

Dell Remote Access Controller 4 Firmware Version 1.60 User's Guide

Notes and Notices



NOTE: A NOTE indicates important information that helps you make better use of your computer.



NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

Information in this document is subject to change without notice.

© 2007 Dell Inc. All rights reserved.

Reproduction in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell*, the *DELL* logo, *Dell OpenManage*, *PowerEdge*, and *PowerVault* are trademarks of Dell Inc.; *Microsoft*, *Active Directory*, *Internet Explorer*, *Windows*, *Windows NT*, *Windows Server*, and *MS-DOS* are registered trademarks and *Windows Vista* is a trademark of Microsoft Corporation; *Novell*, *NetWare*, and *SUSE* are registered trademarks of Novell Corporation; *Red Hat* is a registered trademark of Red Hat, Inc.; *UNIX* is a registered trademark of The Open Group in the United States and other countries.

Copyright 1998-2005 The OpenLDAP Foundation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License. A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>. OpenLDAP is a registered trademark of the OpenLDAP Foundation. Individual files and/or contributed packages may be copyrighted by other parties and subject to additional restrictions. This work is derived from the University of Michigan LDAP v3.3 distribution. Information concerning this software is available at <http://www.umich.edu/~dirsvcs/ldap/>. This work also contains materials derived from public sources. Additional information about OpenLDAP can be obtained at <http://www.openldap.org/>. Portions Copyright 1998-2004 Kurt D. Zeilenga. Portions Copyright 1998-2004 Net Boolean Incorporated. Portions Copyright 2001-2004 IBM Corporation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License. Portions Copyright 1999-2003 Howard Y.H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 1998-2003 Hallvard B. Furuseth. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided "as is" without express or implied warranty. Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Contents

1	DRAC 4 Overview	15
	What's New In This DRAC 4 Release?	15
	DRAC 4 Hardware Features	16
	Hardware Specifications	17
	Power Requirements	17
	Connectors	18
	DRAC 4 Ports	18
	Supported Remote Access Connections	19
	DRAC 4 Security Features	19
	Supported Platforms	20
	Supported Operating Systems	20
	Supported Web Browsers	22
	Supported Web Browsers for 64-Bit Operating Systems	23
	Disabling the Whitelist Feature in Mozilla Firefox	23
	Features	24
	Other Documents You May Need	25

2 Installing and Setting Up the DRAC 4 27

Before You Begin	27
Installing the DRAC 4 Hardware	27
Software Installation and Configuration Overview	28
Installing Your DRAC 4 Software	28
Configuring Your DRAC 4 Software	28
Registering the DRAC Host Name With DNS Using DHCP	29
Installing the Software on the Managed System	29
Configuring the Managed System to Capture the Last Crash Screen	30
Disabling the Windows Automatic Reboot Option	31
Installing the Software on the Management Station	31
Installing the racadm CLI on a Red Hat Enterprise Linux Management Station	32
Uninstalling the racadm CLI on a Red Hat Enterprise Linux Management Station	32
Configuring a Supported Web Browser	33
Configuring Your Web Browser to Connect to the Web-Based Interface	33
Viewing Localized Versions of the Web-Based Interface	34
Installing the Sun Java Plug-In	34
Installing the Sun Java Plug-In to Use Console Redirection	34
Installing the Sun Java Plug-In to Use Mozilla	35

Configuring DRAC 4 Properties	37
Configuring the DRAC 4 Network Settings	37
Configuring the DRAC 4 Network Settings	
Using the Option ROM	38
Adding and Configuring DRAC 4 Users	42
Adding and Configuring SNMP Alerts	42
Updating the DRAC 4 Firmware	42
Clearing the Web Browser Cache	
With Internet Explorer	43
Clearing the Web Browser Cache	
With Mozilla	43
Accessing the DRAC 4 Through a Network	43
Accessing the DRAC 4 Using a	
Supported Web Browser	45
Accessing the DRAC 4 Using Server	
Administrator	45
Accessing the DRAC 4 Using racadm CLI	45
DRAC 4 Software Basics for Red Hat	
Enterprise Linux	45
Additional Information	47
Removing the DRAC 4	47
Removing DRAC 4-Related Applications	
and Drivers	47

3	Configuring the DRAC 4 to Use a Serial or Telnet Text Console	49
	Serial and Telnet Console Features	49
	Enabling and Configuring the Managed System to Use a Serial or Telnet Console	50
	Configuring the System Setup Program on the Managed System	50
	Configuring Red Hat Enterprise Linux for Serial Redirection During Boot	51
	Enabling Login to the Console After Boot	53
	Enabling the Serial/Telnet Console on the DRAC 4	56
	Using the racadm Command to Configure the Settings for the Serial and Telnet Console	57
	Using the Secure Shell (SSH)	59
	Enabling SSH	59
	Changing the SSH Port	59
	Supporting Cryptography Schemes	60
	Connecting to the Managed System Through the Local Serial Port or Telnet Management Station (Client System)	61
	Connecting the DB-9 Cable	61

Configuring the Management Station Terminal Emulation Software	62
Configuring Red Hat Enterprise Linux Minicom for Serial Console Emulation	63
Configuring HyperTerminal for Serial Console Redirection	65
Configuring Red Hat Enterprise Linux XTerm for Telnet Console Redirection	66
Enabling Microsoft Telnet for Telnet Console Redirection	66
Using a Serial or Telnet Console	67
4 Managing and Recovering a Remote System 69	
Accessing the Web-Based Interface	69
Logging In	70
Adding and Configuring DRAC 4 Users and Alerts	71
Adding and Configuring DRAC 4 Users	71
Configuring the DRAC 4 NIC	74
Adding and Configuring SNMP Alerts	77
Managing a Remote System	80
Updating the DRAC 4 Firmware	80
Securing DRAC 4 Communications Using SSL and Digital Certificates	81
Viewing System Information	86
Recovering and Troubleshooting the Managed System	89
First Steps to Troubleshoot a Remote System	89
Managing Power on a Remote System	90

