Eine DigitalSignatur wird zum Authentifizieren der Identität des Unterzeichners einer Datei verwendet und zum Bestätigen, dass der ursprüngliche Dateinhalt seit der Unterzeichnung nicht modifiziert worden ist.

Fall der Gnu Privacy Guard (GPG) noch nicht auf dem System installiert ist, installieren Sie ihn jetzt, damit DigitalSignaturen verifiziert werden können. Um das standardmäßige Verifizierungsverfahren zu verwenden, führen Sie folgende Schritte aus:

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

2. Importieren Sie den öffentlichen Schlüssel in Ihre gpg trust-Datenbank, indem Sie den folgenden Befehl ausführen:

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

 **ANMERKUNG:** Sie müssen über Ihren eigenen Schlüssel verfügen, um das Verfahren abschließen zu können.

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

- a. Geben Sie den folgenden Befehl ein:

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

- b. Geben Sie im GPG-Schlüsselbearbeitungsprogramm **fpr** ein. Die folgende Meldung wird eingeblendet:

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

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

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

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

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

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

Your decision?

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

1 = Ich weiß es nicht oder will es nicht sagen
2 = Ich habe KEIN Vertrauen
3 = Ich habe ein wenig Vertrauen
4 = Ich habe volles Vertrauen
5 = Ich habe absolutes Vertrauen
m = zurück zum Hauptmenü

Ihre Entscheidung?)

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

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


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

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

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

Der öffentliche Schlüssel darf nur einmal importiert und validiert werden.

4. Besorgen Sie sich das erforderliche Paket, z. B. das Linux-DUP oder selbstextrahierende Archiv) sowie seine zugehörige Signaturdatei auf Dells Support-Website unter support.dell.com/support/downloads.

 **ANMERKUNG:** Jedes Linux Update Package enthält eine separate Signaturdatei, die auf derselben Webseite wie das Update Package angezeigt wird. Sie benötigen sowohl das Update Package als auch seine zugehörige Signaturdatei zur Verifizierung. Standardmäßig erhält die Signaturdatei denselben Namen wie den DUP-Dateinamen, mit der Erweiterung **.sign**. Wenn z. B. ein Linux-DUP mit **PE1850-BIOS-LX-A02.BIN** benannt wird, lautet sein Signaturdateiname **PE1850-BIOS-LX-A02.BIN.sign**. Das iDRAC-Firmware-Image hat auch eine zugeordnete **.sign**-Datei, die im selbstextrahierenden Archiv mit dem Firmware-Image enthalten ist. Klicken Sie zum Herunterladen der Dateien mit der rechten Maustaste auf den Download-Link, und verwenden Sie die Dateioption **Ziel speichern unter**....

5. Überprüfen Sie das Update Package:

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

Im folgenden Beispiel werden die Schritte zum Überprüfen eines 1425SC-BIOS-Aktualisierungspakets dargestellt:

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

```
1 PESC1425-BIOS-LX-A01.bin.sign
1 PESC1425-BIOS-LX-A01.bin
```

2. Importieren Sie den öffentlichen Schlüssel, indem Sie die folgende Befehlszeile ausführen:

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

Die folgende Ausgabemeldung wird eingeblendet:

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

```
(gpg: key 23B66A9D: "Dell Computer Corporation (Linux-Systemgruppe) <linux-security@dell.com>" nicht verändert
gpg: Verarbeitete Gesamtanzahl: 1
gpg: unverändert: 1)
```

3. Richten Sie die GPG-Vertrauensstufe für den öffentlichen Schlüssel von Dell ein, wenn Sie dies nicht bereits getan haben.

a. Geben Sie den folgenden Befehl ein:

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

b. Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
fpr
trust
```

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

- d. Geben Sie `y` <Eingabe> ein, um Ihre Auswahl zu bestätigen.
- e. Geben Sie `quit` <Eingabe> ein, um das GPG-Schlüsselbearbeitungsprogramm zu beenden.

Hierdurch wird die Validierung des öffentlichen Schlüssels von Dell abgeschlossen.


4. Verifizieren Sie die Digitalsignatur des PESC1425-BIOS-Pakets durch Ausführen des folgenden Befehls:

```
gpg --verify PESC1425-BIOS-LX-A01.bin.sign PESC1425-BIOS-LX-A01.bin
```

Die folgende Ausgabemeldung wird eingeblendet:

```
gpg: Signature made Thu 14 Apr 2005 04:25:37 AM IST using DSA key ID 23B66A9D
gpg: Good signature from "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>"

(gpg: Signatur vorgenommen Don, 14. Apr 2005 04:25:37 IST mit DSA-Schlüssel-ID 23B66A9D
gpg: Gültige Signatur von "Dell Computer Corporation (Linux-Systemgruppe) <linux-security@dell.com>")
```

 **ANMERKUNG:** Wenn Sie den Schlüssel nicht wie in [Schritt 3](#) dargestellt validiert haben, werden Sie zusätzliche Meldungen erhalten:

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

(gpg: WARNUNG: Dieser Schlüssel ist nicht mit einer vertrauenswürdigen Signatur zertifiziert!
gpg: Es gibt keinen Hinweis darauf, dass die Signatur dem Besitzer gehört.
Primärer Schlüsselfingerabdruck: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D)
```

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

Verwaltungsstation konfigurieren

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Schritte zum Einrichten der Verwaltungsstation](#)
- [Netzwerkvoraussetzungen für die Verwaltungsstation](#)
- [Einen unterstützten Internetbrowser konfigurieren](#)
- [Java-Laufzeitumgebung \(JRE\) installieren](#)
- [Telnet- oder SSH-Clients installieren](#)
- [TFTP-Server installieren](#)
- [Dell OpenManage IT Assistant installieren](#)

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

Schritte zum Einrichten der Verwaltungsstation

Führen Sie zum Einrichten der Verwaltungsstation folgende Schritte aus:

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


Netzwerkvoraussetzungen für die Verwaltungsstation

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

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

Einen unterstützten Internetbrowser konfigurieren

Die folgenden Abschnitte bieten Anleitungen zum Konfigurieren der unterstützten Webbrowser zur Verwendung mit der iDRAC-Webschnittstelle. Eine Liste unterstützter Webbrowser erhalten Sie unter [Unterstützte Internetbrowser](#).

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

Webbrowser zur Verbindung mit der Webschnittstelle konfigurieren

Wenn Sie zur iDRAC-Webschnittstelle von einer Verwaltungsstation aus eine Verbindung herstellen, die über einen Proxyserver mit dem Internet verbunden ist, muss der Webbrowser so konfiguriert werden, dass er von diesem Server aus auf das Internet zugreifen kann.

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

1. Öffnen Sie ein Internetbrowser-Fenster.

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

iDRAC zur Liste vertrauenswürdiger Domänen hinzufügen

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

Lokalisierte Versionen der Webschnittstelle anzeigen

Die iDRAC-Webschnittstelle wird in den folgenden Betriebssystemsprachen unterstützt:

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

Internet Explorer 6.0 (Windows)

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

1. Klicken Sie auf das **Hilfsprogramme**-Menü und wählen Sie **Internetoptionen**.
2. Im Fenster **Internetoptionen** klicken Sie auf **Sprachen**.
3. Im **Fenster** Spracheinstellung klicken Sie auf **Hinzufügen**.
4. Im Fenster **Sprache hinzufügen** wählen Sie eine unterstützte Sprache.
Um mehr als eine Sprache auszuwählen, drücken Sie <Strg>.
5. Wählen Sie Ihre bevorzugte Sprache und klicken Sie auf **Nach oben**, um die Sprache an die Spitze der Liste zu bewegen.
6. Im Fenster **Spracheinstellung** klicken Sie auf **OK**.
7. Klicken Sie auf **OK**.

Firefox 1.5 (Linux)

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

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

7. Klicken Sie auf **OK**.

Gebietsschema in Linux einstellen

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

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

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

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3. Wenn die Werte "zh_CN.UTF-8" einschließen, sind keine Änderungen erforderlich. Wenn die Werte nicht "zh_CN.UTF-8" einschließen, fahren Sie mit Schritt 4 fort.
4. Bearbeiten Sie die Datei `/etc/sysconfig/i18n` mit einem Textverarbeitungsprogramm.
5. Wenden Sie in der Datei folgende Änderungen an:

Aktueller Eintrag:

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

Aktualisierter Eintrag:

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CN.GB2312:zh_CN:zh"
```

6. Melden Sie sich beim Betriebssystem ab und dann wieder an.

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

Whitelist-Funktion in Firefox deaktivieren

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

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


1. Öffnen Sie ein Internetbrowser-Fenster in Firefox.
2. Geben Sie in das Adressfeld `about:config` ein, und drücken Sie auf <Eingabe>.
3. In der Spalte **Einstellungsname** machen Sie `xpinstall.whitelist.required` ausfindig und doppelklicken Sie darauf.

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

4. Suchen Sie in der Namensspalte **Einstellungen** `xpinstall.enabled` auf.

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

Java-Laufzeitumgebung (JRE) installieren

 **ANMERKUNG:** Wenn Sie Internet Explorer-Browser verwenden, ist für den Konsolen-Viewer eine ActiveX-Steuerung bereitgestellt. Sie können den Java-Konsolen-Viewer auch mit Internet Explorer verwenden, wenn Sie eine JRE installieren und den Konsolen-Viewer in der iDRAC-Webschnittstelle konfigurieren, bevor Sie den Viewer starten. Weitere Informationen finden Sie unter [Konfiguration der Konsolenumleitung auf der iDRAC-Webschnittstelle](#).


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

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

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

Telnet- oder SSH-Clients installieren

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

 **ANMERKUNG:** Es kann nur eine aktive Telnet- oder SSH-Verbindung auf einmal zum iDRAC hergestellt sein. Wenn eine aktive Verbindung besteht, werden andere Verbindungsversuche abgelehnt.

Telnet mit iDRAC

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

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

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

Die Rücktaste für die Telnet-Sitzung konfigurieren

Abhängig vom Telnet-Client kann die Verwendung der <Rücktaste> zu unerwarteten Ergebnissen führen. Zum Beispiel kann die Sitzung ein Echo ^h verursachen. Jedoch können die meisten Microsoft und Linux Telnet-Clients für die Verwendung der <Rücktaste> konfiguriert werden.

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

1. Öffnen Sie ein Eingabeaufforderungsfenster (falls erforderlich).
2. Wenn Sie keine Telnet-Sitzung ausführen, geben Sie folgendes ein:

```
telnet
```

Wenn Sie eine Telnet-Sitzung ausführen, drücken Sie <Strg><] >.

3. An der Eingabeaufforderung folgendes eingeben:

```
set bsasdel
```

Die folgende Meldung wird eingeblendet:

```
Backspace will be sent as delete.
```

(Rücktaste wird als Löschen gesendet.)

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

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

```
stty erase ^h
```


2. Geben Sie auf die Eingabeaufforderung hin Folgendes ein:

```
telnet
```

SSH mit iDRAC

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

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

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

Zu beliebigen Zeitpunkten wird jeweils nur eine Telnet- oder SSH-Sitzung unterstützt. Die Sitzungszeitüberschreitung wird durch die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert, wie unter [Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank](#) beschrieben.

Die iDRAC-SSH-Umsetzung unterstützt mehrfache Verschlüsselungs-Schemata, wie in [Tabelle 3-1](#) dargestellt.



 **ANMERKUNG:** SSHv1 wird nicht unterstützt.

Tabelle 3-1. Verschlüsselungs-Schemata

Schema-Typ	Schema
Asymmetrische Verschlüsselung	Diffie-Hellman DSA/DSS 512-1024 (zufällige) Bit pro NIST-Spezifizierung
Symmetrische Verschlüsselung	<ul style="list-style-type: none"> AES256-CBC RIJNDael256-CBC AES192-CBC RIJNDael192-CBC AES128-CBC RIJNDael128-CBC BLOWFISH-128-CBC 3DES-192-CBC ARCFOUR-128
Meldungsintegrität	<ul style="list-style-type: none"> HMAC-SHA1-160 HMAC-SHA1-96 HMAC-MD5-128 HMAC-MD5-96
Authentifizierung	<ul style="list-style-type: none"> Kennwort

TFTP-Server installieren

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

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

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

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

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

Dell OpenManage IT Assistant installieren

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

- 1 CD *Dell Systems Management Consoles* - Enthält die neuesten Systemverwaltungs-Konsolenprodukte von Dell, einschließlich Dell OpenManage IT Assistant.
- 1 CD *Dell PowerEdge Service and Diagnostic Utilities* - Bietet die zur Konfiguration des Systems erforderlichen Hilfsprogramme und stellt Firmware, Diagnoseprogramme sowie Dell-optimierte Treiber für das System zur Verfügung.
- 1 CD *Dell PowerEdge Documentation* - Hilft Ihnen, mit Dokumentationen für Systeme, Systems Management-Softwareprodukten, Peripheriegeräten und RAID-Controllern auf dem neuesten Stand zu bleiben.

- 1 Support-Website und Infodateien von Dell - Sehen Sie in den Infodateien und auf Dells Support-Website unter **support.dell.com** nach aktuellen Informationen zu Ihren Dell-Produkten.

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

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

Verwalteten Server konfigurieren

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Softwareinstallation auf dem verwalteten Server](#)
- [Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz](#)
- [Die Windows-Option Automatischer Neustart deaktivieren](#)

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

Softwareinstallation auf dem verwalteten Server

Die Verwaltungssoftware von Dell schließt die folgenden Funktionen ein:

- 1 Lokale RACADM-CLI - ermöglicht Ihnen, den iDRAC vom verwalteten System aus zu konfigurieren und zu verwalten. Es stellt ein leistungsfähiges Tool für Scripting-Konfiguration und Verwaltungs-Tasks dar.
- 1 Es ist für Server Administrator erforderlich, die iDRAC-Funktion des Bildschirms Letzter Absturz zu verwenden.
- 1 Server Administrator - eine Webschnittstelle, die Ihnen die Verwaltung des Remote-Systems von einem Remote-Host auf dem Netzwerk ermöglicht.
- 1 Server Administrator Instrumentation Service - bietet Zugriff auf detaillierte Fehler- und Leistungsdaten, die von Systemverwaltungsagenten des Industriestandards zusammengetragen werden und ermöglicht die Remote-Verwaltung überwachter Systeme, einschließlich Herunterfahren, Start und Sicherheit.
- 1 Server Administration Storage Management Service - bietet Speicherverwaltungsinformationen in einer integrierten graphischen Ansicht.
- 1 Server Administrator-Protokolle - zeigt Befehlsprotokolle an, die vom System oder an das System ausgegeben wurden, sowie überwachte Hardwareereignisse, POST-Ereignisse und Systemwarnungen. Sie können Protokolle auf der Startseite anzeigen, sie als Reporte ausdrucken oder speichern und Sie per E-Mail an eine designierte Service-Kontaktadresse senden.

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

Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz

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

1. Installieren Sie die Software des verwalteten Servers. Weitere Informationen zum Installieren der Managed Server-Software erhalten Sie im *Server Administrator-Benutzerhandbuch*.
2. Wenn Sie ein Microsoft® Windows®-Betriebssystem ausführen, ist sicherzustellen, dass die Funktion des automatischen Neustarts in den **Windows-Start- und Wiederherstellungs-Einstellungen** abgewählt ist. Siehe [Die Windows-Option Automatischer Neustart deaktivieren](#).
3. Aktivieren Sie den Bildschirm Letzter Absturz (standardmäßig deaktiviert) in der iDRAC-Webschnittstelle.

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

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

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

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

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

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

Die Windows-Option Automatischer Neustart deaktivieren

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

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

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

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

iDRAC mittels der Webschnittstelle konfigurieren

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Zugriff auf die Webschnittstelle](#)
- [iDRAC-NIC konfigurieren](#)
- [Plattformereignisse konfigurieren](#)
- [IPMI konfigurieren](#)
- [iDRAC-Benutzer hinzufügen und konfigurieren](#)
- [iDRAC-Datenübertragungen anhand von SSL- und digitalen Zertifikaten sichern](#)
- [Active Directory-Zertifikate konfigurieren und verwalten](#)
- [Seriell über LAN konfigurieren](#)
- [iDRAC-Dienste konfigurieren](#)
- [iDRAC-Firmware aktualisieren](#)

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

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

Befehle des lokalen RACADM werden vom verwalteten Server aus ausgeführt. Weitere Informationen über lokales RACADM finden Sie unter [Befehlszeilenoberfläche des lokalen RACADM verwenden](#).

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

Zugriff auf die Webschnittstelle

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

1. Öffnen Sie ein unterstütztes Internetbrowser-Fenster.

Weitere Informationen finden Sie unter [Unterstützte Internetbrowser](#).

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

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

`https://<iDRAC-IP-Adresse>:<Schnittstellennummer>`

wobei *iDRAC-IP-Adresse* die IP-Adresse des iDRAC und *Schnittstellennummer* die HTTPS-Schnittstellennummer ist.

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

Anmeldung

Sie können sich entweder als iDRAC-Benutzer oder als Microsoft® Active Directory®-Benutzer anmelden. Standardbenutzername und -kennwort sind **root** bzw. **calvin**.

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

Um sich anzumelden, führen Sie die folgenden Schritte aus.

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

1. Ihren iDRAC-Benutzernamen.

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




1. Ihren Active Directory-Benutzernamen

Active Directory-Namen können in einer beliebigen der folgenden Formen eingegeben werden: `<Domäne>\<Benutzername>`, `<Domäne>/<Benutzername>` oder `<Benutzer>@<Domäne>`. Es wird bei ihnen nicht zwischen Groß- und Kleinschreibung unterschieden. Beispiele sind `dell.com\john_doe` oder `JOHN_DOE@DELL.COM`.

2. Geben Sie in das Feld **Kennwort** Ihr iDRAC-Benutzerkennwort oder Ihr Active Directory-Benutzerkennwort ein. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden.
3. Klicken Sie auf **OK** oder drücken Sie auf **<Eingabe>**.

Abmeldung



1. Klicken Sie in der oberen rechten Ecke des Hauptfensters auf **Abmelden**, um die Sitzung zu schließen.
2. Schließen Sie das Browser-Fenster.

-  **ANMERKUNG:** Die Schaltfläche **Abmeldung** wird erst eingeblendet, wenn Sie sich angemeldet haben.
-  **ANMERKUNG:** Wenn Sie den Browser schließen, ohne sich ordnungsgemäß abzumelden, kann dies dazu führen, dass die Sitzung so lange offen bleibt, bis eine Zeitüberschreitung eintritt. Es wird dringend empfohlen, zum Beenden der Sitzung auf die Schaltfläche **Abmeldung** zu klicken, da die Sitzung andernfalls möglicherweise aktiv bleibt, bis die Sitzungszeitüberschreitung erreicht wurde.
-  **ANMERKUNG:** Das Schließen der iDRAC-Webschnittstelle in Microsoft Internet Explorer anhand der Schließen-Schaltfläche ("x") in der oberen rechten Ecke des Fensters kann zu einem Anwendungsfehler führen. Um dieses Problem zu lösen, laden Sie von der Support-Website von Microsoft unter support.microsoft.com die neueste kumulative Sicherheitsaktualisierung für Internet Explorer herunter.

iDRAC-NIC konfigurieren

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

Netzwerk- und IPMI-LAN-Einstellungen konfigurieren

-  **ANMERKUNG:** Zur Ausführung der folgenden Schritte müssen Sie die Berechtigung **iDRAC konfigurieren** besitzen.
-  **ANMERKUNG:** Die meisten DHCP Server erfordern, dass ein Server ein Client-ID-Token in seiner Reservierungstabelle speichert. Der Client (z. B. iDRAC) muss dieses Token während der DHCP-Verhandlung zur Verfügung stellen. iDRAC liefert die Option der Client-Identifikation unter Verwendung einer Ein-Byte-Schnittstellenummer (0), gefolgt von einer Sechs-Byte-MAC-Adresse.

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

[Tabelle 5-1](#) und [Tabelle 5-2](#) beschreiben die **Netzwerkeinstellungen** und die **IPMI LAN-Einstellungen** auf der **Netzwerk**-Seite.

3. Klicken Sie, wenn Sie die erforderlichen Einstellungen eingegeben haben, auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 5-3](#).

Tabelle 5-1. Netzwerkeinstellungen

Einstellung	Beschreibung
NIC aktivieren	Wenn markiert, weist dies darauf hin, dass die NIC aktiviert ist und die verbleibenden Steuerungen dieser Gruppe aktiviert werden. Wenn eine NIC deaktiviert ist, wird die Datenübertragung zum und vom iDRAC über das Netzwerk blockiert. Die Standardeinstellung ist aus .
Media Access Control (MAC)-Adresse	Zeigt die Medienzugriffssteuerungs-Adresse (MAC) an, die die einzelnen Knoten in einem Netzwerk eindeutig identifiziert. Die MAC-Adresse kann nicht geändert werden.
DHCP verwenden (für NIC-IP-Adresse)	Fordert den iDRAC auf, eine IP-Adresse für die NIC vom Server für das dynamische Host-Konfigurationsprotokoll (DHCP) abzurufen. Deaktiviert auch die Steuerungen für Statische IP-Adresse , Statische Subnetzmaske und Statisches Gateway . Die Standardeinstellung ist aus .
Statische IP-Adresse	Ermöglicht Ihnen, eine statische IP-Adresse für die iDRAC-NIC einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, wählen Sie das Kontrollkästchen DHCP verwenden (für NIC-IP-Adresse) ab.
Statische Subnetzmaske	Ermöglicht Ihnen, eine Subnetzmaske für die iDRAC-NIC einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, wählen Sie zuerst das Kontrollkästchen DHCP verwenden (für NIC-IP-Adresse) ab.
Statischer Gateway	Ermöglicht Ihnen, einen statischen Gateway für die iDRAC-NIC einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, wählen Sie zuerst das Kontrollkästchen DHCP verwenden (für NIC-IP-Adresse) ab.
DHCP zum Abrufen von DNS-Serveradressen verwenden	Aktivieren Sie DHCP zum Abrufen von DNS-Server-Adressen, indem Sie das Kontrollkästchen DHCP zum Abrufen von DNS-Serveradressen verwenden auswählen. Wenn Sie zum Abrufen der DNS-Server-Adressen nicht DHCP verwenden, geben Sie die IP-Adressen in die Felder Statischer bevorzugter DNS-Server und Statischer alternativer DNS-Server ein. Die Standardeinstellung ist aus . ANMERKUNG: Wenn das Kontrollkästchen DHCP zum Abrufen von DNS-Serveradressen verwenden ausgewählt ist, können IP-Adressen nicht in die Felder Statischer bevorzugter DNS-Server und Statischer alternativer DNS-Server eingetragen werden.
Statisch bevorzugter DNS-Server	Ermöglicht dem Benutzer, eine statische IP-Adresse für den bevorzugten DNS-Server einzugeben oder zu bearbeiten. Um diese Einstellung zu ändern, muss zuerst das Kontrollkästchen DHCP zum Abrufen von DNS-Serveradressen verwenden abgewählt werden.

Statisch alternativer DNS-Server	Verwendet die sekundäre DNS Server-IP-Adresse, wenn DHCP zum Abrufen von DNS-Serveradressen verwenden nicht ausgewählt ist. Geben Sie eine IP-Adresse mit 0.0.0.0 ein, wenn kein alternativer DNS-Server vorhanden ist.
iDRAC auf DNS registrieren	Registriert den iDRAC-Namen auf dem DNS-Server. Die Standardeinstellung ist Deaktiviert .
DNS iDRAC-Name	Zeigt den iDRAC-Namen nur an, wenn iDRAC auf DNS registrieren ausgewählt ist. Der Standardname lautet <code>idrac-service_tag</code> , wobei <code>service_tag</code> die Service-Tag-Nummer des Dell-Servers darstellt. Beispiel: <code>idrac-00002</code> .
DHCP für den DNS-Domännennamen verwenden	Verwendet den Standard-DNS-Domännennamen. Wenn das Kästchen nicht ausgewählt ist und die Option iDRAC auf DNS registrieren ausgewählt ist, können Sie den DNS-Domännennamen im Feld DNS-Domänenname ändern. Die Standardeinstellung ist Deaktiviert . ANMERKUNG: Um das Kontrollkästchen DHCP für den DNS-Domännennamen verwenden auszuwählen, müssen Sie auch das Kontrollkästchen DHCP verwenden (für NIC-IP-Adresse) auswählen.
DNS-Domänenname	Der Standard-DNS-Domänenname ist leer. Wenn das Kontrollkästchen DHCP für den DNS-Domännennamen verwenden ausgewählt ist, ist diese Option grau unterlegt, und das Feld kann nicht geändert werden.
Community-Zeichenkette	Enthält die Community-Zeichenkette, die für die vom iDRAC gesendeten Warnungs-Traps des einfachen Netzwerkverwaltungsprotokolls (SNMP) verwendet werden soll. SNMP-Warnungs-Traps werden vom iDRAC übertragen, wenn ein Plattformereignis auftritt. Die Standardeinstellung ist öffentlich .
SMTP-Serveradresse	Die IP-Adresse des Servers des einfachen Mail-Übertragungsprotokolls (SMTP) , mit dem der iDRAC kommuniziert, um im Falle eines Plattformereignisses E-Mail-Warnungen auszusenden. Die Standardeinstellung ist 127.0.0.1 .


Tabelle 5-2. IPMI LAN-Einstellungen

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

Tabelle 5-3. Netzwerkkonfiguration-Seitenschaltflächen

Schaltfläche	Beschreibung
Erweiterte Einstellungen	Öffnet die Seite Netzwerksicherheit , auf der Benutzer den IP-Bereich sowie IP-Blockierungsattribute eingeben können.
Drucken	Druckt die Werte der Netzwerkkonfiguration aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite Netzwerkkonfiguration erneut.
Anwenden	Speichert alle neuen Einstellungen, die Sie auf der Seite Netzwerkkonfiguration vorgenommen haben. ANMERKUNG: Wenn Sie Änderungen an den Einstellungen der NIC-IP-Adresse vornehmen, werden alle Benutzersitzungen geschlossen, und Benutzer müssen unter Verwendung der aktualisierten IP-Adresseneinstellungen eine neue Verbindung zur iDRAC-Webschnittstelle herstellen. Alle anderen Änderungen erfordern, dass die NIC zurückgesetzt wird, was einen kurzen Verlust der Konnektivität verursachen kann.

IP-Filterung und IP-Blockierung konfigurieren

 **ANMERKUNG:** Zum Ausführen der folgenden Schritte müssen Sie die Berechtigung **iDRAC konfigurieren** besitzen.

- Klicken Sie auf **System** → **Remote-Zugriff** → **iDRAC** und dann auf das Register **Netzwerk/Sicherheit**, um die Seite **Netzwerkkonfiguration** zu öffnen.
- Klicken Sie auf **Erweiterte Einstellungen**, um die Netzwerksicherheitseinstellungen zu konfigurieren.

In [Tabelle 5-4](#) werden die Einstellungen der Seite **Netzwerksicherheit** beschrieben.
- Klicken Sie, wenn Sie die Einstellungen konfiguriert haben, auf **Anwenden**.
- Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 5-5](#).

Tabelle 5-4. Einstellungen der Seite Netzwerksicherheit

Einstellungen	Beschreibung
---------------	--------------

IP-Bereich aktiviert	Aktiviert die Funktion zum Prüfen des IP-Bereichs, mit der eine Reihe von IP-Adressen definiert wird, die auf den iDRAC zugreifen können. Die Standardeinstellung ist aus .
IP-Bereichsadresse	Bestimmt die akzeptable IP-Subnetzadresse. Die Standardeinstellung ist 192.168.1.0 .
Subnetzmaske IP-Bereich	Definiert die wichtigen Bitpositionen in der IP-Adresse. Die Subnetzmaske sollte in der Form einer Netzmaske sein, wobei die bedeutenderen Bits alle Einsen (1) sind, mit einem einzelnen Übergang zu Nullen (0) in den niederwertigeren Bits. Die Standardeinstellung ist 255.255.255.0 .
IP-Blockierung aktiviert	Aktiviert die IP-Adressen-Blockierungsfunktion, mit der die Anzahl von fehlerhaften Anmeldeversuchen von einer spezifischen IP-Adresse für einen bestimmten Zeitraum beschränkt wird. Die Standardeinstellung ist aus .
Zählung IP-Blockierungsausfall	Legt die Anzahl der Anmeldefehler von einer bestimmten IP-Adresse fest, bevor Anmeldeversuche von dieser Adresse zurückgewiesen werden. Die Standardeinstellung ist 10 .
Fenster IP-Blockierungsausfall	Bestimmt den Zeitraum in Sekunden, während dessen die Fehler der Zählung IP-Blockausfall auftreten müssen, um die Penalty-Zeit IP-Block auszulösen. Die Standardeinstellung ist 3600 .
Penalty-Zeit IP-Blockierung	Der Zeitraum in Sekunden, während dem Anmeldeversuche von einer IP-Adresse auf Grund übermäßiger Fehler abgewiesen werden. Die Standardeinstellung ist 3600 .

Tabelle 5-5. Schaltflächen Netzwerksicherheitsseite

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

Plattformereignisse konfigurieren

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

Die filterbaren Plattformereignisse werden in [Tabelle 5-6](#) aufgeführt.

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


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

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


Plattformereignisfilter (PEF) konfigurieren

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

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

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


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

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

Plattformereignis-Traps (PET) konfigurieren

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

1. Melden Sie sich über einen unterstützten Webbrowser am Remote-System an. Siehe [Zugriff auf die Webschnittstelle](#).
2. Stellen Sie sicher, dass Sie die unter [Plattformereignisfilter \(PEF\) konfigurieren](#) beschriebenen Verfahren befolgt haben.
3. Konfigurieren Sie Ihre PET-Ziel-IP-Adresse:
 - a. Klicken Sie auf das Kontrollkästchen **Aktivieren** neben der **Ziel-IP-Adresse**, die Sie aktivieren möchten.
 - b. Geben Sie eine IP-Adresse im Kästchen **Ziel-IP-Adresse** ein.

 **ANMERKUNG:** Die Ziel-Community-Zeichenkette muss mit der iDRAC-Community-Zeichenkette identisch sein.


- c. Klicken Sie auf **Anwenden**.

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

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

E-Mail-Warnungen konfigurieren

1. Melden Sie sich über einen unterstützten Webbrowser am Remote-System an.
2. Stellen Sie sicher, dass Sie die unter [Plattformereignisfilter \(PEF\) konfigurieren](#) beschriebenen Verfahren befolgt haben.
3. Konfigurieren Sie Ihre E-Mail-Warnungseinstellungen.
 - a. Klicken Sie auf dem Register **Warnungsverwaltung** auf **E-Mail-Warnungseinstellungen**.
4. Konfigurieren Sie Ihr E-Mail-Warnungsziel.
 - a. Klicken Sie in der Spalte **E-Mail-Warnungsnummer** auf eine Zielnummer. Es gibt vier mögliche Ziele, die Warnungen empfangen können.
 - b. Stellen Sie sicher, dass das Kontrollkästchen **Aktiviert** ausgewählt ist.
 - c. Geben Sie eine gültige E-Mail-Adresse in das Feld **Ziel-E-Mail-Adresse** ein.
 - d. Klicken Sie auf **Anwenden**.


 **ANMERKUNG:** Damit erfolgreich eine Test-E-Mail gesendet werden kann, muss die **SMTP-Server-Adresse** auf der Seite **Netzwerkconfiguration** konfiguriert sein. Die IP-Adresse des **SMTP-Servers** kommuniziert mit dem iDRAC, um im Falle eines Plattformereignisses E-Mail-Warnungen zu senden.

- e. Klicken Sie auf **Senden**, um die konfigurierte E-Mail-Warnung zu testen (falls gewünscht).
- f. Wiederholen Sie Schritt a bis Schritt e für alle restlichen E-Mail-Warnungseinstellungen.

IPMI konfigurieren


1. Melden Sie sich über einen unterstützten Webbrowser am Remote-System an.
2. IPMI über LAN konfigurieren.


- a. Klicken Sie auf **System**→ **Remote-Zugriff**→ iDRAC und dann auf **Netzwerk/Sicherheit**.
- b. Wählen Sie auf der Seite **Netzwerkconfiguration** unter **IPMI LAN-Einstellungen** **IPMI über LAN aktivieren** aus.
- c. Aktualisieren Sie die IPMI LAN-Kanalberechtigungen, falls erforderlich.

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

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

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

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


 **ANMERKUNG:** Der Verschlüsselungsschlüssel muss aus einer geraden Anzahl hexadezimaler Zeichen mit einer maximalen Länge von 20 Zeichen bestehen.

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

- e. Klicken Sie auf **Anwenden**.

3. IPMI-Seriell über LAN (SOL) konfigurieren.

- a. Klicken Sie auf **System**→ **Remote-Zugriff**→ iDRAC.
- b. Klicken Sie auf das Register **Netzwerksicherheit** und dann auf **Seriell über LAN**.
- c. Klicken Sie auf der Seite **Seriell über LAN - Konfiguration** auf das Kontrollkästchen **Seriell über LAN aktivieren**, um Seriell über LAN zu aktivieren.
- d. Aktualisieren Sie die IPMI SOL-Baudrate.

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

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

- e. Klicken Sie auf **Anwenden**.

iDRAC-Benutzer hinzufügen und konfigurieren


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

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

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

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ iDRAC und dann auf das Register **Netzwerk/Sicherheit**.
2. Öffnen Sie die Seite **Benutzer** zur Konfiguration von Benutzern.

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

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

3. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
4. Auf der Seite **Anwenderkonfiguration** konfigurieren Sie die Eigenschaften und Berechtigungen des Benutzers.
[Tabelle 5-7](#) beschreibt die **allgemeinen** Einstellungen zur Konfiguration eines Benutzernamens und -kennworts für iDRAC.
[Tabelle 5-8](#) beschreibt die **IPMI LAN-Berechtigungen** zur Konfiguration der LAN-Berechtigungen des Benutzers.

[Tabelle 5-9](#) beschreibt die **Benutzergruppenberechtigungen** für die Einstellungen **IPMI LAN-Berechtigungen** und **iDRAC-Benutzerberechtigungen**.

[Tabelle 5-10](#) beschreibt die Berechtigungen der **iDRAC-Gruppe**. Wenn Sie eine **iDRAC-Benutzerberechtigung** zum **Administrator**, **Hauptbenutzer** oder **Gastbenutzer** hinzufügen, verändert sich die **iDRAC-Gruppe** zur **benutzerdefinierten Gruppe**.

5. Wenn Sie dies durchgeführt haben, klicken Sie auf **Anwenden**.
6. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 5-11](#).

Tabelle 5-7. Allgemeine Eigenschaften

Eigenschaft	Beschreibung
Benutzer-ID	Enthält eine von 16 voreingestellten Benutzer-ID-Nummern. Dieses Feld darf nicht bearbeitet werden.
Benutzer aktivieren	Wenn markiert, weist dies darauf hin, dass der Benutzerzugriff auf den iDRAC aktiviert ist. Wenn nicht markiert, ist der Benutzerzugriff deaktiviert.
Benutzername	Gibt einen iDRAC-Benutzernamen von bis zu 16 Zeichen an. Jeder Benutzer muss einen eindeutigen Benutzernamen haben. ANMERKUNG: Benutzernamen für den iDRAC dürfen nicht die Zeichen / (Schrägstrich) oder . (Punkt) enthalten. ANMERKUNG: Wenn der Benutzername geändert wird, erscheint der neue Name erst in der Benutzeroberfläche, wenn sich der nächste Benutzer anmeldet.
Kennwort ändern	Aktiviert die Felder Neues Kennwort und Neues Kennwort bestätigen . Wenn diese Felder nicht markiert sind, kann das Kennwort des Benutzers nicht geändert werden .
Neues Kennwort	Aktiviert die Bearbeitung des Kennworts des iDRAC-Benutzers. Geben Sie ein Kennwort mit bis zu 20 Zeichen ein. Die Zeichen werden nicht angezeigt.
Neues Kennwort bestätigen	Geben Sie das Kennwort des iDRAC-Benutzers erneut ein, um es zu bestätigen.

Tabelle 5-8. IPMI LAN-Benutzerberechtigungen

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

Tabelle 5-9. iDRAC-Benutzerberechtigungen

Eigenschaft	Beschreibung
iDRAC-Gruppe	Legt die maximale iDRAC-Benutzerberechtigung für eine der folgenden Möglichkeiten fest: Administrator, Hauptbenutzer, Gastbenutzer, Benutzerdefiniert oder Keine . In Tabelle 5-10 werden iDRAC-Gruppenberechtigungen aufgeführt.
Bei iDRAC anmelden	Ermöglicht dem Benutzer, sich am iDRAC anzumelden.
iDRAC konfigurieren	Ermöglicht dem Benutzer, den iDRAC zu konfigurieren.
Benutzer konfigurieren	Ermöglicht dem Benutzer, spezifischen Benutzern zu erlauben, auf das System zuzugreifen.
Protokolle löschen	Ermöglicht dem Benutzer, die iDRAC-Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Ermöglicht dem Benutzer, RACADM-Befehle auszuführen.
Zugriff auf Konsolenumleitung	Ermöglicht dem Benutzer, die Konsolenumleitung auszuführen.
Zugriff auf Virtueller Datenträger	Ermöglicht dem Benutzer, den virtuellen Datenträger auszuführen und zu verwenden.
Testwarnungen	Ermöglicht dem Benutzer, einem spezifischen Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Tabelle 5-10. iDRAC-Gruppenberechtigungen

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

Tabelle 5-11. Schaltflächen der Benutzerkonfigurationsseite

--	--

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

iDRAC-Datenübertragungen anhand von SSL- und digitalen Zertifikaten sichern

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

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

Secure Sockets Layer (SSL)

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

Ein SSL-aktiviertes System kann die folgenden Tasks ausführen:

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

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

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

Zertifikatssignierungsanforderung (CSR)

Ein CSR ist eine digitale Anforderung an eine Zertifizierungsstelle (CA) für ein sicheres Server-Zertifikat. Sichere Serverzertifikate ermöglichen Clients des Servers, die Identität des Servers, zu dem sie eine Verbindung hergestellt haben, als vertrauenswürdig einzustufen und eine verschlüsselte Sitzung mit dem Server auszuhandeln.

Eine Zertifizierungsstelle ist ein Geschäftsunternehmen, das in der IT-Industrie dafür anerkannt ist, hohe Standards der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger Sicherheitskriterien zu treffen. Beispiele von CAs schließen Thawte und VeriSign ein. Nachdem die Zertifizierungsstelle eine Zertifikatssignierungsanforderung erhalten hat, verifiziert und bestätigt sie die in der Zertifikatssignierungsanforderung enthaltenen Informationen. Wenn der Bewerber die Sicherheitsstandards der Zertifizierungsstelle erfüllt, gibt die Zertifizierungsstelle ein digital signiertes Zertifikat aus, das diesen Bewerber im Hinblick auf Transaktionen über Netzwerke und über das Internet eindeutig identifiziert.

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

Zugriff auf das SSL-Hauptmenü

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

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

[Tabelle 5-12](#) beschreibt die Optionen, die zum Erstellen einer CSR verfügbar sind.

In [Tabelle 5-13](#) werden die verfügbaren Schaltflächen der Seite **SSL-Hauptmenü** beschrieben.


Tabelle 5-12. SSL-Hauptmenüoptionen

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

Tabelle 5-13. SSL-Hauptmenüschaftflächen

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

Neue Zertifikatssignierungsanforderung erstellen

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

1. Wählen Sie auf der Seite **SSL-Hauptmenü** die Option **Neue Zertifikatsignierungsanforderung (CSR) erstellen**, und klicken Sie auf **Weiter**.
2. Geben Sie auf der Seite **Zertifikatsignierungsanforderung (CSR) erstellen** einen Wert für die einzelnen CSR-Attribute ein.
In [Tabelle 5-14](#) werden die Optionen der Seite **Zertifikatsignierungsanforderung erstellen (CSR)** beschrieben.
3. Klicken Sie auf **Erstellen**, um die CSR zu erstellen.
4. Klicken Sie auf **Herunterladen**, um die CSR-Datei auf Ihrem lokalen Computer zu speichern.
5. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 5-15](#).

Tabelle 5-14. Zertifikatssignierungsanforderung (CSR) -Seitenoptionen erstellen

Feld	Beschreibung
Allgemeiner Name	Der genaue Name, der zertifiziert werden soll (normalerweise der Domänenname des Web Servers, z. B. www.xyzfirma.com). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen und Punkte sind gültig. Leerstellen sind nicht gültig.
Organisationsname	Der mit dieser Organisation assoziierte Name (z. B. XYZ Unternehmen). Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Organisationseinheit	Der einer Organisationseinheit, wie z. B. einer Abteilung (z. B. Informationstechnik) zugehörige Name. Nur alphanumerische Zeichen, Bindestriche, Unterstreichungszeichen, Punkte und Leerstellen sind gültig.
Ort	Die Stadt oder ein anderer Standort des Unternehmens, das zertifiziert wird (z. B. München). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie keine Unterstriche oder andere Zeichen, um Wörter zu trennen.
Name des Bundeslandes	Das Bundesland oder die Provinz, in der sich das Unternehmen, das sich für eine Zertifizierung bewirbt, befindet (z. B. Bayern). Nur alphanumerische Zeichen und Leerstellen sind gültig. Verwenden Sie keine Abkürzungen.
Landesvorwahl	Der Name des Landes in dem sich die Einheit, die sich für die Zertifizierung bewirbt, befindet.
E-Mail	Die der CSR zugeordnete E-Mail-Adresse. Geben Sie die E-Mail-Adresse der Firma oder eine beliebige mit der CSR in Verbindung stehende E-Mail-Adresse ein. Dieses Feld ist optional.

Tabelle 5-15. Zertifikatssignierungsanforderung (CSR) -Seitenschnittflächen erstellen

Schaltfläche	Beschreibung
Drucken	Druckt die Werte Zertifikatsignierungsanforderung erstellen aus, die auf dem Bildschirm angezeigt werden.


Aktualisieren	Lädt die Seite Zertifikatsignierungsanforderung erstellen neu .
Erstellen	Erstellt eine CSR und fordert den Benutzer dann auf, sie in einem bestimmten Verzeichnis zu speichern.
Herunterladen	Lädt das Zertifikat auf den lokalen Computer herunter.
Zurück zum SSL-Hauptmenü	Bringt den Benutzer zur Seite SSL-Hauptmenü zurück.

Ein Server-Zertifikat hochladen

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

Die Seite **Zertifikat hochladen** wird eingeblendet.

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

 **ANMERKUNG:** Der **Dateipfad**-Wert zeigt den relativen Pfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad tippen, mit dem vollständigen Pfad und dem gesamten Dateinamen und Dateinamenszusatz.

3. Klicken Sie auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 5-16](#).

Tabelle 5-16. Seitenschaltflächen Zertifikat hochladen

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

Ein Serverzertifikat anzeigen

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

In [Tabelle 5-17](#) werden die Felder und zugehörigen Beschreibungen, die im **Zertifikat**-Fenster aufgeführt werden, beschrieben.

2. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 5-18](#).


Tabelle 5-17. Zertifikat-Informationen


Feld	Beschreibung
Seriennummer	Zertifikatseriennummer
Subjektinformationen	Vom Antragsteller eingegebene Zertifikat-Attribute
Aussteller-Informationen	Zertifikatattribute vom Aussteller zurückgesendet
Gültig von	Ausgabedatum des Zertifikats
Gültig bis	Ablaufdatum des Zertifikats

Tabelle 5-18. Schaltflächen der Seite Serverzertifikat anzeigen

Schaltfläche	Beschreibung
Drucken	Druckt die Werte für Serverzertifikat anzeigen aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite Serverzertifikat anzeigen erneut.
Zurück zum SSL-Hauptmenü	Zurück zur Seite SSL-Hauptmenü .

Active Directory-Zertifikate konfigurieren und verwalten

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

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

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

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

[Tabelle 5-19](#) führt die Optionen der Seite **Active Directory - Hauptmenü** auf.

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

Tabelle 5-19. Optionen der Seite Active Directory-Hauptmenü

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

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

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

Active Directory (Standardschema und Erweitertes Schema) konfigurieren

1. Auf der Seite **Active Directory-Hauptmenü** wählen Sie **Active Directory konfigurieren** und klicken Sie auf **Weiter**.
2. Geben Sie auf der Seite **Active Directory-Konfiguration** die Active Directory-Einstellungen ein.
In [Tabelle 5-21](#) werden die Einstellungen der Seite **Active Directory-Konfiguration und -Verwaltung** beschrieben.
3. Auf **Anwenden klicken**, um die Einstellungen zu speichern.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 5-22](#).
5. Um die Rollengruppen für das Active Directory-Standardschema zu konfigurieren, klicken Sie auf die einzelne Rollengruppe (1-5). Siehe [Tabelle 5-23](#) und [Tabelle 5-24](#).

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

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

Einstellung	Beschreibung
Active Directory aktivieren	Wenn markiert, wird das Active Directory aktiviert. Die Standardeinstellung ist deaktiviert .
ROOT-Domänenname	Der Active Directory ROOT-Domänenname. Diese Standardeinstellung ist leer. Der Name muss ein gültiger Domänenname sein und aus x.y bestehen, wobei x eine ASCII-Zeichenkette mit 1 - 254 Zeichen ohne Leerstellen zwischen den Zeichen und y ein gültiger Domärentyp wie com, edu, gov, int, mil, ne oder org ist. Die Standardeinstellung ist leer.

Zeitüberschreitung	Die Wartezeit in Sekunden, bis die Active Directory-Abfragen beendet werden. Minimaler Wert ist gleich oder größer als 15 Sekunden. Der Standardwert ist 120 .
Verwenden Sie Standardschema	Verwendet das Standardschema mit Active Directory.
Verwenden Sie Erweitertes Schema	Verwendet das erweiterte Schema mit Active Directory.
iDRAC-Name	Der Name, der den iDRAC im Active Directory eindeutig identifiziert. Diese Standardeinstellung ist leer. Der Name muss eine ASCII-Zeichenkette mit 1 - 254 Zeichen ohne Leerstellen zwischen den Zeichen sein.
iDRAC-Domänenname	Der DNS-Name der Domäne, in der sich das Active Directory-iDRAC-Objekt befindet. Diese Standardeinstellung ist leer. Der Name muss ein gültiger Domänenname sein und aus x.y bestehen, wobei x eine ASCII-Zeichenkette mit 1 - 254 Zeichen ohne Leerstellen zwischen den Zeichen und y ein gültiger Domänentyp wie com, edu, gov, int, mil, ne oder org ist.
Rollengruppen	Die Liste der Rollengruppen, die dem iDRAC zugehören. Um die Einstellungen für eine Rollengruppe zu ändern, klicken Sie auf ihre Rollengruppennummer in der Rollengruppenliste.
Gruppenname	Der Name, der die Rollengruppe in dem Active Directory identifiziert, das dem iDRAC zugehört. Diese Standardeinstellung ist leer.
Gruppendomäne	Der Domänentyp, bei dem sich die Rollengruppe befindet.

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

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

Tabelle 5-23. Rollengruppenberechtigungen


Einstellung	Beschreibung
Berechtigungsstufe der Rollengruppe	Legt die maximale iDRAC-Benutzerberechtigung für eine der folgenden Möglichkeiten fest: Administrator , Hauptbenutzer , Gastbenutzer , Keine oder Benutzerdefiniert . In Tabelle 5-24 werden die Rollengruppen-Berechtigungen aufgeführt.
Bei iDRAC anmelden	Erlaubt der Gruppe den Anmeldezugriff auf den iDRAC.
iDRAC konfigurieren	Gibt der Gruppe die Berechtigung, den iDRAC zu konfigurieren.
Benutzer konfigurieren	Gibt der Gruppe die Berechtigung, Benutzer zu konfigurieren.
Protokolle löschen	Erlaubt der Gruppenberechtigung, Protokolle zu löschen.
Serversteuerungsbefehle ausführen	Erlaubt der Gruppenberechtigung, Serversteuerungsbefehle auszuführen.
Zugriff auf Konsolenumleitung	Erlaubt der Gruppe, auf die Konsolenumleitung zuzugreifen.
Zugriff auf Virtueller Datenträger	Erlaubt der Gruppe, auf Virtueller Datenträger zuzugreifen.
Testwarnungen	Erlaubt der Gruppe, einem bestimmten Benutzer Testwarnungen (E-Mail und PET) zu senden.
Diagnosebefehle ausführen	Erlaubt der Gruppenberechtigung, Diagnosebefehle auszuführen.

Tabelle 5-24. Rollengruppenberechtigungen

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

Ein Active Directory CA-Zertifikat hochladen

1. Wählen Sie auf der Seite **Active Directory-Hauptmenü** **Active Directory-Zertifizierungsstellenzertifikat hochladen** aus, und klicken Sie auf **Weiter**.
2. Geben Sie auf der Seite **Zertifikat hochladen** den Dateipfad zum Zertifikat im Feld **Dateipfad** ein, oder klicken Sie auf **Durchsuchen**, um zur Zertifikatdatei zu wechseln.

 **ANMERKUNG:** Der **Dateipfad**-Wert zeigt den relativen Pfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad tippen, mit dem vollständigen Pfad und dem gesamten Dateinamen und Dateinamenszusatz.

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

3. Klicken Sie auf **Anwenden**.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 5-25](#).

Tabelle 5-25. Seitenschaltflächen Zertifikat hochladen

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

iDRAC-Serverzertifikat herunterladen

1. Wählen Sie auf der Seite **Active Directory-Hauptmenü** **iDRAC-Serverzertifikat herunterladen** aus, und klicken Sie auf **Weiter**.
2. Speichern Sie die Datei auf ein Verzeichnis Ihres Systems.
3. Im Fenster **Herunterladen abgeschlossen** auf **Schließen** klicken.

Active Directory CA-Zertifikat ansehen

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

1. Wählen Sie auf der Seite **Active Directory-Hauptmenü** **Active Directory-Zertifizierungsstellenzertifikat anzeigen** aus, und klicken Sie auf **Weiter**.
[Tabelle 5-26](#) beschreibt die Felder und zugehörigen Beschreibungen, die im **Zertifikat**-Fenster aufgeführt sind.
2. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 5-27](#).

Tabelle 5-26. Active Directory CA Zertifikat-Informationen

Feld	Beschreibung
Seriennummer	Zertifikat-Seriennummer.
Subjektinformationen	Vom Subjekt eingegebene Zertifikat-Attribute.
Aussteller-Informationen	Vom Aussteller zurückgegebene Zertifikat-Attribute.
Gültig von	Zertifikat-Ausstellungsdatum.
Gültig bis	Zertifikat-Verfallsdatum.

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

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

Seriell über LAN konfigurieren

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

[Tabelle 5-28](#) enthält Informationen zu den Einstellungen der Seite **Seriell über LAN - Konfiguration**.

3. Klicken Sie auf **Anwenden**.
4. Konfigurieren Sie die erweiterten Einstellungen, falls erforderlich. Klicken Sie andernfalls auf die entsprechende Schaltfläche, um fortzufahren. Siehe [Tabelle 5-29](#).

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

- a. Klicken Sie auf **Erweiterte Einstellungen**.
- b. Konfigurieren Sie auf der Seite **Seriell über LAN - Konfiguration - erweiterte Einstellungen** die erweiterten Einstellungen wie erforderlich. Siehe [Tabelle 5-30](#).
- c. Klicken Sie auf **Anwenden**.
- d. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 5-31](#).

Tabelle 5-28. **Seriell über LAN-Konfigurationsseiteneinstellungen**

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

Tabelle 5-29. **Schaltflächen der Seriell über LAN-Konfigurationsseiten**

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


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


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

Tabelle 5-31. **Seriell über LAN-Konfiguration - erweiterte Einstellung-Seitenschaltflächen**

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

iDRAC-Dienste konfigurieren

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

 **ANMERKUNG:** Wenn Sie für die Dienste Änderungen anwenden, werden die Änderungen sofort wirksam. Bestehende Verbindungen können ohne vorherige Warnung abgebrochen werden.

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

Tabelle 5-32. Webservereinstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert oder deaktiviert den iDRAC-Web Server. Wenn markiert, weist das Kontrollkästchen darauf hin, dass der Web Server aktiviert ist. Die Standardeinstellung ist aktiviert .
Max. Sitzungen	Die maximale Anzahl von gleichzeitigen Sitzungen, die für dieses System zulässig sind. Dieses Feld kann nicht bearbeitet werden. Es können vier Sitzungen gleichzeitig ausgeführt werden.
Aktuelle Sitzungen	Die Anzahl von aktuellen Sitzungen auf dem System, kleiner/gleich Max. Sitzungen . Dieses Feld kann nicht bearbeitet werden.
Zeitüberschreitung	Die Zeit in Sekunden, für die eine Verbindung ungenutzt sein kann. Die Sitzung wird abgebrochen, wenn das Zeitlimit erreicht wird. Änderungen an der Einstellung zur Zeitüberschreitung werden sofort wirksam und führen zu einem Reset des Web Servers. Der Zeitüberschreibungsbereich ist 60 bis 1920 Sekunden. Die Standardeinstellung ist 300 Sekunden.
HTTP-Schnittstellennummer	Die Schnittstelle, an der der iDRAC abhört, ob eine Browser-Verbindung besteht. Die Standardeinstellung ist 80 .
HTTPS-Schnittstellennummer	Die Schnittstelle, an der der iDRAC abhört, ob eine sichere Browser-Verbindung besteht. Die Standardeinstellung ist 443 .

Tabelle 5-33. SSH-Einstellungen

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

Tabelle 5-34. Telnet-Einstellungen

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

Tabelle 5-35. Automatisierte Systemwiederherstellungsagenteinstellung


Einstellung	Beschreibung
Aktiviert	Aktiviert den Automatisierten Systemwiederherstellungsagenten.


Tabelle 5-36. Schaltflächen der Dienstleistungsseite

Schaltfläche	Beschreibung
--------------	--------------


Drucken	Druckt die Seite Dienste aus.
Aktualisieren	Aktualisiert die Seite Dienste .
Änderungen anwenden	Wendet die Seiteneinstellungen für Dienste an.

iDRAC-Firmware aktualisieren

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

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

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

 **ANMERKUNG:** Um die Firmware zu aktualisieren, muss der iDRAC in den Aktualisierungsmodus gesetzt werden. Sobald sich der iDRAC in diesem Modus befindet, wird er automatisch zurückgesetzt, selbst wenn Sie den Aktualisierungsvorgang abbrechen.

3. Klicken Sie auf der Seite **Firmware-Aktualisierung** auf **Weiter**, um den Aktualisierungsvorgang zu starten.
4. Klicken Sie im Fenster **Firmware-Aktualisierung - Hochladen (Seite 1 von 4)** auf **Durchsuchen**, oder geben den Pfad zum heruntergeladenen Firmware-Image an.

Beispiel:

C:\Updates\V1.0*Image_Name*>.

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


5. Klicken Sie auf **Weiter**.
 - 1 Die Datei wird auf den iDRAC hochgeladen. Dieser Vorgang kann mehrere Minuten dauern.

ODER

 - 1 Sie können zu diesem Zeitpunkt auf **Abbrechen** klicken, wenn der Firmware-Aktualisierungsvorgang abgebrochen werden soll. Wenn Sie auf **Abbrechen** klicken, wird der iDRAC in den normalen Betriebsmodus zurückgesetzt.
6. Im Fenster **Firmware-Aktualisierung - Überprüfung (Seite 2 von 4)** werden die Ergebnisse der Überprüfung angezeigt, die für die von Ihnen hochgeladene Image-Datei ausgeführt wurde.
 - 1 Wenn die Image-Datei erfolgreich hochgeladen wurde und alle Überprüfungsvorgänge durchlaufen sind, erscheint eine Meldung mit dem Inhalt, dass das Firmware-Image überprüft wurde.

ODER

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


 **ANMERKUNG:** Wenn Sie die Markierung des Kontrollkästchens **Konfiguration sichern** aufheben, wird der iDRAC auf seine Standardeinstellungen zurückgesetzt. Das LAN ist in den Standardeinstellungen deaktiviert. Sie werden nicht in der Lage sein, sich bei der iDRAC-Webschnittstelle anzumelden. Es wird erforderlich sein, die LAN-Einstellungen unter Verwendung der CMC-Webschnittstelle oder iKVM unter Verwendung des iDRAC-Konfigurationshilfsprogramms während des BIOS-POST neu zu konfigurieren.
7. Standardmäßig ist das Kontrollkästchen **Konfiguration sichern** ausgewählt, um die aktuellen Einstellungen auf dem iDRAC nach einer Erweiterung zu sichern. Wenn Sie nicht wollen, dass die Einstellungen gespeichert werden, wählen Sie das Kontrollkästchen **Konfiguration sichern** ab.
8. Klicken Sie auf **Aktualisierung starten**, um den Aktualisierungsvorgang zu starten. Unterbrechen Sie den Erweiterungsvorgang nicht.
9. Im Fenster **Firmware-Aktualisierung - Aktualisierung wird durchgeführt (Seite 3 von 4)** wird der Erweiterungsstatus angezeigt. Der Fortschritt des in Prozent gemessenen Firmware-Erweiterungsvorgangs wird in der Spalte **Fortschritt** angezeigt.
10. Sobald die Firmware-Aktualisierung abgeschlossen ist, wird das Fenster **Firmware-Aktualisierung - Aktualisierungsergebnisse (Seite 4 von 4)** angezeigt und der iDRAC automatisch zurückgesetzt. Sie müssen das aktuelle Browserfenster schließen und sich mit dem iDRAC erneut verbinden, indem Sie ein neues Browserfenster verwenden.

iDRAC-Firmware mittels CMC wiederherstellen

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

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

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

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

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

1. Laden Sie die neueste iDRAC-Firmware von **support.dell.com** auf den Verwaltungscomputer herunter.
2. Melden Sie sich bei der webbasierten CMC-Schnittstelle an.
3. Klicken Sie auf **Gehäuse in der Systemstruktur**.
4. Klicken Sie auf das Register **Aktualisieren**. Die Seite **Aktualisierbare Komponenten** wird angezeigt. Der Server mit dem wiederherstellbaren iDRAC ist in der Liste enthalten, falls diese vom CMC wiederhergestellt werden kann.
5. Klicken Sie auf **server-*n***, wobei ***n*** die Nummer des Servers ist, dessen iDRAC Sie wiederherstellen möchten.
6. Klicken Sie auf **Durchsuchen**, um zum iDRAC-Firmware-Image zu browsen, das Sie heruntergeladen haben, und klicken Sie auf **Öffnen**.
7. Klicken Sie auf **Firmware-Aktualisierung beginnen**.

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

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

iDRAC mit Microsoft Active Directory verwenden

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Vorteile und Nachteile des Erweiterten Schemas und Standardschemas](#)
- [Übersicht über Erweitertes Schema von Active Directory](#)
- [Übersicht zum Standardschema des Active Directory](#)
- [SSL auf einem Domänen-Controller aktivieren](#)
- [Active Directory zur Anmeldung beim iDRAC verwenden](#)
- [Häufig gestellte Fragen](#)

Ein Verzeichnisdienst führt eine allgemeine Datenbank aller Informationen, die zur Kontrolle von Benutzern, Computern, Druckern und anderer Geräte auf dem Netzwerk erforderlich sind. Wenn Ihre Firma die Microsoft® Active Directory® Service-Software verwendet, kann die Software so konfiguriert werden, dass sie Zugriff auf den iDRAC bietet, wodurch Sie in der Lage sind, bestehenden Benutzern in der Active Directory-Software iDRAC-Benutzerberechtigungen zuzuteilen und diese zu steuern.

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

Sie können Active Directory dazu verwenden, den Benutzerzugriff auf iDRAC über die Lösung eines erweiterten Schemas zu definieren, die die von Dell definierte Active Directory-Objekte oder eine Standardschemalösung einsetzt, die nur Active Directory-Gruppenobjekte verwendet.

Vorteile und Nachteile des Erweiterten Schemas und Standardschemas

Wenn Sie Active Directory zur Konfiguration des Zugriffs auf den iDRAC verwenden, müssen Sie entweder die Lösung des erweiterten Schemas oder des Standardschemas wählen.

Die Vorteile, die Lösung des erweiterten Schemas zu verwenden, sind:

- 1 Alle Access Control-Objekte werden in Active Directory aufrechterhalten.
- 1 Maximale Flexibilität bei der Konfiguration des Benutzerzugriffs auf verschiedene iDRACs mit unterschiedlichen Berechtigungsebenen.

Die Vorteile, die Standardschema-Lösung zu verwenden, sind:

- 1 Es ist keine Schema-Erweiterung erforderlich, weil das Standardschema nur Active Directory-Objekte verwendet.
- 1 Die Konfiguration vom Active Directory aus ist einfach.

Übersicht über Erweitertes Schema von Active Directory

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

- 1 Mit der iDRAC-Webschnittstelle. Siehe [Konfiguration des iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung der Webschnittstelle](#).
- 1 Mit dem RACADM CLI-Hilfsprogramm. Siehe [iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung von RACADM konfigurieren](#).
- 1 Mit der SM-CLP-Befehlszeile. Siehe [iDRAC mit der Schemaerweiterung des Active Directory und SM-CLP konfigurieren](#).

Active Directory-Schema-Verlängerungen

Die Active Directory-Daten sind eine dezentrale Datenbank von Attributen und Klassen. Das Active Directory-Schema enthält die Regeln, die den Typ der Daten bestimmen, die hinzugefügt oder in die Datenbank aufgenommen werden können. Die Benutzerklasse ist ein Beispiel einer Klasse, die in der Datenbank gespeichert wird. Einige Beispiel-Attribute der Benutzerklasse sind Vorname, Nachname, Telefonnummer usw. des Benutzers. Firmen können die Active Directory-Datenbank erweitern, indem sie ihre eigenen einzigartigen Attribute und Klassen hinzufügen, um Umgebungsspezifische Bedürfnisse zu lösen. Dell hat das Schema erweitert, um die Attribute und Klassen zur Unterstützung der Remote-Verwaltungsauthentifizierung und -autorisierung einzuschließen.

Jede(s) Attribut oder Klasse, das/die einem existierenden Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert werden. Um einzigartige IDs innerhalb der Industrie aufrechtzuerhalten, erhält Microsoft eine Datenbank von Active Directory-Objektbezeichnern aufrecht, sodass es garantiert ist, dass hinzugefügte Verlängerungen des Schemas einzigartig ist und nicht miteinander in Konflikt stehen. Um das Schema im Microsoft Active Directory zu erweitern, hat Dell eindeutige OIDs, eindeutige Namenserverlängerungen sowie eindeutig verknüpfte Attribut-IDs für die Attribute und Klassen erhalten, die dem Verzeichnisdienst hinzugefügt worden sind, wie in [Tabelle 6-1](#) dargestellt.

Tabelle 6-1. Object Identifier des Dell Active Directory

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

Übersicht von RAC-Schema-Verlängerungen

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

Objektübersicht des Active Directory

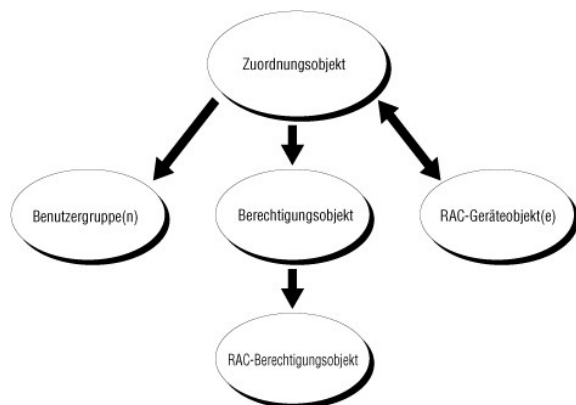
Für jedes der physischen RACs auf dem Netzwerk, das Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein RAC-Geräteobjekt erstellen. Sie können so viele Zuordnungsobjekte erstellen, wie gewünscht, und jedes Zuordnungsobjekt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

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

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

[Abbildung 6-1](#) zeigt, dass das Zuordnungsobjekt die Verbindung enthält, die für die gesamte Authentifizierung und Autorisierung erforderlich ist.

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



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

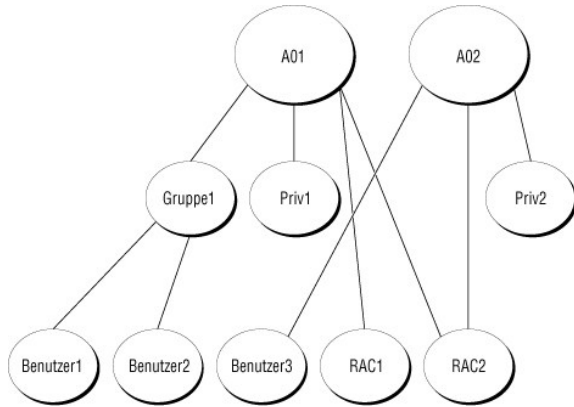
Sie können eine beliebige Anzahl an Zuordnungsobjekten erstellen. Es ist jedoch erforderlich, dass Sie mindestens ein Zuordnungsobjekt erstellen, und Sie müssen ein RAC-Geräteobjekt für jeden RAC (iDRAC) auf dem Netzwerk besitzen, das zum Zweck der Authentifizierung und Autorisierung mit dem RAC (iDRAC)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

Das Zuordnungsobjekt berücksichtigt so viele oder wenige Benutzer und/oder Gruppen sowie RAC-Geräteobjekte. Aber das Zuordnungsobjekt enthält nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die "Benutzer", die auf den RACs über "Berechtigungen" verfügen.

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

Wenn Sie Universalgruppen von unterschiedlichen Domänen hinzufügen, erstellen Sie ein Zuordnungsobjekt mit der Universalreichweite. Die durch das Dell Schema-Erweiterungsdienstprogramm erstellten Standardzuordnungsobjekte sind domänenlokale Gruppen und arbeiten nicht mit Universalgruppen von anderen Domänen.

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



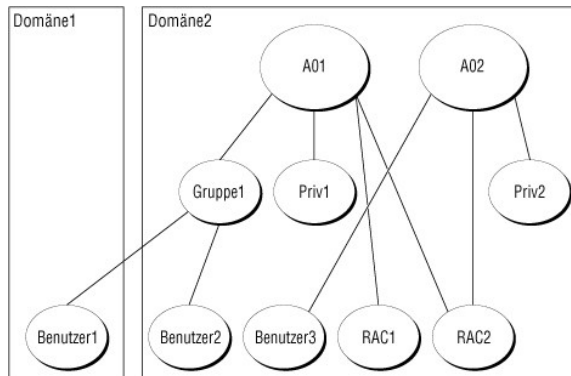
Um die Objekte für das Einzeldomänen-Szenario zu konfigurieren, führen Sie die folgenden Tasks aus:

1. Erstellen Sie zwei Zuordnungsobjekt.
2. Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die beiden iDRACS repräsentieren sollen.
3. Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) und Ber2 Anmeldeberechtigungen hat.
4. Gruppieren Sie Benutzer1 und Benutzer2 in Gruppe1.
5. Fügen Sie Group1 als Mitglieder im Zuordnungsobjekt 1 (AO1), Ber1 als Berechtigungsobjekte in AO1, und RAC1, RAC2 als RAC-Geräte in AO1 hinzu.
6. Fügen Sie User3 als Mitglied im Zuordnungsobjekt 2 (AO2), Ber2 als Berechtigungsobjekte in AO2, und RAC2 als RAC-Geräte in AO2 hinzu.

Ausführliche Anleitungen erhalten Sie unter [iDRAC-Benutzer und -Berechtigungen zum Active Directory hinzufügen](#).

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

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



Um die Objekte für das Szenario für eine einzelne Domäne zu konfigurieren, führen Sie die folgenden Aufgaben aus:

1. Stellen Sie sicher, dass die Domänenfunktion im nativen oder Windows-2003-Modus ist.
2. Erstellen Sie zwei Zuordnungsobjekte, AO1 (mit universellem Bereich) und AO2 in jeder Domäne.
[Abbildung 6-3](#) zeigt die Objekte in Domain2.
3. Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die beiden iDRACS repräsentieren sollen.
4. Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) und Ber2 Anmeldeberechtigungen hat.
5. Gruppieren Sie Benutzer1 und Benutzer2 in Gruppe1. Der Gruppenbereich von Gruppe1 muss universal sein.

6. Fügen Sie Group1 als Mitglieder im Zuordnungsobjekt 1 (AO1), Ber1 als Berechtigungsobjekte in AO1, und RAC1, RAC2 als RAC-Geräte in AO1 hinzu.
7. Fügen Sie User3 als Mitglied im Zuordnungsobjekt 2 (AO2), Ber2 als Berechtigungsobjekte in AO2, und RAC2 als RAC-Geräte in AO2 hinzu.

Schemaerweiterung des Active Directory zum Zugriff auf iDRAC konfigurieren

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

1. Erweitern Sie das Active Directory-Schema (siehe [Erweiterung des Active Directory-Schemas](#)).
2. Erweitern Sie das Active Directory-Benutzer- und Computer-Snap-In (siehe [Dell Erweiterung auf die Active Directory-Benutzer und das Computer-Snap-In installieren](#)).
3. Fügen Sie dem Active Directory iDRAC-Benutzer und deren Berechtigungen hinzu (siehe [iDRAC-Benutzer und -Berechtigungen zum Active Directory hinzufügen](#)).
4. Aktivieren Sie SSL auf Ihren einzelnen Domänen-Controllern (siehe [SSL auf einem Domänen-Controller aktivieren](#)).
5. Konfigurieren Sie die iDRAC-Active Directory-Eigenschaften, indem Sie entweder die iDRAC-Webschnittstelle oder den RACADM verwenden (siehe [Konfiguration des iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung der Webschnittstelle](#) oder [iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung von RACADM konfigurieren](#)).

Erweiterung des Active Directory-Schemas

Mit der Erweiterung des Active Directory-Schemas werden eine Dell organisatorische Einheit, Schemaklassen und -attribute und Beispielsberechtigungen und Zuordnungsobjekte zum Active Directory-Schema hinzugefügt. **Bevor Sie das Schema erweitern, vergewissern Sie sich, dass Sie Schema-Admin-Berechtigungen auf dem Schema Master Flexible Single Master Operation (FSMO)-Rollenbesitzer des Domänenwaldes haben.**

Das Schema kann anhand einer der folgenden Möglichkeiten erweitert werden:

1. Dell Schemaerweiterungsdienstprogramm
1. LDIF-Skript-Datei

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


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

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

Zur Verwendung der LDIF-Dateien siehe die Anleitungen in der Infodatei im Verzeichnis **LDIF_Dateien**. Informationen zum Verwenden der Dell-Schemaerweiterung zur Erweiterung des Active Directory-Schemas finden Sie unter [Dell Schema-Erweiterung verwenden](#).

Sie können die Schema-Erweiterung oder LDIF-Dateien kopieren und von jedem Standort aus ausführen.

Dell Schema-Erweiterung verwenden

 **HINWEIS:** Die Dell Schema-Erweiterung verwendet die Datei **SchemaExtenderOem.ini**. Um sicherzustellen, dass das Dell Schemaerweiterungsdienstprogramm richtig funktioniert, modifizieren Sie den Namen dieser Datei nicht.

1. Klicken Sie auf **Weiter** auf dem **Willkommen**-Bildschirm.
2. Lesen Sie die Warnung genau, und klicken Sie auf **Weiter**.
3. Wählen Sie **Aktuelle Anmeldezeugnisse verwenden** oder geben Sie einen Benutzernamen und Kennwort mit Schema-Administratorberechtigungen ein .
4. Klicken Sie auf **Weiter**, um die Dell Schemaerweiterung auszuführen.
5. Klicken Sie auf **Fertig stellen**.

Das Schema wird erweitert. Um die Schema-Erweiterung zu überprüfen, verwenden Sie die Microsoft Verwaltungskonsole (MMC) und das Active Directory Schema-Snap-In, um die Existenz der folgenden Elemente zu überprüfen:

1. Klassen (siehe [Tabelle 6-2](#) bis [Tabelle 6-7](#))
1. Attribute ([Tabelle 6-8](#))

Weitere Informationen zum Aktivieren und Verwenden des Active Directory-Schema-Snap-In in der MCC stehen in Ihrer Microsoft-Dokumentation zur Verfügung.

Tabelle 6-2. Klassendefinitionen für Klassen, die dem Active Directory-Schema hinzugefügt wurden

Klassenname	Zugewiesene Objektkennummer (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-Klasse

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Beschreibung	Repräsentiert das Dell RAC-Gerät. Das RAC-Gerät muss als dellRacDevice im Active Directory konfiguriert werden. Anhand dieser Konfiguration kann der iDRAC LDAP-Abfragen (Lightweight Directory Access Protocol) an das Active Directory senden.
Klassentyp	Strukturklasse
Superklassen	dellProduct
Attribute	dellSchemaVersion dellRacType

Tabelle 6-4. dellAssociationObject-Klasse

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Beschreibung	Repräsentiert das Dell Zuordnungsobjekt. Das Zuordnungsobjekt enthält die Verbindung zwischen den Benutzern und den Geräten.
Klassentyp	Strukturklasse
Superklassen	Gruppe
Attribute	dellProductMembers dellPrivilegeMember

Tabelle 6-5. dellRAC4Privileges-Klasse

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Beschreibung	Wird verwendet, um die Berechtigungen (Autorisierungsrechte) für das iDRAC-Gerät zu definieren.
Klassentyp	Hilfsklasse
Superklassen	Keine
Attribute	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Tabelle 6-6. dellPrivileges-Klasse

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Beschreibung	Wird als Container-Klasse für die Dell Berechtigungen (Autorisierungsrechte) verwendet.
Klassentyp	Strukturklasse
Superklassen	Benutzer
Attribute	dellRAC4Privileges

Tabelle 6-7. dellProduct-Klasse

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Beschreibung	Die Hauptklasse, von der alle Dell Produkte abgeleitet werden.
Klassentyp	Strukturklasse
Superklassen	Computer
Attribute	dellAssociationMembers

Tabelle 6-8. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden

Attributname/Beschreibung	Zugewiesene OID/Syntax-Objektbezeichner	Einzel geschätzt
dellPrivilegeMember Liste von Dell Berechtigungsobjekten, die zu diesem Attribut gehören.	1.2.840.113556.1.8000.1280.1.1.2.1 Bemerkenswerter Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Die Liste von Dell Rac-Geräten, die zu dieser Rolle gehören. Dieses Attribut ist die Vorwärtsverbindung zur dellAssociationMembers-Rückwärtsverbindung. Link-ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Bemerkenswerter Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE, wenn der Benutzer Anmelderechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.3 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.4 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.5 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE, wenn der Benutzer Protokolllöschrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.7 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE, wenn der Benutzer Konsolenumleitungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.8 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE, wenn der Benutzer Virtuelle Datenträgerrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE, wenn der Benutzer Testwarnungsberechtigungen auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.10 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE, wenn der Benutzer Debug-Befehlsadministratorenrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion Die aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren.	1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Dieses Attribut ist der aktuelle RAC-Typ für das DellRacDevice-Objekt und die rückwärts gerichtete Verknüpfung zur Vorwärtsverknüpfung von dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Die Liste von dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist die Rückwärtsverbindung zum dellProductMembers verbundenen Attribut. Link-ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Bemerkenswerter Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Dell Erweiterung auf die Active Directory-Benutzer und das Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch das Active Directory-Benutzer- und Computer-Snap-In erweitern, sodass der Administrator RAC- (iDRAC)-Geräte, Benutzer und Benutzergruppen, RAC-Zuordnungen und RAC-Berechtigungen verwalten kann.

Wenn Sie die Systems Management-Software anhand der CD *Dell Systems Management Consoles* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsverfahrens die Option **Dell-Erweiterung für das Active Directory-Benutzer- und Computer-Snap-In** auswählen. Zusätzliche Anleitungen zum Installieren von Systems Management-Software stehen im *Schnellinstallationshandbuch zu Dell OpenManage-Software* zur Verfügung.

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

Administrator-Pack installieren

Das Administrator-Pack muss auf jedem System installiert werden, das die Active Directory-iDRAC-Objekte verwaltet. Wenn Sie den Administrator-Pack nicht installieren, können Sie das Dell RAC-Objekt im Container nicht ansehen.

Weitere Informationen erhalten Sie unter [Active Directory-Benutzer und Computer-Snap-In öffnen](#).

Active Directory-Benutzer und Computer-Snap-In öffnen

Um die Active Directory-Benutzer und Computer-Snap-In zu öffnen, führen Sie die folgenden Schritte aus:

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

Wenn Sie nicht auf dem Domänen-Controller angemeldet sind, muss das entsprechende Microsoft Administrator-Pack auf dem lokalen System installiert sein. Klicken Sie zur Installation dieses Administrator-Packs auf **Start** → **Ausführen**, geben Sie `mmc` ein, und drücken Sie auf **Eingabe**.

Die Verwaltungskonsolle von Microsoft (MMC) wird eingeblendet.

2. Klicken Sie im Fenster der **Konsole 1** auf **Datei** (oder **Konsole** auf Systemen, die Windows 2000 ausführen).
3. Klicken Sie auf **Snap-In hinzufügen/entfernen**.
4. Wählen Sie das **Active Directory-Benutzer- und Computer-Snap-In**, und klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **Schließen** und klicken Sie auf **OK**.

iDRAC-Benutzer und -Berechtigungen zum Active Directory hinzufügen

Mit dem von Dell erweiterten Active Directory-Benutzer- und Computer-Snap-In können Sie iDRAC-Benutzer und -Berechtigungen hinzufügen, indem Sie RAC-, Zuordnungs- und Berechtigungsobjekte erstellen. Um jede Objektart hinzuzufügen, führen Sie die folgenden Verfahren aus:

- 1 Ein RAC-Geräteobjekt erstellen
- 1 Ein Berechtigungsobjekt erstellen
- 1 Zuordnungsobjekt erstellen
- 1 Einem Zuordnungsobjekt Objekte hinzufügen


Ein RAC-Geräteobjekt erstellen

1. Im Fenster MMC-**Konsolenstamm** klicken Sie mit der rechten Maustaste auf einen Container.
2. Wählen Sie **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 iDRAC-Namen identisch sein, den Sie in [Schritt a](#) von [Konfiguration des iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung der Webschnittstelle](#) eingeben werden.
4. Wählen Sie **RAC-Geräteobjekt**.
5. Klicken Sie auf **OK**.

Ein Berechtigungsobjekt erstellen

 **ANMERKUNG:** Ein Berechtigungsobjekt muss in der gleichen Domäne wie das verwandte Zuordnungsobjekt erstellt werden.

1. Im Fenster **Konsolenstamm** (MCC), klicken Sie mit der rechten Maustaste auf einen Container.
2. Wählen Sie **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**.
5. Klicken Sie auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf das von Ihnen erstellte Objekt und wählen Sie **Eigenschaften**.
7. Klicken Sie auf das Register **RAC-Berechtigungen**, und wählen Sie die Berechtigungen aus, die der Benutzer erhalten soll (weitere Informationen finden Sie unter [iDRAC-Benutzerberechtigungen](#)).

Zuordnungsobjekt erstellen

Das Zuordnungsobjekt wird aus einer Gruppe abgeleitet und muss einen Gruppentyp enthalten. Die Zuordnungsreichweite gibt den Sicherheitsgruppentyp für das Zuordnungsobjekt an. Wenn Sie ein Zuordnungsobjekt erstellen, müssen Sie die Zuordnungsreichweite wählen, die sich auf den Typ der Objekte bezieht, die hinzugefügt werden sollen.

Wenn z. B. **Universal** gewählt wird, bedeutet das, dass Zuordnungsobjekte nur verfügbar sind, wenn die Active Directory-Domäne im Native- oder einem höheren Modus arbeitet.

1. Im Fenster **Konsolenstamm** (MCC), klicken Sie mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu→Dell-RAC-Objekt** aus.
Dadurch wird das Fenster **Neues Objekt** geöffnet.
3. Geben Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Zuordnungsobjekt**.
5. Wählen Sie die Reichweite für das **Zuordnungsobjekt** aus.
6. Klicken Sie auf **OK**.

Einem Zuordnungsobjekt Objekte hinzufügen

Durch Anwendung des Fensters **Zuordnungsobjekteigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und RAC-Geräte oder RAC-Gerätegruppen zuordnen. Wenn das System den Windows 2000-Modus oder höher verwendet, müssen Sie universale Gruppen verwenden, um Domänen mit Ihren Benutzern oder RAC-Objekten mit einzuschließen.

Sie können Gruppen von Benutzern und RAC-Geräten hinzufügen. Die Verfahren zum Erstellen von Dell-bezogenen Gruppen und nicht-Dell-bezogenen Gruppen sind identisch.

Benutzer oder Benutzergruppen hinzufügen

1. Klicken Sie mit der rechten Maustaste auf das **Zuordnungsobjekt** und wählen Sie **Eigenschaften**.
2. Klicken Sie auf das Register **Benutzer** und klicken Sie **Hinzufügen**.
3. Geben Sie den Benutzer- oder Benutzergruppennamen ein und klicken Sie auf **OK**.

Klicken Sie auf das Register **Berechtigungsobjekt**, um die Berechtigung hinzuzufügen, die die Benutzer- oder Benutzergruppenberechtigungen definiert, während ein RAC-Gerät authentifiziert wird. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

Berechtigungen hinzufügen

1. Wählen Sie das Register **Berechtigungsobjekt** aus, und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Berechtigungsobjektnamen ein und klicken Sie auf **OK**.

Klicken Sie auf das Register **Produkte**, um ein oder mehrere RAC-Geräte zur Zuordnung hinzuzufügen. Die assoziierten Geräte geben die mit dem Netzwerk verbundenen RAC-Geräte an, die für die definierten Benutzer oder Benutzergruppen verfügbar sind. Mehrere RAC-Geräte können einem Zuordnungsobjekt hinzugefügt werden.


RAC-Geräte oder RAC-Gerätegruppen hinzufügen

Um RAC-Geräte oder RAC-Gerätegruppen hinzuzufügen:

1. Wählen Sie das Register **Produkte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Namen des RAC-Geräts oder der RAC-Gerätegruppe ein und klicken Sie auf **OK**.
3. Klicken Sie im Fenster **Eigenschaften** auf **Anwenden** und dann auf **OK**.

Konfiguration des iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung der Webschnittstelle

1. Öffnen Sie ein unterstütztes Internetbrowser-Fenster.
2. Melden Sie sich bei der iDRAC-Webschnittstelle an.
3. Klicken Sie auf **System**→**Remote-Zugriff**.
4. Klicken Sie auf das Register **Konfiguration** und wählen Sie **Active Directory**.
5. Auf der Seite **Active Directory-Hauptmenü** wählen Sie **Active Directory konfigurieren** und klicken Sie auf **Weiter**.
6. Im Abschnitt Allgemeine Einstellungen:
 - a. Wählen Sie das Kontrollkästchen **Active Directory aktivieren**
 - b. Geben Sie den **Root-Domännennamen** ein. Der **Root-Domänenname** ist der vollständig qualifizierte Root-Domänenname für den Wald.
 - c. Geben Sie die **Zeitüberschreitungs**-Zeit in Sekunden ein.
7. Klicken Sie auf **Erweitertes Schema verwenden** im Abschnitt Auswahl des Active Directory-Schemas.
8. Im Abschnitt Erweiterte Schemaeinstellungen:
 - a. Geben Sie den **DRAC-Namen** ein. Dieser Name muss identisch mit dem allgemeinen Namen des neuen RAC-Objekts sein, das Sie in Ihrem Domänen-Controller erstellt haben (siehe [Schritt 3](#) unter "[Ein RAC-Geräteobjekt erstellen](#)").
 - b. Geben Sie den **DRAC-Domännennamen** ein (z. B. `iDRAC.com`). Verwenden Sie den NetBIOS-Namen nicht. Der **DRAC-Domänenname** ist der vollständig qualifizierte Domänenname der Sub-Domäne, in der sich das RAC-Geräteobjekt befindet.
9. Klicken Sie auf **Anwenden** um die Active Directory-Einstellungen zu speichern.
10. Auf **Zurück zum Active Directory-Hauptmenü** klicken.
11. Laden Sie das Stamm-Zertifizierungsstellenzertifikat der Domänengesamtstruktur zum iDRAC hoch.
 - a. Wählen Sie die Optionsschaltfläche **Active Directory-Zertifizierungsstellenzertifikat hochladen** aus, und klicken Sie dann auf **Weiter**.
 - b. Geben Sie auf der Seite **Zertifikat hochladen** den Dateipfad des Zertifikats ein oder suchen Sie die Zertifikat-Datei.

 **ANMERKUNG:** Der Dateipfad-Wert zeigt den relativen Pfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad tippen, mit dem vollständigen Pfad und dem gesamten Dateinamen und Dateinamenszusatz.

Die SSL-Zertifikate des Domänen-Controllers sollten vom Stamm-CA unterzeichnet worden sein. Halten Sie das Stamm-Zertifizierungsstellenzertifikat auf Ihrer Verwaltungsstation bereit, die auf den iDRAC zugreift (siehe [Domänen-Controller-Stamm-CA-Zertifikat exportieren](#)).

 - c. Klicken Sie auf **Anwenden**.

Der iDRAC-Web Server startet automatisch neu, wenn Sie auf **Anwenden** klicken.
12. Melden Sie sich beim iDRAC ab und dann wieder an, um die Funktionskonfiguration für das iDRAC-Active Directory durchzuführen.

13. Klicken Sie auf **System**→ **Remote-Zugriff**.
14. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**.
15. Wenn **DHCP verwenden (für die NIC-IP-Adresse)** unter **Netzwerk-Einstellungen** gewählt wird, dann wählen Sie **DHCP verwenden, um DNS Server-Adresse zu erhalten**.

Wenn Sie eine DNS-Server-IP-Adresse von Hand eingeben möchten, wählen Sie **DHCP zum Abrufen von DNS-Serveradressen verwenden** ab und geben Sie die primäre und alternative DNS-Server-IP-Adresse ein.

16. Klicken Sie auf **Änderungen anwenden**.

Die Funktionskonfiguration für das iDRAC-Schemaerweiterungs-Active Directory wurde durchgeführt.

iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung von RACADM konfigurieren

Verwenden Sie die folgenden Befehle, um die iDRAC-Active Directory-Funktion mit der Schemaerweiterung zu konfigurieren, indem Sie das RACADM-CLI-Hilfsprogramm anstelle der Webschnittstelle verwenden.

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

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

racadm config -g cfgActiveDirectory -o cfgADType 1

racadm config -g cfgActiveDirectory -o cfgAD RacDomain <RAC-FQDN>

racadm config -g cfgActiveDirectory -o cfgADRootDomain <Stamm-FQDN>

racadm config -g cfgActiveDirectory -o cfgAD RacName <RAC-allgemeiner-Name>

racadm sslcertupload -t 0x2 -f <Stamm-Zertifizierungsstellen-Zertifikat-TFTP-URI>

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

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

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

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


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

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

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

4. Drücken Sie auf **Eingabe**, um die iDRAC-Active Directory-Funktionskonfiguration durchzuführen.

iDRAC mit der Schemaerweiterung des Active Directory und SM-CLP konfigurieren

 **ANMERKUNG:** Es ist erforderlich, dass ein TFTP-Server ausgeführt wird, von dem aus Sie das Stamm-Zertifizierungsstellenzertifikat abrufen und auf das Sie das iDRAC-Serverzertifikat speichern können.

Verwenden Sie die folgenden Befehle, um die iDRAC-Active Directory-Funktion mit dem erweiterten Schema unter Verwendung von SM-CLP zu konfigurieren.

1. Melden Sie sich unter Verwendung von Telnet oder SSH beim iDRAC an, und geben Sie die folgenden SM-CLP-Befehle ein:

```
cd /system/spl/oem Dell_ adservice1

set enablestate=1

set oem Dell_ schematype=1

set oem Dell_ adracdomain=<RAC-FQDN>

set oem Dell_ adrootdomain=<Stamm-FQDN>

set oem Dell_ adracname=<RAC-allgemeiner-Name>
```

```

set /system1/spl/oemdel1_ssl1 oemdel1_certtype=AD

load -source <Stamm-Zertifizierungsstellen-Zertifikat-TFTP-URI>

set /system1/spl/oemdel1_ssl1 oemdel1_certtype=SSL
dump -destination <DRAC-Server-Zertifikat-TFTP-URI> /system1/spl/oemdel1_ssl1

```

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

```

set /system1/spl/enetport1/lanendpt1/ipendpt1/\
dnsendpt1 oemdel1_serversfromdhcp=1

```

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

```

set /system1/spl/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdel1_serversfromdhcp=0

set /system1/spl/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesapl dnsserveraddress=<primäre-DNS-IP-Adresse>

set /system1/spl/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesapl dnsserveraddress=<sekundäre-DNS-IP-Adresse>

```

Übersicht zum Standardschema des Active Directory

Wie in [Abbildung 6-4](#) dargestellt, erfordert die Verwendung des Standardschemas zur Integration des Active Directory die Konfiguration sowohl im Active Directory als auch auf dem iDRAC. Auf der Active Directory-Seite wird ein Standardgruppenobjekt als eine Rollengruppe verwendet. Ein Benutzer, der Zugriff auf den iDRAC besitzt, wird ein Mitglied der Rollengruppe sein. Um diesem Benutzer Zugriff auf einen bestimmten iDRAC zu gewähren, muss der Rollengruppenname und dessen Domänenname auf dem bestimmten iDRAC konfiguriert werden. Im Gegensatz zur Schemaerweiterungslösung wird die Rolle und die Berechtigungsebene auf jedem iDRAC und nicht im Active Directory definiert. Auf jedem iDRAC können bis zu fünf Rollengruppen konfiguriert und definiert werden. [Tabelle 5-10](#) zeigt die Berechtigungsebene der Rollengruppen an, und [Tabelle 6-9](#) die standardmäßigen Rollengruppen-Einstellungen.

Abbildung 6-4. iDRAC-Konfiguration mit Microsoft Active Directory und dem Standardschema

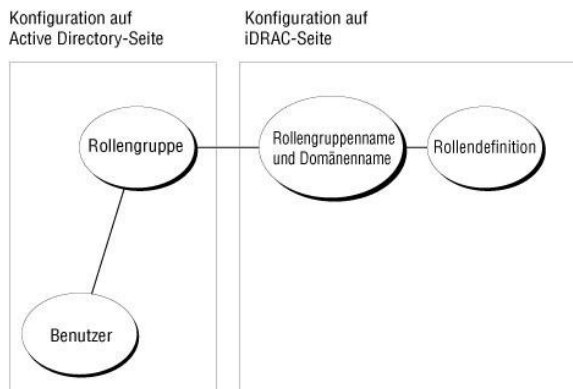


Tabelle 6-9. Standardeinstellungsberechtigungen der Rollengruppe

Standardeinstellungsberechtigungsstufe	Berechtigungen gewährt	Bit-Maske
Administrator	Anmeldung bei iDRAC, iDRAC konfigurieren, Benutzer konfigurieren, Protokolle löschen , Serversteuerungsbefehle ausführen , Zugriff auf Konsolenumleitung, Zugriff auf Virtueller Datenträger, Testwarnungen, Diagnosebefehle ausführen	0x000001ff
Hauptbenutzer	Anmeldung bei iDRAC, Protokolle löschen , Serversteuerungsbefehle ausführen , Zugriff auf Konsolenumleitung, Zugriff auf Virtueller Datenträger , Testwarnungen	0x000000f9
Gastbenutzer	Bei iDRAC anmelden	0x00000001
Keine	Keine zugewiesenen Berechtigungen	0x00000000
Keine	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bit-Maskenwerte werden nur verwendet, wenn das Standardschema mit RACADM eingestellt wird.

Das Standardschema kann auf zwei Arten im Active Directory aktiviert werden:

- 1 Mit der iDRAC-Web-Benutzeroberfläche. Siehe [Konfiguration des iDRAC anhand der Schemaerweiterung des Active Directory und der Webschnittstelle](#).
- 1 Mit dem RACADM CLI-Hilfsprogramm. Siehe [Konfiguration des iDRAC anhand des Standardschemas von Active Directory und RACADM](#).

Standardschema von Active Directory zum Zugriff auf iDRAC konfigurieren

Bevor ein Active Directory-Benutzer auf den iDRAC zugreifen kann, müssen die folgenden Schritte zur Konfiguration des Active Directory ausgeführt werden:

1. Auf einem Active Directory-Server (Domänen-Controller) das Active Directory-Benutzer- und Computer-Snap-In öffnen.
2. Erstellen Sie eine Gruppe oder wählen Sie eine vorhandene Gruppe aus. Der Name der Gruppe und der Name dieser Domäne müssen auf dem iDRAC entweder über die Webschnittstelle, über RACADM oder über SM-CLP konfiguriert werden (siehe [Konfiguration des iDRAC anhand der Schemaerweiterung des Active Directory und der Webschnittstelle](#) oder [Konfiguration des iDRAC anhand des Standardschemas von Active Directory und RACADM](#)).
3. Fügen Sie den Active Directory-Benutzer als Mitglied der Active Directory-Gruppe hinzu, um auf den iDRAC zuzugreifen.

Konfiguration des iDRAC anhand der Schemaerweiterung des Active Directory und der Webschnittstelle

1. Öffnen Sie ein unterstütztes Internetbrowser-Fenster.
2. Melden Sie sich an der iDRAC-Webschnittstelle an.
3. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC** und dann auf das Register **Konfiguration**.
4. Wählen Sie **Active Directory** aus, um die Seite **Active Directory-Hauptmenü** zu öffnen.
5. Auf der Seite **Active Directory-Hauptmenü** wählen Sie **Active Directory konfigurieren** und klicken Sie auf **Weiter**.
6. Im Abschnitt Allgemeine Einstellungen:
 - a. Wählen Sie das Kontrollkästchen **Active Directory aktivieren**
 - b. Geben Sie den **Root-Domännennamen** ein. Der **Root-Domänenname** ist der vollständig qualifizierte Root-Domänenname für den Wald.
 - c. Geben Sie die **Zeitüberschreitungs**-Zeit in Sekunden ein.
7. Klicken Sie auf **Standardschema verwenden** im Abschnitt Auswahl des Active Directory-Schemas.
8. Klicken Sie auf **Anwenden** um die Active Directory-Einstellungen zu speichern.
9. Klicken Sie in der Spalte **Rollengruppen** des Abschnitts zu den Standardschemaeinstellungen auf eine **Rollengruppe**.

Die Seite **Rollengruppe konfigurieren** wird angezeigt, die den **Gruppennamen**, die **Gruppenomäne** und **Berechtigungen der Rollengruppe** beinhaltet.
10. Geben Sie den **Gruppennamen** ein. Der Gruppenname identifiziert die Rollengruppe in dem Active Directory, das mit dem iDRAC in Verbindung steht.
11. Geben Sie die **Gruppenomäne** ein. Der **Gruppenomänenname** ist der vollständig qualifizierte Root-Domänenname für den Wald.
12. Stellen Sie auf der Seite **Berechtigungen der Rollengruppe** die Gruppenberechtigungen ein.

[Tabelle 5-10](#) beschreibt die **Berechtigungen der Rollengruppe**.

Wenn Sie eine Berechtigung modifizieren, wird die vorhandene **Rollengruppenberechtigung** (**Administrator**, **Hauptbenutzer** oder **Gastbenutzer**) auf Grundlage der modifizierten Berechtigungen entweder zur benutzerdefinierten Gruppe oder zur entsprechenden **Rollengruppenberechtigung** verändert.
13. Klicken Sie auf **Anwenden** um die Rollengruppeneinstellungen zu speichern.
14. Klicken Sie auf **Zurück zur Active Directory-Konfiguration und Verwaltung**.
15. Auf **Zurück zum Active Directory-Hauptmenü** klicken.
16. Laden Sie das Stamm-Zertifizierungsstellenzertifikat der Domänengesamtstruktur zum iDRAC hoch.
 - a. Wählen Sie die Optionsschaltfläche **Active Directory-Zertifizierungsstellenzertifikat hochladen** aus, und klicken Sie dann auf **Weiter**.
 - b. Geben Sie auf der Seite **Zertifikat hochladen** den Dateipfad des Zertifikats ein oder suchen Sie die Zertifikat-Datei.

 **ANMERKUNG:** Der Dateipfad-Wert zeigt den relativen Pfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad tippen, mit dem vollständigen Pfad und dem gesamten Dateinamen und Dateinamenszusatz.

Die SSL-Zertifikate des Domänen-Controllers sollten vom Stamm-CA unterzeichnet worden sein. Halten Sie das Stamm-Zertifizierungsstellenzertifikat auf Ihrer Verwaltungsstation bereit, die auf den iDRAC zugreift (siehe [Stamm-Zertifizierungsstellenzertifikat des Domänen-Controllers exportieren](#)).

- c. Klicken Sie auf **Anwenden**.

Der iDRAC-Web Server startet automatisch neu, wenn Sie auf **Anwenden** klicken.

17. Melden Sie sich beim iDRAC ab und dann wieder an, um die Funktionskonfiguration für das iDRAC-Active Directory durchzuführen.
18. Klicken Sie auf **System**→ **Remote-Zugriff**.
19. Klicken Sie auf das Register **Konfiguration** und dann auf **Netzwerk**.
20. Wenn **DHCP verwenden (für die NIC-IP-Adresse)** unter **Netzwerk-Einstellungen** gewählt wird, dann wählen Sie **DHCP verwenden, um DNS Server-Adresse zu erhalten**.

Wenn Sie eine DNS-Server-IP-Adresse von Hand eingeben möchten, wählen Sie **DHCP zum Abrufen von DNS-Serveradressen verwenden** ab und geben Sie die primäre und alternative DNS-Server-IP-Adresse ein.

21. Klicken Sie auf **Änderungen anwenden**.


Die Funktionskonfiguration für das iDRAC-Standardschemaerweiterungs-Active Directory wurde durchgeführt.

Konfiguration des iDRAC anhand des Standardschemas von Active Directory und RACADM

Verwenden Sie die folgenden Befehle, um die iDRAC-Active Directory-Funktion mit dem Standardschema zu konfigurieren, indem Sie RACADM-CLI anstelle der Webschnittstelle verwenden.

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

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgActiveDirectory -o cfgADRootDomain <Stamm-FQDN>
racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupName <allgemeiner-Name-der-Rollengruppe>
racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupDomain <RAC-FQDN>
racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupPrivilege <Berechtigungen-Bitmaske>
racadm sslcertupload -t 0x2 -f <Stamm-Zertifizierungsstellen-Zertifikat-TFTP-URI>
racadm sslcertdownload -t 0x1 -f <RAC-SSL-Zertifikat-TFTP-URI>
```

 **ANMERKUNG:** Informationen zu Bitmaskenwerten finden Sie in [Tabelle B-1](#).


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

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

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

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 <primäre-DNS-IP-Adresse>
racadm config -g cfgLanNetworking -o cfgDNSServer2 <sekundäre-DNS-IP-Adresse>
```

Konfiguration des iDRAC anhand des Standardschemas von Active Directory und SM-CLP

 **ANMERKUNG:** Zertifikate können nicht unter Verwendung von SM-CLP hochgeladen werden. Verwenden Sie stattdessen die iDRAC-Webschnittstelle oder die Befehle des lokalen RACADM.

Verwenden Sie die folgenden Befehle, um die iDRAC-Active Directory-Funktion mit dem Standardschema unter Verwendung von SM-CLP zu konfigurieren.

1. Melden Sie sich unter Verwendung von Telnet oder SSH am iDRAC an, und geben Sie die folgenden SM-CLP-Befehle ein:

```
cd /system/spl/oem Dell_adservice1
set enablestate=1
```

```
set oemdel1_schematype=2
```

```
set oemdel1_adracdomain=<RAC-FQDN>
```

2. Geben Sie die folgenden Befehle für jede der fünf Active Directory-Rollengruppen ein:

```
set /system1/spl/groupN oemdel1_groupname=<RollengruppeN-allgemeiner-Name>
```

```
set /system1/spl/groupN oemdel1_groupdomain=<RAC-FQDN>
```

```
set /system1/spl/groupN oemdel1_groupprivilege=<Benutzerberechtigungs-Bitmaske>
```

wobei *N* eine Zahl von 1 bis 5 ist.

3. Geben Sie die folgenden Befehle zum Einstellen der Active Directory-SSL-Zertifizierungen ein.

```
set /system1/spl/oemdel1_ssl1 oemdel1_certtype=AD  
load -source <Stamm-Zertifizierungsstellen-Zertifikat-TFTP-URI>
```

```
set /system1/spl/oemdel1_ssl1 oemdel1_certtype=SSL
```

```
dump -destination <iDRAC-Serverzertifikat-TFTP-URI> /system1/spl/oemdel1_ssl1
```

4. Wenn DHCP auf dem iDRAC aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie den folgenden SM-CLP-Befehl ein:

```
set /system1/spl/enetport1/lanendpt1/  
ipendpt1/dnsendpt1 oemdel1_serversfromdhcp=1
```

5. Wenn DHCP auf dem iDRAC deaktiviert ist oder Sie Ihre DNS-IP-Adressen manuell eingeben möchten, geben Sie die folgenden SM-CLP-Befehle ein:

```
set /system1/spl/enetport1/lanendpt1/  
ipendpt1/dnsendpt1 oemdel1_serversfromdhcp=0
```

```
set /system1/spl/enetport1/lanendpt1/ipendpt1/  
dnsendpt1/remotesapl dnsserveraddress=<primäre-DNS-IP-Adresse>
```