Using the SEL	91
Using the DRAC 4 Log	92
Viewing the Last System Crash Screen	93
Using the Diagnostic Console	94
Troubleshooting Network Problems	96
Troubleshooting Alerting Problems	98
Frequently Asked Questions	102
5 Using the DRAC 4 With Microsoft Active Directory	105
Advantages and Disadvantages of Extended Schema and Standard Schema	105
Extended Schema Active Directory Overview	106
Active Directory Schema Extensions	106
Overview of the RAC Schema Extensions	107
Active Directory Object Overview	107
Configuring Active Directory to Access Your DRAC 4	111
Extending the Active Directory Schema	111
Using the Dell Schema Extender	112
Installing the Dell Extension to the Active Directory Users and Computers Snap-In	117
Adding DRAC 4 Users and Privileges to Active Directory	119
Configuring the DRAC 4 with Extended Schema Active Directory and the Web-Based Interface	121
Configuring the DRAC 4 with Extended Schema Active Directory and the racadm CLI	123

	Standard Schema Active Directory Overview	125
	Configuring Standard Schema Active Directory to Access Your DRAC 4	127
	Configuring the DRAC 4 with Standard Schema Active Directory and the racadm CLI	127
	Enabling SSL on a Domain Controller	128
	Exporting the Domain Controller Root CA Certificate	129
	Importing the DRAC 4 Firmware SSL Certificate	130
	Using Active Directory to Log In to the DRAC 4	131
	4096-Bit Key Encryption	131
	Frequently Asked Questions	132
6	Using Console Redirection	135
	Overview	135
	Using Console Redirection	135
	Keyboard, Video, and Mouse Encryption	136
	Opening a Console Redirection Session	136
	Frequently Asked Questions	139
7	Configuring and Using Virtual Media	147
	Overview	147
	Installing the Virtual Media Plug-In	149
	Windows-Based Management Station	149
	Linux-Based Management Station	149

Using the Virtual Media Feature	150
Booting From the Virtual Media	150
Installing Operating Systems Using Virtual Media	151
Using Virtual Media When the Server's Operating System Is Running	152
Enabling and Disabling the Virtual Media Feature	152
Configuring the Virtual Floppy Feature For Your Operating System	153
Configuring the Virtual Floppy Feature as a Super Floppy	154
Configuring the Virtual Floppy as a Hard Drive	154
Frequently Asked Questions	155

8 Using the Serial and racadm Commands 163

Using a Serial or Telnet Console	163
Logging into the DRAC 4	163
Starting a Text Console	164
Viewing a List of Serial/Telnet Commands	164
Using the racadm CLI	166
racadm Command Description	166
racadm Synopsis	167
racadm Options	168
racadm Subcommand Descriptions	169
racadm Error Messages	171

Configuring Multiple DRAC 4s	171
Configuration File Overview	171
Creating a DRAC 4 Configuration File	172
Configuration File Example	176
Using the racadm Utility to Configure the DRAC 4	177
Before Adding a DRAC 4 User	177
Adding a DRAC 4 User Without Alert Capabilities	178
Adding a DRAC 4 User With Alerting Capabilities	179
Adding a DRAC 4 User With Permissions	181
Configuring DRAC 4 Network Properties	181
Frequently Asked Questions	182
9 Troubleshooting	185
Troubleshooting the DRAC 4	185
A racadm Subcommand Man Pages	187
help	187
arp	188
cleararscreen	188
config/getconfig	189
coredump	193
coredumpdelete	195
fwupdate	195

getssninfo	200
getsysinfo	201
getractable	204
ifconfig	205
netstat	205
ping	206
setniccfg/getniccfg	206
getsvctag	208
racdump	208
racreset	209
racresetcfg	211
serveraction	212
getraclog	213
clrraclog	214
getsel	214
clrsel	215
gettracelog	216
setrac	216
sslcsrgen	218
sslcertupload	220
sslcertdownload	221

sslcertview	222
testemail	224
testtrap	225
vmdisconnect	225
B DRAC 4 Property Database Group and Object Definitions	227
idRacInfo	227
cfgLanNetworking	229
cfgCurrentLanNetworking	234
cfgRemoteHosts	236
cfgUserAdmin	238
cfgTraps	242
cfgSessionManagement	244
cfgSerial	246
cfgNetTuning	251
cfgOobSnpmp	257
cfgRacTuning	258
ifcRacManagedNodeOs	262
cfgRacSecurity	263
cfgRacVirtual	266
cfgActiveDirectory	267

cfgStandardSchema	271
Event Filter Operation and Event Mask Properties . . .	273
DRAC 4-Generated Event Mask Definitions	273
System-Generated Alert Mask Definitions	275
Alert Filter Properties	276
Alert Test Commands	276
Glossary	279
Index	287

DRAC 4 Overview

The Dell™ Remote Access Controller 4 (DRAC 4) is a systems management hardware and software solution designed to provide remote management capabilities, crashed system recovery, and power control functions for Dell PowerEdge™ systems.

By communicating with the system's baseboard management controller (BMC), the DRAC 4 can be configured to send you email alerts for warnings or errors related to voltages, temperatures, and fan speeds. The DRAC 4 also logs event data and the most recent crash screen (for systems running the Microsoft® Windows® operating system only) to help you diagnose the probable cause of a system crash.

Depending on your system, the DRAC 4 hardware is either a daughter card (DRAC 4/I) or a half-length PCI card (DRAC 4/P). The DRAC 4/I and DRAC 4/P are identical except for the hardware differences (see "DRAC 4 Hardware Features").

The DRAC 4 has its own microprocessor and memory, and is powered by the system in which it is installed. The DRAC 4 may be preinstalled on your system, or available separately in a kit.

To get started with the DRAC 4, see "Installing and Setting Up the DRAC 4."

What's New In This DRAC 4 Release?

For this release, the DRAC 4 firmware version 1.60:

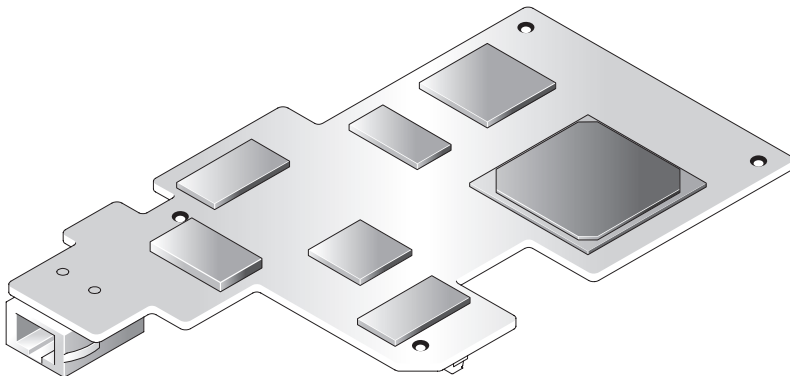
- Supports Microsoft Windows Server® 2008.
- Supports an option to allow users to specify LDAP or Global Catalog servers to handle user authentication.
- Provides the ability to specify a list of LDAP servers and Global Catalog servers.

- Supports a new macro—<RightCtrl> + <ScrLck><ScrLck> key code sequence to initiate a crash dump of the Microsoft Windows operating system. For more information, see the Microsoft Knowledge Base at: <http://support.microsoft.com/kb/256986/>
 - **NOTE:** You must keep the <RightCtrl> key pressed during the additional keystrokes.
- Provides DRAC 4/P support on the Dell PowerVault™ 100.

DRAC 4 Hardware Features

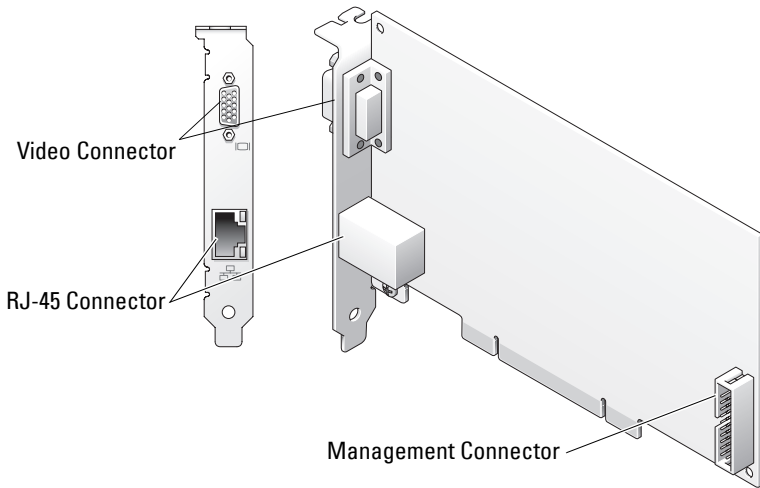
Figure 1-1 shows the DRAC 4/I hardware features and Figure 1-2 shows the DRAC 4/P hardware features.

Figure 1-1. DRAC 4/I Hardware Features



RJ-45 Connector

Figure 1-2. DRAC 4/P Hardware Features



Hardware Specifications


Power Requirements

Table 1-1 lists the power requirements for the DRAC 4.

Table 1-1. DRAC 4 Power Requirements

System Power
1.2 A on +3.3 V AUX (maximum)
550 mA on +3.3 V main (maximum)
0 mA on +5V main (maximum)

Connectors

 **NOTE:** The DRAC 4 hardware installation instructions are located in the *Installing a Remote Access Card* document or the *Installation and Troubleshooting Guide* included with your system. Ensure that you connect the management cable and the local video monitor (if present) to the DRAC 4/P in PCI slot 4.

The DRAC 4 provides a dedicated 10/100 Mbps RJ-45 NIC and a connector for mounting the card to the system board. The DRAC 4/P also provides a video connector, and a 30-pin Management Connector.

DRAC 4 Ports

Table 1-2 identifies the ports used by the DRAC 4. This information is required when opening firewalls for remote access to a DRAC 4.

Table 1-2. DRAC 4 Port Numbers

DRAC 4 Port Number	Used For
Ports on DRAC 4 listening for connection (server):	
22	Secure Shell (configurable)
23	Telnet (configurable)
80	HTTP (configurable)
161	SNMP Agent (not configurable)
443	HTTPS (configurable)
3668	Virtual Media server (configurable)
5869	Remote racadm spcmp server (not configurable)
5900	Console Redirection (configurable)
Ports that DRAC 4 uses as a client:	
25	SMTP (not configurable)
53	DNS (not configurable)
68	DHCP-assigned IP address
69	TFTP (not configurable)
162	SNMP trap (not configurable)
636	LDAP (not configurable)
3269	LDAP for global catalog (GC) (not configurable)

Supported Remote Access Connections

Table 1-3 lists the features of each type of connection.

Table 1-3. Supported Remote Access Connections

Connection	Features
DRAC 4 NIC	<ul style="list-style-type: none">• 10/100 Mbps Ethernet• DHCP support• SNMP traps and email event notification• Dedicated network interface for the DRAC 4 Web-based interface• Support for Telnet console and racadm CLI commands including system boot, reset, power-on, and shutdown commands
Serial port	<ul style="list-style-type: none">• Support for Serial console and racadm CLI commands including system boot, reset, power-on, and shutdown commands• Support for text-only console redirection to a VT-100 terminal or terminal emulator

DRAC 4 Security Features

The DRAC 4 provides the following security features:

- User authentication through Microsoft Active Directory® (optional) or hardware-stored user IDs and passwords
- Role-based authority, which provides each user with specific privileges
- User ID and password configuration through the Web-based interface or racadm CLI
- racadm CLI and Web-based interface operation, which supports 40-bit SSL encryption and 128-bit SSL encryption (for countries where 40-bit is not acceptable).