```
set /system1/spl/enetport1/lanendpt1/ipendpt1/  
dnsendpt1/remotesapl dnsserveraddress=<sekundäre-DNS-IP-Adresse>
```

SSL auf einem Domänen-Controller aktivieren

Wenn Sie die Microsoft Enterprise Stamm-CA verwenden, um alle Domänen-Controller-SSL-Zertifikate automatisch zuzuweisen, müssen Sie die folgenden Schritte ausführen, um SSL auf jedem Domänen-Controller zu aktivieren.

1. Installieren Sie eine Microsoft Enterprise-Stamm-CA auf einem Domänen-Controller.
 - a. Wählen Sie **Start**→ **Systemsteuerung**→ **Software** aus.
 - b. Wählen Sie **Windows-Komponenten hinzufügen/entfernen**.
 - c. Im **Assistent für Windows-Komponenten** wählen Sie das Kontrollkästchen **Zertifikatsdienste**.
 - d. Wählen Sie **Enterprise Stamm-CA** als **CA-Typ** und klicken Sie auf **Weiter**.
 - e. Geben Sie **Allgemeiner Name dieser Zertifizierungsstelle**, klicken Sie auf **Weiter** und klicken Sie auf **Fertig stellen**.
2. Aktivieren Sie SSL auf jedem Ihrer Domänen-Controller durch Installieren des SSL-Zertifikats für jeden Controller.
 - a. Klicken Sie auf **Start**→ **Verwaltung**→ **Domänen-Sicherheitsrichtlinie**.
 - b. Erweitern Sie den Ordner **Öffentliche Schlüsselregeln**, klicken Sie mit der rechten Maustaste **Automatische Zertifikatanforderungseinstellungen** und klicken Sie auf **Automatische Zertifikatsanforderung**.
 - c. Im **Assistent für automatische Zertifikatsanforderung** klicken Sie auf **Weiter** und wählen Sie **Domänen-Controller**.
 - d. Klicken Sie auf **Weiter** und klicken Sie auf **Fertig stellen**.

Domänen-Controller-Stamm-CA-Zertifikat exportieren

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

1. Suchen Sie den Domänen-Controller, der den Microsoft Enterprise CA-Dienst ausführt.
2. Klicken Sie auf **Start**→ **Ausführen**.

3. Geben Sie in das Feld **Ausführen** mmc ein und klicken Sie auf **OK**.
4. Klicken Sie im Fenster **Konsole 1** (MMC) auf **Datei** (oder auf **Konsole** auf Windows 2000-Systemen) und wählen Sie **Snap-In hinzufügen/entfernen**.
5. Im Fenster **Snap-In hinzufügen/entfernen** klicken Sie auf **Hinzufügen**.
6. Im Fenster **Eigenständiges Snap-In hinzufügen** wählen Sie **Zertifikate** und klicken Sie auf **Hinzufügen**.
7. Wählen Sie das Konto **Computer** und klicken sie auf **Weiter**.
8. Wählen Sie **Lokaler Computer** und klicken Sie auf **Fertig stellen**.
9. Klicken Sie auf **OK**.
10. **Im Fenster Konsole 1** erweitern Sie den Ordner **Zertifikate**, erweitern Sie den Ordner **Persönlich** und klicken Sie auf den Ordner **Zertifikate**.
11. **Machen Sie das Stammzertifizierungsstellenzertifikat ausfindig** und klicken Sie mit der rechten Maustaste darauf, wählen Sie **Alle Aufgaben** und klicken Sie auf **Exportieren....**
12. Im **Zertifikatsexport-Assistent** klicken sie auf **Weiter** und wählen Sie **Nein, exportieren Sie nicht den privaten Schlüssel**.
13. Klicken Sie auf **Weiter** und wählen Sie **Base-64 kodierte .509 (.cer)** als das Format.
14. Auf **Weiter** klicken und das Zertifikat in einem Verzeichnis auf Ihrem System speichern.
15. Laden Sie das in [Schritt 14](#) gespeicherte Zertifikat zum iDRAC hoch.


Um das Zertifikat unter Verwendung von RACADM hochzuladen, lesen Sie den Abschnitt [Konfiguration des iDRAC mit der Schemaerweiterung des Active Directory unter Verwendung der Webschnittstelle](#).


Um das Zertifikat mittels der Webschnittstelle hochzuladen, führen Sie das folgende Verfahren aus:

- a. Öffnen Sie ein unterstütztes Internetbrowser-Fenster.
- b. Melden Sie sich bei der iDRAC-Webschnittstelle an.
- c. Klicken Sie auf **System**→ **Remote-Zugriff** und dann auf das Register **Konfiguration**.
- d. Klicken Sie auf **Sicherheit**, um die Seite **Hauptmenü des Sicherheitszertifikats** zu öffnen.
- e. Auf der Seite **Sicherheitszertifikat-Hauptmenü** wählen Sie **Server-Zertifikat hochladen** und klicken Sie auf **Anwenden**.
- f. Führen Sie auf dem Bildschirm **Zertifikat hochladen** eins der folgenden Verfahren aus:
 - o Klicken Sie auf **Durchsuchen**, und wählen Sie das Zertifikat aus.
 - o Geben Sie in das Feld **Wert** den Pfad zum Zertifikat ein.
- g. Klicken Sie auf **Anwenden**.

SSL-Zertifikat der iDRAC-Firmware importieren

Wenden Sie das folgende Verfahren an, um das iDRAC-Firmware-SSL-Zertifikat in alle vertrauenswürdigen Zertifikatlisten der Domänen-Controller zu importieren.

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

 **ANMERKUNG:** Wenn das iDRAC-Firmware-SSL-Zertifikat von einer bekannten Zertifizierungsstelle signiert ist, ist es nicht erforderlich, die in diesem Abschnitt beschriebenen Schritte auszuführen.

Das iDRAC-SSL-Zertifikat ist identisch mit dem Zertifikat, das für den iDRAC-Web Server verwendet wird. Alle iDRACs werden mit einem selbstsignierten Standardzertifikat versendet.

Wählen Sie zum Zugreifen auf das Zertifikat unter Verwendung der iDRAC-Webschnittstelle **Konfiguration**→ **Active Directory**→ **iDRAC-Serverzertifikat herunterladen** aus.

1. Öffnen Sie auf dem Domänen-Controller ein **MMC-Konsolen-Fenster**, und wählen Sie **Zertifikate**→ **Vertrauenswürdige Stammzertifizierungsstellen** aus.
2. Rechts-klicken Sie auf **Zertifikate**, wählen Sie **Alle Aufgaben** und klicken sie auf **Import**.
3. Klicken Sie auf **Weiter** und browsen Sie zur SSL-Zertifikat-Datei.
4. Installieren Sie das RAC-SSL-Zertifikat in der **Trusted Root Certification Authority** jedes Domänen-Controllers.

Wenn Sie Ihr eigenes Zertifikat installiert haben, stellen Sie sicher, dass die CA, die Ihr Zertifikat unterschreibt auf der Liste von **zuverlässigen Stammzertifikatzertifizierungsstelle** ist. Wenn die Zertifizierungsstelle nicht auf der Liste ist, müssen Sie sie auf allen Ihren Domänen-Controllern installieren.

5. Klicken Sie auf **Weiter** und wählen Sie, ob Windows die Zertifikatsstelle, basierend auf dem Zertifikattyp, automatisch wählen soll oder wechseln Sie zu einer Stelle Ihrer Wahl.
6. Klicken Sie auf **Fertig stellen** und klicken Sie auf **OK**.

Active Directory zur Anmeldung beim iDRAC verwenden

Sie können Active Directory verwenden, um sich unter Verwendung der Webschnittstelle am iDRAC anzumelden. Verwenden Sie zur Eingabe Ihres Benutzernamens eines der folgenden Formate aus:

<Benutzername@Domäne>

oder


<Domäne>\<Benutzername>

oder

<Domäne>/<Benutzername>

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

Leerstellen und Sonderzeichen (z.B. \, / oder @) sind weder im Benutzernamen noch im Domänennamen zulässig.

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

Häufig gestellte Fragen

In [Tabelle 6-10](#) werden häufig gestellte Fragen und Antworten aufgeführt.

Tabelle 6-10. iDRAC mit dem Active Directory verwenden: Häufig gestellte Fragen

Frage	Antwort
Kann ich mich am iDRAC anmelden, indem ich Active Directory über mehrfache Strukturen verwende?	Ja. Der Abfragealgorithmus des iDRAC-Active Directory unterstützt mehrfache Strukturen in einer einzelnen Gesamtstruktur.
Funktioniert die Anmeldung am iDRAC anhand von Active Directory im gemischten Modus (d. h. die Domänen-Controller in der Gesamtstruktur führen verschiedene Betriebssysteme aus, wie z. B. Microsoft Windows NT® 4.0, Windows 2000 oder Windows Server 2003)?	Ja. Im gemischten Modus müssen sich alle durch das iDRAC-Abfrageverfahren verwendeten Objekte (unter Benutzer, RAC-Geräteobjekt und Zuordnungsobjekt) in derselben Domäne befinden. Das Dell-erweiterte Active Directory Users and Computers Snap-In überprüft den Modus und beschränkt Benutzer, um Objekte über Domänen hinweg zu erstellen, wenn es im Mischmodus ist.
Unterstützt die Verwendung des iDRAC mit Active Directory mehrfache Domänenumgebungen?	Ja. Der Domänenwalfunktionslevel muss im nativen Modus oder Windows-2003-Modus sein. Außerdem müssen die Gruppen unter dem Zuordnungsobjekt, RAC-Benutzerobjekte und RAC-Geräteobjekte (einschließlich des Zuordnungsobjekts) universale Gruppen sein.
Können diese Dell-erweiterten Objekte (Dell-Zuordnungsobjekt, Dell RAC-Gerät und Dell-Berechtigungsobjekt) in verschiedenen Domänen sein?	Das Zuordnungsobjekt und das Berechtigungsobjekt müssen in derselben Domäne sein. Mit Dell erweiterten Active Directory-Benutzern und Computer-Snap-In müssen Sie diese zwei Objekte in derselben Domäne erstellen. Andere Objekte können sich in verschiedenen Domänen befinden.
Gibt es irgendwelche Einschränkungen der Domänen-Controller-SSL-Konfiguration?	Ja. SSL-Zertifikate aller Active Directory-Server in der Gesamtstruktur müssen von der gleichen Stammzertifizierungsstelle signiert werden, da iDRAC nur das Hochladen eines einzigen vertrauenswürdigen Zertifizierungsstellen-SSL-Zertifikats zulässt.
Ich habe ein neues RAC-Zertifikat erstellt und hochgeladen, und jetzt startet die Webschnittstelle nicht.	Wenn Sie Zertifikatsdienste von Microsoft verwenden, um das RAC-Zertifikat zu erstellen, ist eine mögliche Ursache davon dass Sie Benutzerzertifikat wählten anstatt Webzertifikat als Sie das Zertifikat erstellen. Erstellen Sie zur Wiederherstellung eine CSR und dann ein neues Webzertifikat über die Microsoft-Zertifikatsdienste, und laden Sie es unter Verwendung der RACADM-CLI vom verwalteten Server, indem Sie die folgenden RACADM-Befehle verwenden: racadm sslsrsgen [-g] [-u] [-f {Dateiname}] racadm sslcertupload-t 1-f {web_sslcert}
Was kann ich tun, wenn ich mich mit Active Directory-Authentifizierung nicht am iDRAC anmelden kann? Wie kann ich eine Lösung für das Problem finden?	<ol style="list-style-type: none"> 1. Stellen Sie sicher, dass Sie die richtige Benutzerdomänenname während einer Anmeldung verwendet wird und nicht der NetBIOS-Name. 2. Wenn Sie ein lokales iDRAC-Benutzerkonto besitzen, melden Sie sich mit Ihren lokalen Anmeldeinformationen am iDRAC an.

Nachdem Sie angemeldet sind, die folgenden Schritte ausführen:

- a. Stellen Sie sicher, dass das Kästchen **Active Directory aktivieren** auf der iDRAC-Seite **Active Directory-Konfiguration** markiert ist.
- b. Stellen Sie sicher, dass die DNS-Einstellung auf der iDRAC-Seite **Netzwerkkonfiguration** korrekt ist.
- c. Stellen Sie sicher, dass Sie das Active Directory-Zertifikat von Ihrer Active Directory-Stammzertifizierungsstelle zum iDRAC hochgeladen haben.
- d. **Überprüfen Sie die Domänen-Controller SSL-Zertifikate**, um sicherzustellen, dass sie nicht abgelaufen sind.
- e. Stellen Sie sicher, dass **DRAC -Name**, **Root-Domänenname** und **DRAC - Domänenname** mit Ihrer Active Directory-Umgebungskonfiguration **übereinstimmen**.
- f. Stellen Sie sicher, dass das iDRAC-Kennwort maximal 127 Zeichen aufweist. Während der iDRAC Kennwörter von bis zu 256 Zeichen unterstützen kann, unterstützt Active Directory nur Kennwörter, die maximal 127 Zeichen lang sind.

[Zurück zum Inhaltsverzeichnis](#)

GUI-Konsolenumleitung verwenden

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Übersicht](#)
- [Konsolenumleitung verwenden](#)
- [Video Viewer verwenden](#)
- [Häufig gestellte Fragen](#)


Dieser Abschnitt enthält Informationen über die Anwendung der iDRAC-Konsolenumleitungsfunktion.

Übersicht

Mit der iDRAC-Konsolenumleitungsfunktion können Sie im Remote-Zugriff im grafischen Modus oder Textmodus auf die lokale Konsole zugreifen. Mittels der Konsolenumleitung können Sie ein oder mehrere iDRAC-aktivierte Systeme von einem Standort aus steuern.

Es ist nicht notwendig, vor jedem Server zu sitzen, um alle routinemäßigen Wartungsvorgänge auszuführen. Sie können die Server stattdessen auf Ihrem Desktop- oder Laptop-Computer von einem beliebigen Standort aus verwalten. Sie können auch die Informationen mit anderen - im Remote-Zugriff und sofort teilen.

Konsolenumleitung verwenden

 **HINWEIS:** Wenn Sie eine Konsolenumleitungssitzung öffnen, zeigt der verwaltete Server nicht an, dass die Konsole umgeleitet worden ist.

Die Seite **Konsolenumleitung** ermöglicht Ihnen, das Remote-System zu verwalten, indem Sie Tastatur, Video und Maus auf Ihrer lokalen Verwaltungsstation verwenden, um die entsprechenden Geräte auf einem verwalteten Remote-Server zu steuern. Diese Funktion kann in Verbindung mit der virtuellen Datenträgerfunktion verwendet werden, um Remote-Softwareinstallationen auszuführen.

Die folgenden Regeln gelten für eine Konsolenumleitungssitzung:

- 1 Es können maximal zwei gleichzeitige Konsolenumleitungssitzungen unterstützt werden. Beide Sitzungen zeigen dieselbe Konsole des verwalteten Servers gleichzeitig an.
- 1 Eine Konsolenumleitungssitzung sollte auf dem verwalteten System nicht über einen Webbrowser gestartet werden.
- 1 Die erforderliche verfügbare Netzwerk-Mindestbandbreite beträgt 1 MB/s.

Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

[Tabelle 7-1](#) führt die unterstützten Bildschirmauflösungen und entsprechende Bildwiederholfrequenzen für eine Konsolenumleitungssitzung auf, die auf dem verwalteten Server ausgeführt wird.


Tabelle 7-1. Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

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

Verwaltungsstation konfigurieren

Zur Verwendung von Konsolenumleitung auf Ihrer Verwaltungsstation führen Sie die folgenden Verfahren aus:

1. Einen unterstützten Internetbrowser installieren und konfigurieren. Siehe die folgenden Abschnitte für weiterführende Informationen:
 - 1 [Unterstützte Internetbrowser](#)

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

1. [Einen unterstützten Internetbrowser konfigurieren](#)
 2. Wenn Sie Firefox verwenden oder den Java Viewer mit Internet Explorer verwenden möchten, installieren Sie eine Java-Laufzeitumgebung (JRE). Siehe [Java-Laufzeitumgebung \(JRE\) installieren](#).
 3. Es wird empfohlen, die Bildschirmauflösung auf 1280x1024 Pixel oder höher zu konfigurieren.
- HINWEIS:** Wenn Sie eine aktive Konsolenumleitungssitzung haben und ein Monitor mit niedriger Auflösung an der iKVM angeschlossen wird, wird die Serverkonsolenauflösung eventuell zurückgesetzt, wenn der Server auf der lokalen Konsole ausgewählt wird. Wenn der Server ein Linux-Betriebssystem ausführt, kann eine X11-Konsole auf dem lokalen Monitor eventuell nicht angezeigt werden. Durch Drücken auf <Strg><Alt><F1> auf der iKVM wird Linux auf eine Textkonsole geschaltet.


Konfiguration der Konsolenumleitung auf der iDRAC-Webschnittstelle

Um auf der iDRAC-Webschnittstelle eine Konsolenumleitung zu konfigurieren, führen Sie folgende Schritte aus:

1. Klicken Sie auf **System** und dann auf das Register **Konsole**.
2. Klicken Sie auf **Konfiguration**, um die Seite **Konsolenumleitungskonfiguration** zu öffnen.
3. Konfigurieren Sie die Konsolenumleitungseigenschaften. [Tabelle 7-2](#) beschreibt die Einstellungen für Konsolenumleitung.
4. Wenn Sie dies durchgeführt haben, klicken Sie auf **Anwenden**.
5. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 7-3](#).

Tabelle 7-2. Konfigurationseigenschaften der Konsolenumleitung

Eigenschaft	Beschreibung
Aktiviert	Klicken Sie, um die Konsolenumleitung zu aktivieren oder zu deaktivieren. Markiert zeigt an, dass die Konsolenumleitung aktiviert ist. Nicht markiert zeigt an, dass die Konsolenumleitung deaktiviert ist. Die Standardeinstellung ist aktiviert .
Max. Sitzungen	Zeigt die Anzahl der maximal möglichen Konsolenumleitungssitzungen an - 1 oder 2 . Verwenden Sie das Drop-Down-Menü, um die maximal zulässigen Konsolenumleitungs-Sitzungen zu ändern. Die Standardeinstellung ist 2 .
Aktive Sitzungen	Zeigt die Anzahl der Sitzungen Aktiver Konsolen an. Dieses Feld ist schreibgeschützt.
Tastatur- und Mausschnittstellennummer	Die Netzwerkschnittstellennummer, die zur Verbindung mit der Tastatur/Maus-Option der Konsolenumleitung verwendet wird. Dieser Datenverkehr ist immer verschlüsselt. Diese Zahl muss eventuell geändert werden, wenn ein anderes Programm die Standardschnittstelle verwendet. Die Standardeinstellung ist 5900 .
Videoschnittstellennummer	Die Netzwerkschnittstellennummer, die zur Verbindung mit dem Konsolenumleitungs-Bildschirmdienst verwendet wird. Diese Einstellung muss eventuell geändert werden, wenn ein anderes Programm die Standardschnittstelle verwendet. Die Standardeinstellung ist 5901 .
Videoverschlüsselung aktiviert	Markiert zeigt an, dass die Videoverschlüsselung aktiviert ist. Der zur Videoschnittstelle übertragene Datenverkehr ist verschlüsselt. Nicht markiert zeigt an, dass die Videoverschlüsselung deaktiviert ist. Der zur Videoschnittstelle übertragene Datenverkehr ist nicht verschlüsselt. Die Standardeinstellung ist Verschlüsselt. Ein Deaktivieren der Verschlüsselung kann die Leistung auf langsameren Netzwerken verbessern.
Mausmodus	Wählen Sie Windows , wenn der verwaltete Server auf einem Windows-Betriebssystem ausführt. Wählen Sie Linux aus, wenn Ihr Server auf Linux ausgeführt wird. Wählen Sie Kein , wenn der Server weder auf einem Windows- noch auf einem Linux-Betriebssystem ausführt. Die Standardeinstellung ist Windows .
Konsolen-Plugin-Typ für IE	Wenn der Internet Explorer auf einem Windows-Betriebssystem verwendet wird, können die folgenden Viewer ausgewählt werden: <i>ActiveX - Der ActiveX-Konsolenumleitungs-Viewer</i> <i>Java - Java-Konsolenumleitungs-Viewer.</i> ANMERKUNG: Auf dem Client-System muss die Java-Laufzeitumgebung installiert sein, damit der Java-Viewer verwendet werden kann.
Lokale Konsole deaktivieren	Wenn markiert, weist dies darauf hin, dass die Ausgabe an den iKVM-Monitor während der Konsolenumleitung deaktiviert wird. Hierdurch wird sichergestellt, dass die unter Verwendung der Konsolenumleitung ausgeführten Tasks auf dem lokalen Monitor des verwalteten Servers nicht sichtbar sind.

 **ANMERKUNG:** Informationen zur Verwendung des virtuellen Datenträgers mit Konsolenumleitung finden Sie unter [Virtuellen Datenträger konfigurieren und verwenden](#).

Die Schaltflächen in [Tabelle 7-5](#) sind auf der Seite **Konsolenumleitungskonfiguration** verfügbar.

Tabelle 7-3. Schaltflächen der Konsolenumleitungskonfigurationsseite

Schaltfläche	Definition
Drucken	Druckt die Seite Konsolenumleitungskonfiguration
Aktualisieren	Lädt die Seite Konsolenumleitungskonfiguration neu
Anwenden	Speichert alle neuen Einstellungen, die an der Konsolenumleitung vorgenommen wurden.

Konsolenumleitung auf der SM-CLP-Befehlszeilenoberfläche konfigurieren

Konsolenumleitungssitzung öffnen

Wenn Sie eine Konsolenumleitungssitzung öffnen, startet die Dell Virtual KVM Viewer-Anwendung, und das Desktop des Remote-Systems wird im Viewer eingeblendet. Über die Anwendung des virtuellen KVM Viewers können die Maus- und Tastaturfunktionen des Systems von einer lokalen Verwaltungsstation aus gesteuert werden.


Um auf der Webschnittstelle eine Konsolenumleitungssitzung zu öffnen, führen Sie folgende Schritte aus:

1. Klicken Sie auf **System** und dann auf das Register **Konsole**.
2. Verwenden Sie auf der Seite **Konsolenumleitung** die Informationen von [Tabelle 7-4](#), um sicherzustellen, dass eine Konsolenumleitungssitzung verfügbar ist.

Wenn Sie einen der angezeigten Eigenschaftswerte neu konfigurieren möchten, finden Sie entsprechende Informationen unter [Konfiguration der Konsolenumleitung auf der iDRAC-Webschnittstelle](#).

Tabelle 7-4. Informationen zur Seite Konsolenumleitung

Eigenschaft	Beschreibung
Konsolenumleitung aktiviert	Ja/Nein
Videoverschlüsselung aktiviert	Ja/Nein
Max. Sitzungen	Zeigt die maximale Anzahl unterstützter Konsolenumleitungssitzungen an
Aktuelle Sitzungen	Zeigt die aktuelle Anzahl aktiver Konsolenumleitungssitzungen an
Mausmodus	Zeigt die aktuell geltende Mausbeschleunigung an. Der Modus Mausbeschleunigung sollte auf der Grundlage des Typs des installierten Betriebssystems auf dem verwalteten Server ausgewählt werden.
Konsolen-Plugin-Typ	Zeigt den aktuell konfigurierten Plugin-Typ. ActiveX - Ein Active-X-Viewer wird gestartet. Der Active-X-Viewer funktioniert während der Ausführung auf einem Windows-Betriebssystem nur im Internet Explorer. Java - Ein Java-Viewer wird gestartet. Der Java-Viewer kann in jedem Browser, einschließlich Internet Explorer, verwendet werden. Wenn Ihr Client auf einem anderen Betriebssystem als Windows ausgeführt wird, müssen Sie den Java-Viewer verwenden. Wenn Sie auf den iDRAC zugreifen, indem Sie den Internet Explorer während der Ausführung auf einem Windows-Betriebssystem verwenden, können Sie entweder Active-X oder Java als Plugin-Typ auswählen.
Lokale Konsole	Nicht markiert, wenn die lokale Konsole nicht deaktiviert wurde. Wenn markiert, kann keine Person über die iKVM-Verbindung auf dem Gehäuse auf die Konsole zugreifen.


 **ANMERKUNG:** Informationen zur Verwendung des virtuellen Datenträgers mit Konsolenumleitung finden Sie unter [Virtuellen Datenträger konfigurieren und verwenden](#).


Die Schaltflächen in [Tabelle 7-5](#) sind auf der Seite **Konsolenumleitung** verfügbar.

Tabelle 7-5. Schaltflächen der Seite Konsolenumleitung

Schaltfläche	Definition
Aktualisieren	Lädt die Seite Konsolenumleitungskonfiguration neu
Viewer starten	Öffnet eine Konsolenumleitungssitzung auf dem Remote-Ziel-System.
Drucken	Druckt die Seite Konsolenumleitungskonfiguration

3. Ist eine Konsolenumleitungssitzung verfügbar, klicken Sie auf **Viewer starten**.

 **HINWEIS:** Mehrere Meldungskästen können angezeigt werden, nachdem Sie die Anwendung starten. Um nicht freigegebenen Zugang zur Anwendung zu verhindern, müssen Sie innerhalb drei Minuten durch diese Nachrichtenfenster wechseln. Sonst werden Sie aufgefordert, die Anwendung erneut zu starten.

 **ANMERKUNG:** Wenn in den folgenden Schritten ein oder mehrere **Sicherheitswarnungs**-Fenster eingeblendet werden, lesen Sie die Informationen im jeweiligen Fenster und klicken Sie auf **Ja**, um fortzufahren.

Die Verwaltungsstation wird mit dem iDRAC verbunden, und der Desktop des Remote-Systems wird in der Dell-Digital-KVM-Viewer-Anwendung angezeigt.

4. Zwei Mauszeiger erscheinen im Viewer-Fenster: einer für das Remote-System und einer für das lokale System. Die beiden Mauszeiger müssen synchronisiert werden, damit der Remote-Mauszeiger dem lokalen Mauszeiger folgt. Siehe [Synchronisieren der Mauszeiger](#).

Video Viewer verwenden

Der Video Viewer bietet eine Benutzerschnittstelle zwischen der Verwaltungsstation und dem verwalteten Server, wodurch der Desktop des verwalteten Servers sichtbar wird und die Maus- und Tastaturfunktionen von der Verwaltungsstation aus gesteuert werden können. Wenn Sie eine Verbindung zum Remote-System erstellen, wird der Video Viewer in einem eigenen Fenster gestartet.

Der Video Viewer bietet die Möglichkeit verschiedener Steuerungseinstellungen wie Farbmodus, Maussynchronisation, Snapshots, Tastaturmakros und Zugriff auf den virtuellen Datenträger. Klicken Sie auf **Hilfe**, um weitere Informationen über diese Funktionen zu erhalten.

Wenn Sie eine Konsolenumleitungssitzung starten und der Video Viewer erscheint, ist es eventuell notwendig, den Farbmodus einzustellen und die Mauszeiger zu synchronisieren.

[Tabelle 7-6](#) beschreibt die Menüoptionen, die im Viewer zum Gebrauch verfügbar sind.

Tabelle 7-6. Auswahlmöglichkeiten auf der Viewer-Menüleiste

Menüartikel	Artikel	Beschreibung
Video	Anhalten	Hält die Konsolenumleitung vorübergehend an.
	Wieder aufnehmen	Nimmt die Konsolenumleitung wieder auf.
	Aktualisieren	Zeichnet die Bildschirmanzeige des Viewers neu.
	Aktuellen Bildschirminhalt erfassen	Erfasst den aktuellen Remote-Systembildschirm in einer .bmp -Datei auf Windows oder in einer .png -Datei auf Linux. Ein Dialogfeld wird angezeigt, in dem Sie die Datei zu einem angegebenen Standort speichern können.
	Vollbildschirm	Um den Video Viewer auf Vollbildschirmmodus zu erweitern, wählen Sie Vollbildschirm im Videomenü aus.
	Beenden	Wenn Sie die Konsole nicht mehr verwenden und sich abgemeldet haben (durch Verwendung des Abmeldevorgangs des Remote-Systems), wählen Sie im Videomenü Beenden , um das Fenster Video Viewer zu schließen.
Tastatur	Rechte Alt-Taste halten	Wählen Sie dieses Element aus, bevor Sie Tasten verwenden, die mit der rechten <Alt> -Taste kombiniert werden sollen.
	Linke Alt-Taste halten	Wählen Sie dieses Element, bevor Sie Tasten verwenden, die mit der linken <Alt> -Taste kombiniert werden sollen.
	Linke Windows-Taste	Wählen Sie Gedrückt halten aus, bevor Sie Zeichen eingeben, die mit der linken Windows-Taste kombiniert werden sollen. Wählen Sie Drücken und loslassen aus, um einen Tastenanschlag der linken Windows-Taste zu senden.
	Rechte Windows-Taste	Wählen Sie Gedrückt halten aus, bevor Sie Zeichen eingeben, die mit der rechten Windows-Taste kombiniert werden sollen. Wählen Sie Drücken und loslassen aus, um einen Tastenanschlag der rechten Windows-Taste zu senden.
	Makros	Wenn Sie ein Makro auswählen oder den für das Makro angegebenen Hotkey eingeben, wird die Maßnahme auf dem Remote-System ausgeführt. Der Video Viewer bietet die folgenden Makros: <ul style="list-style-type: none"> 1 Strg-Alt-Entf 1 Alt-Tab 1 Alt-Esc 1 Strg-Esc 1 Alt-Leerzeichen 1 Alt-Eingabe 1 Alt-Bindestrich 1 Alt-F4 1 Druck 1 Alt-Druck 1 F1 1 Anhalten 1 Alt+m
	Tastaturdurchgang	Im Modus Tastaturdurchgang können alle Tastaturfunktionen auf dem Client zum Server umgeleitet werden.
Maus	Cursor synchronisieren	Im Mausmenü können Sie den Cursor synchronisieren, damit die Maus auf dem Client zur Maus auf dem Server umgeleitet wird.
Optionen	Farbmodus	Ermöglicht Ihnen, zur Verbesserung der Leistung über das Netzwerk eine Farbtiefe auszuwählen. Wenn Sie z. B. Software vom virtuellen Datenträger installieren, können Sie die niedrigste Farbtiefe auswählen (3-Bit grau), damit der Konsolen-Viewer weniger Netzwerkbandbreite verwendet und mehr Bandbreite verbleibt, um Daten vom Datenträger zu übertragen. Der Farbmodus kann auf 15-Bit Farbe, 7-Bit Farbe, 4-Bit Farbe, 4-Bit grau und 3-Bit grau eingestellt werden.
Datenträger	Assistent des virtuellen Datenträgers	Das Datenträgermenü bietet Zugriff auf den Assistenten des Virtuellen Datenträgers, wodurch Sie zu einem Gerät oder einem Image umleiten können, wie z. B.: <ul style="list-style-type: none"> 1 Diskettenlaufwerk 1 CD

		<ul style="list-style-type: none"> 1 DVD 1 Image im ISO-Format 1 USB-Flash-Laufwerk <p>Informationen zur Funktion des virtuellen Datenträgers finden Sie unter Virtuellen Datenträger konfigurieren und verwenden.</p> <p>Wenn Sie den virtuellen Datenträger verwenden, muss das Konsolen-Viewer-Fenster aktiv sein.</p>
Hilfe	-	Aktiviert das Hilfe-Menü.

Synchronisieren der Mauszeiger

Wenn Sie mittels Konsolenumleitung eine Verbindung zu einem Remote-PowerEdge-System herstellen, kann die Geschwindigkeit der Mausbeschleunigung auf dem Remote-System eventuell nicht mit dem Mauszeiger auf der Verwaltungsstation synchronisiert werden, was dazu führt, dass zwei Mauszeiger im Video Viewer-Fenster erscheinen.

Zum Synchronisieren der Mauszeiger klicken Sie auf **Maus** → **Cursor synchronisieren**, oder drücken Sie auf <Alt><M>.

Das Menü zum Synchronisieren des Cursors lässt sich umschalten. Stellen Sie sicher, dass sich neben dem Menüelement ein Häkchen befindet, damit die Maussynchronisation aktiv ist.


Stellen Sie bei der Verwendung von Red Hat® Linux® oder Novell® SUSE® Linux sicher, dass der Mausmodus für Linux konfiguriert ist, bevor Sie den Viewer starten. Hilfe bei der Konfiguration steht unter [Konfiguration der Konsolenumleitung auf der iDRAC-Webschnittstelle](#) zur Verfügung. Die Standardmauseinstellungen des Betriebssystems werden zur Steuerung des Mausfelds auf dem Bildschirm der iDRAC-Konsolenumleitung verwendet.

Lokale Konsole deaktivieren oder aktivieren

Sie können den iDRAC so konfigurieren, dass iKVM-Verbindungen über die iDRAC-Webschnittstelle nicht zulässig sind. Wenn die lokale Konsole deaktiviert ist, wird in der Liste der Server (OSCAR) ein gelber Statuspunkt angezeigt, um darauf hinzuweisen, dass die Konsole im iDRAC geschlossen ist. Wenn die lokale Konsole aktiviert ist, ist der Statuspunkt grün.

Wenn Sie sicherstellen möchten, dass Sie exklusiven Zugriff auf die Konsole des verwalteten Servers haben, müssen Sie die lokale Konsole deaktivieren und die **Max. Sitzungen** auf der Seite **Konsolenumleitung** auf 1 neu konfigurieren.

 **ANKERKUNGEN:** Die Funktion der lokalen Konsole wird auf allen x9xx PowerEdge-Systemen außer PowerEdge SC1435 und 6950 unterstützt.

 **ANMERKUNG:** Das Deaktivieren (Ausschalten) des lokalen Videos auf dem Server führt dazu, dass der Monitor, die Tastatur und die Maus, die an den iKVM angeschlossen sind, deaktiviert werden.

Wenden Sie zum Deaktivieren oder Aktivieren der lokalen Konsole das folgende Verfahren an:

- Öffnen Sie auf Ihrer Verwaltungsstation einen unterstützten Webbrowser, und melden Sie sich am iDRAC an. Weitere Informationen finden Sie unter [Zugriff auf die Webschnittstelle](#).
- Klicken Sie auf **System**, dann auf das Register **Konsole** und dann auf **Konfiguration**.
- Wenn auf dem Server lokales Video deaktiviert (ausgeschaltet) werden soll, wählen Sie auf der Seite **Konsolenumleitungskonfiguration** das Kontrollkästchen **Lokale Konsole deaktivieren** aus, und klicken Sie dann auf **Anwenden**. Der Standardwert ist **AUS**.
- Wenn auf dem Server lokales Video aktiviert (eingeschaltet) werden soll, wählen Sie auf der Seite **Konsolenumleitungskonfiguration** das Kontrollkästchen **Lokale Konsole deaktivieren** ab, und klicken Sie dann auf **Anwenden**.

Die Seite **Konsolenumleitung** zeigt den Status des lokalen Server-Videos an.

Häufig gestellte Fragen

[Tabelle 7-7](#) führt häufig gestellte Fragen und Antworten auf.

Tabelle 7-7. Konsolenumleitung verwenden: Häufig gestellte Fragen

Frage	Antwort
Kann eine neue Remote-Konsolen-Videositzung gestartet werden, wenn der lokale Video auf dem Server ausgeschaltet ist?	Ja.
Warum dauert es 15 Sekunden, um den lokalen Video auf dem Server auszuschalten, nachdem eine Aufforderung zum Ausschalten des lokalen Videos erteilt wurde?	Hierdurch wird einem lokalen Benutzer die Gelegenheit gegeben, Maßnahmen durchzuführen, bevor das Video ausgeschaltet wird.
Gibt es beim Einschalten des lokalen Videos eine Zeitverzögerung?	Nein. Sobald der iDRAC eine Aufforderung zum EIN schalten des lokalen Videos erhält, wird das Video sofort eingeschaltet.
Kann der lokale Benutzer das Video auch ausschalten?	Ja, ein lokaler Benutzer kann die lokale RACADM-CLI verwenden, um das Video auszuschalten.

Kann der lokale Benutzer das Video auch einschalten?	Nein. Wenn die lokale Konsole deaktiviert ist, sind auch die Tastatur und die Maus des lokalen Benutzers deaktiviert, und Einstellungsänderungen sind nicht möglich.
Werden beim Ausschalten des lokalen Videos auch die lokale Tastatur und Maus ausgeschaltet?	Ja.
Wird durch das Ausschalten der lokalen Konsole auch das Video der Remote-Konsolensitzung ausgeschaltet?	Nein, das Ein- oder Ausschalten des lokalen Videos ist unabhängig von der Remote-Konsolensitzung.
Welche Berechtigungen sind für einen iDRAC-Benutzer erforderlich, um das lokale Server-Video ein- oder auszuschalten?	Jeder Benutzer mit iDRAC-Konfigurationsberechtigungen kann die lokale Konsole ein- oder ausschalten.
Wie kann ich den aktuellen Status des lokalen Server-Videos erhalten?	Der Status wird auf der Seite Konsolenumleitungskonfiguration der iDRAC-Webschnittstelle angezeigt. Der RACADM-CLI-Befehl racadm getconfig -g cfgRacTuning zeigt den Status im Objekt cfgRacTuneLocalServerVideo an. Der Status wird auch auf der iKVM-OSCAR-Anzeige sichtbar. Wenn die lokale Konsole aktiviert ist, erscheint neben dem Servernamen eine grüne Statusanzeige . Wenn sie deaktiviert ist, weist ein gelber Punkt darauf hin, dass die lokale Konsole vom iDRAC gesperrt ist.
Ich kann vom Konsolenumleitungsfenster aus die Unterseite des Systembildschirms nicht sehen.	Stellen Sie sicher, dass die Monitorauflösung der Verwaltungsstation auf 1280x1024 eingestellt ist.
Das Konsolenfenster ist entstellt.	Für den Konsolen-Viewer auf Linux ist ein UTF-8-Zeichensatz erforderlich. Überprüfen Sie Ihr Gebietsschema, und setzen Sie den Zeichensatz ggf. zurück. Weitere Informationen finden Sie unter Gebietsschema in Linux einstellen .
Warum wird auf dem verwalteten Server ein leerer Bildschirm eingeblendet, wenn das Windows 2000-Betriebssystem lädt?	Auf dem verwalteten Server befindet sich nicht der richtige ATI-Videotreiber. Es ist erforderlich, den Videotreiber unter Verwendung der CD <i>Dell PowerEdge Installation and Server Management</i> zu aktualisieren.
Warum synchronisiert die Maus nicht in DOS, wenn die Konsolenumleitung ausgeführt wird?	Der Dell BIOS emuliert den Maustreiber als PS/2-Maus. Die PS/2-Maus verwendet absichtlich die relative Position für den Mauszeiger, wodurch die Synchronisationsverzögerung verursacht wird. iDRAC besitzt einen USB-Maustreiber, der eine absolute Position und eine genauere Verfolgung des Mauszeigers ermöglicht. Selbst wenn der iDRAC die absolute USB-Mausposition auf das Dell-BIOS überträgt, würde die BIOS-Emulation sie auf die relative Position zurücksetzen, und das Verhalten würde unverändert bleiben. Um dieses Problem zu beheben, stellen Sie in der Konsolenumleitungskonfiguration den Mausmodus auf KEINE ein.
Warum synchronisiert die Maus nicht unter der Textkonsole von Linux?	Virtueller KVM erfordert den USB Maus-Treiber, aber der USB Maus-Treiber ist nur unter dem X-Windows-Betriebssystem verfügbar.
Ich habe immer noch Probleme mit der Maus-Synchronisation.	Stellen Sie sicher, dass vor dem Beginn einer Konsolenumleitungssitzung die richtige Maus für das Betriebssystem ausgewählt ist. Stellen Sie sicher, dass im Maus-Menü Maus synchronisieren markiert ist. Drücken Sie auf <Alt><M> , oder wählen Sie Maus → Maus synchronisieren aus, um die Maussynchronisation umzuschalten. Wenn die Synchronisation aktiviert wird, wird neben der Auswahl im Maus-Menü ein Häkchen eingeblendet .
Warum kann ich keine Tastatur oder Maus verwenden, während ich ein Microsoft®-Betriebssystem mittels iDRAC 5-Konsolenumleitung im Remote-Zugriff installiere?	Wenn Sie im Remote-Zugriff auf ein unterstütztes Microsoft-Betriebssystem auf einem System auf dem die Konsolenumleitung im BIOS aktiviert ist installieren, erhalten Sie eine EMS-Verbindungsmeldung, die verlangt, dass Sie OK wählen bevor Sie fortfahren können . Sie können nicht die Maus verwenden, um OK im Remote-Zugriff auszuwählen. Sie müssen entweder auf dem lokalen System OK auswählen, oder den im Remote-Zugriff verwalteten Server neu starten und neu installieren und dann die Konsolenumleitung im BIOS ausschalten. Diese Nachricht wird durch Microsoft erstellt, um den Benutzer zu alarmieren, dass Konsolenumleitung aktiviert ist. Um sicherzustellen, dass diese Meldung nicht erscheint, schalten Sie die Konsolenumleitung im BIOS immer aus, bevor Sie ein Betriebssystem im Remote-Zugriff installieren.
Warum zeigt der Num Lock-Anzeiger auf meiner Verwaltungsstation nicht den Status des Num Lock auf dem Remote-Server an?	Wenn über den iDRAC auf die Num-Taste zugegriffen wird, stimmt die Num-Taste auf der Verwaltungsstation nicht unbedingt mit dem Zustand der Num-Taste auf dem Remote-Server überein. Der Zustand von Num Lock ist von der Einstellung auf dem Remote-Server abhängig, wenn die Remote-Sitzung unabhängig vom Zustand des Num Lock auf der Verwaltungsstation verbunden wird.
Warum werden mehrere Session Viewer-Fenster eingeblendet, wenn ich vom lokalen Host aus eine Konsolenumleitungssitzung aufbaue?	Eine Konsolenumleitungssitzung wird vom lokalen System aus konfiguriert. Dies wird nicht unterstützt.
Erhalte ich eine Warnungsmeldung, wenn ich eine Konsolenumleitungssitzung ausführe und ein lokaler Benutzer auf den verwalteten Server zugreift?	Nein Wenn ein lokaler Benutzer auf das System zugreift, haben Sie beide Kontrolle über das System.
Welche Bandbreite brauche ich für eine Konsolenumleitungssitzung?	Dell empfiehlt eine 5 MB/s-Verbindung für gute Leistung. Eine 1 MB/s-Verbindung ist die vorgeschriebene Mindestleistung.
Was sind die Mindestsystemanforderungen für meine Verwaltungsstation für die Ausführung der Konsolenumleitung?	Die Verwaltungsstation erfordert einen Intel Pentium III 500-MHz-Prozessor mit mindestens 256 MB RAM.

[Zurück zum Inhaltsverzeichnis](#)

Virtuellen Datenträger konfigurieren und verwenden

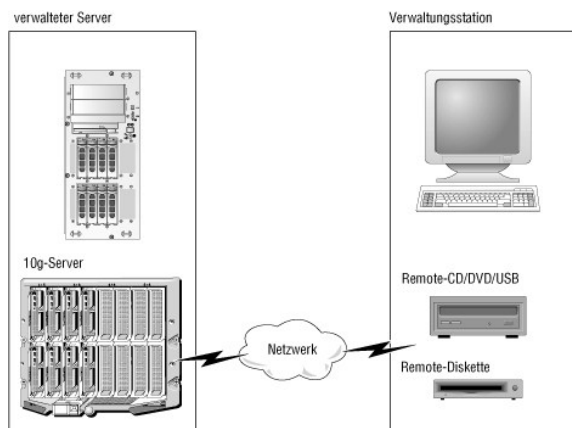
Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Übersicht](#)
- [Virtuellen Datenträger konfigurieren](#)
- [Virtuellen Datenträger ausführen](#)
- [Häufig gestellte Fragen](#)

Übersicht

Die Funktion **Virtueller Datenträger**, auf die über den Konsolenumleitungs-Viewer zugegriffen werden kann, bietet dem verwalteten Server Zugriff auf Datenträger, die mit einem Remote-System auf dem Netzwerk verbunden sind. [Abbildung 8-1](#) zeigt die Gesamtarchitektur des **virtuellen Datenträgers**.

Abbildung 8-1. Gesamte Architektur des virtuellen Datenträgers



Mit dem **virtuellen Datenträger** können Administratoren im Remote-Zugriff verwaltete Server starten, Anwendungen installieren, Treiber aktualisieren oder sogar neue Betriebssysteme von virtuellen CD/DVD- und Disketten-Laufwerken installieren.

ANMERKUNG: Der **virtuelle Datenträger** erfordert eine verfügbare Mindestnetzwerkbandbreite von 128 kbps.

Virtueller Datenträger definiert zwei Geräte für das Betriebssystem und das BIOS des verwalteten Servers: ein Diskettengerät und ein optisches Festplattengerät.

Die Verwaltungsstation enthält die physischen Datenträger oder Bilddatei über das Netzwerk. Wenn zum **virtuellen Datenträger** eine Verbindung hergestellt ist, werden alle Anforderungen eines Zugriffs der Verwaltungsstation auf das virtuelle CD-/Disketten-Laufwerk über das Netzwerk an die Verwaltungsstation geleitet. Das Verbinden des **virtuellen Datenträgers** erscheint als identisch mit dem Einsetzen von Datenträgern in physische Geräte. Wenn keine Verbindung zum virtuellen Datenträger hergestellt ist, verhalten sich virtuelle Geräte auf dem verwalteten Server wie zwei Laufwerke ohne Datenträger.

[Tabelle 8-1](#) enthält die unterstützten Laufwerk-Verbindungen für virtuelle Disketten- und virtuelle optische Laufwerke.

ANMERKUNG: Das Verändern von **virtuellen Datenträgern**, während eine Verbindung zu ihnen besteht, könnte zu einem Anhalten der Systemstartsequenz führen.

Tabelle 8-1. Unterstützte Laufwerk-Verbindungen

Unterstützte Virtuelle Diskettenlaufwerk-Verbindungen	Unterstützte Virtuelle Optische Laufwerk-Verbindungen
Legacy 1.44 Diskettenlaufwerk mit einer 1.44 Diskette	CD-ROM, DVD, CDRW, Kombinationslaufwerk mit CD-ROM-Datenträger
USB-Diskettenlaufwerk mit einer 1.44 Diskette	CD-ROM/DVD-Image-Datei im Format ISO9660
1.44 Diskettenabbild	USB-CD-ROM-Laufwerk mit CD-ROM-Datenträger
USB-Wechselplatte	

Windows-basierte Verwaltungsstation

Um die Funktion des **virtuellen Datenträgers** auf einer Verwaltungsstation mit dem Betriebssystem Microsoft® Windows® auszuführen, installieren Sie eine unterstützte Internet Explorer-Version mit dem ActiveX-Steuerungs-Plugin. Setzen Sie die Browsersicherheit auf **Mittel** oder eine niedrigere Einstellung, damit der Internet Explorer signierte ActiveX-Steuerungen herunterladen und installieren kann.

Weitere Informationen finden Sie unter [Unterstützte Internetbrowser](#).

Zum Installieren von ActiveX müssen Sie über Administratorrechte verfügen. Vor der Installation der ActiveX-Steuerung kann Internet Explorer eine Sicherheitswarnung zeigen. Um das Installationsverfahren für ActiveX Control abzuschließen, akzeptieren Sie die ActiveX Control, wenn Internet Explorer Sie mit einer Sicherheitswarnung dazu auffordert.

Linux-basierte Verwaltungsstation

Um die Funktion des virtuellen Datenträgers auf einer Verwaltungsstation mit Linux-Betriebssystem auszuführen, installieren Sie eine unterstützte Version von Firefox. Weitere Informationen finden Sie unter [Unterstützte Internetbrowser](#).

Zum Ausführen des Konsolenumleitungs-Plugin ist eine Java-Laufzeitumgebung (JRE) erforderlich. Sie können eine JRE von java.sun.com herunterladen. JRE-Version 1.6 oder höher wird empfohlen.

Virtuellen Datenträger konfigurieren

1. Melden Sie sich bei der iDRAC-Webschnittstelle an.
2. Wählen Sie in der Navigationsstruktur **System** aus, und klicken Sie auf das Register **Konsole**.
3. Klicken Sie auf **Konfiguration** → **Virtueller Datenträger**, um die Einstellungen des virtuellen Datenträgers zu konfigurieren.

[Tabelle 8-2](#) beschreibt die Konfigurationswerte des **virtuellen Datenträgers**.

4. Klicken Sie, wenn Sie die Einstellungen konfiguriert haben, auf **Anwenden**.
5. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 8-3](#).

Tabelle 8-2. Konfigurationsoptionen des virtuellen Datenträgers

Attribut	Wert
Virtuellen Datenträger anschließen	Verbinden - Schließt den Virtuellen Datenträger umgehend an den Server an. Abtrennen - Trennt den Virtuellen Datenträger umgehend vom Server ab. Automatisch verbinden - Schließt den virtuellen Datenträger nur dann am Server an, wenn eine Sitzung des virtuellen Datenträgers gestartet wird.
Maximale Sitzungen	Zeigt die maximale Anzahl zulässiger Virtueller Datenträger -Sitzungen an. Diese beträgt immer 1.
Aktive Sitzungen	Zeigt die aktuelle Anzahl von Sitzungen des virtuellen Datenträgers an.
Virtueller Datenträger-Verschlüsselung aktiviert	Klicken Sie auf das Kontrollkästchen, um die Verschlüsselung auf Verbindungen des Virtuellen Datenträgers zu aktivieren oder zu deaktivieren. Markieren aktiviert die Verschlüsselung; das Aufheben der Markierung deaktiviert die Verschlüsselung.
Schnittstellennummer des virtuellen Datenträgers	Die Netzwerkschnittstellennummer, die zur Verbindung mit dem Dienst des virtuellen Datenträgers ohne Verschlüsselung verwendet wird. Zwei hintereinander liegende Schnittstellen, die an der festgelegten Schnittstellennummer beginnen, werden verwendet, um zum Virtuellen Datenträger -Dienst zu verbinden. Die Schnittstellennummer, die der festgelegten Schnittstelle folgt, darf nicht für einen anderen iDRAC-Dienst konfiguriert werden. Die Standardeinstellung ist 3668 .
SSL-Schnittstellennummer des virtuellen Datenträgers	Die Netzwerkschnittstellennummer, für verschlüsselte Verbindungen zum Virtuellen Datenträger -Dienst verwendet wird. Zwei hintereinander liegende Schnittstellen, die an der festgelegten Schnittstellennummer beginnen, werden verwendet, um zum Virtuellen Datenträger -Dienst zu verbinden. Die Schnittstellennummer, die der festgelegten Schnittstelle folgt, darf nicht für einen anderen iDRAC-Dienst konfiguriert werden. Die Standardeinstellung ist 3670 .
Diskettenemulation	Zeigt an, ob der virtuelle Datenträger dem Server als Diskettenlaufwerk oder USB-Schlüssel angezeigt wird. Wenn Diskettenemulation markiert ist, wird das virtuelle Datenträger gerät auf dem Server als Diskettengerät angezeigt. Wenn es nicht ausgewählt ist, wird es als USB-Schlüssellaufwerk angezeigt.
Start einmalig aktivieren	Wählen Sie dieses Kästchen aus, um die Option Start einmalig aktivieren zu aktivieren. Diese Option beendet die Sitzung des Virtuellen Datenträgers automatisch, nachdem der Server einmalig gestartet wurde. Diese Option ist nützlich für automatische Bereitstellungen.

Tabelle 8-3. Schaltflächen der Konfigurationsseite des virtuellen Datenträgers

Schaltfläche	Beschreibung
Drucken	Druckt die Werte der Konsolenkonfiguration aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite Konsolenkonfiguration erneut.
Anwenden	Speichert alle neuen Einstellungen, die auf der Seite Konsolenkonfiguration vorgenommen wurden.

Virtuellen Datenträger ausführen

- ➡ **HINWEIS:** Geben Sie keinen **racreset**-Befehl aus, wenn eine Sitzung eines **virtuellen Datenträgers** ausgeführt wird. Andernfalls könnten unerwünschte Ergebnisse einschließlich Datenverlust auftreten.
- ➡ **HINWEIS:** Die Anwendung des Konsolen-Viewer -Fensters muss während dem Zugriff auf den virtuellen Datenträger aktiv bleiben.

1. Öffnen Sie einen unterstützten Webbrowser auf Ihrer Verwaltungsstation. Siehe [Unterstützte Internetbrowser](#).

➡ **HINWEIS:** Konsolenumleitung und der **virtuelle Datenträger** unterstützen nur 32-Bit-Webbrowser. Die Verwendung von 64-Bit-Webbrowsern kann zu unerwarteten Ergebnissen oder Fehlern führen.

2. Starten Sie die iDRAC-Webschnittstelle. [Zugriff auf die Webschnittstelle](#).
3. Wählen Sie in der Navigationsstruktur **System** aus, und klicken Sie auf das Register **Konsole**.

Die Seite **Konsolenumleitung** wird eingeblendet. Wenn Sie Werte angezeigter Attribute ändern möchten, finden Sie entsprechende Informationen unter [Virtuellen Datenträger konfigurieren](#).

🗒 **ANMERKUNG:** Die **Disketten-Abbilddatei** unter **Diskettenlaufwerk** (wenn anwendbar) kann erscheinen, da dieses Gerät als virtuelle Diskette virtualisiert sein kann. Sie können ein optisches Laufwerk und eine Floppy gleichzeitig oder ein einzelnes Laufwerk auswählen.

🗒 **ANMERKUNG:** Die Laufwerkbuchstaben des virtuellen Geräts auf dem verwalteten Server entsprechen nicht den Buchstaben des physischen Laufwerks auf der Verwaltungsstation.

🗒 **ANMERKUNG:** Der **virtuelle Datenträger** funktioniert auf Clients des Windows-Betriebssystems, die mit Internet Explorer Enhanced Security konfiguriert sind, eventuell nicht korrekt. Um dieses Problem zu lösen, ziehen Sie die Dokumentation zu Ihrem Microsoft-Betriebssystem zurate oder setzen sich mit Ihrem Administratoren in Verbindung.

4. Klicken Sie auf **Viewer starten**.

🗒 **ANMERKUNG:** Auf Linux wird die Datei **viewer.jsp** auf das Desktop heruntergeladen, und ein Dialogfeld befragt Sie, welche Maßnahme auf die Datei angewendet werden soll. Wählen Sie die Option **Mit Programm öffnen** aus, und wählen Sie dann die Anwendung **javaws** aus, die sich im Unterverzeichnis **bin** des JRE-Installationsverzeichnis befindet.

Die Anwendung **iDRACView** wird in einem separaten Fenster gestartet.

5. Klicken Sie auf **Datenträger → Assistent des virtuellen Datenträgers...**

Der Assistent zur Datenträgerumleitung wird eingeblendet.

6. Zeigen Sie das Statusfenster an. Wenn eine Datenträgerverbindung besteht, muss diese vor dem Verbinden mit einer anderen Datenträgerquelle zuerst unterbrochen werden. Klicken Sie rechts neben dem Datenträger, dessen Verbindung Sie unterbrechen möchten, auf **Unterbrechen**.
7. Wählen Sie die Optionsschaltfläche neben den Datenträgertypen aus, zu denen eine Verbindung hergestellt werden soll.

Sie können eine Optionsschaltfläche im Abschnitt **Disketten-/USB-Laufwerk** und eine im Abschnitt **CD-/DVD-Laufwerk** auswählen.

Wenn Sie eine Verbindung zu einem Disketten-Image oder einem ISO-Image herstellen möchten, geben Sie (auf Ihrem lokalen Computer) den Pfad zum Image ein, oder klicken Sie auf die Schaltfläche **Durchsuchen**, um zum Image zu browsen.

8. Klicken Sie neben jedem ausgewählten Datenträgertyp auf die Schaltfläche **Verbinden**.

Die Verbindung zum Datenträger ist hergestellt, und das Statusfenster ist aktualisiert.

9. Klicken Sie auf die Schaltfläche **Schließen**.

Virtuellen Datenträger unterbrechen

1. Klicken Sie auf **Datenträger → Assistent des virtuellen Datenträgers...**

2. Klicken Sie neben dem Datenträger, dessen Verbindung unterbrochen werden soll, auf **Unterbrechen**.

Die Verbindung zum Datenträger ist unterbrochen, und das Statusfenster ist aktualisiert.

3. Klicken Sie auf **Schließen**.

Vom virtuellen Datenträger starten

Das System-BIOS ermöglicht Ihnen, von virtuellen optischen Laufwerken oder virtuellen Diskettenlaufwerken aus zu starten. Während des POST öffnen Sie das BIOS-Setup-Fenster und überprüfen Sie, dass die virtuellen Laufwerke aktiviert und in der richtigen Reihenfolge aufgeführt werden.

Um die BIOS-Einstellung zu ändern, führen Sie die folgenden Schritte aus:

1. Starten Sie den verwalteten Server.
2. Drücken Sie <F2>, um das BIOS Setup-Fenster einzugeben.
3. Rollen Sie zur Startsequenz und drücken Sie auf <Eingabe>.

Im Popup-Fenster werden die virtuellen optischen Laufwerke und virtuellen Diskettenlaufwerke mit den Standardstartgeräten aufgeführt.

4. Stellen Sie sicher, dass das virtuelle Laufwerk aktiviert ist und als das erste Gerät mit startfähigem Datenträger aufgeführt wird. Falls erforderlich, folgen Sie den Bildschirmanleitungen zur Modifikation der Startreihenfolge.
5. Speichern Sie die Änderungen und beenden Sie.

Der verwaltete Server startet neu.

Basierend auf der Startreihenfolge versucht der verwaltete Server von einem startfähigen Gerät aus zu starten. Wenn das virtuelle Gerät angeschlossen ist und startfähige Datenträger vorhanden sind, startet das System zum virtuellen Gerät. Ansonsten ignoriert das System das Gerät - ähnlich einem physischen Gerät ohne startfähige Datenträger.

Betriebssysteme mit Hilfe von virtuellen Datenträgern verwenden

In diesem Abschnitt wird eine manuelle, interaktive Methode zum Installieren des Betriebssystems auf der Verwaltungsstation beschrieben, die mehrere Stunden in Anspruch nehmen kann. Ein geskriptetes Betriebssystem-Installationsverfahren unter Verwendung des **virtuellen Datenträgers** dauert möglicherweise weniger als 15 Minuten. Weitere Informationen finden Sie unter [Das Betriebssystem bereitstellen](#).

1. Überprüfen Sie folgendes:
 - 1 Die Betriebssystem-Installations-CD ist in das Verwaltungsstation-CD-Laufwerk eingelegt.
 - 1 Das lokale CD-Laufwerk ist ausgewählt.
 - 1 Sie sind mit den virtuellen Laufwerken verbunden.
2. Befolgen Sie die Schritte zum Starten vom virtuellen Datenträger aus im Abschnitt [Vom virtuellen Datenträger starten](#), um sicherzustellen, dass das BIOS so eingestellt ist, dass es auf dem CD-Laufwerk startet, von dem aus die Installation vorgenommen wird.
3. Folgen Sie den Bildschirmanleitungen, um die Installation abzuschließen.

Verwendung des virtuellen Datenträgers, wenn das Betriebssystem des Servers ausgeführt wird

Windows-basierte Systeme

Auf Windows-Systemen werden die Laufwerke der virtuellen Datenträger automatisch geladen, wenn sie angeschlossen und mit einem Laufwerkbuchstaben konfiguriert sind.

Verwendung der virtuellen Laufwerke von Windows ist der Verwendung Ihrer physischen Laufwerke ähnlich. Wenn Sie über den Assistenten des virtuellen Datenträgers eine Verbindung zum Datenträger herstellen, ist der Datenträger am System verfügbar, wenn Sie auf das Laufwerk klicken und dessen Inhalt durchsuchen.

Linux-basierte Systeme

Abhängig von der Konfiguration der Software auf Ihrem System dürfen die virtuellen Datenträgerlaufwerke nicht automatisch geladen werden. Wenn Ihre Laufwerke nicht automatisch geladen werden, laden Sie sie unter Verwendung des Linux-Befehls **Laden** manuell.

Häufig gestellte Fragen

In [Tabelle 8-4](#) werden häufig gestellte Fragen und Antworten aufgeführt.

Tabelle 8-4. Virtuellen Datenträger verwenden: Häufig gestellte Fragen

Frage	Antwort
Manchmal bemerke ich, dass die Clientenverbindung meines virtuellen Datenträgers nachlässt. Warum?	Wenn bei einem Netzwerk eine Zeitüberschreitung eintritt, trennt die iDRAC-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Wenn die Konfigurationseinstellungen des virtuellen Datenträgers in der iDRAC-Webschnittstelle oder

	<p>durch Befehle des lokalen RACADM geändert werden, wird die Verbindung aller verbundener Datenträger bei Übernahme der Konfigurationsänderung unterbrochen.</p> <p>Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie den Assistenten des virtuellen Datenträgers.</p>
Welche Betriebssysteme unterstützen den iDRAC?	Eine Liste unterstützter Betriebssysteme befindet sich unter Unterstützte Betriebssysteme .
Welche Webbrowser unterstützen den iDRAC?	Unterstützte Internetbrowser enthält eine Liste unterstützter Webbrowser.
Warum verliere ich manchmal meine Clientverbindung?	<ul style="list-style-type: none"> 1 Sie können Ihre Clientverbindung verlieren, wenn das Netzwerk langsam ist oder wenn Sie die CD im Clientsystem-CD-Laufwerk ändern. Beispiel: Wenn Sie die CD im Clientsystem-CD-Laufwerk wechseln, hat die neue CD u. U. eine Autostart-Funktion. Wenn das der Fall ist, kann die Firmware eine Zeitüberschreitung haben und die Verbindung kann verloren gehen, wenn das Clientsystem zu viel Zeit beansprucht, bevor es bereit ist, die CD zu lesen. Wenn eine Verbindung verloren geht, vom GUI wieder anschließen und den vorherigen Vorgang fortfahren. 1 Wenn bei einem Netzwerk eine Zeitüberschreitung eintritt, trennt die iDRAC-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Laufwerk. Es ist auch möglich, dass jemand die Konfigurationseinstellungen des virtuellen Datenträgers in der Webschnittstelle oder durch Eingabe von RADACM-Befehlen verändert hat. Um die Verbindung zum virtuellen Laufwerk wieder herzustellen, verwenden Sie die Funktion des virtuellen Datenträgers.
Eine Installation des Windows-Betriebssystems scheint zu lange zu dauern. Warum?	Wenn Sie das Windows-Betriebssystem über die CD <i>Dell PowerEdge Installation and Server Management</i> und über eine langsame Netzwerkverbindung installieren, ist für das Installationsverfahren auf Grund der Netzwerklatenzzeit eventuell ein höherer Zeitaufwand erforderlich, um auf die iDRAC-Webschnittstelle zuzugreifen. Im Installationsfenster wird der Installationsfortschritt nicht angezeigt, doch das Installationsverfahren wird durchgeführt.
Ich zeige den Inhalt eines Diskettenlaufwerks oder eines USB-Speicherschlüssels an. Wenn ich versuche, über dasselbe Laufwerk eine Verbindung zum virtuellen Datenträger herzustellen, erhalte ich eine Verbindungs-Fehlermeldung and werde gebeten, den Vorgang zu wiederholen. Warum?	Ein Simultanzugriff auf virtuelle Diskettenlaufwerke ist nicht zulässig. Vor dem Versuch, das Laufwerk zu virtualisieren, ist die Anwendung zum Anzeigen des Laufwerkinhalts zu schließen.
Wie konfiguriere ich mein virtuelles Gerät als startfähiges Gerät?	Greifen Sie auf dem verwalteten Server auf das BIOS-Setup zu, und wechseln Sie zum Startmenü. Machen Sie die virtuelle CD, die virtuelle Floppy oder den Virtual Flash ausfindig, und ändern Sie die Gerätestartreihenfolge wie erforderlich. Um z. B. von einem CD-Laufwerk zu starten, konfigurieren Sie das CD-Laufwerk als erstes Laufwerk in der Startreihenfolge.
Von welchen Arten von Datenträgern kann ich starten?	<p>Mit dem iDRAC können Sie von den folgenden startfähigen Datenträgern aus starten:</p> <ul style="list-style-type: none"> 1 CDROM/DVD-Datenträger 1 ISO 9660-Image 1 1.44-Diskette oder Floppy-Image 1 USB-Schlüssel, der vom Betriebssystem als Wechselplatte erkannt wird 1 USB-Schlüssel-Image
Wie kann ich meine USB-Taste startfähig machen?	<p>Suchen Sie unter support.dell.com nach dem Dell-Startdienstprogramm, einem Windows-Programm, mit dem Sie den Dell-USB-Schlüssel startfähig machen können.</p> <p>Sie können auch über eine Windows 98-Startdiskette starten und Systemdateien von der Startdiskette auf Ihren USB-Schlüssel kopieren. Geben Sie z. B. an der DOS-Eingabeaufforderung den folgenden Befehl ein:</p> <pre>sys a: x: /s</pre> <p>wobei x: der USB-Schlüssel ist, der startfähig gemacht werden soll.</p> <p>Sie können auch das Dell Startdienstprogramm verwenden, um einen startfähigen USB-Schlüssel zu erstellen. Dieses Dienstprogramm ist nur mit USB-Schlüsseln kompatibel, die von Dell mit einer Schutzmarke versehen wurden. Um das Dienstprogramm herunterzuladen, öffnen Sie einen Webbrowser, wechseln Sie zu Dells Support-Website unter support.dell.com, und suchen Sie nach der Datei R122672.exe.</p>
Ich kann mein virtuelles Floppy-Gerät auf einem System, das das Betriebssystem Red Hat® Enterprise Linux® oder SUSE® Linux ausführt, nicht finden. Mein virtueller Datenträger ist angeschlossen, und ich bin mit meiner Remote-Floppy verbunden. Was soll ich tun?	<p>Bei einigen Linux-Versionen erfolgt die automatische Ladung des virtuellen Diskettenlaufwerks und des virtuellen CD-Laufwerks auf unterschiedliche Weise. Um das virtuelle Diskettenlaufwerk zu laden, machen Sie den Geräteknoden ausfindig, den Linux dem virtuellen Diskettenlaufwerk zuweist. Führen Sie folgenden Schritte aus, um das virtuelle Diskettenlaufwerk korrekt zu finden und zu laden:</p> <ol style="list-style-type: none"> 1. Öffnen Sie eine Linux-Eingabeaufforderung, und führen Sie den folgenden Befehl aus: <pre>grep "Virtual Floppy" /var/log/messages</pre> 2. Finden Sie den letzten Eintrag dieser Meldung und notieren Sie die Zeit. 3. An der Linux-Eingabeaufforderung führen Sie den folgenden Befehl aus: <pre>grep "hh:mm:ss" /var/log/messages</pre> <p>wobei:</p> <pre>hh:mm:ss</pre> <p>hh:mm:ss ist der Zeitstempel der Meldung, die in Schritt 1 von grep zurückgegeben wurde.</p> 4. Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls, und finden Sie den Gerätenamen, der der virtuellen Dell-Diskette gegeben wurde. 5. Stellen Sie sicher, dass das virtuelle Diskettenlaufwerk angeschlossen ist und eine Verbindung zu ihm besteht. 6. Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus: <pre>mount /dev/sdx /mnt/floppy</pre> <p>wobei:</p> <pre>/dev/sdx</pre> <p>der in Schritt 4 gefundene Gerätenamen ist</p>

	/mnt/floppy ist der Bereitstellungspunkt.
Welche Dateisystemtypen werden auf meinem virtuellen Diskettenlaufwerk unterstützt?	Ihr virtuelles Diskettenlaufwerk unterstützt FAT16- oder FAT32-Dateisysteme.
Als ich im Remote-Zugriff anhand der iDRAC-Webschnittstelle eine Firmware-Aktualisierung ausgeführt habe, wurden meine virtuellen Laufwerke vom Server entfernt. Warum?	Firmware-Aktualisierungen führen zu einem Reset des iDRAC, einem Abbruch der Remote-Verbindung sowie zum Entladen der virtuellen Laufwerke. Die Laufwerke erscheinen wieder, wenn der iDRAC-Reset abgeschlossen ist.

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

Befehlszeilenoberfläche des lokalen RACADM verwenden

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [RACADM-Befehl verwenden](#)
- [RACADM-Unterbefehle](#)
- [RACADM-Dienstprogramm zum Konfigurieren des iDRAC verwenden](#)
- [iDRAC-Konfigurationsdatei verwenden](#)
- [Mehrfache iDRACs konfigurieren](#)

Die Befehlszeilenoberfläche (CLI) des lokalen RACADM bietet Zugriff auf die iDRAC-Verwaltungsfunktionen vom verwalteten Server aus. RACADM bietet Zugriff auf dieselben Funktionen wie die iDRAC-Webschnittstelle. RACADM kann jedoch in Skripten verwendet werden, um die Konfiguration mehrerer Server und iDRACs zu erleichtern, bei denen die Webschnittstelle nützlicher für die interaktive Verwaltung ist.

Befehle des lokalen RACADM verwenden zum Zugriff auf den iDRAC vom verwalteten Server aus keine Netzwerkverbindungen. Dies bedeutet, dass Sie Befehle des lokalen RACADM verwenden können, um den anfänglichen iDRAC-Netzwerkbetrieb zu konfigurieren.

Weitere Informationen über das Konfigurieren mehrerer iDRACs erhalten Sie unter [Mehrfache iDRACs konfigurieren](#).

Dieser Abschnitt enthält die folgenden Informationen:

- 1 RACADM von einer Eingabeaufforderung aus verwenden
- 1 iDRAC mit dem Befehl `racadm` konfigurieren
- 1 RACADM-Konfigurationsdatei zur Konfiguration mehrerer iDRACs verwenden

RACADM-Befehl verwenden

RACADM-Befehle werden lokal (auf dem verwalteten Server) über eine Befehlseingabeaufforderung oder eine Shell-Eingabeaufforderung ausgeführt.

Melden Sie sich am verwalteten Server an, starten Sie eine Befehls-Shell, und geben Sie in folgendem Format Befehle des lokalen RACADM ein:

```
racadm <Unterbefehl> -g <Gruppe> -o <Objekt> <Wert>
```

Ohne Optionen zeigt der Befehl RACADM Informationen zum allgemeinen Gebrauch an. Geben Sie zur Anzeige des RACADM-Unterbefehls Folgendes ein:

```
racadm-Hilfe
```

Die Liste der Unterbefehle enthält alle Befehle, die durch den iDRAC unterstützt werden.

Um für einen Unterbefehl Hilfe zu erhalten, geben Sie Folgendes ein:

```
racadm help-<Unterbefehl>
```

Der Befehl zeigt die Syntax- und Befehlszeilenoptionen für den Unterbefehl an.

RACADM-Unterbefehle

[Tabelle 9-1](#) enthält eine Beschreibung der einzelnen RACADM-Unterbefehle, die Sie in RACADM ausführen können. Eine ausführliche Auflistung der RACADM-Unterbefehle einschließlich der Syntax und gültiger Einträge befinden sich in der [Übersicht der RACADM-Unterbefehle](#).

Tabelle 9-1. RACADM-Unterbefehle

Befehl	Beschreibung
<code>clr raclog</code>	Löscht das iDRAC-Protokoll. Nach dem Löschvorgang wird ein einzelner Eintrag vorgenommen, um den Benutzer anzuzeigen sowie die Uhrzeit, zu der das Protokoll gelöscht wurde.
<code>clr sel</code>	Löscht die Einträge des Systemereignisprotokolls des verwalteten Servers.
<code>config</code>	Konfiguriert den iDRAC.
<code>get config</code>	Zeigt die aktuellen iDRAC-Konfigurationseigenschaften an.
<code>get nic cfg</code>	Zeigt die derzeitige IP-Konfiguration für den Controller an.
<code>get rac log</code>	Zeigt das iDRAC-Protokoll an.
<code>get race time</code>	Zeigt die iDRAC-Zeit an.
<code>get ssn info</code>	Zeigt Informationen über aktive Sitzungen an.
<code>get svctag</code>	Zeigt Service-Tag-Nummern an.
<code>get sys info</code>	Zeigt Informationen zu iDRAC und verwaltetem Server, einschließlich IP-Konfiguration, Hardwaremodell, Firmware-Versionen und Betriebssystem an.
<code>get trace log</code>	Zeigt das Ablaufverfolgungsprotokoll des iDRAC an. Bei Verwendung mit <code>-i</code> zeigt der Befehl die Anzahl von Einträgen im iDRAC-

	Ablaufverfolgungsprotokoll an.
Hilfe	Führt iDRAC-Unterbefehle auf.
Hilfe - <i><Unterbefehl></i>	Listet die Verwendungsaussage für den angegebenen Unterbefehl auf.
racreset	Setzt den iDRAC zurück.
racresetcfg	Setzt den iDRAC auf die Standardkonfiguration zurück.
serveraction	Führt Stromverwaltungsvorgänge auf dem verwalteten Server aus.
setniccfg	Stellt die IP-Konfiguration für den Controller ein.
sslcertdownload	Lädt ein CA-Zertifikat herunter.
sslcertupload	Lädt ein Zertifizierungsstellenzertifikat oder Serverzertifikat zum iDRAC hoch.
sslcertview	Zeigt ein Zertifizierungsstellenzertifikat oder Serverzertifikat im iDRAC an.
sslcsrgen	Erstellt und lädt die SSL-CSR herunter.
testemail	Zwingt den iDRAC, eine E-Mail über den iDRAC zu senden.
testtrap	Zwingt den iDRAC, eine SNMP-Warnung über die iDRAC-NIC zu senden.
vmdisconnect	Zwingt eine Verbindung des virtuellen Datenträgers zu schließen.

RACADM-Dienstprogramm zum Konfigurieren des iDRAC verwenden

In diesem Abschnitt wird beschrieben, wie RACADM zum Ausführen verschiedener iDRAC-Konfigurations-Tasks verwendet wird.

Aktuelle iDRAC-Einstellungen anzeigen

Der RACADM-Unterbefehl **getconfig** ruft aktuelle Konfigurationseinstellungen vom iDRAC ab. Die Konfigurationswerte werden in *Gruppen* organisiert, die ein oder mehrere *Objekt(e)* enthalten, wobei die Objekte *Werte* haben.

Eine vollständige Beschreibung der Gruppen und Objekte finden Sie unter [Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank](#).

Geben Sie zum Anzeigen einer Liste aller iDRAC-Gruppen den folgenden Befehl ein:

```
racadm getconfig -h
```


Geben Sie zum Anzeigen der Objekte und Werte für eine bestimmte Gruppe den folgenden Befehl ein:


```
racadm getconfig -g <Gruppe>
```


Beispiel: Um eine Liste aller **cfgLanNetworking**-Gruppenobjekteinstellungen anzuzeigen, geben Sie den folgenden Befehl ein:

```
racadm getconfig -g cfgLanNetworking
```

iDRAC-Benutzer mit RACADM verwalten

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

 **ANMERKUNG:** Wenn Sie einen neuen iDRAC konfigurieren oder den Befehl **racadm racresetcfg** ausgeführt haben, ist der einzige aktuelle Benutzer **root** mit dem Kennwort **calvin**.

 **ANMERKUNG:** Benutzer können im Lauf der Zeit aktiviert und deaktiviert werden. Infolgedessen kann ein Benutzer auf jedem iDRAC eine unterschiedliche Indexnummer besitzen.

Sie können in der iDRAC-Eigenschaftendatenbank bis zu 15 Benutzer konfigurieren. (Ein sechzehnter Benutzer ist für den IPMI LAN-Benutzer reserviert.) Überprüfen Sie, bevor Sie einen iDRAC-Benutzer manuell aktivieren, ob aktuelle Benutzer vorhanden sind.


Um nachzuprüfen, ob ein Benutzer besteht, geben Sie den folgenden Befehl an der Eingabeaufforderung ein:

```
racadm getconfig -u <Benutzername>
```

ODER

Geben Sie den folgenden Befehl einmal für jeden Index von 1 bis 16 ein:

```
racadm getconfig -g cfgUserAdmin -i <Index>
```

 **ANMERKUNG:** Sie können auch **racadm getconfig -f <Dateiname>** eingeben und die erstellte Datei *<Dateiname>* anzeigen, die alle Benutzer sowie alle anderen iDRAC-Konfigurationsparameter einschließt.

Mehrere Parameter und Objekt-ID werden mit ihren aktuellen Werten angezeigt. Zwei Objekte von Interesse sind:

```
# cfgUserAdminIndex=nn
```

```
cfgUserAdminUserName=
```

Wenn das Objekt `cfgUserAdminUserName` keinen Wert besitzt, steht diese Indexnummer, die durch das Objekt `cfgUserAdminIndex` angezeigt wird, zur Verfügung. Wenn hinter dem = ein Name erscheint, ist dieser Index diesem Benutzernamen zugewiesen.

iDRAC-Benutzer hinzufügen

Führen Sie zum Hinzufügen eines neuen Benutzers zum iDRAC folgende Schritte aus:

1. Geben Sie den Benutzernamen ein.
2. Geben Sie das Kennwort ein.
3. Stellen Sie die Benutzerberechtigung zum Anmelden am iDRAC ein.
4. Aktivieren Sie den Benutzer.

Beispiel

Das folgende Beispiel beschreibt, wie man dem iDRAC einen neuen Benutzer namens "John" mit dem Kennwort "123456" und Anmeldeberechtigung hinzufügt.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
racadm config -g cfgUserAdmin -o cfgUserPrivilege -i 2 0x00000001
racadm config -g cfgUserAdmin -o cfgUserAdminEnable -i 2 1
```

Verwenden Sie zum Verifizieren des neuen Benutzers einen der folgenden Befehle:

```
racadm getconfig -u john
racadm getconfig -g cfgUserAdmin -i 2
```

iDRAC-Benutzer mit Berechtigungen aktivieren

Um einem Benutzer bestimmte administrative (rollenbasierte) Berechtigungen zu erteilen, stellen Sie die Eigenschaft `cfgUserAdminPrivilege` auf eine Bitmaske ein, die aus den in [Tabelle 9-2](#) gezeigten Werte konstruiert ist:

Tabelle 9-2. Bit-Masken für Benutzerberechtigungen

Benutzerberechtigung	Berechtigungs-Bitmaske
Bei iDRAC anmelden	0x00000001
iDRAC konfigurieren	0x00000002
Benutzer konfigurieren	0x00000004
Protokolle löschen	0x00000008
Serversteuerungsbefehle ausführen	0x00000010
Zugriff auf Konsolenumleitung	0x00000020
Zugriff auf Virtueller Datenträger	0x00000040
Testwarnungen	0x00000080
Debug-Befehle ausführen	0x0000100

Um dem Benutzer z. B. die Berechtigungen **iDRAC konfigurieren**, **Benutzer konfigurieren**, **Protokolle löschen** und **Zugriff auf Konsolenumleitung** zu erteilen, fügen Sie die Werte `0x00000002`, `0x00000004`, `0x00000008` und `0x00000010` hinzu, um die Bitmap `0x0000002E` zu konstruieren. Geben Sie dann den folgenden Befehl zum Einstellen der Berechtigung ein:

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x0000002E
```

iDRAC-Benutzer entfernen

Wenn sie RACADM verwenden, müssen Benutzer manuell und einzeln deaktiviert werden. Benutzer können nicht mittels einer Konfigurationsdatei gelöscht werden.

Im folgenden Beispiel wird die Befehls-Syntax gezeigt, die zum Löschen eines Benutzers des RAC verwendet werden kann:


```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <Index">
```

Eine Null-Kette doppelter Anführungszeichen (""") weist den iDRAC an, die Benutzerkonfiguration am angegebenen Index zu entfernen und die Benutzerkonfiguration auf die ursprünglichen Werkseinstellungen zurückzusetzen.

Testen von E-Mail-Warnmeldungen

Mit der iDRAC-E-Mail-Warnungsfunktion können Benutzer E-Mail-Warnungen erhalten, wenn auf dem verwalteten Server ein kritisches Ereignis auftritt. Das folgende Beispiel zeigt, wie man die E-Mail-Warnungsfunktion testet, um sicherzustellen, dass der iDRAC ordnungsgemäß E-Mail-Warnungen über das Netzwerk senden kann.

```
racadm testemail -i 2
```


 **ANMERKUNG:** Stellen Sie sicher, dass die SMTP- und E-Mail-Warnungseinstellungen konfiguriert sind, bevor Sie die E-Mail-Warnungsfunktion testen. Weitere Informationen finden Sie unter [E-Mail-Warnungen konfigurieren](#).

iDRAC-SNMP-Trap-Warnungsfunktion testen

Die iDRAC-SNMP-Trap-Warnungsfunktion ermöglicht den SNMP-Trap-Abhörkonfigurationen, Traps für Systemereignisse zu empfangen, die auf dem verwalteten Server auftreten.

Das folgende Beispiel zeigt, wie ein Benutzer die SNMP-Trap-Warnungsfunktion testen kann.

```
racadm testtrap -i 2
```

 **ANMERKUNG:** Bevor Sie die iDRAC-SNMP-Trap-Warnungsfunktion testen, stellen Sie sicher, dass die SNMP- und Trap-Einstellungen ordnungsgemäß konfiguriert sind. Diese Einstellungen können anhand der Beschreibungen zu den Unterbefehlen **testtrap** und **testemail** konfiguriert werden.

iDRAC-Netzwerkeigenschaften konfigurieren

Geben Sie folgendes ein, um eine Liste verfügbarer Netzwerkeigenschaften zu erhalten:

```
racadm getconfig -g cfgLanNetworking
```


Wenn DHCP zum Erhalt einer IP-Adresse verwendet werden soll, kann der folgende Befehl zum Schreiben des Objekts **cfgNicUseDhcp** und zum Aktivieren dieser Funktion verwendet werden.

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

Die Befehle enthalten dieselbe Konfigurationsfunktionalität wie das iDRAC-Konfigurationsdienstprogramm, wenn Sie dazu aufgefordert werden, <Strg><E> zu drücken. Weitere Informationen zum Konfigurieren von Netzwerkeigenschaften mit dem iDRAC-Konfigurationshilfsprogramm finden Sie unter [LAN](#).

Im folgenden Beispiel wird gezeigt, wie der Befehl zur Konfiguration gewünschter LAN-Netzwerkeigenschaften verwendet werden kann.


```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0
racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5
racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1
racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002
racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

 **ANMERKUNG:** Wenn **cfgNicEnable** auf **0** gesetzt ist, wird das iDRAC-LAN selbst dann deaktiviert, wenn DHCP aktiviert ist.

IPMI konfigurieren

1. Konfigurieren Sie IPMI über LAN, indem Sie den folgenden Befehl eingeben:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

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

- a. Aktualisieren Sie die IPMI-Kanalberechtigungen, indem Sie den folgenden Befehl eingeben:

```
racadm config -g cfgIpmlan -o cfgIpmlanPrivilegeLimit <Stufe>
```


wobei <Stufe> eine der folgenden ist:

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

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

```
racadm config -g cfgIpmlan -o cfgIpmlanPrivilegeLimit 2
```

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


 **ANMERKUNG:** Der iDRAC-IPMI unterstützt das RMCP+-Protokoll. Die IPMI 2.0-Spezifikationen enthalten weitere Informationen.

```
racadm config -g cfgIpmlan -o cfgIpmlanEncryptionKey <Schlüssel>
```

wobei <Schlüssel> ein aus 20 Zeichen bestehender Verschlüsselungsschlüssel in einem gültigen Hexadezimal-Format ist.

2. Konfigurieren Sie IPMI-SOL (Seriell über LAN), indem Sie den folgenden Befehl verwenden:

```
racadm config -g cfgIpmsol -o cfgIpmsolEnable 1
```

 **NOTE:** Die IPMI SOL-Mindestberechtigungsebene bestimmt die Mindestberechtigung, die zur Aktivierung von IPMI SOL erforderlich ist. Weitere Informationen enthält die IPMI 2.0 Spezifikation.

- a. Aktualisieren Sie die IPMI-SOL-Mindestberechtigungsebene unter Verwendung des folgenden Befehls:


```
racadm config -g cfgIpmsol -o cfgIpmsolMinPrivilege <Stufe>
```

wobei <Stufe> eine der folgenden ist:

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

Beispiel: Um die IPMI-Berechtigungen für 2 zu konfigurieren (Benutzer), geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmsol -o cfgIpmsolMinPrivilege 2
```

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

- b. Aktualisieren Sie die IPMI-SOL-Baudrate unter Verwendung des folgenden Befehls:


```
racadm config -g cfgIpmsol -o cfgIpmsolBaudRate <Baud-Rate>
```

wobei <Baud-Rate> 19200, 57600 oder 115200 Bit/s ist.

Beispiel:

```
racadm config -g cfgIpmsol -o cfgIpmsolBaudRate 57600
```

- c. Aktivieren Sie SOL, indem Sie an der Eingabeaufforderung den folgenden Befehl eingeben.

 **ANMERKUNG:** SOL kann für jeden einzelnen Benutzer aktiviert oder deaktiviert werden.

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <ID> 2
```

wobei <ID> die eindeutige ID des Benutzers ist.

PEF konfigurieren

Sie können die Maßnahme konfigurieren, die iDRAC bei den einzelnen Plattformwarnungen ergreifen soll. [Tabelle 9-3](#) führt die möglichen Maßnahmen sowie den Wert auf, anhand dessen Sie in RACADM identifiziert werden können.

Tabelle 9-3. Plattformereignismaßnahme

--	--

Maßnahme	Wert
Keine Maßnahme	0
Ausschalten	1
Neustarten	2
Aus- und einschalten	3

1. Konfigurieren Sie PEF-Maßnahmen unter Verwendung des folgenden Befehls:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i <Index> <Maßnahme-Wert>
```

wobei <Index> der PEF-Index ist (siehe [Tabelle 5-6](#)) und <Maßnahme-Wert> ein Wert aus [Tabelle 9-3](#).

Um beispielsweise PEF zum Neustarten des Systems und zum Senden einer IPMI-Warnung zu aktivieren, wenn auf dem Prozessor ein kritisches Ereignis festgestellt wird, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2
```

PET konfigurieren

1. Aktivieren Sie globale Warnungen unter Verwendung des folgenden Befehls:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

2. Aktivieren Sie PET unter Verwendung des folgenden Befehls:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <Index> <0|1>
```

wobei <Index> der PET-Zielindex ist und 0 oder 1 PET deaktivieren bzw. PET aktivieren.

Beispiel: um PET mit dem Index 4 zu aktivieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
```

3. Konfigurieren Sie Ihre PET-Regel unter Verwendung des folgenden Befehls:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <Index> <IP-Adresse>
```

wobei <Index> der PET-Zielindex und <IP-Adresse> die Ziel-IP-Adresse des Systems ist, das die Plattformereigniswarnungen empfängt.

4. Community-Namenzeichenkette konfigurieren.

An der Eingabeaufforderung geben Sie Folgendes ein:

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <Name>
```

wobei <Name> der PET-Community-Name ist.

E-Mail-Warnungen konfigurieren

1. Aktivieren Sie globale Warnungen, indem Sie den folgenden Befehl eingeben:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

2. Aktivieren Sie E-Mail-Warnungen, indem Sie die folgenden Befehle eingeben:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <Index> <0|1>
```

wobei <Index> der E-Mail-Zielindex ist und 0 die E-Mail-Warnung deaktiviert oder 1 den Wert aktiviert. Der E-Mail-Ziel-Index kann ein Wert von 1 bis 4 sein.

Beispiel: Um E-Mail mit dem Index 4 zu aktivieren, tippen Sie den folgenden Befehl:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
```

3. Konfigurieren Sie Ihre E-Mail-Einstellungen, indem Sie den folgenden Befehl eingeben:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <E-Mail-Adresse>
```

wobei 1 der E-Mail-Zielindex und <E-Mail-Adresse> die Ziel-E-Mail-Adresse ist, die die Plattformereigniswarnungen empfängt.

4. Geben Sie zum Konfigurieren einer benutzerdefinierten Meldung den folgenden Befehl ein:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <Index> <Benutzerdefinierte-Meldung>
```

wobei <Index> der E-Mail-Zielindex und <benutzerdefinierte Meldung> die benutzerdefinierte Meldung ist.

5. Testen Sie die konfigurierte E-Mail-Warnung, falls gewünscht, indem Sie den folgenden Befehl eingeben:

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

wobei <Index> der zu testende E-Mail-Zielindex ist.

IP-Filterung konfigurieren (IpBereich)

Die IP-Adressenfilterung (oder *IP-Bereichsüberprüfung*) gestattet den iDRAC-Zugriff nur von Clients oder Verwaltungsstationen, deren IP-Adressen innerhalb eines vom Benutzer angegebenen Bereiches liegen. Alle anderen Anmeldeaufforderungen werden abgewiesen.

Die IP-Entstörung vergleicht die IP-Adresse einer eingehenden Anmeldung mit dem IP-Adressenbereich, der in den folgenden **cfgRacTuning**-Eigenschaften angegeben wird:

- 1 cfgRacTuneIpRangeAddr
- 1 cfgRacTuneIpRangeMask

Die Eigenschaft **cfgRacTuneIpRangeMask** wird sowohl auf die eingehende IP-Adresse als auch auf die **cfgRacTuneIpRangeAddr**-Eigenschaften angewendet. Sind die Ergebnisse identisch, wird für die eingehende Anmeldeaufforderung der Zugriff auf den iDRAC zugelassen. Anmeldungen von IP-Adressen außerhalb dieses Bereiches erhalten eine Fehlermeldung.

Die Anmeldung wird fortgeführt, wenn der folgende Ausdruck Null entspricht:

```
cfgRacTuneIpRangeMask & (<eingehende-IP-Adresse> ^ cfgRacTuneIpRangeAddr)
```

wobei & das binäre UND der Mengen und ^ das binäre ausschließliche ODER ist.

Eine vollständige Liste von **cfgRacTuning**-Eigenschaften finden Sie unter [cfgRacTuning](#).

Tabelle 9-4. IP-Adressenfiltrierung (IpRange) -Eigenschaften


Eigenschaft	Beschreibung
cfgRacTuneIpRangeEnable	Aktiviert die IP-Bereichsüberprüfungsfunktion.
cfgRacTuneIpRangeAddr	Bestimmt das akzeptable IP-Adressen-Bitmuster, abhängig von den Einsen (1) in der Subnetzmaske. Diese Eigenschaft wird bitweise mit cfgRacTuneIpRangeMask "geundet", um den oberen Teil der zugelassenen IP-Adresse zu bestimmen. Die Anmeldung wird für alle IP-Adressen, die in den oberen Bits dieses Bit-Muster aufweisen, zugelassen. Anmeldungen von IP-Adressen, die außerhalb dieses Bereiches stattfinden, schlagen fehl. Für die Standardwerte der einzelnen Eigenschaften ist für die Anmeldung ein Adressenbereich von 192.168.1.0 bis 192.168.1.255 zulässig.
cfgRacTuneIpRangeMask	Definiert die wichtigen Bitpositionen in der IP-Adresse. Die Maske sollte in der Form einer Netzmaske sein, wobei die bedeutenderen Bits alle Einsen (1) sind, mit einem einzelnen Übergang zu Nullen (0) in den niederwertigeren Bits.

IP-Filterung konfigurieren

Führen Sie zur Konfiguration der IP-Filterung in der Webschnittstelle folgende Schritte aus:

1. Klicken Sie auf **System** → **Remote-Zugriff** → **iDRAC** → **Netzwerk/Sicherheit**.
2. Klicken Sie auf der Seite **Netzwerkkonfiguration** auf **Erweiterte Einstellungen**.
3. Markieren Sie das Kontrollkästchen **IP-Bereich aktiviert**, und geben Sie die **IP-Bereichsadresse** und die **Subnetzmaske IP-Bereich** ein.
4. Klicken Sie auf **Anwenden**.

Im Folgenden sind Beispiele zur Verwendung des lokalen RACADM zum Einstellen der IP-Filterung aufgeführt.

 **ANMERKUNG:** Weitere Informationen zu RACADM und RACADM-Befehlen befinden sich unter [Befehlszeilenoberfläche des lokalen RACADM verwenden](#).

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

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

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



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

2. Zur Beschränkung der Anmeldung auf einen kleinen Satz von vier angrenzenden IP-Adressen (zum Beispiel: 192.168.0.212 bis 192.168.0.215), wählen Sie alle außer den niederwertigsten zwei Bit in der Maske, wie unten gezeigt:

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

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

Das letzte Byte der Bereichsmaske ist auf 252 eingestellt, das Dezimaläquivalent von 11111100b.

IP-Filter - Richtlinien

Verwenden Sie die folgenden Richtlinien, wenn Sie den IP-Filter aktivieren:

- 1 Stellen Sie sicher, dass **cfgRacTuneIpRangeMask** in Form einer Netzmaske konfiguriert ist, bei der alle höchstwertigen Bits Einsen (1) sind (was das Subnetz in der Maske definiert), mit einem Übergang zu nur Nullen (0) in den niederwertigeren Bits.
- 1 Verwenden Sie die Basisadresse des gewünschten Bereiches als Wert von **cfgRacTuneIpRangeAddr**. Der binäre 32-Bit-Wert dieser Adresse sollte Nullen in allen niederwertigen Bits haben, wo Nullen in der Maske sind.


IP-Blockierung konfigurieren

Durch IP-Blockierung wird dynamisch festgestellt, wenn von einer bestimmten IP-Adresse aus übermäßige Anmeldefehlschläge auftreten und die Adresse blockiert bzw. daran gehindert wird, eine bestimmte Zeit lang eine Anmeldung am iDRAC durchzuführen.

Die Funktionen der IP-Blockierung schließen ein:

- 1 Die Anzahl zulässiger Anmeldefehlschläge (**cfgRacTuneIpBlkFailCount**)
- 1 Die Zeitspanne in Sekunden, während der diese Fehler auftreten müssen (**cfgRacTuneIpBlkFailWindow**)
- 1 Die Zeitdauer in Sekunden, während der die blockierte IP-Adresse daran gehindert wird, eine Sitzung herzustellen, nachdem die zulässige Anzahl von Fehlern überschritten wurde (**cfgRacTuneIpBlkPenaltyTime**)

Wenn sich Anmeldefehler von einer spezifischen IP-Adresse aus ansammeln, werden sie durch einen internen Schalter registriert. Wenn sich der Benutzer erfolgreich anmeldet, wird das Fehlerprotokoll gelöscht, und der interne Zähler wird zurückgesetzt.

 **ANMERKUNG:** Wenn Anmeldeversuche von der Client-IP-Adresse abgelehnt werden, können einige SSH-Clients die folgende Meldung anzeigen: ssh exchange identification: Verbindung vom Remote Host geschlossen.

Eine vollständige Liste der **cfgRacTune**-Eigenschaften finden Sie unter [Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank](#).

In den [Einschränkungseigenschaften zur Anmeldewiederholung](#) werden die benutzerdefinierten Parameter aufgeführt.

Tabelle 9-5. Anmeldungswiederholungs-Beschränkungseigenschaften

Eigenschaft	Definition
cfgRacTuneIpBlkEnable	Aktiviert die IP-Blockierungsfunktion. Wenn innerhalb eines bestimmten Zeitraums aufeinander folgende Fehler (cfgRacTuneIpBlkFailCount) von einer einzelnen IP-Adresse aus festgestellt werden (cfgRacTuneIpBlkFailWindow), werden alle weiteren Versuche, von dieser Adresse aus eine Sitzung herzustellen, während eines bestimmten Zeitraums zurückgewiesen (cfgRacTuneIpBlkPenaltyTime).
cfgRacTuneIpBlkFailCount	Legt die Anzahl von Anmeldefehlern einer IP-Adresse fest, bevor die Anmeldeversuche zurückgewiesen werden.
cfgRacTuneIpBlkFailWindow	Die Zeitspanne in Sekunden, während der die fehlgeschlagenen Versuche gezählt werden. Wenn die Fehler diese Grenze überschreiten, werden sie aus dem Zähler gelöscht.
cfgRacTuneIpBlkPenaltyTime	Definiert den Zeitraum in Sekunden, während dem Anmeldeversuche von einer IP-Adresse aus auf Grund übermäßiger Fehler zurückgewiesen werden.

IP-Blockieren aktivieren

Das folgende Beispiel hindert eine Client-IP-Adresse fünf Minuten lang daran, eine Sitzung zu beginnen, wenn dieser Client innerhalb einer Minute fünf fehlerhafte Anmeldeversuche durchführt.

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

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
```



```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

Das folgende Beispiel verhindert mehr als drei fehlerhafte Versuche innerhalb einer Minute, und verhindert eine Stunde lang zusätzliche Anmeldeversuche.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 360
```

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

Die Telnet-/SSH-Konsole kann lokal (auf dem verwalteten Server) unter Verwendung von RACADM-Befehlen konfiguriert werden.

-  **ANMERKUNG:** Um die Befehle in diesem Abschnitt ausführen zu können, müssen Sie über die Berechtigung **iDRAC konfigurieren** verfügen.
-  **ANMERKUNG:** Eine Neukonfiguration von Telnet- oder SSH-Einstellungen im iDRAC führt dazu, dass alle aktuellen Sitzungen ohne vorherige Warnung beendet werden.

Um Telnet und SSH vom lokalen RACADM zu aktivieren, melden Sie sich am verwalteten Server an, und geben Sie auf eine entsprechende Eingabeaufforderung hin die folgenden Befehle ein:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Ändern Sie zum Deaktivieren des Telnet- oder SSH-Diensts den Wert von 1 zu 0:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 0
racadm config -g cfgSerial -o cfgSerialSshEnable 0
```

Geben Sie den folgenden Befehl ein, um die Telnet-Schnittstellennummer auf dem iDRAC zu ändern.