NOTE: Telnet does not support SSL encryption.

- Session time-out configuration (in minutes) through the Web-based interface or racadm CLI

- Configurable IP ports (where applicable)
- Secure Shell (SSH), which uses an encrypted transport layer for higher security. SSH is available on DRAC 4 firmware 1.40 and later.

Supported Platforms

The DRAC 4/I is supported on the following Dell systems:

- PowerEdge 1850
- PowerEdge 2800
- PowerEdge 2850

The DRAC 4/P is supported on the following systems:

- PowerVault 100
- PowerEdge 800
- PowerEdge 830
- PowerEdge 840
- PowerEdge 850
- PowerEdge 860
- PowerEdge 1800
- PowerEdge 6800
- PowerEdge 6850
- PowerEdge R200

Supported Operating Systems

Table 1-4 lists the operating systems that support the DRAC 4.

See the *Dell Systems Software Support Matrix* located on the Dell Support website at support.dell.com for specific operating system support for each platform listed in "Supported Platforms."

Table 1-4. Supported Operating Systems

Operating System Family	Operating System
Microsoft	Microsoft Windows Server™ 2008 Web, Standard, Enterprise, and Core Edition (x86) Microsoft Windows Server 2008 Standard, Enterprise, DataCenter, and Core Edition (x64) Windows 2000 Advanced Server™ with Service Pack 4 (SP4) Windows Server 2000® with SP4 Windows Server 2003 R2 Enterprise, Standard, and Web Editions with SP2 (32-bit) Windows Server 2003 R2 Standard and Enterprise Edition with SP2 (32-bit x86_64) Windows Server 2003 Standard and Enterprise Editions x64 Editions with SP1 Windows Small Business Server 2003 Standard and Premium Editions Windows Small Business Server 2003 with SP1 Windows Storage Server 2003 R2 Express and Workgroup x64 Editions (x86_64) Windows Vista™

Table 1-4. Supported Operating Systems (continued)

Operating System Family	Operating System
Red Hat®	Enterprise Linux® WS, ES, and AS (version 3) (x86 and x86_64)
	Enterprise Linux WS, ES, and AS (version 4) (ia32 and x86_64)
	Enterprise Linux WS, ES, and AS (version 4) (x86 and x86_64)
	Enterprise Linux WS, ES, and AS (Version 4.5) (x86)
	Enterprise Linux WS, ES, and AS (Version 4.5) (x86_64)
	Enterprise Linux WS and AS (Version 4.5) (ia64)
	Enterprise Linux 5 (x86 and x86_64)
	NOTE: When using DRAC 4 with Red Hat Enterprise Linux (version 5) systems, support is limited to a managed node and racadm CLI; managed console (web-based interface) is not supported.
SUSE®	Linux Enterprise Server 9 with SP3 (x86_64)
	Linux Enterprise Server 9 with Update 2 and 3 (x86_64)
	Linux Enterprise Server 10 with Update 3 (x86_64) Gold

Supported Web Browsers

Table 1-5 lists the Web browsers that support the DRAC 4.

See the *Dell Systems Software Support Matrix* located on the Dell Support website at support.dell.com for the latest information.



NOTE: The Console Redirection feature requires that you install a supported Java Virtual Machine (JVM). For a list of the supported JVM plug-ins, see the DRAC 4 readme on the Dell Support website at support.dell.com on the Systems Management documentation Web page.



NOTICE: The Virtual Media client requires that you use Microsoft Internet Explorer® if using a Windows operating system.

Table 1-5. Supported Web Browsers

Operating System	Supported Web Browser
Windows	Internet Explorer 6.0 (32-bit) with SP2 for Windows XP and Windows 2003 R2 SP2 only. Internet Explorer 7.0 for Windows Vista, Windows XP, and Windows 2003 R2 SP2 only. NOTE: When you are using Internet Explorer on systems running Microsoft Windows, to view localized versions of the DRAC 4 Web-based interface, open the Windows Control Panel , double-click the Regional Options icon, and select the desired locale from the Your locale (location) drop-down menu.
Linux	Mozilla Firefox 1.5 (32-bit) on SUSE Linux (version 10) only. Mozilla Firefox 2.0 (32-bit).

Supported Web Browsers for 64-Bit Operating Systems

If your system is running a supported 64-bit operating system (see Table 1-4), install and run a supported 32-bit Web browser (see Table 1-5). Otherwise, you may experience unexpected results when running Virtual Media and other processes.

If your system is running a supported 64-bit version of Windows, the supported 32-bit version of Internet Explorer is installed by default.

If your system is running a supported 64-bit version of Red Hat Enterprise Linux, install the supported version of Mozilla or Mozilla Firefox. These Web browsers are located on your operating system CDs that are included with your system and on the Mozilla website located at www.mozilla.org/download.html.

Disabling the Whitelist Feature in Mozilla Firefox

Firefox includes a "whitelist" feature that provides additional security. When the whitelist feature is enabled, the browser requires user permission to install plug-ins for each distinct site that hosts the plug-in. This process requires you to install a plug-in for each distinct RAC IP/DNSname, even though the plug-in versions are identical.

To disable the whitelist feature and avoid repetitive, unnecessary plug-in installations, perform the following steps:

- 1 Open a Firefox Web browser window.
- 2 In the address field, type the following and press <Enter>:
`about:config`
- 3 In the **Preference Name** column, locate and double-click `xpinstall.whitelist.required`.
The values for **Preference Name**, **Status**, **Type**, and **Value** change to bold text. The **Status** value changes to **user set** and the **Value** value changes to **false**.
- 4 In the **Preferences Name** column, locate `xpinstall.enabled`.
- 5 Ensure that **Value** is **true**. If not, double-click `xpinstall.enabled` to set **Value** to **true**.

Features

The following is a list of features available on the DRAC 4.

- Dynamic registration of the DRAC 4 name in the Domain Name System (DNS).
- Ability to log into DRAC with a short domain name. If the user domain name does not contain a period (.), then the specified root domain will be appended to the user domain name. For example, if the root domain is set to `xyz.com`, and you try to log in as `abc\username`, the DRAC 4 will take the login name as `username@abc.xyz.com`.
- Remote management and monitoring of a system through the DRAC 4 Web-based interface, serial connection, or telnet connection.
- Configuring Microsoft Active Directory to give you access to the DRAC 4, allows you to add and control the DRAC 4 user privileges of your existing users in your Active Directory.
- Console redirection that allows you to remotely use the managed system keyboard, video, and mouse functions.
- Virtual Media feature that enables the managed system to remotely access a diskette or CD located on the management station.

- Access to the system event log (SEL) and DRAC 4 logs and last crash screen (of the crashed or unresponsive system) independent of the operating system state.
- Integrated launch of the DRAC 4 interface from Server Administrator and IT Assistant.
- Ability to alert you to potential problems on the managed system by sending either an email message or an SNMP trap through the DRAC 4 NIC to a management station.
- Ability to configure the DRAC 4 and update DRAC 4 firmware locally or remotely using the racadm command-line utility, a scriptable interface.
- Ability to perform power management functions, such as shutdown and reset, remotely from a management console.
- Password-level security management and SSL encryption.
- Role-based authority that provides assignable permissions for different systems management tasks.

Other Documents You May Need

In addition to this *User's Guide*, the following documents provide additional information about the setup and operation of the DRAC 4 in your system:

- DRAC 4 online help provides information about using the Web-based interface.
- The *Dell OpenManage IT Assistant User's Guide* and the *Dell OpenManage IT Assistant Reference Guide* provide information about IT Assistant.
- The *Dell OpenManage Server Administrator's User's Guide* provides information about installing and using Server Administrator.
- The *Dell OpenManage Server Administrator SNMP Reference Guide* documents the Server Administrator SNMP management information base (MIB). The MIB defines variables that extend the standard MIB to cover the capabilities of systems management agents.
- The *Dell Systems Software Support Matrix* provides information about the various Dell systems, the operating systems supported by these systems, and the Dell OpenManage components that can be installed on these systems.

The following system documents are also available to provide more information about the system in which your DRAC 4 is installed:

- The *Product Information Guide* provides important safety and regulatory information. Warranty information may be included within this document or as a separate document.
- The *Rack Installation Guide* and *Rack Installation Instructions* included with your rack solution describes how to install your system into a rack.
- The *Getting Started Guide* provides an overview to initially set up your system.
- The *User's Guide* provides information about system features and technical specifications.
- The *Installation and Troubleshooting Guide* describes how to troubleshoot the system and install or replace system components.
- The *Dell OpenManage Server Administrator Compatibility Guide* provides the latest information about supported operating systems and web browsers.
- Systems management software documentation describes the features, requirements, installation, and basic operation of the software.
- Operating system documentation describes how to install (if necessary), configure, and use the operating system software.
- Documentation for any components you purchased separately provides information to configure and install these options.
- Updates are sometimes included with the system to describe changes to the system, software, and/or documentation.



NOTE: Always read the updates first because they often supersede information in other documents.

Release notes or readme files may be included to provide last-minute updates to the system or documentation or advanced technical reference material intended for experienced users or technicians. See your DRAC 4 readme for more information about the DRAC 4. This readme is available on the Dell Support website at support.dell.com along with this guide on the Systems Management documentation Web page.

Installing and Setting Up the DRAC 4

This chapter provides information about how to install and setup your DRAC 4 hardware and software.

Before You Begin

Gather the following items that came with your system prior to installing and configuring the DRAC 4 software.

- DRAC 4 hardware (already installed or in the optional kit)
- The instructions for installing DRAC 4 in this chapter
- *Dell Systems Console and Agent* CD
- *Dell Systems Documentation* CD

Installing the DRAC 4 Hardware



NOTE: The DRAC 4 connection emulates a USB keyboard connection. As a result, when you restart the system, the system will not notify you if your keyboard is not attached.

The DRAC 4 may be preinstalled on your system, or available separately in a kit. To get started with the DRAC 4 that is already installed on your system, see "Software Installation and Configuration Overview."

If a DRAC 4 is not installed on your system, see the *Installing a Remote Access Card* document that came with your DRAC 4 kit or see your platform *Installation and Troubleshooting Guide* for hardware installation instructions before proceeding.



NOTE: Removing expansion cards, such as the DRAC 4, is documented in the *Installation and Troubleshooting Guide* that is included with your system.

Software Installation and Configuration Overview

This section provides a high-level overview of the DRAC 4 software installation and configuration process. Configure your DRAC 4 using the Web-based interface, racadm CLI, or Serial/Telnet console. Network configuration can also be performed using operating system utilities (Option ROM).

For more information about the DRAC 4 software components, see "Installing the Software on the Managed System."



NOTE: For basic information about using the Red Hat Enterprise Linux operating system, see "DRAC 4 Software Basics for Red Hat Enterprise Linux."


Installing Your DRAC 4 Software


To install your DRAC 4 software, perform the following steps in order:

- 1 Update the system BIOS.
- 2 Install the software on the managed system. See "Installing the Software on the Managed System."
- 3 Install the software on the management station. See "Installing the Software on the Management Station."

Configuring Your DRAC 4 Software

To configure your DRAC 4 software, perform the following steps in order:


- 1 Select one of the following configuration tools:
 -  **NOTICE:** Using more than one configuration tool at the same time may generate unexpected results.
 - Web-based interface
 - racadm CLI
 - Serial/Telnet console
 - Operating system utilities (Option ROM)
- 2 Configure the DRAC 4 network settings. See "Configuring the DRAC 4 Network Settings."
- 3 Add and configure DRAC 4 users. See "Adding and Configuring DRAC 4 Users."