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <neue Schnittstellennummer>
```

Geben Sie z. B. zum Ändern der Telnet-Schnittstelle von der Standardeinstellung 22 auf 8022 den folgenden Befehl ein:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

Eine vollständige Liste verfügbarer RACADM-CLI-Befehle steht unter [Befehlszeilenoberfläche des lokalen RACADM verwenden](#) zur Verfügung.

iDRAC-Konfigurationsdatei verwenden

Eine iDRAC-Konfigurationsdatei ist eine Textdatei, die eine Darstellung der Werte in der iDRAC-Datenbank enthält. Der RACADM-Unterbefehl **getconfig** kann zum Erstellen einer Konfigurationsdatei verwendet werden, die die aktuellen Werte des iDRAC enthält. Sie können dann die Datei bearbeiten und den RACADM-Unterbefehl **config -f** zum Zurückladen der Datei in den iDRAC verwenden, oder die Konfiguration auf andere iDRACs kopieren.

iDRAC-Konfigurationsdatei erstellen

Die Konfigurationsdatei ist eine (unformatierte) Klartextdatei. Es können alle gültigen Dateinamen verwendet werden; die gebräuchliche Dateierweiterung **.cfg** wird empfohlen.

Die Konfigurationsdatei kann:

- 1 Mit einem Textbearbeitungsprogramm erstellt werden
- 1 Über den RACADM-Unterbefehl **getconfig** vom iDRAC abgerufen werden
- 1 Über den RACADM-Unterbefehl **getconfig** vom iDRAC abgerufen und dann bearbeitet werden

Geben Sie zum Abrufen einer Konfigurationsdatei unter Verwendung des RACADM-Befehls **getconfig** den folgenden Befehl an einer Eingabeaufforderung auf dem verwalteten Server ein:

```
racadm getconfig -f myconfig.cfg
```

Anhand dieses Befehls wird die Datei **myconfig.cfg** im aktuellen Verzeichnis erstellt.

Syntax der Konfigurationsdatei

-  **HINWEIS:** Bearbeiten Sie die Konfigurationsdatei mit einem Klartext-Bearbeitungsprogramm wie z. B. **Notepad** auf Windows oder **vi** auf Linux. Das Dienstprogramm **racadm** parst nur ASCII-Text. Formatierung verwirrt den Parser, wodurch die iDRAC-Datenbank **beschädigt werden kann**.

In diesem Abschnitt wird das Format der Konfigurationsdatei beschrieben.

- 1 Zeilen, die mit einem # beginnen, sind Kommentare.

Ein Kommentar *must* in der ersten Spalte der Zeile beginnen. Ein #-Zeichen wird in jeder anderen Spalte als normales #-Zeichen behandelt.

Beispiel:

```
#  
# This is a comment  
  
[cfgUserAdmin]  
  
cfgUserAdminPrivilege=4
```

- 1 Alle Gruppeneinträge müssen sich zwischen den Zeichen [und] befinden.

Das Anfangszeichen [, das einen Gruppennamen anzeigt, *must* in Spalte eins beginnen. Dieser Gruppename *must* vor allen anderen Objekten in dieser Gruppe angegeben werden. Objekte, denen kein Gruppename zugewiesen ist, erzeugen Fehler. Die Konfigurationsdaten werden in Gruppen organisiert, wie unter [Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank](#) definiert.

Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objektes:

Beispiel:

```
[cfgLanNetworking] (Gruppenname)  
  
cfgNicIpAddress=143.154.133.121 (Objektname)
```

- 1 Parameter werden als *Objekt=Wert*-Paare ohne Leerzeichen zwischen Objekt, = und Wert angegeben.

Leerzeichen, das eingeschlossen wird, wenn der Wert ignoriert wurde. Ein Leerzeichen innerhalb einer Wertezeichenkette bleibt unverändert. Alle Zeichen rechts neben = werden unverändert übernommen (z. B. ein zweites = oder ein #, [,] usw.).

- 1 Der Parser ignoriert einen Index-Objekteintrag.

Sie können *nicht* bestimmen, welcher Index verwendet wird. Wenn der Index bereits vorhanden ist, wird dieser entweder verwendet oder es wird ein neuer Eintrag im ersten verfügbaren Index für diese Gruppe erstellt.

Der Befehl `racadm getconfig -f <Dateiname>` setzt einen Kommentar vor die Index-Objekte, wodurch Ihnen ermöglicht wird, die enthaltenen Kommentare zu sehen.

 **ANMERKUNG:** Sie können eine indizierte Gruppe manuell erstellen, indem Sie den folgenden Befehl verwenden:
`racadm config -g <Gruppenname> -o <verankertes-Objekt> -i <Index> <eindeutiger-Ankername>`

- 1 Die Zeile für eine indizierte Gruppe *kann nicht* aus einer Konfigurationsdatei gelöscht werden.

Ein indiziertes Objekt muss manuell anhand des folgenden Befehls gelöscht werden:

```
racadm config -g <Gruppenname> -o <Objektname> -i <Index> ""
```

 **ANMERKUNG:** Eine NULL-Zeichenkette (durch zwei "" Zeichen identifiziert) weist den iDRAC an, den Index für die angegebene Gruppe zu löschen.

Um den Inhalt einer indizierten Gruppe anzuzeigen, verwenden Sie den folgenden Befehl:

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

- 1 Bei indizierten Gruppen *must* der Objektanker das erste Objekt nach dem []-Paar sein. Es folgen Beispiele der derzeitigen indizierten Gruppen:

```
[cfgUserAdmin]  
  
cfgUserAdminUserName=<Benutzername>
```

- 1 Wenn die Analyse auf eine indizierte Gruppe trifft, ist es der Wert des anhängenden Objektes, der die verschiedenen Indizes unterscheidet.

Der Parser liest in allen Indizes aus dem iDRAC für diese Gruppe. Alle Objekte innerhalb dieser Gruppe sind einfache Modifizierungen, wenn der iDRAC konfiguriert wird. Wenn ein modifiziertes Objekt einen neuen Index darstellt, wird der Index während der Konfiguration auf dem iDRAC erstellt.

- 1 Es ist nicht möglich, einen gewünschten Index in einer Konfigurationsdatei zu bestimmen.

Indizes können erstellt und gelöscht werden, sodass die Gruppe im Laufe der Zeit durch genutzte und ungenutzte Indizes fragmentiert wird. Wenn ein Index vorhanden ist, wird er bearbeitet. Wenn kein Index vorhanden ist, wird der erste verfügbare Index verwendet. Diese Methode sorgt für Flexibilität, wenn indizierte Einträge hinzugefügt werden, wobei der Benutzer keine genauen Index-Übereinstimmungen zwischen allen verwalteten RACs herzustellen braucht. Neue Benutzer werden dem ersten verfügbaren Index hinzugefügt. Eine Konfigurationsdatei, die auf einem iDRAC korrekt parst und ausgeführt wird, kann auf einem anderen iDRAC möglicherweise nicht korrekt ausgeführt werden, falls alle Indizes belegt sind und ein neuer Benutzer hinzugefügt werden muss.

iDRAC-IP-Adresse in einer Konfigurationsdatei modifizieren

Wenn Sie die iDRAC-IP-Adresse in der Konfigurationsdatei modifizieren, entfernen Sie alle unnötigen `<variabel>=<Wert>`-Einträge. Es verbleibt nur die tatsächliche Bezeichnung der variablen Gruppe mit "[und "]" einschließlich der beiden `<variabel>=<Wert>`-Einträge, die sich auf die Änderung der IP-Adresse beziehen.

Beispiel:


```
#  
# Object Group "cfgLanNetworking"  
#  
[cfgLanNetworking]  
cfgNicIpAddress=10.35.10.110  
cfgNicGateway=10.35.10.1
```

Diese Datei wird durch folgende Einträge ergänzt:


```
#  
# Object Group "cfgLanNetworking"  
#  
[cfgLanNetworking]  
cfgNicIpAddress=10.35.9.143  
# comment, the rest of this line is ignored  
cfgNicGateway=10.35.9.1
```

Konfigurationsdatei in den iDRAC laden

Der Befehl `racadm config -f <Dateiname>` parst die Konfigurationsdatei, um zu überprüfen, ob gültige Gruppen- und Objektnamen vorhanden sind und Syntaxregeln befolgt werden. Weist die Datei keine Fehler auf, aktualisiert der Befehl die iDRAC-Datenbank mit dem Dateiinhalte.

 **ANMERKUNG:** Wenn Sie nur die Syntax überprüfen, jedoch nicht die iDRAC-Datenbank aktualisieren möchten, fügen Sie dem Unterbefehl `config` die Option `-c` hinzu.

Fehler in der Konfigurationsdatei werden mit der Zeilennummer sowie einer Meldung markiert, die das Problem beschreibt. Bevor die Konfigurationsdatei den iDRAC aktualisieren kann, müssen alle Fehler korrigiert worden sein.

 **HINWEIS:** Verwenden Sie den Unterbefehl `racresetcfg`, um die Datenbank und die iDRAC-NIC-Einstellungen auf die ursprünglichen Standardeinstellungen zurückzusetzen und alle Benutzer und Benutzerkonfigurationen zu entfernen. Während der Stammbenutzer weiterhin verfügbar ist, werden die Einstellungen anderer Benutzer auch auf die Standardeinstellungen zurückgesetzt.

Bevor Sie den Befehl `racadm config -f <Dateiname>` ausführen, können Sie den Unterbefehl `racreset` ausführen, um den iDRAC auf seine Standardeinstellungen zurückzusetzen. Stellen Sie sicher, dass die zu ladende Konfigurationsdatei alle gewünschten Objekte, Benutzer, Indizes und anderen Parameter enthält.

Um den iDRAC mit der Konfigurationsdatei zu aktualisieren, führen Sie an der Eingabeaufforderung des verwalteten Servers den folgenden Befehl aus:

```
racadm config -f <Dateiname>
```

Nachdem der Befehl abgeschlossen wurde, können Sie den RACADM-Unterbefehl `getconfig` ausführen, um zu bestätigen, dass die Aktualisierung erfolgreich verlief.

Mehrfache iDRACs konfigurieren


Anhand einer Konfigurationsdatei können Sie andere iDRACs mit identischen Eigenschaften konfigurieren. Führen Sie zur Konfiguration mehrerer iDRACs die folgenden Schritte aus:

1. Erstellen Sie die Konfigurationsdatei von dem iDRAC aus, dessen Einstellungen Sie auf den anderen replizieren möchten. Geben Sie an einer Eingabeaufforderung des verwalteten Servers den folgenden Befehl ein:

```
racadm getconfig -f <Dateiname>
```

wobei `<Dateiname>` der Name einer Datei zum Speichern der iDRAC-Eigenschaften ist, wie z. B. `myconfig.cfg`.

Weitere Informationen finden Sie unter [iDRAC-Konfigurationsdatei erstellen](#).

 **ANMERKUNG:** Einige Konfigurationsdateien enthalten eindeutige iDRAC-Informationen (wie die statische IP-Adresse), die vor dem Exportieren der Datei zu anderen iDRACs geändert werden müssen.

2. Bearbeiten Sie die im vorherigen Schritt erstellte Konfigurationsdatei, und entfernen Sie alle Einstellungen oder kommentieren Sie alle Einstellungen aus, die Sie *nicht* replizieren möchten.

3. Kopieren Sie die bearbeitete Konfigurationsdatei auf ein Netzlaufwerk, auf dem alle verwalteten Server, deren iDRAC konfiguriert werden soll, auf sie zugreifen können.

4. Führen Sie für jeden iDRAC, den Sie konfigurieren möchten, Folgendes aus:

a. Melden Sie sich am verwalteten Server an, und starten Sie eine Eingabeaufforderung.

b. Wenn Sie den iDRAC von den Standardeinstellungen aus neu konfigurieren möchten, geben Sie den folgenden Befehl ein:

```
racadm racreset
```

c. Laden Sie die Konfigurationsdatei anhand des folgenden Befehls in den iDRAC:

```
racadm config -f <Dateiname>
```

wobei <Dateiname> der Name der von Ihnen erstellten Konfigurationsdatei ist. Schließen Sie den vollständigen Pfad mit ein, wenn sich die Datei nicht im Arbeitsverzeichnis befindet.

d. Setzen Sie den konfigurierten iDRAC durch Eingabe des folgenden Befehls zurück:

```
Racadm-Reset
```

[Zurück zum Inhaltsverzeichnis](#)


[Zurück zum Inhaltsverzeichnis](#)

iDRAC-SM-CLP-Befehlszeilenoberfläche verwenden

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Systemverwaltung mit SM-CLP](#)
- [iDRAC-SM-CLP-Support](#)
- [SM-CLP-Funktionen](#)
- [MAP-Adressbereich navigieren](#)
- [Verb Anzeigen verwenden](#)
- [Beispiele des iDRAC-SM-CLP](#)
- [Seriell über LAN \(SOL\) mit Telnet oder SSH verwenden](#)

Dieser Abschnitt bietet Informationen zum SMWG-SM-CLP (Serververwaltungs-Workgroup, Serververwaltungs-Befehlszeilenprotokoll), das im iDRAC integriert ist.

 **ANMERKUNG:** Für diesen Abschnitt wird angenommen, dass Sie mit der SMASH-Initiative (Systemverwaltungsarchitektur für Serverhardware) und den SMWG SM-CLP-Angaben vertraut sind. Weitere Information über diese Angaben finden Sie auf der Website zur Distributed Management Task Force (DMTF) unter www.dmtf.org.

Das iDRAC-SM-CLP ist ein Protokoll, das von der DMTF und der SMWG betrieben wird, um für Systemverwaltungs-CLI-Umsetzungen Standards zu bieten. Viele Ansätze basieren auf einer definierten SMASH-Architektur, die als Fundament für mehr genormte Systems Management-Komponentensätze dienen soll. Der SMWG SM-CLP ist eine Unterkomponente der gesamten von DMTF verfolgten SMASH-Bemühungen.

SM-CLP bietet einen Teilsatz der Funktionalität, die von der Befehlszeilenoberfläche des lokalen RACADM zur Verfügung gestellt wird, jedoch über einen unterschiedlichen Zugriffspfad. SM-CLP wird innerhalb des iDRAC ausgeführt und RACADM auf dem verwalteten Server. Bei RACADM handelt es sich außerdem um eine Dell-proprietäre Schnittstelle, wobei SM-CLP eine Industriestandardschnittstelle ist. Eine Zuweisung der RACADM- und SM-CLP-Befehle ist unter [RACADM- und SM-CLP-Äquivalenzen](#) dargestellt.

Systemverwaltung mit SM-CLP

Das iDRAC-SM-CLP ermöglicht Ihnen die Verwaltung der folgenden Systemfunktionen über eine Befehlszeile oder ein Skript:

- 1 Server-Stromverwaltung - Einschalten, herunterfahren oder das System neu starten
- 1 Systemereignisprotokoll (SEL) -Verwaltung - Anzeige oder Löschen der SEL-Datensätze
- 1 iDRAC-Benutzerkontoverwaltung
- 1 Active Directory-Konfiguration
- 1 iDRAC-LAN-Konfiguration
- 1 Erstellung einer SSL-Zertifikatsignaturanforderung (CSR)
- 1 Konfiguration des virtuellen Datenträgers
- 1 SOL-Umleitung (Seriell über LAN) über Telnet oder SSH

iDRAC-SM-CLP-Support

SM-CLP wird von der iDRAC-Firmware gehostet und unterstützt Telnet- und SSH-Verbindungen. Die iDRAC-SM-CLP-Schnittstelle basiert auf der SM-CLP-Spezifikation Version 1.0, bereitgestellt von der DMTF-Organisation.

Die folgenden Abschnitte enthalten eine Übersicht der SM-CLP-Funktion, die vom iDRAC gehostet wird.

SM-CLP-Funktionen

Die SM-CLP-Spezifikation enthält einen allgemeinen Satz von SM-CLP-Standardverben, die für das einfache Systems Management über CLI verwendet werden können.

SM-CLP fördert das Konzept von Verben und Zielen, um Systemkonfigurationsfähigkeiten durch die CLI bereitzustellen. Das Verb zeigt den auszuführenden Vorgang an, und das Ziel bestimmt die Einheit (oder das Objekt), die den Vorgang ausführt.

Im Folgenden wird die Syntax der SM-CLP-Befehlszeile dargestellt:

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

[Tabelle 10-1](#) bietet eine Liste der Verben, die die iDRAC-CLI unterstützt, die Syntax der einzelnen Befehle sowie eine Liste der Optionen, die das Verb unterstützt.

Tabelle 10-1. Unterstützte SM-CLP-CLI-Verben

--	--	--

Verb	Beschreibung	Optionen
cd	Navigiert mithilfe der Shell durch den Adressbereich des verwalteten Systems. Syntax: cd [Optionen] [Ziel]	-default, -examine, -help, -output, -version
delete	Löscht ein Objekt-Beispiel. Syntax: delete [Optionen] Ziel	-examine, -help, -output, -version
dump	Bewegt ein Binärbild von MAP zu URI. dump -destination <URI> [Optionen] [Ziel]	-destination, -examine, -help, -output, -version
exit	Beendet SM-CLP Shell-Sitzung. Syntax: exit [Optionen]	-help, -output, -version
help	Zeigt Hilfe für SM-CLP-Befehle an. help	-examine, -help, -output, -version
load	Bewegt ein Binärbild zu MAP von URI. Syntax: load -source <URI> [Optionen] [Ziel]	-examine, -help, -output, -source, -version
reset	Setzt das Ziel zurück. Syntax: reset [Optionen] [Ziel]	-examine, -help, -output, -version
set	Stellt die Eigenschaften eines Ziels ein Syntax: set [Optionen] [Ziel] <Eigenschaftennamen>=<Wert>	-examine, -help, -output, -version
show	Zeigt die Zieleigenschaften, Verben, und Unterziele an. Syntax: show [Optionen] [Ziel] <Eigenschaftennamen>=<Wert>	-all, -default, -display, -examine, -help, -level, -output, -version
start	Startet ein Ziel. Syntax: start [Optionen] [Ziel]	-examine, -force, -help, -output, -version
stop	Führt ein Ziel herunter. Syntax: stop [Optionen] [Ziel]	-examine, -force, -help, -output, -state, -version, -wait
version	Zeigt die Versionsattribute eines Ziels an. Syntax: version [Optionen]	-examine, -help, -output, -version

[Tabelle 10-2](#) beschreibt die SM-CLP-Optionen. Einige Optionen haben abgekürzte Formen, wie in der Tabelle gezeigt.

Tabelle 10-2. Unterstützte SM-CLP-Optionen

SM-CLP-Option	Beschreibung
-all, -a	Beauftragt das Verb, alle möglichen Funktionen auszuführen.
-destination	Bestimmt den Speicherort, an dem ein Image im Dump-Befehl gespeichert wird. Syntax: -destination <URI>
-display, -d	Filtert die Befehlsausgabe. Syntax:

	-display <Eigenschaften Ziele Verben>[, <Eigenschaften Ziele Verben>]*
-examine, -x	Beauftragt den Befehlsprozessor, die Befehl-Syntax zu validieren, ohne den Befehl auszuführen.
-help, -h	Zeigt Hilfe für das Verb an.
-level, -l	Weist das Verb an, an Zielen auf zusätzlichen Stufen unterhalb des festgelegten Ziels zu arbeiten. Syntax: -level <n alle>
-output, -o	Legt das Format für die Ausgabe fest. Syntax: -output <Text clpsv clpxml>
-source	Legt den Speicherort eines Image in einem Ladebefehl fest. Syntax: -source <URI>
-version, -v	Zeigt die SMASH-CLP-Versionsnummer an.

MAP-Adressbereich navigieren

ANMERKUNG: Auf SM-CLP-Adresspfaden können der Schrägstrich (/) und der umgekehrte Schrägstrich (\) miteinander vertauscht werden. Ein umgekehrter Schrägstrich am Ende einer Befehlszeile führt jedoch den Befehl in der nächsten Zeile fort und wird ignoriert, wenn der Befehl geparkt wird.

Objekte, die mit dem SM-CLP verwaltet werden können, werden durch Ziele repräsentiert, die in einem hierarchischen Bereich, Adressbereich des Verwaltungszugriffspunkts (MAP) genannt, angeordnet sind. Ein Adresspfad legt den Pfad vom Adressbereichsstamm zu einem Objekt im Adressbereich fest.

Das Stammziel wird durch einen Schrägstrich (/) oder einen umgekehrten Schrägstrich (\) dargestellt. Es ist der standardmäßige Ausgangspunkt, wenn Sie sich am iDRAC anmelden. Wechseln Sie vom Stamm herunter, indem Sie das Verb cd verwenden. Wenn Sie z. B. zum dritten Eintrag des Systemereignisprotokolls (SEL) wechseln möchten, geben Sie den folgenden Befehl ein:

```
->cd /system1/sp1/logs1/record3
```

Geben Sie das Verb cd ohne Ziel ein, um Ihren aktuellen Standort im Adressbereich zu finden. Die Abkürzungen .. und . funktionieren wie in Windows und Linux: .. bezieht sich auf die Parent-Ebene, und . bezieht sich auf die aktuelle Ebene.

Ziele

[Tabelle 10-3](#) bietet eine Liste von Zielen, die über das SM-CLP zur Verfügung stehen.

Tabelle 10-3. SM-CLP-Ziele

Ziel	Definition
/system1/	Das verwaltete System-Ziel.
/system1/sp1	Der Dienstprozessor.
/system1/sol1	Ziel Seriell über LAN.
/system1/sp1/account1 bis /system1/sp1/account16	Die sechzehn lokalen iDRAC-Benutzerkonten. account1 ist das Stammkonto.
/system1/sp1/enetport1	Die iDRAC-NIC-MAC-Adresse.
/system1/sp1/enetport1/lanendpt1/ ipendpt1	Die Einstellungen für iDRAC-IP, Gateway und Netzmaske.
/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1	Die Einstellungen des iDRAC-DNS-Servers.
/system1/sp1/group1 bis /system1/sp1/group5	Die Active Directory-Standardschemagruppen.
/system1/sp1/logs1	Das Protokollsammelziel.
/system1/sp1/logs1/record1	Ein einzelnes SEL-Datensatzbeispiel auf dem verwalteten System.
/system1/sp1/logs1/records	Das SEL-Ziel auf dem verwalteten System.
/system1/sp1/oemdel_l_racsecurity1	Speicher für Parameter, die zum Erstellen einer Zertifikatsignierungsanforderung verwendet werden.
/system1/sp1/oemdel_ssl1	Status der SSL-Zertifikatanforderung.
/system1/sp1/oemdel_vmservice1	Konfiguration und Zustand des virtuellen Datenträgers.

Verb Anzeigen verwenden

Um mehr über ein Ziel zu erfahren, verwenden Sie das Verb show. Dieses Verb zeigt die Eigenschaften des Ziels, untergeordnete Ziele sowie eine Liste der SM-

CLP-Verben an, die an diesem Ort zulässig sind.

Option -display verwenden

Anhand der Option **show -display** können Sie die Befehlsausgabe auf eines oder mehrere der folgenden Elemente einschränken: Eigenschaften, Ziele, Verben. Wenn Sie z. B. nur die Eigenschaften und Ziele des aktuellen Orts anzeigen möchten, verwenden Sie den folgenden Befehl:

```
show -d properties,targets /system1/sp1/account1
```

Wenn Sie nur bestimmte Eigenschaften auflisten möchten, qualifizieren Sie sie, wie im folgenden Befehl gezeigt:

```
show -d properties=(userid,username) /system1/sp1/account1
```

Wenn Sie nur eine Eigenschaft anzeigen möchten, können Sie die Klammern auslassen.

Option -level verwenden

Die Option **show -level** führt **show** über zusätzlichen Ebenen unterhalb des festgelegten Ziels aus. Wenn Sie z. B. die Eigenschaften **username** und **userid** der Ziele **account16** bis **account1** unterhalb von **/system1/sp1** anzeigen möchten, könnten Sie den folgenden Befehl eingeben:

```
show -l 1 -d properties=(userid,username) /system1/sp1/account*
```

Wenn Sie alle Ziele und Eigenschaften im Adressbereich anzeigen möchten, verwenden Sie die Option **-l all**, wie im folgenden Befehl:

```
show -l all -d properties /
```

Option -output verwenden

Die Option **-output** legt eines von vier Formaten für die Ausgabe von SM-CLP-Verben fest: **text**, **clpcsv**, **keyword** und **clpxml**.

Das Standardformat ist **text**, die am einfachsten lesbare Ausgabe. Das Format **clpcsv** ist ein Format, bei dem Werte durch Kommas getrennt werden. Es eignet sich dazu, in ein Tabellenkalkulationsprogramm geladen zu werden. Das Format **keyword** gibt Informationen als eine Liste von **keyword=value**-Paaren (eines pro Zeile) aus. Das Format **clpxml** ist ein XML-Dokument, das ein **response-XML-Element** enthält. Die DMTF hat die Formate **clpcsv** und **clpxml** festgelegt, und ihre Bestimmungen können auf der DMTF-Website unter www.dmtf.org eingesehen werden.

Das folgende Beispiel zeigt, wie der Inhalt des SEL in XML ausgegeben werden kann:

```
show -l all -output format=clpxml /system1/sp1/logs1
```

Beispiele des iDRAC-SM-CLP

Die folgenden Unterabschnitte enthalten Beispiele zur Verwendung des SM-CLP, um folgende Vorgänge auszuführen:

- 1 Server-Stromverwaltung
- 1 SEL-Management
- 1 MAP-Ziel-Navigierung
- 1 Anzeigesystemeigenschaften
- 1 iDRAC-IP-Adresse, Subnetzmaske und Gateway-Adresse einstellen

Server-Stromverwaltung

[Tabelle 10-4](#) enthält Beispiele für die Verwendung von SM-CLP zur Ausführung von Stromverwaltungsvorgängen auf einem verwalteten Server.

Tabelle 10-4. Server-Stromverwaltungsvorgänge

Vorgang	Syntax
Anmeldung am iDRAC über die SSH-Schnittstelle	>ssh 192.168.0.120 >login: root >password:
Server herunterfahren	->stop /system1 system1 has been stopped successfully (System1 wurde erfolgreich angehalten)
Server von einem ausgeschalteten Zustand hochfahren	->start /system1 system1 has been started successfully (System1 wurde erfolgreich gestartet)

Server neu starten	<pre>-->reset /system1 system1 has been reset successfully (System1 wurde erfolgreich zurückgesetzt)</pre>
--------------------	---

SEL-Management

[Tabelle 10-5](#) enthält Beispiele für die Verwendung von SM-CLP zum Ausführen von mit SEL in Beziehung stehenden Vorgängen auf dem verwalteten System.

Tabelle 10-5. SEL-Verwaltungsvorgänge

Vorgang	Syntax
SEL ansehen	<pre>-->show /system1/sp1/logs1 Targets: record1 record2 record3 record4 record5 Properties: Description=IPMI SEL MaxNumberOfRecords=512 CurrentNumberOfRecords=5 Verbs: cd delete exit help show version</pre>
SEL-Datensatz ansehen	<pre>-->show /system1/sp1/logs1/record4 ufip=/system1/sp1/logs1/log1/record4 Properties: Caption=Not defined Description=Backplane Drive 0: drive slot sensor for Backplane, drive presence was asserted ElementName=Not Supported LogCreationClassName=CIM_RecordLog LogName=IPMI SEL CreationClassName=CIM_LogRecord RecordID=4 MessageTimeStamp=16:37:10,January 13,2007 Verbs: cd exit help show version</pre>
SEL löschen	<pre>-->delete /system1/sp1/logs1 All records deleted successfully</pre>

MAP Ziel-Navigation

[Tabelle 10-6](#) enthält Beispiele für die Verwendung des Verbs `cd`, um innerhalb des MAP zu navigieren. In allen Beispielen wird angenommen, dass das ausgängliche Standardziel `'/'` ist.

Tabelle 10-6. Map-Zielnavigationsvorgänge

Vorgang	Syntax
Zum System-Ziel wechseln und einen Neustart durchführen	<pre>-->cd system1 -->reset</pre> <p>ANMERKUNG: Das aktuelle Standardeinstellungsziel ist <code>'/'</code>.</p>
Wechseln Sie zum SEL-Ziel und zeigen Sie die Protokolldatensätze an	<pre>-->cd system1 -->cd sp1 -->cd logs1 -->show -->cd system1/sp1/logs1 -->show</pre>
Aktuelles Ziel anzeigen	<pre>-->cd.</pre>

Eine Stufe höher gehen	->cd..
Shell beenden	->exit

iDRAC-IP-Adresse, Subnetzmaske und Gateway-Adresse einstellen

Die Verwendung des SM-CLP zum Aktualisieren der iDRAC-Netzwerkeigenschaften wird über zwei Verfahren ausgeführt:

- Stellen Sie unter `/system1/sp1/enetport1/lanendpt1/ipendpt1` neue Werte für die NIC-Eigenschaften ein:
 - `oem Dell_nicenable` - auf 1 einstellen, um iDRAC-Netzwerkbetrieb zu aktivieren, auf 0, um zu deaktivieren
 - `ipaddress` - die IP-Adresse
 - `subnetmask` - die Subnetzmaske
 - `oem Dell_usedhcp` - auf 1 einstellen, um die Verwendung von DHCP zum Einstellen der Eigenschaften `ipaddress` und `subnetmask` zu aktivieren, auf 0 einstellen, um statische Werte einzustellen
- Übernehmen Sie die neuen Werte, indem Sie die Eigenschaft `committed` auf 1 einstellen.

Immer wenn die Eigenschaft `commit` den Wert 1 hat, sind die aktuellen Einstellungen der Eigenschaften aktiv. Wenn Sie eine Eigenschaft ändern, wird die Eigenschaft `commit` auf 0 zurückgesetzt, um darauf hinzuweisen, dass die Werte nicht übernommen wurden.

ANMERKUNG: Die Eigenschaft `commit` wirkt sich nur auf die Eigenschaften am MAP-Ort `/system1/sp1/enetport1/lanendpt1/ipendpt1` aus. Alle anderen SM-CLP-Befehle werden sofort wirksam.

ANMERKUNG: Wenn Sie lokales RACADM zum Einstellen der iDRAC-Netzwerkeigenschaften verwenden, werden Ihre Änderungen sofort wirksam, da lokales RACADM nicht auf eine Netzwerkverbindung angewiesen ist.

Wenn Sie die Änderungen übernehmen, werden die neuen Netzwerkeinstellungen wirksam, was dazu führt, dass Ihre Telnet- oder ssh-Sitzung abgebrochen wird. Indem Sie den Schritt `commit` einführen, können Sie die Beendigung Ihrer Sitzung so lange verzögern, bis Sie alle SM-CLP-Befehle ausgeführt haben.

[Tabelle 10-7](#) zeigt Beispiele zum Einstellen der iDRAC-Eigenschaften unter Verwendung des SM-CLP.

Tabelle 10-7. iDRAC-Netzwerkeigenschaften mit SM-CLP einstellen

Vorgang	Syntax
Wechseln Sie zum Speicherort der iDRAC-NIC-Eigenschaften	->cd /system1/sp1/enetport1/lanendpt1/ipendpt1
Stellen Sie die neue IP-Adresse ein	->set ipaddress=10.10.10.10
Stellen Sie die Subnetzmaske ein	->set subnetmask=255.255.255.255
Schalten Sie das DHCP-Flag ein	->set oem Dell_usedhcp=1
Aktivieren Sie die NIC	->set oem Dell_nicenable=1
Übernehmen Sie die Änderungen	->set committed=1

iDRAC-Firmware mittels SM-CLP aktualisieren

Um die iDRAC-Firmware unter Verwendung des SM-CLP zu aktualisieren, müssen Sie den TFTP-URI des Dell Update Package kennen.

Führen Sie zum Aktualisieren der Firmware unter Verwendung des SM-CLP die folgenden Schritte aus:

- Melden Sie sich über Telnet oder SSH am iDRAC an.
- Überprüfen Sie die aktuelle Firmware-Version, indem Sie den folgenden Befehl eingeben:

```
version
```

- Geben Sie den folgenden Befehl ein:

```
load -source tftp://<tftp-Server>/<Aktualisierungspfad> /system1/sp1
```

wobei `<tftp-Server>` der DNS-Name oder die IP-Adresse des TFTP-Servers ist und `<Aktualisierungspfad>` der Pfad zum Aktualisierungspaket auf dem TFTP-Server.

Ihre Telnet- oder SSH-Sitzung wird abgebrochen werden. Sie müssen eventuell mehrere Minuten abwarten, bis die Firmware-Aktualisierung abgeschlossen ist.

- Um zu überprüfen, ob die neue Firmware geschrieben wurde, starten Sie eine neue Telnet- oder SSH-Sitzung und geben den Versionsbefehl erneut ein.

Seriell über LAN (SOL) mit Telnet oder SSH verwenden

Verwenden Sie eine Telnet- oder SSH-Konsole auf Ihrer Verwaltungsstation, um zum iDRAC eine Verbindung herzustellen, und leiten Sie dann die serielle Schnittstelle des verwalteten Servers in Ihre Konsole um. Diese Funktion stellt eine Alternative zu IPMI SOL dar, für die ein Dienstprogramm wie **solproxy** zum Übersetzen des seriellen Stroms an und von Netzwerkpakete(n) erforderlich ist. Die iDRAC SOL-Implementierung macht ein zusätzliches Dienstprogramm überflüssig, da die seriell-zu-Netzwerk-Übersetzung innerhalb des iDRAC stattfindet.

Die verwendete Telnet- oder SSH-Konsole sollte in der Lage sein, die Daten zu interpretieren, die von der seriellen Schnittstelle des verwalteten Servers ankommen, und auf diese Daten zu reagieren. Die serielle Schnittstelle wird normalerweise an eine Shell angeschlossen, die ein ANSI- oder VT100-Terminal emuliert.

Sie können unter Verwendung von Telnet eine Verbindung zur IPMI LAN-SOL-Schnittstelle - Schnittstelle 2100 - herstellen. Die serielle Konsole wird automatisch auf Ihre Telnet-Konsole umgeleitet.

Mit SSH oder Telnet können Sie zum iDRAC auf die gleiche Weise wie zum SM-CLP eine Verbindung herstellen. Die SOL-Umleitung kann dann vom Ziel `/system1/sol1` aus gestartet werden.

Weitere Informationen zur Verwendung von Telnet- und SSH-Clients mit iDRAC finden Sie unter [Telnet- oder SSH-Clients installieren](#).

SOL über Telnet mit HyperTerminal auf Microsoft Windows verwenden

1. Wählen Sie **Start** → **Alle Programme** → **Zubehör** → **Kommunikation** → **HyperTerminal** aus.
2. Geben Sie für die Verbindung einen Namen ein, wählen Sie ein Symbol aus, und klicken Sie auf **OK**.
3. Wählen Sie im Feld **Verbindung herstellen über** aus der Liste **TCP/IP (Winsock)** aus.
4. Geben Sie in das Feld **Host-Adresse** den DNS-Namen oder die IP-Adresse ein.
5. Geben Sie in das Feld **Schnittstellenummer** die Telnet-Schnittstellenummer ein.
6. Klicken Sie auf **OK**.

Klicken Sie zum Beenden der SOL-Sitzung auf das Symbol zum Abbrechen der HyperTerminal-Verbindung.

SOL über Telnet mit Linux verwenden

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

1. Starten Sie eine Shell.
2. Stellen Sie anhand des folgenden Befehls eine Verbindung zum iDRAC her:

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

 **ANMERKUNG:** Wenn Sie die Standard-Schnittstellenummer für den Telnet-Dienst, 23, geändert haben, fügen Sie die Schnittstellenummer an das Ende des **telnet**-Befehls hinzu.

3. Geben Sie zum Starten von SOL den folgenden Befehl ein:

```
start /system1/sol1
```

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

Wenn Sie bereit sind, SOL zu beenden, geben Sie `<Strg>+]` ein (halten Sie **Strg** gedrückt, geben Sie eine rechte eckige Klammer ein, und lassen Sie dann die Tasten los). Eine Telnet-Eingabeaufforderung wird angezeigt. Geben Sie `quit` ein, um Telnet zu beenden.

SOL über SSH verwenden

Anhand des Ziels `/system1/sol1` können Sie die serielle Schnittstelle des verwalteten Servers in Ihre SSH-Konsole umleiten.

1. Stellen Sie anhand von OpenSSH oder PuTTY eine Verbindung zum iDRAC her.
2. Geben Sie zum Starten von SOL den folgenden Befehl ein:

```
start /system1/sol1
```

Hierdurch werden Sie mit der seriellen Schnittstelle des verwalteten Servers verbunden. Die SM-CLP-Befehle stehen Ihnen nicht mehr zur Verfügung.

Wenn Sie bereit sind, die SOL-Umleitung zu beenden, geben Sie `<Strg>+ .` ein. (Halten Sie **Strg** gedrückt, geben Sie einen Punkt ein, und lassen Sie dann die

Tasten los). Die SSH-Sitzung wird jetzt geschlossen.

Wenn SOL gestartet wurde, können Sie nicht zum SM-CLP zurückkehren. Sie müssen die SSH-Sitzung beenden und eine neue starten, um das SM-CLP verwenden zu können.

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

Betriebssystem mittels iVM-CLI bereitstellen

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Bevor Sie Beginnen](#)
- [Eine startfähige Abbilddatei erstellen](#)
- [Vorbereitung auf die Bereitstellung](#)
- [Das Betriebssystem bereitstellen](#)
- [Befehlszeilenoberfläche-Dienstprogramm des Virtuellen Datenträgers verwenden](#)

Das Dienstprogramm Befehlszeilenoberfläche des virtuellen Datenträgers (iVM-CLI) ist eine Befehlszeilenoberfläche, die die Funktionen des virtuellen Datenträgers von der Verwaltungsstation zum iDRAC im Remote-System bereitstellt. Mit iVM-CLI und geskripteten Methoden können Sie Ihr Betriebssystem auf mehreren Remote-Systemen in Ihrem Netzwerk einsetzen.

Dieser Abschnitt gibt Auskunft über die Integration des iVM-CLI-Dienstprogramms in Ihrem Betriebsnetz.

Bevor Sie Beginnen

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

Remote-System-Anforderungen

- 1 Der iDRAC ist auf jedem Remote-System konfiguriert.

Netzwerk-Anforderungen

Eine Netzwerkreigabe muss die folgenden Komponenten enthalten:

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

Die Image-Datei muss das ISO-Image einer Betriebssystem-CD oder einer CD/DVD mit einem dem Industriestandard entsprechenden startfähigen Format sein.

Eine startfähige Abbilddatei erstellen

Bevor Sie die Abbilddatei den Remote-Systemen bereitstellen, stellen Sie sicher, dass ein unterstütztes System von der Datei starten kann. Um die Image-Datei zu prüfen, übertragen Sie sie mithilfe der iDRAC-Webbenutzeroberfläche auf ein Testsystem und führen dann einen Neustart des Systems durch.

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

Erstellen einer Abbilddatei für Linux-Systeme

Verwenden Sie das Datenvervielfältigungs-Dienstprogramm (dd), um eine startfähige Image-Datei für das Linux-System zu erstellen.

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

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

Beispiel:

```
dd if=/dev/sdc0 of=mycd.img
```

Abbilddatei für Windows-Systeme erstellen

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

Vorbereitung auf die Bereitstellung

Remote-Systeme konfigurieren

1. Erstellen Sie eine Netzwerkfreigabe, auf die über die Verwaltungsstation zugegriffen werden kann.
2. Kopieren Sie die Betriebssystem-Dateien zur Netzwerkfreigabe.
3. Wenn Sie eine startfähige, vorkonfigurierte Bereitstellungs-Abbilddatei zur Bereitstellung des Betriebssystems zu den Remote-Systemen haben, können Sie diesen Schritt überspringen.

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

Zum Bereitstellen eines Microsoft® Windows®-Betriebssystems kann die Image-Datei z. B. Programme enthalten, die den von Microsoft Systems Management Server (SMS) verwendeten Bereitstellungsverfahren ähnlich sind.

Wenn Sie die Abbilddatei erstellen, führen Sie folgendes aus:

- 1 Befolgen Sie die netzwerkbasieren Standardinstallationsverfahren
 - 1 Kennzeichnen Sie das Bereitstellungsimage als "read only", um sicherzustellen, dass jedes Zielsystem startet und dasselbe Bereitstellungsverfahren ausführt
4. Führen Sie eins der folgenden Verfahren aus:
 - 1 Integrieren Sie **ipmitool** und die Befehlszeilenoberfläche des virtuellen Datenträgers (iVM-CLI) in Ihre bestehende Betriebssystem-Bereitstellungsanwendung. Verwenden Sie das Beispielskript **ivmdeploy** als Orientierungshilfe beim Verwenden des Dienstprogramms.
 - 1 Verwenden Sie das vorhandene **ivmdeploy**-Skript, um Ihr Betriebssystem bereitzustellen.

Das Betriebssystem bereitstellen

Verwenden Sie das iVM-Dienstprogramm und das im Dienstprogramm enthaltene **ivmdeploy**-Skript, um das Betriebssystem Ihren Remote-Systemen bereitzustellen.

Sehen Sie sich, bevor Sie beginnen, das **ivmdeploy**-Beispielskript an, das mit dem iVM-CLI-Dienstprogramm enthalten ist. Das Skript zeigt die detaillierten Schritte auf, die zur Bereitstellung des Betriebssystems an Remote-Systemen in Ihrem Netzwerk erforderlich sind.

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

1. Führt die iDRAC-IP-Adressen der Remote-Systeme auf, die in der Textdatei **ip.txt** bereitgestellt werden (eine IP-Adresse pro Zeile).
2. Legen Sie eine startfähige Betriebssystem-CD oder -DVD in das Laufwerk des Client-Datenträgers ein.
3. Führen Sie an der Befehlszeile **ivmdeploy** aus.

Geben Sie zum Ausführen des **ivmdeploy**-Skripts den folgenden Befehl an der Befehlszeile ein:

```
ivmdeploy -r ip.txt -u <idrac-Benutzer> -p <idrac-Kennwt> -c {<iso9660-img> | <Pfad>}
```

wo:

- 1 <idrac-Benutzer> ist der iDRAC-Benutzername, z. B. **root**
- 1 <idrac-Kennwt> ist das Kennwort für den iDRAC-Benutzer, z. B. **calvin**
- 1 <iso9660-img> ist der Pfad zu einem ISO9660-Image der Betriebssystem-Installations-CD-ROM oder -DVD
- 1 <Pfad> ist der Pfad zu dem Gerät, das die Betriebssystem-Installations-CD-ROM oder -DVD enthält


Das **ivmdeploy**-Skript leitet seine Befehlszeilenoptionen an das Dienstprogramm **ivmcli** weiter. Einzelheiten zu diesen Optionen finden Sie unter [Befehlszeilenoptionen](#). Das Skript verarbeitet die Option **-r** auf leicht unterschiedliche Weise als die Option **ivmcli -r**. Wenn das Argument der Option **-r** der Name einer vorhandenen Datei ist, liest das Skript iDRAC-IP-Adressen von der festgelegten Datei und führt das Dienstprogramm **ivmcli** einmal pro Zeile aus. Ist das Argument der Option **-r** kein Dateiname, sollte es die Adresse eines einzelnen iDRAC sein. In diesem Fall arbeitet die Option **-r** wie für das Dienstprogramm **ivmcli** beschrieben.

Das **ivmdeploy**-Skript unterstützt die Installation nur über eine CD/DVD oder ein CD/DVD-ISO9660-Image. Wenn Sie die Installation über eine Diskette oder ein Diskettenimage vornehmen müssen, können Sie das Skript zur Verwendung der Option **ivmcli -f** modifizieren.

Befehlszeilenoberfläche-Dienstprogramm des Virtuellen Datenträgers verwenden

Das Dienstprogramm Befehlszeilenoberfläche des virtuellen Datenträgers (iVM-CLI) ist eine schreibbare Befehlszeilenoberfläche, die die Funktionen des virtuellen Datenträgers von der Verwaltungsstation zum iDRAC bereitstellt.

Das iVM-CLI-Dienstprogramm bietet die folgenden Funktionen:

 **ANMERKUNG:** Beim Virtualisieren von schreibgeschützten Abbilddateien, können mehrere Sitzungen dieselben Abbilddateiträger teilen. Beim Virtualisieren von physischen Laufwerken kann nur jeweils eine Sitzung auf ein gegebenes physisches Laufwerk zugreifen.

- 1 Wechselmediengeräte oder Bilddateien, die mit den Plug-Ins des Virtuellen Datenträgers übereinstimmen
- 1 Automatische Terminierung, wenn die Einmal-Startoption der iDRAC-Firmware aktiviert ist.
- 1 Sichere Datenübertragung zum iDRAC mittels SSL-Verschlüsselung

Stellen Sie vor dem Ausführen des Dienstprogramms sicher, dass Sie für den iDRAC über Benutzerberechtigungen des virtuellen Datenträgers verfügen.

Wenn das Betriebssystem Administratorrechte oder eine betriebssystemspezifische Berechtigung oder Gruppenmitgliedschaft unterstützt, sind Administratorrechte auch zum Ausführen des iVM-CLI-Befehls erforderlich.

Der Administrator des Client-Systems kontrolliert Benutzergruppen und Berechtigungen und dadurch die Benutzer, die das Dienstprogramm ausführen können.

Für Windows-Systeme müssen Sie über Hauptbenutzerberechtigungen verfügen, um das iVM-CLI-Dienstprogramm auszuführen.


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

iVM-CLI-Dienstprogramm installieren

Das iVM-CLI-Dienstprogramm befindet sich auf der CD *Dell OpenManage™ Systems Management Consoles*, die im Systemverwaltungssoftware-Kit zu Dell OpenManage enthalten ist. Legen Sie zur Installation des Dienstprogramms die CD *System Management Consoles* in das CD-Laufwerk des Systems ein, und befolgen Sie die auf dem Bildschirm eingeblendeten Anleitungen.

Die CD *Systems Management Consoles* enthält die neuesten System Management-Softwareprodukte, einschließlich Diagnose, Speicherverwaltung, RAS-Dienst und RACADM-Dienstprogramm. Diese CD enthält auch Infodateien mit den neuesten Produktinformationen über die Systemverwaltungssoftware.

Die CD *Systems Management Consoles* enthält **ivmdeploy** ein Beispielskript, das illustriert, wie man die iVM-CLI- und RACADM-Dienstprogramme zur Bereitstellung von Software an verschiedene Remote-Systeme verwendet.

 **ANMERKUNG:** Das **ivmdeploy**-Skript hängt bei seiner Installation von den anderen, in seinem Verzeichnis vorhandenen, Dateien ab. Wenn Sie das Skript von einem anderen Verzeichnis aus verwenden möchten, müssen Sie alle Dateien mit ihm installieren.

Befehlszeilenoptionen

Die iVM-CLI-Schnittstelle ist auf Windows- und Linux-Systemen identisch. Das Dienstprogramm verwendet Optionen, die mit den RACADM-Dienstprogrammoptionen übereinstimmen. Eine Option zur Angabe der iDRAC-IP-Adresse erfordert z. B. dieselbe Syntax für die RACADM- und iVM-CLI-Dienstprogramme.

Das Format eines iVM-CLI-Befehls lautet:

```
ivmcli [Parameter] [Betriebssystem_Shell_Optionen]
```

Bei der Befehlszeilensyntax wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter "[iVM-CLI-Parameter](#)".

Wenn das Remote-System die Befehle akzeptiert und der iDRAC die Verbindung genehmigt, wird der Befehl weiterhin ausgeführt, bis eines von Folgendem zutrifft:

- 1 Die iVM-CLI-Verbindung wird aus einem beliebigen Grund abgebrochen.
- 1 Das Verfahren wird mit einer Betriebssystemsteuerung manuell terminiert. Beispiel: In Windows können Sie den Task-Manager verwenden, um das Verfahren zu beenden.

iVM-CLI-Parameter

iDRAC-IP-Adresse