- 4 Configure the Web browser to connect to the Web-based interface. See "Configuring a Supported Web Browser."
- 5 Install the Sun Java plug-in. See "Installing the Sun Java Plug-In."
 -  **NOTE:** The Sun Java plug-in is only required if you are using the Console Redirection feature.
- 6 Disable the Windows Automatic Reboot Option. See "Disabling the Windows Automatic Reboot Option."
- 7 Update the DRAC 4 Firmware. See "Updating the DRAC 4 Firmware."
- 8 Access the DRAC 4 through a network. See "Accessing the DRAC 4 Through a Network."

Registering the DRAC Host Name With DNS Using DHCP

In DRAC 4 version 1.40 and later, you can configure your DHCP server to dynamically register the DRAC DNS name in your DNS server database. By enabling encryption in both the DHCP and DNS servers, the DRAC DNS name can be registered in a secure environment.

To configure your DRAC to allow the DHCP server to update the DNS database, set the `cfgNicUseDhcp` object value to 1 (TRUE) and `cfgDNSRegisterRac` object value to 0 (FALSE). With this configuration, the DRAC will supply `cfgDNSRacName` to the DHCP server. See "cfgLanNetworking" for information about these object property settings.

 **NOTE:** When you configure the DRAC, the DHCP server must also be configured to perform the DNS database update.

Installing the Software on the Managed System

Installing software on the managed system is optional. Without the managed system software, you lose the ability to use the `racadm` locally, and for the RAC to capture the last crash screen.

To install the managed system software, install the software on the managed system using the *Dell Systems Console and Agent* CD. For instructions about how to install this software, see your *Quick Installation Guide* or *Server Administrator User's Guide*.

Managed system software will install your choices from the following components on the managed system: the appropriate version of Server Administrator and the appropriate DRAC 4 agent or only the DRAC 4 agent.



NOTE: Do not install the DRAC 4 management station software and the DRAC 4 managed system software on the same system.

Depending on the operating system, the DRAC 4 agent consists of either Microsoft Windows services, Novell NLMs, or Red Hat Enterprise Linux agents. The DRAC 4 agent automatically starts when you boot the managed system. If you install only the DRAC 4 agent, you will not have the ability to view the system's last crash screen or use the Watchdog feature. For more information about the last crash screen, see "Viewing the Last System Crash Screen." For more information about the Watchdog feature, see "System Information."

Configuring the Managed System to Capture the Last Crash Screen

Before the DRAC 4 can capture the last crash screen, configure the managed system with the following prerequisites.

- 1 Install the managed system software. For more information about installing the managed system software, see the *Server Administrator User's Guide*.
- 2 Run a supported Microsoft Windows operating system with the Windows "automatically reboot" feature deselected in the **Windows Startup and Recovery Settings**.
- 3 Enable the watchdog timer and set the watchdog recovery action to **Reset**, **Power Off**, or **Power Cycle**. To configure the watchdog timer, you must use Server Administrator or IT Assistant. For information about how to configure the watchdog timer, see the *Server Administrator User's Guide* or the *IT Assistant User's Guide*. To ensure that the last crash screen can be captured, the watchdog timer must be set to 30 seconds or greater. The default setting is 480 seconds or 8 minutes.

The last crash screen is not available when the Watchdog recovery action is set to **Shutdown** or **Power Cycle** if the managed system is powered off.

Disabling the Windows Automatic Reboot Option

To ensure that the DRAC 4 Web-based interface last crash screen feature works properly, disable the **Automatic Reboot** option on managed systems running the Microsoft Windows Server 2003 and Windows 2000 Server operating systems.

Disabling the Automatic Reboot Option in Windows Server 2003

- 1 Open the Windows **Control Panel** and double-click the System icon.
- 2 Click the **Advanced** tab.
- 3 Under **Startup and Recovery**, click **Settings**.
- 4 Deselect the **Automatically Reboot** check box.

Disabling the Automatic Reboot Option in Windows 2000 Server


- 1 Open the Windows **Control Panel** and double-click the System icon.
- 2 Click the **Advanced** tab.
- 3 Click **Startup and Recovery...**
- 4 Deselect the **Automatically Reboot** check box.

Installing the Software on the Management Station

Your system includes the Dell OpenManage System Management Software Kit. This kit includes, but is not limited to, the following components:

- *Dell Systems Build and Update Utility* CD — A bootable CD that provides the tools you need to install your operating system, configure and update your system. The CD enables you to streamline Dell system deployment and redeployment.
- *Dell Systems Console and Agent* CD — Contains all the latest Dell systems management software products such as Dell OpenManage Server Administrator and console products including Dell OpenManage IT Assistant.
- *Dell Systems Service and Diagnostics Tools* CD — Provides the tools you need to configure your system and delivers the latest BIOS, firmware, diagnostics, and Dell-optimized drivers for your system.


- *Dell Systems Documentation* CD — Helps you stay current with documentation for systems, systems management software products, peripherals, and RAID controllers.

 **NOTE:** Starting with Dell OpenManage version 5.3, you can also obtain all the above components from the *Dell Systems Management Tools and Documentation* DVD and the *Dell Server Updates* DVD.

For instructions about installing Server Administrator software, see your *Server Administrator User's Guide*.

Installing the racadm CLI on a Red Hat Enterprise Linux Management Station

You must install the racadm CLI on a management station running Red Hat Enterprise Linux so that the remote racadm functions can be used.

 **NOTE:** The racadm CLI utility is installed automatically for all other supported operating systems when you install the *Dell Systems Console and Agent* CD.

To install the racadm CLI utility, insert the *Dell Systems Console and Agent* CD in the management station's CD drive and type the following commands from a command prompt:

```
mount /mnt/cdrom
cd /mnt/cdrom
rpm -ivh linux/rac/*.rpm
```

For help with the **racadm** command, type the **man racadm** or **racadm help** command after issuing the previous commands. For more information about the racadm CLI, see "Using the Serial and racadm Commands."

Uninstalling the racadm CLI on a Red Hat Enterprise Linux Management Station

You can uninstall the racadm CLI by issuing the following command from a command prompt:

```
- rpm -e racadm
```


Configuring a Supported Web Browser

The following sections provide instructions for configuring the supported Web browsers. For a list of supported Web browsers, see "Supported Web Browsers."

Configuring Your Web Browser to Connect to the Web-Based Interface

If you are connecting to the DRAC 4 Web-based interface from a management station that connects to the Internet through a proxy server, you must configure the Web browser to access the Internet from this server.

Configuring Internet Explorer

To configure your Internet Explorer Web browser to access a proxy server, perform the following steps:

- 1 Open a Web browser window.
- 1 Click **Tools** and select **Internet Options**.
- 2 From the **Internet Options** window, click the **Connections** tab.
- 3 Under **Local Area Network (LAN) settings**, click **LAN Settings**.
- 4 If the **Use a proxy server** box is selected, select the **Bypass proxy server for local addresses** box.
- 5 Click **OK** twice.

Configuring Firefox

To configure your Firefox Web browser to access a proxy server, perform the following steps:

- 1 Open a Web browser window.
- 1 Click **Tools** and select **Options**.
- 2 From the **Options** window, click **General**.
- 3 In the **General** window in the **Connection** box, click **Connection Settings**.
- 4 In the **Connection Settings** window, select **Manual proxy configuration**.
- 5 Enter the proxy and port information in the appropriate fields.
- 6 Click **OK** twice.

Viewing Localized Versions of the Web-Based Interface

The DRAC 4 Web-based interface is supported on the following Windows operating system languages:

- French
- German
- Spanish
- Japanese
- Simplified Chinese

To view a localized version of the DRAC 4 Web-based interface in Internet Explorer, perform the following steps:

- 1 Click the **Tools** menu and select **Internet Options**.
- 2 In the **Internet Options** window, click **Languages**.
- 3 In the **Language Preference** window, click **Add**.
- 4 In the **Add Language** window, select a supported language.
To select more than one language, press <Ctrl>.
- 5 Select your preferred language and click **Move Up** to move the language to the top of the list.
- 6 Click **OK**.
- 7 In the **Language Preference** window, click **OK**.

Installing the Sun Java Plug-In

All browsers must have the supported Sun Java plug-in 1.4.2 or later installed to use the DRAC 4 Console Redirection feature.

Installing the Sun Java Plug-In to Use Console Redirection

Prior to using Console Redirection on Windows systems, install the supported Sun Java plug-in and clear and disable the Java cache from the Java plug-in control panel.

To install the Sun java plug-in, go to <http://java.sun.com>, download JRE 1.4.2 or later, and follow the instructions on screen.

To clear the Java cache on a Windows operating system, perform the following steps:

- 1 Click **Settings**→**Control Panel**→**Java Plug-in Control Panel**.
- 2 Click the **Cache** tab.
- 3 Click **Clear**.
- 4 Deselect the **Enable Caching** check box to disable cache.
- 5 Click **Apply**.
- 6 Close and restart the browser.

Installing the Sun Java Plug-In to Use Mozilla



NOTE: For a list of the latest supported Java Virtual Machine (JVM) plug-ins, see the **racread.txt** file located on the *Dell Systems Console and Agent CD* or at the Dell Support website at support.dell.com.

You must install the Java plug-in 1.4.2 or later to use the DRAC 4 Virtual KVM feature with the Mozilla Web browser. To install the Java plug-in, perform the following steps:

- 1 Launch the installation script by using the following commands from the script directory:

```
chmod a+x j2re-1_4_<version number>-linux-i586-  
rpm.bin
```

```
./j2re-1_4_<version number>-linux-i586-rpm.bin
```

The script displays a binary license agreement, and prompts you to accept before continuing the installation.

After you accept the license agreement, the installation script creates the following file in the current directory:

```
j2re-1_4_<version number>-linux-i586.rpm
```

- 2 Log in as the root user.

At the command prompt, type:

```
su <power_user_password>
```

- 3 Install the Java plug-in packages that comprise the Java 2 Runtime Environment (JRE).

At the command prompt, type:

```
rpm -iv j2re-1_4<version number>-linux-i586.rpm
```

The Java plug-in packages are installed on your system.

- 4 Delete the symbolic link to the previous Java plug-in version (if applicable).



NOTE: Only one Java plug-in can be registered at a time. If you have never registered a Java plug-in, go to step 5. Otherwise, follow the procedure in this step.

Most Mozilla installations use symbolic links to where the Java plug-in is located. The name of the symbolic link is `libjavaplugin_oji.so`, which is in the `/plugins` subdirectory of Mozilla.

To delete the symbolic link, type:

```
cd /usr/lib/mozilla<version number>/plugins
rm libjavaplugin_oji.so
```

- 5 Register the Java plug-in.

Locate the `libjavaplugin_oji.so` file in the `j2re1.4<version number>` directory. Usually, it is located in the `/i386/ns600` or `/i386/ns610` subdirectory.

- 6 Create a symbolic link to the new Java plug-in.

Use the **create a symbolic link** feature in Mozilla that points to the `libjavaplugin_oji.so` file in the `/i386/ns610` subdirectory.

At the command prompt, type:

```
cd <Mozilla>/plugins
ln s j2re1.4<version number>/plugin/i386/ns610/lib
javaplugin_oji.so libjavaplugin_oji.so
```



NOTE: Create the link using the `/plugins` subdirectory of Mozilla. You cannot create the link from the `<JRE>` directory.