```
-r <iDRAC-IP-Adresse>[:<iDRAC-SSL-Schnittstelle>]
```

Dieser Parameter bietet die iDRAC-IP-Adresse und die SSL-Schnittstelle, die das Dienstprogramm zum Herstellen einer Verbindung des virtuellen Datenträgers zum Ziel-iDRAC benötigt. Wenn Sie eine ungültige IP-Adresse oder einen ungültigen DDNS-Namen eingeben, wird eine Fehlermeldung angezeigt, und der Befehl wird terminiert.

wobei *<iDRAC-IP-Adresse>* eine gültige, eindeutige IP-Adresse oder der iDRAC-DDNS-Name (dynamisches Domänenamenssystem) ist, falls unterstützt. Wenn *<iDRAC-SSL-Schnittstelle>* ausgelassen wird, wird die Schnittstelle 443 (die Standardschnittstelle) verwendet. Solange die iDRAC-Standard-SSL-Schnittstelle nicht geändert wird, ist die optionale SSL-Schnittstelle nicht erforderlich.

iDRAC-Benutzername

-u <iDRAC-Benutzername>

Dieser Parameter enthält den iDRAC-Benutzernamen, der den virtuellen Datenträger ausführen wird.

Der <iDRAC-Benutzername> muss die folgenden Attribute aufweisen:

- 1 Gültiger Benutzername
- 1 iDRAC - Benutzerberechtigung für den virtuellen Datenträger

Wenn die iDRAC-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt, und der Befehl wird terminiert.

iDRAC-Benutzerkennwort

-p <iDRAC-Benutzerkennwort>

Dieser Parameter enthält das Kennwort für den angegebenen iDRAC-Benutzer.

Wenn die iDRAC-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt, und der Befehl wird terminiert.

Diskette/Festplatten-Gerät oder -Abbilddatei

-f {<Gerätename> | <Image-Datei>}

wobei <Gerätename> ein gültiger Laufwerkbuchstabe (bei Windows-Systemen) oder ein gültiger Gerätekomponentenname ist, einschließlich der Partitionsnummer des bereitstellbaren Dateisystems, falls zutreffend (bei Linux-Systemen), und wobei <Image-Datei> der Dateiname und Pfad einer gültigen Image-Datei ist.

Dieser Parameter bestimmt das Gerät oder die Datei, die die virtuelle Disketten-/Festplattendatenträger liefern.

Beispiel: Eine Abbilddatei wird wie folgt angegeben:

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

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

Wenn die Datei nicht schreibgeschützt ist, kann der virtuelle Datenträger zur Abbilddatei schreiben. Konfigurieren Sie das Betriebssystem, um eine Diskettenabbilddatei, die nicht überschrieben werden soll, mit Schreibschutz zu versehen.

Beispiel: Ein Gerät wird wie folgt angegeben:

-f a:\ (Windows-System)

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

Wenn das Gerät eine Schreibschutzfähigkeit bietet, können Sie diese Fähigkeit zum Sicherstellen verwenden, dass der virtuelle Datenträger nicht zum Datenträger schreiben wird.

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

CD/DVD-Gerät oder -Abbilddatei

-c {<Gerätename> | <Image-Datei>}

wobei <Gerätename> ein gültiger CD/DVD-Laufwerkbuchstabe (bei Windows-Systemen) oder ein gültiger CD/DVD-Gerätedateiname (bei Linux-Systemen) ist, und wobei <Image-Datei> der Dateiname und Pfad einer gültigen ISO-9660-Image-Datei ist.

Dieser Parameter bestimmt das Gerät oder die Datei, das/die virtuellen CD/DVD-ROM-Datenträger liefert:

Beispiel: Eine Abbilddatei wird wie folgt angegeben:

-c c:\temp\mydvd.img (Windows-Systeme)

-c /tmp/mydvd.img (Linux-Systeme)

Beispiel: Ein Gerät wird wie folgt angegeben:

-c d:\ (Windows-Systeme)

-c /dev/cdrom (Linux-Systeme)

Lassen Sie diesen Parameter aus der Befehlszeile aus, wenn Sie keine CD/DVD-Datenträger virtualisieren. Wenn ein ungültiger Wert festgestellt wird, wird eine Fehlermeldung angezeigt und der Befehl beendet.

Geben Sie mit dem Befehl mindestens einen Datenträgertyp (Diskette oder CD/DVD-Laufwerk) an, es sei denn, es werden nur Switch-Optionen vorgegeben. Ansonsten wird eine Fehlermeldung angezeigt und der Befehl mit einem Fehler beendet.

Versionsanzeige

-v

Dieser Parameter wird zur Anzeige der iVM-CLI-Dienstprogrammversion verwendet. Wenn keine anderen Nichtschalteroptionen geboten werden, endet der Befehl ohne Fehlermeldung.

Hilfeanzeige

-h

Dieser Parameter zeigt eine Zusammenfassung der iVM-CLI-Dienstprogrammparameter an. Wenn keine anderen Nichtschalteroptionen geboten werden, wird der Befehl ohne Fehler beendet.

Manuelle Anzeige

-m

Dieser Parameter zeigt eine detaillierte "man-Seite" für das iVM-CLI-Dienstprogramm an, einschließlich von Beschreibungen aller möglicher Optionen.

Verschlüsselte Daten

-e

Wenn dieser Parameter in der Befehlszeile enthalten ist, verwendet die iVM-CLI einen SSL-verschlüsselten Kanal zur Übertragung von Daten zwischen der Verwaltungsstation und dem iDRAC im Remote-System. Wenn dieser Parameter nicht in der Befehlszeile enthalten ist, wird die Datenübertragung nicht verschlüsselt.

iVM-CLI -Betriebssystem, Shell-Optionen

Die folgenden Betriebssystemfunktionen können in der iVM-CLI-Befehlszeile verwendet werden:

- 1 stderr/Stdout-Umleitung - Leitet jede gedruckte Dienstprogrammausgabe zu einer Datei um.

Die Verwendung des "größer als"-Zeichens (>), gefolgt von einem Dateinamen, überschreibt z. B. die angegebene Datei mit der gedruckten Ausgabe des iVM-CLI-Dienstprogramms.

 **ANMERKUNG:** Das iVM-CLI-Dienstprogramm liest nicht von der Standardeingabe (**stdin**). Infolgedessen ist keine **stdin**-Umleitung erforderlich.

- 1 Ausführung im Hintergrund - Standardmäßig wird das iVM-CLI-Dienstprogramm im Vordergrund ausgeführt. Verwenden Sie die Befehlsshell-Funktionen des Betriebssystems, um das Dienstprogramm zu veranlassen, im Hintergrund auszuführen. Zum Beispiel veranlasst unter einem Linux-Betriebssystem das Et-Zeichen (&) nach einem Befehl, dass das Programm als neues Hintergrundverfahren erzeugt wird.

Diese letztere Methode ist bei Skriptprogrammen nützlich, da dem Skript nach dem Starten eines neuen Vorgangs für den iVM-CLI-Befehl ermöglicht wird, fortzufahren (andernfalls würde das Skript blockieren, bis das iVM-CLI-Programm beendet ist). Wenn auf diese Weise mehrere iVM-CLI-Instanzen gestartet werden und eine oder mehrere Befehlsinstanzen manuell beendet werden müssen, sind die betriebssystemspezifischen Einrichtungen zum Auflisten und Beenden von Verfahren zu verwenden.

iVM-CLI -Rückgabecodes

0 = kein Fehler

1 = kann keine Verbindung aufbauen

2 = iVM-CLI-Befehlszeilenfehler

3 = RAC-Firmware-Verbindung abgebrochen

Textmeldungen (nur auf Englisch) werden auch zur Standardfehlerausgabe ausgegeben, wenn Fehler festgestellt werden.

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

iDRAC-Konfigurationshilfsprogramm verwenden

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Übersicht](#)
- [iDRAC-Konfigurationshilfsprogramm starten](#)
- [iDRAC-Konfigurationshilfsprogramm verwenden](#)

Übersicht

Das iDRAC-Konfigurationshilfsprogramm ist eine Vorstart-Konfigurationsumgebung, die Ihnen ermöglicht, Parameter für den iDRAC und den verwalteten Server anzuzeigen und einzustellen. Genauer gesagt können Sie:


- 1 Die Firmware-Revisionsnummern für die Firmware des iDRAC und der primären Rückwandplatine anzeigen
- 1 Das lokale Netzwerk des iDRAC konfigurieren, aktivieren oder deaktivieren
- 1 IPMI über LAN aktivieren oder deaktivieren
- 1 Ein LAN-PET-Ziel (Plattformereignis-Trap) aktivieren
- 1 Die Geräte des virtuellen Datenträgers verbinden oder abtrennen
- 1 Den administrativen Benutzernamen bzw. das administrative Kennwort ändern
- 1 Die iDRAC-Konfiguration auf die Werkseinstellungen zurücksetzen
- 1 SEL-Meldungen (Systemereignisprotokoll) anzeigen oder Meldungen aus dem Protokoll löschen

Die Tasks, die Sie anhand des iDRAC-Konfigurationshilfsprogramms ausführen können, können auch unter Verwendung anderer Dienstprogramme ausgeführt werden, die durch den iDRAC oder die OpenManage-Software zur Verfügung gestellt werden. Diese Dienstprogramme schließen die Webschnittstelle, die SM-CLP-Befehlszeilenoberfläche, die Befehlszeilenoberfläche des lokalen RACADM und, im Falle einfacher Netzwerkkonfiguration während der erstmaligen CMC-Konfiguration, das CMC-LCD ein.

iDRAC-Konfigurationshilfsprogramm starten

Zum erstmaligen Zugreifen auf das iDRAC-Konfigurationshilfsprogramm oder nach dem Zurücksetzen des iDRAC auf seine Standardeinstellungen muss eine iKVM-verbundene Konsole verwendet werden.

1. Geben Sie auf der Tastatur, die mit der iKVM-Konsole verbunden ist, <Druck> ein, um das iKVM-OSCAR-Menü (Onscreen-Konfiguration und -Berichterstattung) anzuzeigen. Verwenden Sie die Tasten <Nach oben> und <Nach unten>, um den Steckplatz zu markieren, der den Server enthält, und drücken Sie dann auf <Eingabe>.
2. Schalten Sie den Server ein, oder starten Sie ihn neu, indem Sie an seiner Vorderseite auf den Netzschalter drücken.
3. Wenn Sie die Meldung **Drücken Sie für das Remote-Zugriffs-Setup innerhalb von 5 Sek. auf <Strg-E>.....** sehen, drücken Sie sofort auf <Strg><E>.

 **ANMERKUNG:** Wenn das Betriebssystem zu laden beginnt, bevor Sie auf <Strg><E> drücken, lassen Sie das System den Startvorgang beenden, starten Sie dann den Server erneut und wiederholen Sie den Vorgang.

Das iDRAC-Konfigurationshilfsprogramm wird angezeigt. Die ersten beiden Zeilen bieten Informationen zur iDRAC-Firmware und zu den Firmware-Revisionen der primären Rückwandplatine. Die Revisionsstufen können nützlich sein, wenn Sie bestimmen möchten, ob ein Firmware-Upgrade erforderlich ist.

Die iDRAC-Firmware ist der Teil der Firmware, der für externe Schnittstellen zuständig ist, wie z. B. die Webschnittstellen oder das SM-CLP. Die Firmware der primären Rückwandplatine ist der Teil der Firmware, der mit der Serverhardware-Umgebung gekoppelt wird und diese überwacht.

iDRAC-Konfigurationshilfsprogramm verwenden

Unterhalb der Firmware-Revisionsmeldungen besteht der Rest des iDRAC-Konfigurationshilfsprogramms aus einem Menü von Elementen, auf die Sie über die Tasten <Nach oben> und <Nach unten> zugreifen können.

- 1 Wenn ein Menüelement zu einem Untermenü oder einem bearbeitbaren Textfeld führt, drücken Sie auf <Eingabe>, um auf das Element zuzugreifen, und auf <Esc>, um es zu verlassen, wenn Sie es fertig konfiguriert haben.
- 1 Wenn ein Element auswählbare Werte besitzt, wie Ja/Nein oder Aktiviert/Deaktiviert, drücken Sie auf <Nach links>, <Nach rechts> oder auf die <Leertaste>, um einen Wert auszuwählen.
- 1 Kann ein Element nicht bearbeitet werden, wird es blau angezeigt. Einige Elemente werden abhängig von anderen getroffenen Auswahlen bearbeitbar.
- 1 In der unteren Zeile des Bildschirms werden Anleitungen zum aktuellen Element angezeigt. Sie können auf <F1> drücken, um bzgl. des aktuellen Elements Hilfe aufzurufen.
- 1 Wenn Sie mit der Verwendung des iDRAC-Konfigurationshilfsprogramms fertig sind, drücken Sie auf <Esc>, um das Beenden-Menü anzuzeigen, in dem Sie wählen können, Ihre Änderungen zu speichern oder abzulehnen, oder zum Hilfsprogramm zurückzukehren.

In den folgenden Abschnitten werden die Menüelemente des iDRAC-Konfigurationshilfsprogramms beschrieben.

LAN

Verwenden Sie die Tasten <Nach links> und <Nach rechts> sowie die Leertaste, um zwischen **Aktiviert** und **Deaktiviert** auszuwählen.

Das iDRAC-LAN ist in der Standardkonfiguration deaktiviert. Das LAN muss aktiviert sein, damit der Gebrauch der iDRAC-Einrichtungen, wie z. B. der Webschnittstelle, des Telnet/SSH-Zugriffs auf die SM-CLP-Befehlszeilenoberfläche, der Konsolenumleitung und des virtuellen Datenträgers, gestattet wird.

Wenn Sie wählen, das LAN zu deaktivieren, wird die folgende Warnung angezeigt:

iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF.

(iDRAC-bandexterne Schnittstelle wird deaktiviert, wenn der LAN-Kanal AUS ist.)

Drücken Sie auf eine beliebige Taste, um die Meldung zu löschen und fortzufahren.

Die Meldung informiert Sie darüber, dass zusätzlich zu den Einrichtungen, auf die Sie über die direkte Verbindung zu den iDRAC-HTTP-, HTTPS-, Telnet- oder SSH-Schnittstellen zugreifen, der bandexterne Verwaltungsnetzwerkdatenverkehr (wie z. B. IPMI-Meldungen, die von einer Verwaltungsstation aus an den iDRAC gesendet werden) nicht empfangen werden kann, wenn das LAN deaktiviert ist. Die Schnittstelle des lokalen iDRAC bleibt verfügbar und kann zur Neukonfiguration des iDRAC-LAN verwendet werden.

IPMI über LAN (Ein/Aus)

Verwenden Sie die Tasten <Nach links> und <Nach rechts> sowie die Leertaste, um zwischen **Ein** und **Aus** zu wählen. Wenn **Aus** ausgewählt ist, akzeptiert der iDRAC keine IPMI-Meldungen, die über die LAN-Schnittstelle eingehen.

Wenn Sie **Aus** auswählen, wird die folgende Warnung angezeigt:

iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF.

(iDRAC-bandexterne Schnittstelle wird deaktiviert, wenn der LAN-Kanal AUS ist.)

Drücken Sie auf eine beliebige Taste, um die Meldung zu löschen und fortzufahren. Unter [LAN](#) finden Sie eine Erklärung der Meldung.

LAN-Parameter

Drücken Sie auf <Eingabe>, um das Untermenü der LAN-Parameter anzuzeigen. Wenn Sie die Konfiguration der LAN-Parameter abgeschlossen haben, drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln.

Tabelle 12-1. LAN-Parameter


Element	Beschreibung
Verschlüsselungsschlüssel RMCP+	Drücken Sie auf <Eingabe>, um den Wert zu bearbeiten, und auf <Esc>, wenn Sie den Vorgang abgeschlossen haben. Der Verschlüsselungsschlüssel RMCP+ ist eine aus 40 Zeichen bestehende hexadezimale Zeichenkette (Zeichen 0-9, a-f und A-F). RMCP+ ist eine IPMI-Erweiterung, die der IPMI Authentifizierung und Verschlüsselung hinzufügt. Der Standardwert ist eine aus 40 Nullen bestehende Zeichenkette.
IP-Adressenquelle	Wählen Sie zwischen DHCP und Statisch aus. Wenn DHCP ausgewählt ist, werden die Felder Ethernet-IP-Adresse , Subnetzmaske und Standard-Gateway von einem DHCP-Server abgerufen. Wenn auf dem Netzwerk kein DHCP-Server gefunden werden konnte, werden die Felder auf Null eingestellt. Wenn Statisch ausgewählt ist, werden die Elemente Ethernet-IP-Adresse , Subnetzmaske und Standard-Gateway bearbeitbar.
Ethernet-IP-Adresse	Wenn die IP-Adressenquelle auf DHCP eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse an. Wenn die IP-Adressenquelle auf Statisch eingestellt ist, geben Sie die IP-Adresse ein, die dem iDRAC zugewiesen werden soll. Die Standardeinstellung ist 192.168.0.120 plus die Nummer des Steckplatzes, in dem sich der Server befindet.
MAC-Adresse	Dies ist die nicht bearbeitbare MAC-Adresse der iDRAC-Netzwerkschnittstelle.
Subnetzmaske	Wenn die IP-Adressenquelle auf DHCP eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene Subnetzmaskenadresse an. Wenn die IP-Adressenquelle auf Statisch eingestellt ist, geben Sie die Subnetzmaske für den iDRAC ein. Die Standardeinstellung ist 255.255.255.0 .
Standard-Gateway	Wenn die IP-Adressenquelle auf DHCP eingestellt ist, zeigt dieses Feld die vom DHCP abgerufene IP-Adresse des Standard-Gateways an. Wenn die IP-Adressenquelle auf Statisch eingestellt ist, geben Sie die IP-Adresse des Standard-Gateways ein. Die Standardeinstellung ist 192.168.0.1 .
LAN-Warnung aktiviert	Wählen Sie Ein aus, um die PET-LAN-Warnung (Plattformereignis-Trap) zu aktivieren.

Warnungsregel, Eintrag 1	Wählen Sie Aktivieren oder Deaktivieren aus, um das erste Warnungsziel zu aktivieren.
Warnungsziel 1	Geben Sie die IP-Adresse ein, an die PET-LAN-Warnungen weitergeleitet werden sollen.
Zeichenkette des Host-Namens	Drücken Sie zur Bearbeitung auf <Eingabe>. Geben Sie den Namen des Hosts für PET-Warnungen ein.
DNS-Server von DHCP	Wählen Sie Ein aus, um DNS-Server-Adressen von einem DHCP-Dienst auf dem Netzwerk abzurufen. Wählen Sie Aus aus, um die unten stehenden DNS-Server-Adressen zu bestimmen.
DNS-Server 1	Wenn DNS-Server von DHCP Aus ist, geben Sie die IP-Adresse des ersten DNS-Servers ein.
DNS-Server 2	Wenn DNS-Server von DHCP Aus ist, geben Sie die IP-Adresse des zweiten DNS-Servers ein.
iDRAC-Name registrieren	Wählen Sie Ein , um den iDRAC-Namen im DNS-Dienst zu registrieren. Wählen Sie Aus , wenn Sie nicht möchten, dass Benutzer in der Lage sein sollen, den iDRAC-Namen im DNS zu finden.
iDRAC-Name	Wenn iDRAC-Name registrieren auf Ein eingestellt ist, drücken Sie auf <Eingabe>, um das Textfeld Aktueller DNS-iDRAC-Name zu bearbeiten. Drücken Sie auf <Eingabe>, wenn Sie den iDRAC-Namen fertig bearbeitet haben. Drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln. Der iDRAC-Name muss ein gültiger DNS-Host-Name sein.
Domänenname von DHCP	Wählen Sie Ein aus, wenn Sie den Domännennamen von einem DHCP-Dienst auf dem Netzwerk abrufen möchten. Wählen Sie Aus , wenn Sie den Domännennamen festlegen möchten.
Domänenname	Wenn Domänenname von DHCP Aus ist, drücken Sie auf <Eingabe>, um das Textfeld Aktueller Domänenname zu bearbeiten. Drücken Sie auf <Eingabe>, wenn Sie mit der Bearbeitung fertig sind. Drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln. Der Domänenname muss sich auf eine gültige DNS-Domäne beziehen, wie z. B. meinefirma.com.

Virtueller Datenträger

Verwenden Sie die Tasten <Nach links> und <Nach rechts>, um **Verbunden** oder **Abgetrennt** auszuwählen. Wenn Sie **Verbunden** auswählen, werden die virtuellen Datenträgergeräte mit dem USB-Bus verbunden. Hierdurch werden sie während **Konsolenumleitungs**-Sitzungen verfügbar gemacht.

Wenn Sie **Abgetrennt** auswählen, können Benutzer während **Konsolenumleitungs**-Sitzungen nicht auf virtuelle Datenträgergerät zugreifen.

 **ANMERKUNG:** Um ein USB-Flashlaufwerk mit der Funktion **Virtueller Datenträger** zu verwenden, muss der **Emulationstyp des USB-Flashlaufwerks** im BIOS-Setup-Dienstprogramm auf **Festplatte** eingestellt sein. Sie können auf das BIOS-Setup-Dienstprogramm zugreifen, indem Sie während des Serverstarts auf <F2> drücken. Wenn der **Emulationstyp des USB-Flashlaufwerks** auf **Automatisch** eingestellt ist, erscheint das Flashlaufwerk dem System als Diskettenlaufwerk.

LAN-Benutzerkonfiguration


Der LAN-Benutzer ist das iDRAC-Administratorkonto, das standardmäßig **root** ist. Drücken Sie auf <Eingabe>, um das Untermenü der LAN-Benutzerkonfiguration anzuzeigen. Wenn Sie die Konfiguration des LAN-Benutzers abgeschlossen haben, drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzukehren.

Tabelle 12-2. LAN-Benutzerkonfigurationsseite

Artikel	Beschreibung
Kontozugriff	Wählen Sie Aktiviert aus, um das Administratorkonto zu aktivieren. Wählen Sie Deaktiviert aus, um das Administratorkonto zu deaktivieren.
Kontoberechtigung	Wählen Sie zwischen Admin , Benutzer , Operator und Kein Zugriff aus.
Kontobenutzername	Drücken Sie auf <Eingabe>, um den Benutzernamen zu bearbeiten, und dann auf <Esc>, wenn Sie den Vorgang beendet haben. Der Standardbenutzername ist root .
Kennwort eingeben	Geben Sie das neue Kennwort für das Administratorkonto ein. Die Zeichen werden nicht auf der Anzeige wiedergegeben, während Sie sie eingeben.
Kennwort bestätigen	Geben Sie das neue Kennwort für das Administratorkonto erneut ein. Wenn die eingegebenen Zeichen nicht mit den im Feld Kennwort eingeben eingegebenen Zeichen übereinstimmen, wird eine Meldung angezeigt, und das Kennwort muss erneut eingegeben werden.

Auf Standardeinstellung zurücksetzen

Verwenden Sie das Menü **Auf Standardeinstellung zurücksetzen**, um alle iDRAC-Konfigurationselemente auf die Werkseinstellungen zurückzusetzen. Dies ist eventuell z. B. dann erforderlich, wenn Sie das Kennwort des administrativen Benutzers vergessen haben oder den iDRAC von den Standardeinstellungen neu konfigurieren möchten.

 **ANMERKUNG:** Als Standardkonfiguration ist der iDRAC-Netzwerkbetrieb deaktiviert. Sie können den iDRAC erst dann über das Netzwerk neu konfigurieren, wenn Sie das iDRAC-Netzwerk im iDRAC-Konfigurationshilfsprogramm aktiviert haben.

Drücken Sie auf <Eingabe>, um das Element auszuwählen. Die folgende Warnungsmeldung wird eingeblendet:

Resetting to factory defaults will restore remote Non-Volatile user settings. Continue?

< NO (Cancel) >

< YES (Continue) >

(Durch das Zurücksetzen auf die Werkseinstellungen werden die nichtflüchtigen Remote-Benutzereinstellungen wiederhergestellt. Vorgang fortsetzen?)

< NEIN (Abbrechen) >


< JA (Fortfahren) >

Wählen Sie **JA** aus, und drücken Sie auf <Eingabe>, um den iDRAC auf die Standardeinstellungen zurückzusetzen.

Menü des Systemereignisprotokolls

Das Menü **Systemereignisprotokoll** ermöglicht Ihnen, Meldungen des Systemereignisprotokolls (SEL) anzuzeigen und die Protokollmeldungen zu löschen. Drücken Sie auf <Eingabe>, um das **Menü des Systemereignisprotokolls** anzuzeigen. Das System zählt die Protokolleinträge und zeigt dann die Gesamtanzahl von Einträgen sowie die aktuellste Meldung an. Das SEL speichert maximal 512 Meldungen.

Um SEL-Meldungen anzuzeigen, wählen Sie **Systemereignisprotokoll anzeigen** aus und drücken Sie auf <Eingabe>. Verwenden Sie die Taste <Nach links>, um die vorhergehende (ältere) Meldung zu verschieben, und die Taste <Nach rechts>, um die nächste (neuere) Meldung zu verschieben. Geben Sie eine Eintragsnummer an, um zu diesem Eintrag zu wechseln. Drücken Sie auf <Esc>, wenn Sie mit dem Anzeigen von SEL-Meldungen fertig sind.

 **ANMERKUNG:** Sie können das SEL nur im iDRAC-Konfigurationshilfsprogramm oder in der iDRAC-Webschnittstelle löschen.

Wählen Sie zum Löschen des SEL **Systemereignisprotokoll löschen** aus, und drücken Sie auf <Eingabe>.

Wenn Sie mit der Verwendung des SEL-Menüs fertig sind, drücken Sie auf <Esc>, um zum vorhergehenden Menü zurückzuwechseln.

iDRAC-Konfigurationshilfsprogramm beenden

Wenn Sie mit den Änderungen der iDRAC-Konfiguration fertig sind, drücken Sie auf die Taste <Esc>, um das Menü **Beenden** anzuzeigen.

Wählen Sie **Änderungen speichern und beenden** aus, und drücken Sie dann auf <Eingabe>, um Ihre Änderungen beizubehalten.

Wählen Sie **Änderungen ablehnen und beenden** aus, und drücken Sie auf <Eingabe>, um alle vorgenommenen Änderungen zu ignorieren.

Wählen Sie **Zu Setup zurückwechseln** aus, und drücken Sie auf <Eingabe>, um zum iDRAC-Konfigurationshilfsprogramm zurückzuwechseln.

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

Wiederherstellung und Fehlerbehebung des verwalteten Servers

Integrated Dell™ Remote Access Controller, Firmware-Version 1.00:
Benutzerhandbuch

- [Sicherheit geht vor - für Sie und Ihr System](#)
- [Problemanzeigen](#)
- [Hilfsprogramme zum Lösen von Problemen](#)
- [Fehlerbehebung und häufig gestellte Fragen](#)

In diesem Abschnitt wird erklärt, wie Tasks mithilfe der iDRAC-Einrichtungen ausgeführt werden, die sich auf die Diagnose und die Fehlerbehebung eines im Remote-Zugriff verwalteten Servers beziehen. Er enthält die folgenden Unterabschnitte:

- 1 Problemeanzeigen - hilft Ihnen, Meldungen und andere Systemanzeigen zu finden, die zu einer Problemdiagnose führen können
- 1 Hilfsprogramme zur Problemlösung - beschreibt iDRAC-Hilfsprogramme, die Sie zur Fehlerbehebung des Systems verwenden können
- 1 Fehlerbehebung und häufig gestellte Fragen - Antworten zu typischen Situationen, denen Sie begegnen könnten

Sicherheit geht vor - für Sie und Ihr System

Um bestimmte Verfahren in diesem Abschnitt ausführen zu können, müssen Sie mit dem Gehäuse, dem PowerEdge-Server oder anderen Hardwaremodulen arbeiten. Versuchen Sie nicht, die Hardware des Systems zu warten, es sei denn, Sie befolgen die Erklärungen in diesem Handbuch und an anderer Stelle in Ihrer Systemdokumentation.

⚠ VORSICHT: Viele Arten von Reparaturen dürfen nur von einem zugelassenen Servicetechniker ausgeführt werden. Sie sollten nur Fehlerbehebungsmaßnahmen ausführen und einfache Reparaturen vornehmen, wenn dies in Ihrer Produktdokumentation genehmigt ist, oder wenn Sie online bzw. telefonisch von einem Service- und Support-Team entsprechende Anleitungen erhalten. **Jegliche Schäden, die auf Wartungsmaßnahmen zurückzuführen sind, die nicht von Dell genehmigt wurden, sind nicht durch Ihre Garantie gedeckt.** Lesen und befolgen Sie die Sicherheitshinweise, die mit dem Produkt geliefert wurden.

Problemanzeigen

Die in diesem Abschnitt beschriebenen Anzeichen weisen darauf hin, dass im System ein Problem vorliegen könnte.

LED-Anzeigen

Das anfängliche Anzeichen eines Systemproblems könnte über die LEDs am Gehäuse oder an den im System installierten Komponenten angezeigt werden. Die folgenden Komponenten und Module besitzen Status-LEDs:

- 1 Gehäuse-LCD-Anzeige
- 1 Server
- 1 Lüfter
- 1 CMCs
- 1 E/A-Module
- 1 Netzteile

Die einzelne LED des Gehäuse-LCD fasst den Status aller Komponenten im System zusammen. Eine ständig leuchtende blaue LED des LCD zeigt an, dass auf dem System keine Fehlerzustände festgestellt wurden. Eine blinkende gelbe LED des LCD zeigt an, dass ein Fehlerzustand bzw. mehrere Fehlerzustände festgestellt wurden.

Wenn am Gehäuse-LCD eine gelbe LED blinkt, können Sie über das LCD-Menü herausfinden, welche Komponente fehlerhaft ist. Hilfe bei der Verwendung des LCD finden Sie im *Benutzerhandbuch zu Dell CMC Firmware, Version 1.0*.

[Tabelle 13-1](#) beschreibt die Bedeutungen der LED des PowerEdge-Servers:

Tabelle 13-1. Server-LED-Anzeigen

LED-Anzeige	Bedeutung
ständig grün leuchtend	Der Server ist eingeschaltet. Ein Fehlen der grünen LED bedeutet, dass der Server nicht eingeschaltet ist.
ständig blau leuchtend	Der iDRAC ist fehlerfrei.
gelb blinkend	Der iDRAC hat einen Fehlerzustand festgestellt oder aktualisiert gerade die Firmware.
blau blinkend	Ein Benutzer hat die Locator-ID für diesen Server aktiviert.

Anzeigen für Hardwareprobleme

Anzeichen dafür, dass bei einem Modul ein Hardwareproblem vorliegt, schließen folgende ein:

- 1 Gerät kann nicht hochgefahren werden
- 1 Laute Lüfter
- 1 Verlust der Netzwerkkonnektivität
- 1 Warnungen zu Batterie, Temperatur, Spannung oder Stromüberwachungssensor
- 1 Festplattenfehler
- 1 Fehler des USB-Datenträgers
- 1 Physischer Schaden durch Fallenlassen, Wasser oder andere äußerliche Einwirkung

Sollte ein solches Problem auftreten, können Sie versuchen, es anhand der folgenden Strategien zu beheben:

- 1 Setzen Sie das Modul noch einmal ein, und starten Sie es erneut
- 1 Versuchen Sie, das Modul in einem anderen Schacht des Gehäuses einzusetzen
- 1 Versuchen Sie, Festplatten oder USB-Schlüssel auszutauschen
- 1 Schließen Sie die Strom- und Netzkabel erneut an, oder tauschen Sie sie aus

Wenn das Problem durch Befolgen dieser Schritte nicht behoben werden kann, ziehen Sie das *Hardwarebenutzerhandbuch* zurate, um spezifische Fehlerbehebungsinformationen für das Hardwaregerät zu erhalten.

Weitere Problemanzeigen

Tabelle 13-2. Problemanzeigen

Achten Sie auf Folgendes:	Maßnahme:
Warnungsmeldungen von der Systems Management Software	Siehe Dokumentation zu Systems Management Software.
Meldungen im Systemereignisprotokoll	Siehe Systemereignisprotokoll (SEL) überprüfen .
Meldungen der POST-Codes beim Start	Siehe POST-Codes überprüfen .
Meldungen auf dem Bildschirm Letzter Absturz	Siehe Bildschirm Letzter Systemabsturz anzeigen .
Meldungen im iDRAC-Protokoll	Siehe iDRAC-Protokoll anzeigen .

Hilfsprogramme zum Lösen von Problemen


In diesem Abschnitt werden iDRAC-Einrichtungen beschrieben, die Sie zur Diagnose von Problemen auf dem System verwenden können, besonders wenn Probleme im Remote-Zugriff gelöst werden sollen.




- 1 Überprüfen des Systemzustands
- 1 Systemereignisprotokoll auf Fehlermeldungen überprüfen
- 1 POST-Codes überprüfen
- 1 Bildschirm des letzten Systemabsturzes anzeigen
- 1 iDRAC-Protokoll anzeigen
- 1 Zugriff auf Systeminformationen
- 1 Verwalteten Server im Gehäuse identifizieren
- 1 Diagnosekonsole verwenden
- 1 Netzstrom auf einem Remote-System verwalten

Überprüfen des Systemzustands

Wenn Sie sich an der iDRAC-Webschnittstelle anmelden, beschreibt die erste angezeigte Seite den Zustand der Systemkomponenten. [Tabelle 13-3](#) beschreibt die Bedeutung der Systemzustandsanzeigen.

Tabelle 13-3. Systemzustandsanzeigen

Anzeige	Beschreibung
	Eine grüne Markierung zeigt eine gesunde (normale) Status-Bedingung an.

	Ein gelbes Dreieck, das ein Ausrufezeichen enthält, zeigt eine Warnungs (nichtkritische) -Status-Bedingung an.
	Ein rotes X zeigt eine kritische (Misserfolg) Status-Bedingung an.
	Ein Fragezeichen-Symbol zeigt an, dass der Status unbekannt ist.

Klicken Sie auf der Seite **Funktionszustand** auf eine beliebige Komponente, um Informationen zur Komponente anzuzeigen. Sensormesswerte werden für Batterien, Temperaturen, Spannungen und Stromüberwachung angezeigt, was bei der Diagnose gewisser Problemtypen hilfreich ist. Die Informationsseiten zu iDRAC und CMC bieten nützliche Informationen zu aktuellem Status und Konfiguration.

Systemereignisprotokoll (SEL) überprüfen

Auf der Seite **SEL-Protokoll** werden Meldungen zu Ereignissen angezeigt, die auf dem verwalteten Server auftreten.

Führen Sie zum Anzeigen des **Systemereignisprotokolls** folgende Schritte aus:

1. Klicken Sie auf **System** und dann auf das Register **Protokolle**.
2. Klicken Sie auf **Systemereignisprotokoll**, um die Seite **Systemereignisprotokoll** anzuzeigen.

Die Seite **Systemereignisprotokoll** blendet eine Systemzustandsanzeige (siehe [Tabelle 13-3](#)), einen Zeitstempel sowie eine Beschreibung des Ereignisses ein.

3. Klicken Sie auf die entsprechende Schaltfläche der Seite **Systemereignisprotokoll**, um fortzufahren (siehe [Tabelle 13-4](#)).

Tabelle 13-4. SEL-Seitenschaltflächen

Schaltfläche	Maßnahme
Drucken	Druckt das SEL in der Sortierreihenfolge aus, in der es im Fenster angezeigt wird.
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, über das Sie das SEL 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 herunter, die auf der Microsoft®-Support-Website unter support.microsoft.com verfügbar ist.
Aktualisieren	Lädt die Seite SEL neu.

POST-Codes überprüfen

Die Seite **POST-Code** zeigt den letzten POST-Code des Systems vor dem Start des Betriebssystems an. POST-Codes zeigen den Fortschritt des System-BIOS an, kennzeichnen verschiedene Phasen der Startsequenz von Power-on-Reset und ermöglichen Ihnen, jegliche Fehler bezüglich des Systemstarts zu diagnostizieren.

 **ANMERKUNG:** Zeigen Sie den Text für die Nummern der POST-Code-Meldungen auf der LCD-Anzeige an, oder lesen Sie ihn im *Hardwarebenutzerhandbuch*.

Führen Sie zum Anzeigen der POST-Codes folgende Schritte aus:

1. Klicken Sie auf **System**, das Register **Protokolle** und dann auf **POST-Codes**.


Die Seite **POST-Codes** blendet eine Systemzustandsanzeige (siehe [Tabelle 13-3](#)), einen Hexadezimalcode sowie eine Beschreibung des Codes ein.

2. Klicken Sie auf die entsprechende Schaltfläche der Seite **POST-Code**, um fortzufahren (siehe [Tabelle 13-5](#)).

Tabelle 13-5. POST-Code-Schaltflächen

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

Bildschirm Letzter Systemabsturz anzeigen

 **HINWEIS:** Die Funktion Bildschirm Letzter Absturz muss im Server Administrator und in der iDRAC-Webschnittstelle konfiguriert werden. Anleitungen zur Konfiguration dieser Funktion finden Sie unter [Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz](#).

Auf der Seite **Bildschirm Letzter Absturz** wird der letzte Absturzbildschirm mit Informationen über die Ereignisse vor dem Systemausfall angezeigt. Das Image des letzten Systemabsturzes ist im Persistent Store des iDRAC gespeichert und steht im Remote-Zugriff zur Verfügung.

Zur Ansicht der Seite **Bildschirm Letzter Absturz** führen Sie die folgenden Schritte aus:


1. Klicken Sie auf **System**, das Register **Protokolle** und dann auf **Letzter Absturz**.

Die Seite **Bildschirm Letzter Absturz** führt die in [Tabelle 13-6](#) gezeigten Schaltflächen auf:

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

Tabelle 13-6. Schaltflächen des Bildschirms Letzter Absturz

Schaltfläche	Maßnahme
Drucken	Druckt die Seite Bildschirm Letzter Absturz .
Speichern	Öffnet ein Pop-up-Fenster, über das Sie die Seite Bildschirm Letzter Absturz in einem Verzeichnis Ihrer Wahl speichern können.
Löschen	Löscht die Seite Bildschirm Letzter Absturz .
Aktualisieren	Lädt die Seite Bildschirm Letzter Absturz erneut.

 **ANMERKUNG:** Auf Grund von Schwankungen im Zeitgeber für Autom. Wiederherstellung kann der **Bildschirm Letzter Absturz** eventuell nicht erfasst werden, wenn der System-Reset-Zeitgeber mit einem zu hohen Wert konfiguriert ist. Die Standardeinstellung ist 480 Sekunden. Stellen Sie den System-Reset-Zeitgeber mit dem Server Administrator oder IT Assistent auf 60 Sekunden ein, und vergewissern Sie sich, dass der **Bildschirm Letzter Absturz** korrekt funktioniert. Zusätzliche Informationen erhalten Sie unter [Konfiguration des verwalteten Servers zum Erfassen des Bildschirms Letzter Absturz](#).

iDRAC-Protokoll anzeigen

Das **iDRAC-Protokoll** ist ein beständiges Protokoll, das in der iDRAC-Firmware aufrechterhalten wird. Das Protokoll enthält eine Liste von Benutzermaßnahmen (wie z. B. An- und Abmelden, Änderungen der Sicherheitsregeln) und Warnungen, die vom iDRAC ausgegeben werden. Die ältesten Einträge werden überschrieben, wenn das Protokoll voll wird.

Während das **Systemereignisprotokoll (SEL)** Einträge von Ereignissen enthält, die auf dem verwalteten Server auftreten, enthält das **iDRAC-Protokoll** Einträge von Ereignissen, die im iDRAC auftreten.

Führen Sie zum Zugriff auf das iDRAC-Protokoll folgende Schritte aus:

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

Das iDRAC-Protokoll enthält die Informationen in [Tabelle 13-7](#).

Tabelle 13-7. Informationen zur iDRAC-Protokollseite

Feld	Beschreibung
Datum/Uhrzeit	Datum und Uhrzeit (z. B. 19. Dez. 16:55:47). Der iDRAC stellt seine Uhr nach der Uhr des verwalteten Servers. Wenn der DRAC beim anfänglichen Start nicht mit dem verwalteten Server kommunizieren kann, wird die Zeit als die Zeichenkette Systemstart angezeigt.
Quelle	Die Schnittstelle, die das Ereignis ausgelöst hat.
Beschreibung	Eine kurze Beschreibung des Ereignisses und der Name des Benutzers, der sich am iDRAC angemeldet hat.

Verwendung der Schaltflächen auf der iDRAC-Anmeldeseite

Die Seite **iDRAC-Protokoll** enthält die folgenden Schaltflächen (siehe [Tabelle 13-8](#)):

Tabelle 13-8. Schaltflächen des iDRAC-Protokolls

Schaltfläche	Maßnahme
Drucken	Druckt die Seite iDRAC-Protokoll aus.
Protokoll löschen	Löscht die Einträge des iDRAC-Protokolls. ANMERKUNG: Die Schaltfläche Protokoll löschen erscheint nur, wenn Sie die Berechtigung Protokolle löschen besitzen.

Speichern unter	Öffnet ein Popup-Fenster, das Ihnen ermöglicht, das iDRAC-Protokoll in einem Verzeichnis Ihrer Wahl zu speichern. ANMERKUNG: Wenn Sie Internet Explorer verwenden und beim Speichern auf ein Problem stoßen, laden Sie die kumulative Sicherheitsaktualisierung für Internet Explorer herunter, die auf der Support-Website von Microsoft unter support.microsoft.com verfügbar ist.
Aktualisieren	Lädt die Seite iDRAC-Protokoll neu.

Systeminformationen anzeigen

Die Seite **Systemzusammenfassung** enthält Informationen über die folgenden Systemkomponenten:

- 1 Hauptsystemgehäuse
- 1 Integrierter Dell Remote Access Controller

Klicken Sie zum Zugreifen auf die Systeminformationen auf **System**→ **Eigenschaften**.

Hauptsystemgehäuse

[Tabelle 13-9](#) und [Tabelle 13-10](#) beschreiben die Eigenschaften der Hauptsystemgehäuse.

Tabelle 13-9. Systeminformationsfelder

Feld	Beschreibung
Beschreibung	Gibt eine Systembeschreibung.
BIOS-Version	Führt die System-BIOS-Version auf.
Service-Tag-Nummer	Führt die Service-Tag-Nummer des Systems auf.
Host-Name	Stellt den Namen des Host-Systems zur Verfügung.
BS-Name	Führt das auf dem System ausgeführte Betriebssystem auf.

Tabelle 13-10. Autom. Wiederherstellungsfelder

Feld	Beschreibung
Wiederherstellungsmaßnahme	Wenn festgestellt wird, dass das System <i>hängt</i> , kann der iDRAC zum Ausführen der folgenden Maßnahmen konfiguriert werden: Keine Maßnahme , Hardware-Reset , Herunterfahren oder Aus- und einschalten .
Anfänglicher Countdown	Die Anzahl der Sekunden nach Feststellung eines <i>hängenden Systems</i> , nach denen der iDRAC eine Wiederherstellungsmaßnahme ausführt.
Vorhandener Countdown	Der aktuelle Wert in Sekunden des Countdown-Zeitgebers.

Integrierter Dell Remote Access Controller

In [Tabelle 13-11](#) werden die iDRAC-Eigenschaften beschrieben.

Tabelle 13-11. iDRAC-Informationsfelder

Feld	Beschreibung
Datum/Uhrzeit	Zeigt das aktuelle Datum bzw. die aktuelle Uhrzeit auf dem iDRAC in MGZ an.
Firmware-Version	Führt die Version der iDRAC-Firmware auf.
Firmware aktualisiert	Führt das Datum der letzten Firmware-Aktualisierung auf. Das Datum wird im UTC-Format angezeigt, z. B.: Tue, 8 May 2007, 22:18:21 UTC.
IP-Adresse	Die 32-Bit-Adresse, die die Netzwerkschnittstelle identifiziert. Der Wert wird im <i>Punktrennungs</i> -Format angezeigt, z. B. 143.166.154.127.
Gateway	Die IP-Adresse des Gateways, die als Brücke zu anderen Netzwerken dient. Dieser Wert wird im <i>Punktrennungs</i> -Format angegeben, z. B. 143.166.150.5.
Subnetzmaske	Die Subnetzmaske identifiziert die Abschnitte einer IP-Adresse, bei denen es sich um das erweiterte Netzwerkpräfix und die Host-Nummer handelt. Der Wert wird im <i>Punktrennungs</i> -Format angezeigt, z. B. 255.255.0.0.
MAC-Adresse	Die MAC-Adresse (Medienzugriffssteuerung), die jede NIC im Netzwerk eindeutig identifiziert, z. B. 00-00-0c-ac-08. Hierbei handelt es sich um eine von Dell zugewiesene ID, die nicht bearbeitet werden kann.
DHCP aktiviert	Aktiviert weist darauf hin, dass das dynamische Host-Konfigurationsprotokoll (DHCP) aktiviert ist. Deaktiviert weist darauf hin, dass DHCP <i>nicht</i> aktiviert ist.

Verwalteten Server im Gehäuse identifizieren

In das PowerEdge M1000-e-Gehäuse können bis zu 16 Server eingebaut werden. Um einen bestimmten Server im Gehäuse aufzufinden, können Sie die iDRAC-Webschnittstelle verwenden, um auf dem Server eine blaue, blinkende LED einzuschalten. Wenn Sie die LED einschalten, können Sie die Anzahl von Sekunden festlegen, während denen die LED blinken soll, um sicherzustellen, dass Sie das Gehäuse erreichen können, während die LED noch blinkt. Durch die Eingabe von 0 blinkt die LED so lange weiter, bis Sie sie deaktivieren.

Führen Sie zum Identifizieren des Servers Folgendes aus:

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC**→ **Fehlerbehebung**.
2. Markieren Sie auf der Seite **Identifizieren** das Wertekästchen neben **Server identifizieren**.
3. Geben Sie im Feld **Server-Zeitüberschreitung identifizieren** die Anzahl von Sekunden ein, während denen die LED blinken soll. Geben Sie 0 ein, wenn die LED so lange blinken soll, bis Sie sie deaktivieren.
4. Klicken Sie auf **Anwenden**.

Eine blaue LED auf dem Server wird während der festgelegten Anzahl von Sekunden blinken.

Wenn Sie 0 eingegeben haben, damit die LED weiterblinkt, führen Sie die folgenden Schritte aus, um Sie zu deaktivieren:

1. Klicken Sie auf **System**→ **Remote-Zugriff**→ **iDRAC**→ **Fehlerbehebung**.
2. Heben Sie auf der Seite **Identifizieren** die Markierung des Wertekästchens neben **Server identifizieren** auf.
3. Klicken Sie auf **Anwenden**.

Diagnosekonsole verwenden

Der iDRAC enthält einen Standardsatz von Netzwerkdiagnosehilfsprogrammen (siehe [Tabelle 13-12](#)), die den mit Microsoft® Windows®- oder Linux-basierten Systemen gelieferten Hilfsprogrammen ähnlich sind. Mit der iDRAC-Webschnittstelle können Sie auf die Hilfsprogramme zum Netzwerk-Debuggen zugreifen.

Führen Sie zum Zugriff auf die Seite **Diagnosekonsole** folgende Schritte aus:

1. Klicken Sie auf **System**→ **iDRAC**→ **Fehlerbehebung**.
2. Klicken Sie auf das **Diagnose**-Register.

[Tabelle 13-12](#) beschreibt die Befehle, die auf der Seite **Diagnosekonsole** eingegeben werden können. Geben Sie einen Befehl ein und klicken Sie auf **Senden**. Die Debug-Ergebnisse werden auf der Seite **Diagnosekonsole** angezeigt.

Klicken Sie auf die Schaltfläche **Löschen**, um die durch den vorhergehenden Befehl angezeigten Ergebnisse zu löschen.

Zum Aktualisieren der Seite **Diagnosekonsole** klicken Sie auf **Aktualisieren**.

Tabelle 13-12. 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 Routing-Tabelle.
ping <IP-Adresse>	Überprüft, ob die Ziel-IP-Adresse unter Verwendung des Inhalts der aktuellen Routing-Tabelle vom iDRAC aus erreichbar ist. Ein Ziel-IP-Adresse muss im Feld rechts von dieser Option eingegeben werden. Ein ICMP- (Internetsteuerungsmeldungsprotokoll) Echo-Paket wird zur Ziel-IP-Adresse basierend auf dem aktuellen Inhalt der Routing-Tabelle gesendet.
gettracelog	Zeigt das Ablaufverfolgungsprotokoll des iDRAC an. Weitere Informationen erhalten Sie unter gettracelog .

Netzstrom auf einem Remote-System verwalten

Mit dem iDRAC können im Remote-Zugriff mehrere Stromverwaltungsmaßnahmen auf dem verwalteten Server durchgeführt werden. Verwenden Sie die Seite Stromverwaltung, um während eines Neustarts, und um das System ein- und auszuschalten, ein ordentliches Herunterfahren durch das Betriebssystem durchzuführen.

 **ANMERKUNG:** Sie müssen die Berechtigung **Server-Maßnahmenbefehle ausführen** besitzen, um Stromverwaltungsmaßnahmen auszuführen. Hilfe bei der Konfiguration von Benutzerberechtigungen finden Sie unter [iDRAC-Benutzer hinzufügen und konfigurieren](#).

1. Klicken Sie auf **System** und dann auf das Register **Stromverwaltung**.
2. Wählen Sie eine **Stromsteuerungsmaßnahme** aus, z. B. **System zurücksetzen (Softwareneustart)**. [Tabelle 13-13](#) bietet Informationen zu Stromsteuerungsmaßnahmen.
3. Klicken Sie auf **Anwenden**, um die ausgewählte Maßnahme auszuführen.
4. Klicken Sie zum Fortfahren auf die entsprechende Schaltfläche. Siehe [Tabelle 13-14](#).

Tabelle 13-13. Stromsteuerungsmaßnahmen

System einschalten	Schaltet den Systemstrom ein (äquivalent zum Drücken des Netzschalters, wenn der Serverstrom ausgeschaltet ist).
System ausschalten	Schaltet den Systemstrom ein (äquivalent zum Drücken des Netzschalters, wenn der Serverstrom eingeschaltet ist).
NMI (nicht-maskierbarer Interrupt)	Sendet einen Interrupt hoher Stufe ans Betriebssystem, was dazu führt, dass das System den Vorgang unterbricht, um kritische Diagnose- und Fehlerbehebungsaktivitäten zu ermöglichen.
Ordentliches Herunterfahren	Versucht, das Betriebssystem sauber herunterzufahren und schaltet dann das System aus. Hierfür ist ein ACPI-abhängiges Betriebssystem (Advanced Configuration and Power Interface) erforderlich, das systemgesteuerte Stromverwaltung ermöglicht.
System zurücksetzen (Softwareneustart)	Startet das System neu, ohne es auszuschalten (Softwareneustart).
System aus- und einschalten	Schaltet das System aus und startet es dann neu (Hardwareneustart).

Tabelle 13-14. Schaltflächen der Stromverwaltungs-Seite

Schaltfläche	Maßnahme
Drucken	Drückt die Werte der Stromverwaltung aus, die auf dem Bildschirm angezeigt werden.
Aktualisieren	Lädt die Seite Stromverwaltung erneut.
Anwenden	Speichert alle neuen Einstellungen, die Sie bei der Betrachtung der Seite Stromverwaltung vornehmen.

Fehlerbehebung und häufig gestellte Fragen

[Tabelle 13-15](#) enthält häufig gestellte Fragen zu Fehlerbehebungsproblemen.

Tabelle 13-15. Häufig gestellte Fragen/Fehlerbehebung

Frage	Antwort
Die LED auf dem Server blinkt gelb.	Überprüfen Sie das SEL auf Meldungen, und löschen Sie das SEL dann, um die blinkende LED zu stoppen. Von der iDRAC-Webschnittstelle: <ol style="list-style-type: none">1. Siehe Systemereignisprotokoll (SEL) überprüfen. Vom SM-CLP: <ol style="list-style-type: none">1. Siehe SEL-Management Vom iDRAC-Konfigurationshilfsprogramm: <ol style="list-style-type: none">1. Siehe Menü des Systemereignisprotokolls
Auf dem Server ist eine blaue blinkende LED.	Ein Benutzer hat die Locator-ID für den Server aktiviert. Dies ist ein Signal, das zum Identifizieren des Servers im Gehäuse behilflich ist. Informationen zu dieser Funktion finden Sie unter Verwalteten Server im Gehäuse identifizieren .
Wie kann ich die IP-Adresse des iDRAC finden?	Von der CMC-Webschnittstelle: <ol style="list-style-type: none">1. Klicken Sie auf Gehäuse → Server und dann auf das Register Setup.2. Klicken Sie auf Bereitstellen.3. Lesen Sie die IP-Adresse für Ihren Server aus der angezeigten Tabelle ab. Von der iKVM: <ol style="list-style-type: none">1. Starten Sie den Server neu, und geben Sie das iDRAC-Konfigurationshilfsprogramm durch Drücken auf <Strg><E> ein ODER 1. Warten Sie darauf, dass die IP-Adresse während des BIOS-POST angezeigt wird. ODER

	<p>1 Wählen Sie im OSCAR die "Dell CMC"-Konsole aus, um sich über eine lokale serielle Verbindung am CMC anzumelden.</p> <p>CMC-RACADM-Befehle können über diese Verbindung ausgegeben werden. Eine vollständige Liste der CMC-RACADM-Unterbefehle steht im <i>Benutzerhandbuch zu CMC Firmware, Version 1.0 zur Verfügung</i>.</p>
Wie kann ich die IP-Adresse des iDRAC finden? (fortgesetzt)	<p>Beispiel:</p> <pre>\$ racadm getniccfg -m server-1</pre> <p>DHCP Enabled = 1 IP Address = 192.168.0.1 Subnet Mask = 255.255.255.0 Gateway = 192.168.0.1</p> <p>Von lokalem RACADM:</p> <ol style="list-style-type: none"> Geben Sie den folgenden Befehl an einer Eingabeaufforderung ein: <pre>racadm getsysinfo</pre> <p>Vom LCD:</p> <ol style="list-style-type: none"> Markieren Sie im Hauptmenü das Element Server, und drücken Sie auf die Schaltfläche mit dem Häkchen. Wählen Sie den Server aus, dessen IP-Adresse Sie suchen, und drücken Sie auf die Schaltfläche mit dem Häkchen.
Wie kann ich die IP-Adresse des CMC finden?	<p>Von der iDRAC-Webschnittstelle:</p> <ol style="list-style-type: none"> Klicken Sie auf System → Remote-Zugriff → CMC. <p>Die CMC-IP-Adresse wird auf der Seite Zusammenfassung angezeigt.</p> <p>ODER</p> <ol style="list-style-type: none"> Wählen Sie im OSCAR die "Dell CMC"-Konsole aus, um sich über eine lokale serielle Verbindung am CMC anzumelden. CMC-RACADM-Befehle können über diese Verbindung ausgegeben werden. Eine vollständige Liste der CMC-RACADM-Unterbefehle steht im <i>Benutzerhandbuch zu CMC Firmware, Version 1.0 zur Verfügung</i>. <pre>\$ racadm getniccfg -m chassis</pre> <p>NIC Enabled = 1 DHCP Enabled = 1 Static IP Address = 192.168.0.120 Static Subnet Mask = 255.255.255.0 Static Gateway = 192.168.0.1 Current IP Address = 10.35.155.151 Current Subnet Mask = 255.255.255.0 Current Gateway = 10.35.155.1 Speed = Autonegotiate Duplex = Autonegotiate</p>
Die iDRAC-Netzwerkverbindung funktioniert nicht.	<ol style="list-style-type: none"> Stellen Sie sicher, dass das LAN-Kabel am CMC angeschlossen ist. Stellen Sie sicher, dass das iDRAC-LAN aktiviert ist.
Ich habe den Server in das Gehäuse eingesetzt und den Netzschalter gedrückt, aber nichts ist passiert.	<ol style="list-style-type: none"> Der iDRAC braucht etwa 30 Sekunden, um initialisiert zu werden, bevor der Server hochfahren kann. Warten Sie 30 Sekunden, und drücken Sie dann den Netzschalter noch einmal. Überprüfen Sie das Strombudget des CMC. Das Strombudget für das Gehäuse wurde möglicherweise überschritten.
Ich habe den Benutzernamen und das Kennwort für den iDRAC-Administrator vergessen.	<p>Sie müssen den iDRAC auf seine Standardeinstellungen wiederherstellen.</p> <ol style="list-style-type: none"> Starten Sie den Server neu, und drücken Sie auf <Strg><E>, wenn Sie zur Eingabe des iDRAC-Konfigurationshilfsprogramms aufgefordert werden. Markieren Sie im Menü des Konfigurationshilfsprogramms Auf Standardeinstellung zurücksetzen, und drücken Sie auf <Eingabe>. <p>Weitere Informationen finden Sie unter Auf Standardeinstellung zurücksetzen.</p>
Wie kann ich den Namen des Steckplatzes für meinen Server ändern?	<ol style="list-style-type: none"> Melden Sie sich bei der CMC-Webschnittstelle an. Öffnen Sie die Gehäusestruktur, und klicken Sie auf Server. Klicken Sie auf das Register Setup. Geben Sie den neuen Namen für den Steckplatz in die Zeile für den Server ein. Klicken Sie auf Anwenden.
Wenn eine Konsolenumleitungssitzung von der iDRAC-Webschnittstelle aus gestartet wird, wird ein ActiveX-Sicherheits-Popup eingeblendet.	<p>Der iDRAC ist möglicherweise keine vertrauenswürdige Site für den Client-Browser.</p> <p>Um zu verhindern, dass jedes Mal, wenn Sie eine Konsolenumleitungssitzung beginnen, ein Sicherheits-Popup eingeblendet wird, fügen Sie den iDRAC einfach der Liste vertrauenswürdiger Sites hinzu:</p> <ol style="list-style-type: none"> Klicken Sie auf Extras → Internetoptionen... → Sicherheit → Vertrauenswürdige Sites. Klicken Sie auf Sites, und geben Sie die IP-Adresse oder den DNS-Namen des iDRAC ein. Klicken Sie auf Hinzufügen.
Wenn ich eine Konsolenumleitungssitzung starte, ist der Viewer-Bildschirm leer.	<p>Wenn Sie die Berechtigung Virtueller Datenträger besitzen, jedoch nicht die Berechtigung Konsolenumleitung, können Sie den Viewer starten und hierdurch auf die Funktion des virtuellen</p>

	Datenträgers zugreifen, aber die Konsole des verwalteten Servers wird nicht angezeigt.
Der iDRAC startet nicht.	<p>Entfernen Sie den Server und setzen Sie ihn erneut ein.</p> <p>Überprüfen Sie die CMC-Webschnittstelle, um zu sehen, ob der iDRAC als aktualisierbare Komponente erscheint. Ist dies der Fall, folgen Sie den Anleitungen unter iDRAC-Firmware mittels CMC wiederherstellen.</p> <p>Wird das Problem hierdurch nicht gelöst, setzen Sie sich mit dem technischen Support in Verbindung.</p>
Beim Versuch, den verwalteten Server zu starten, ist die Betriebsanzeige grün, aber es ist überhaupt kein POST bzw. kein Video vorhanden.	<p>Dies kann eintreten, wenn beliebige der folgenden Zustände zutreffen:</p> <ul style="list-style-type: none"> 1 Speicher ist nicht installiert oder ist unzugänglich. 1 Die CPU ist nicht installiert oder ist unzugänglich. 1 Die Video-Riser-Karte fehlt oder ist falsch verbunden. <p>Sehen Sie außerdem nach Fehlermeldungen im iDRAC-Protokoll, von der iDRAC-Webschnittstelle oder vom LCD.</p>

[Zurück zum Inhaltsverzeichnis](#)

[Zurück zum Inhaltsverzeichnis](#)

Glossar

Active Directory

Active Directory ist ein zentralisiertes und standardisiertes System, das Netzwerkverwaltung von Benutzerdaten, Sicherheit und verteilten Ressourcen automatisiert, und Interoperation mit anderen Verzeichnissen aktiviert. Active Directory wird insbesondere für verteilte Netzwerkanschlussumgebungen hergestellt.

AGP

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

ARP

Akronym für Address Resolution Protocol (Adressenauflösungsprotokoll), wobei es sich um eine Methode handelt, die Ethernet-Adresse eines Hosts aus seiner Internet-Adresse zu ermitteln.

ASCII

Akronym für American Standard Code for Information Interchange (US-Standardcode für Informationsaustausch). Eine Codedarstellung zur Anzeige oder zum Drucken von Buchstaben, Zahlen und anderen Zeichen.

BIOS

Akronym für Basic Input/Output System (Grundlegendes Eingabe-/Ausgabesystem), wobei es sich um den Teil der System-Software handelt, der die Schnittstelle unterster Ebene zu Peripheriegeräten darstellt und der die erste Stufe des Systemstartprozesses steuert, einschließlich des Ladens des Betriebssystems in den Speicher.

Bus

Eine Reihe von Leitern, über die verschiedene Funktionseinheiten in einem Computer verbunden sind. Busse werden nach der Art der transportierten Daten benannt, wie z. B. Datenbus, Adressbus oder PCI-Bus.

CA

Eine Zertifizierungsstelle ist ein Geschäftsunternehmen, das in der IT-Industrie dafür anerkannt ist, hohe Standards der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger Sicherheitskriterien zu treffen. Beispiele von CAs schließen Thawte und VeriSign ein. Nachdem die CA Ihre CSR erhält, prüfen und überprüfen die in der CSR enthaltenen Informationen. Wenn der Bewerber die Sicherheitsstandards von CA erfüllt, gibt die CA ein Zertifikat an den Bewerber aus, das diesen Bewerber identifiziert, um Transaktionen über Netzwerke und auf dem Internet vorzunehmen.

CD

Abkürzung für Compact Disc.

CHAP

Akronym für Challenge Handshake Authentication Protocol (Challenge Handshake Authentifizierungsprotokoll), wobei es sich um eine Authentifizierungsmethode handelt, die von PPP-Servern zur Überprüfung der Identität des Herstellers der Verbindung verwendet wird.

CIM

Akronym für das Allgemeine Informationsmodell, das ein für das Verwalten von Betriebssystemen auf einem Netzwerk bestimmtes Protokolle ist.

CLI

Abkürzung für die Befehlszeilenschnittstelle.

CLP

Abkürzung für das Befehlszeilenprotokoll.

CMC

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

CSR

Abkürzung für die Zertifikatssignierungsanforderung.

DDNS

Abkürzung für das dynamische Domänennamenssystem.

DHCP

Abkürzung für Dynamic Host Configuration Protocol (Dynamisches Host-Konfigurationsprotokoll), wobei es sich um ein Protokoll handelt, mit dem IP-Adressen für Computer in einem lokalen Netzwerk dynamisch zugewiesen werden können.

DLL

Abkürzung für die Bibliothek für dynamisches Verbinden, die eine Bibliothek von kleinen Programmen ist, von denen eins, wenn erforderlich, durch ein größeres Programm gerufen werden kann, das im System läuft. Das kleine Programm, das das größere Programm mit einem spezifischen Gerät wie ein Drucker oder Scanner kommunizieren lässt, wird oft als ein DLL-Programm (oder Datei) präsentiert.

DMTF

Abkürzung für Distributed Management Task Force.

DNS

Abkürzung für das Domänennamenssystem.

DSU

Abkürzung für Disk Storage Unit (Festplattenspeichereinheit).

erweitertes Schema

Eine mit Active Directory verwendete Lösung zum Bestimmen von Benutzerzugriffen auf iDRAC; verwendet Dell-definierte Active Directory-Objekte.

FQDN

Akronym für Völlig Qualifizierte Domännennamen. Microsoft ® Active Directory ® unterstützt nur FQDN bis zu maximal 64 Bytes.

FSMO

Flexibler einzelner übergeordneter Vorgang. Dies ist die Art und Weise von Microsoft, die Atomarität des Erweiterungsvorgangs zu garantieren.

GMT

Abkürzung für Greenwich Mean Time (Mittlere Greenwich-Zeit), wobei es sich um die Standard-Uhrzeit handelt, die an jedem Ort der Welt gültig ist. GMT stellt normalerweise die mittlere Sonnenzeit entlang des Nullmeridians dar, der durch das Greenwich Observatory außerhalb von London, GB verläuft.

GPIO

Abkürzung für allgemeine Eingabe/Ausgabe.

GRUB

Akronym für GRand Unified Bootloader, ein neuer und allgemein verwendeter Linux-Lader.

GUI

Abkürzung für Graphical User Interface (Graphische Benutzeroberfläche), die eine Anzeigebereich eines Computers darstellt, in der Elemente wie z. B. Fenster, Dialogfelder und Schaltflächen verwendet werden, im Gegensatz zu einer Befehlsaufforderungsschnittstelle, in der alle Eingaben und Anzeigen als Text dargestellt werden.

Hardwareprotokoll

Zeichnet durch den iDRAC und den CMC erstellte Ereignisse auf.

IAMT

Intel® Active Management Technology - Liefert sicherere Systemverwaltungsfähigkeiten, egal, ob der Computer ein- oder ausgeschaltet ist, und auch dann, wenn das System nicht reagiert.

ICMB

Abkürzung für Intelligent Enclosure Management Bus (Intelligenter Gehäuseverwaltungsbus).

ICMP

Abkürzung für Internet-Steuerungsmeldungsprotokoll.

ID

Abkürzung für Identifier (Bezeichner), wird normalerweise als Bezeichnung für einen Benutzer-Bezeichner (Benutzer-ID) oder Objekt-Bezeichner (Objekt-ID) verwendet.

iDRAC

Abkürzung für den Dell Remote Access Controller 5.

iDRAC

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

IP

Abkürzung für Internet Protocol (Internet-Protokoll), wobei es sich um die Netzwerkschicht für TCP/IP handelt. IP ermöglicht Paket-Routing, Fragmentierung und Reorganisation.

IPMB

Abkürzung für den intelligenten Plattformverwaltungsbus, der ein in der Systemverwaltungstechnologie verwendeter Bus ist.

IPMI

Abkürzung für Intelligent Platform Management Interface (Intelligente Plattformverwaltungsschnittstelle), wobei es sich um einen Teil der Systemverwaltungstechnologie handelt.

Kbps

Abkürzung für Kilobits per Second (Kilobit pro Sekunde), wobei es sich um eine Datentransferrate handelt.

Konsolenumleitung

Konsolenumleitung ist eine Funktion, die den Anzeigebildschirm sowie die Maus- und Tastaturfunktionen eines verwalteten Systems an die entsprechenden Geräte einer Verwaltungsstation umleitet. Sie können dann die Systemkonsole der Verwaltungsstation zur Steuerung des verwalteten Servers verwenden.

LAN

Abkürzung für Local Area Network (Lokales Netzwerk).

LDAP

Abkürzung für das Leichtgewichtsverzeichniszugriffsprotokoll.

LED

Abkürzung für Light-Emitting Diode (Leuchtdiode).

LOM

Abkürzung für Local area network On Motherboard (Lokales Netz auf der Hauptplatine).

MAC

Akronym für Media Access Control (Medienzugriffssteuerung), wobei es sich um eine Netzwerkunterschicht zwischen einem Netzwerkknoten und der physikalischen Netzwerkschicht handelt.

MAC-Adresse

Akronym für Datenträger-Access Control-Adresse, die eine einzigartige in den physischen Komponenten einer NIC eingebettete Adresse ist.

MAPE

Abkürzung für Manageability Access Point (Verwaltungsfunktionenzugriffspunkt).

Mbps

Abkürzung für Megabits per Second (Megabit pro Sekunde), wobei es sich um eine Datentransferrate handelt.

MIB

Abkürzung für Management Information Base (Verwaltungsinformationsbasis).

MI

Abkürzung für Media Independent Interface (Datenträgerunabhängige Schnittstelle).

NAS

Abkürzung für dem Netzwerk beigefügter Speicher.

NIC

Abkürzung für die Netzwerkschnittstellenkarte. Eine in einem Computer installierte Adapterleiterplatte, um eine direktleitende Verbindung zu einem Netzwerk zu bieten.

OID

Abkürzung für Objektbezeichner.

OSCAR

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

PCI

Abkürzung für Peripheral Component Interconnect (Verbindung peripherer Komponenten), wobei es sich um eine Standardschnittstellen- und Bustechnologie zum Anschluss von Peripheriegeräten an ein System und zur Kommunikation mit diesen Peripheriegeräten handelt.

POST

Akronym für Power-On Self-Test (Einschaltselbsttest), wobei es sich um eine Folge von Diagnosetests handelt, die automatisch beim Einschalten eines Systems ausgeführt werden.

PPP

Abkürzung für Point-to-Point Protocol (Punkt-zu-Punkt-Protokoll), wobei es sich um das Standardinternetprotokoll zur Übertragung von Netzwerkschicht-Datagrammen (wie z. B. IP-Pakete) über serielle Punkt-zu-Punkt-Verknüpfungen handelt.

RAC

Abkürzung für Remote Access Controller (Remote Access Controller).

RAM disk

Ein speicherresidentes Programm, das ein Festplattenlaufwerk emuliert. Der iDRAC besitzt eine RAM-Platte im Speicher.

RAM

Akronym für Random-Access Memory (Speicher mit wahlfreiem Zugriff). RAM ist der allgemeine lesbare und beschreibbare Speicher in Systemen und im iDRAC.

ROM

Akronym für Read-Only Memory (Nur-Lesen-Speicher). Speicher, von dem Daten gelesen werden können, auf den jedoch keine Daten geschrieben werden können.

RPM

Abkürzung für Red Hat® Package Manager, der ein Paketverwaltungssystem für das Red Hat Enterprise Linux®-Betriebssystem ist, das bei der Installation von Softwarepaketen hilft. Es ist einem Installationsprogramm ähnlich.

SAC

Akronym für Microsoft Special Administration Console.

SAP

Abkürzung für den Service-Zugriffspunkt.

SEL

Akronym für das Systemereignisprotokoll.

SMI

Abkürzung für das Systems Management Interrrupt.

SMTP

Abkürzung für Simple Mail Transfer Protocol (Einfaches Mail-Übertragungsprotokoll), das verwendet wird, um elektronische Post zwischen Systemen, gewöhnlich über ein Ethernet, zu übertragen.

SMWG

Abkürzung für Systems Management Working Group (Systems Management- Arbeitsgruppe).

SNMP-Trap

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

SSH

Abkürzung für Secure Shell.

SSL

Abkürzung für die Secure Socket Layer (Sichere Sockelschicht).

Standardschema

Eine mit Active Directory verwendete Lösung zum Bestimmen von Benutzerzugriffen auf iDRAC; verwendet nur Active Directory-Gruppenobjekte.

TAP

Abkürzung für Telelocator Alphanumeric Protocol (Telelocator alphanumerisches Protokoll), wobei es sich um ein Protokoll zum Senden von Anfragen an einen Funkrufdienst handelt.

TCP/IP

Abkürzung für Transmission Control Protocol/Internet Protocol (Übertragungssteuerungsprotokoll/Internetprotokoll), das den Standard-Ethernetprotokollsatz repräsentiert, der die Protokolle der Netzwerkschicht und der Übertragungsschicht enthält.

TFTP

Abkürzung für Trivial File Transfer Protocol (Trivial-Dateiübertragungsprotokoll), wobei es sich um ein einfaches Dateiübertragungsprotokoll handelt, das zum Herunterladen von Startcode auf datenträgerlose Geräte oder Systeme verwendet wird.

UPS (USV)

Abkürzung für Unterbrechungsfreie Stromversorgung.

USB

Abkürzung für den Universalen Seriellen Bus.

UTC

Abkürzung für Universal Coordinated Time (Koordinierte Weltzeit). *Siehe* GMT.

verwalteter Server

Der verwaltete Server ist das System, in dem der iDRAC integriert ist.

Verwaltungsstation

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

VLAN

Abkürzung für Virtual Local Area Network (Virtuelles lokales Netzwerk).

VNC

Abkürzung für Virtual Network Computing (Virtueller Netzwerkbetrieb).

VT-100

Abkürzung für Video Terminal 100, das von den meisten allgemeinen Terminal-Emulationsprogrammen verwendet wird.

WAN

Abkürzung für Wide Area Network (Weitbereichsnetzwerk).

[Zurück zum Inhaltsverzeichnis](#)