7 Ensure that your updated JRE software is installed and registered on your system.

- a Open a Mozilla Web browser window.
- b In the Web browser window, click **Tools** and select **Web Development**→**Java Console**.

The JRE version is displayed at the top of the **Java Console** window.

If the version that is shown is not the same as the version you downloaded or if the Java Console menu option is grayed out, the software is not registered.

Configuring DRAC 4 Properties

You can configure all of the DRAC 4 properties (network, users, alerts, etc.) using the Web-based interface, or racadm CLI.


For more information about how to use the Web-based interface, see "Accessing the Web-Based Interface." For more information about how to use the racadm CLI through a serial or telnet see "Using the Serial and racadm Commands."

Configuring the DRAC 4 Network Settings

 **NOTICE:** Changing your DRAC 4 Network settings may disconnect your current network connection.

Configure the DRAC 4 network settings using one of the following tools:

- Option ROM — See "Configuring the DRAC 4 Network Settings Using the Option ROM."
- Web-based Interface — See "Configuring the DRAC 4 NIC."
- racadm CLI — See "cfgLanNetworking."

 **NOTE:** If you are deploying the DRAC 4 in a Red Hat Enterprise Linux environment, see "Installing the racadm CLI on a Red Hat Enterprise Linux Management Station."

Configuring the DRAC 4 Network Settings Using the Option ROM

The DRAC 4 contains an integrated NIC with a default IP address of 192.168.0.120 and a default gateway of 192.168.0.1. To use the DRAC 4 IDE Option ROM utility to configure these settings and a limited number of additional DRAC 4 network settings, perform the following steps:

- 1 Access the DRAC 4 IDE Option ROM utility during the managed system's boot process.

Within 5 seconds after the DRAC 4 banner, firmware version, and current NIC IP address appear, press <Ctrl><d>.

The **Setup** screen appears. Below the screen title is the **Network Interface Properties** menu.

- 2 Select and change the DRAC 4 NIC properties (see Table 2-1). The Virtual Media settings are on page two.

Use the following guidelines when changing the DRAC 4 NIC properties:

- Use the <Page Up> and <Page Down> keys to move between the two pages.
- All menu selections are not case sensitive.
- Type one-key stroke selections.



NOTE: When modifying any of the following options, press <Esc> while typing the value to avoid modifying the current value. If you press <Option Edit> and it toggles a setting (changes the setting between only two possible values), press <Option Edit> again to change the value back to the original setting. Pressing <Esc> will not undo a modification after you type a new value. Toggle options are not affected when you press <Esc>.

Table 2-1. DRAC 4 IDE Option ROM Utility Properties

Properties	Description
NIC Current TCP/IP Configuration	Displays the current IP address, netmask, and gateway assigned to the DRAC 4 from the DHCP server. NOTE: If DHCP is enabled on the card and the DHCP system is not working properly, the category displays Unavailable for each option, and the following message blinks below the option labels: Waiting for response from DHCP Server

Table 2-1. DRAC 4 IDE Option ROM Utility Properties (continued)

Properties	Description
DNS Current Configuration	Displays the current IP address assigned to the DHCP server.
NIC TCP/IP Configuration Options	
Use DHCP is:	Indicates whether the DHCP system has assigned the DRAC 4 IP address or whether the DRAC 4 is using a preset static IP address. The available settings are Enabled and Disabled . Press <d> to toggle the setting. When this option is selected, the other options in this group are grayed out.
Static IP-Addr	Indicates the preset static DRAC 4 IP address if DHCP is disabled. The default address is 192.168.0.120. Press <i> to change this address.
Static Netmask	Indicates the preset static masked DRAC 4 IP address if DHCP is disabled. The default is 255.255.255.0. Press <n> to change this mask.
Static Gateway	Indicates the preset static gateway (router or switch address) of the DRAC 4 address if DHCP is disabled. The default is 192.168.0.1. Press <g> to change the address.
Ethernet Configuration Options	
NIC is:	Indicates whether the DRAC 4 NIC setting is Enabled or Disabled . Press <e> to toggle the setting. When selected, the DRAC 4 NIC can be used for remote access. You must select this option to be able to configure the remaining options on this screen.
Auto-Negotiate is:	Indicates whether the DRAC 4 automatically configures LAN speed and duplex settings. The available settings are Enabled and Disabled . If this option is not selected, the user settings are used. Press <a> to toggle the setting.
LAN Speed Setting	Indicates the DRAC 4 NIC communications speed. The available settings are 10 Base-T and 100 Base-T . 10 Base-T represents a communication speed of 10 Mb per second. 100 Base-T represents a speed of 100 Mb per second. Press <s> to toggle this setting. This option is not available when the Auto Negotiate setting is enabled.

Table 2-1. DRAC 4 IDE Option ROM Utility Properties (continued)

Properties	Description
LAN Duplex Setting	Indicates the DRAC 4 NIC duplex setting. The available settings are Half Duplex and Full Duplex . When set to Half Duplex , the NIC communicates in one direction at a time, indicating that the NIC can only receive or transmit information at any given moment. When set to Full Duplex , the NIC communicates in both directions simultaneously. Press <x> to toggle to this setting. This option is not available when the Auto Negotiate setting is enabled.
DNS Configuration Options	
Servers from DHCP	The available settings are Disabled and Enabled . Press <u> to toggle the setting. The default setting is Disabled , which indicates that the DRAC 4 is using preset static IP addresses. When this option is selected, the DHCP server provides the DNS server IP addresses. If Use DHCP (described earlier in this table) is set to Disabled , this option is grayed out and you cannot modify this field.
Static DNS Server 1:	Indicates the preset static IP address of the first DNS server that the DRAC 4 uses if Servers from DHCP is disabled. The default is 192.168.0.5. Press <1> to change this address. If Servers from DHCP is Enabled , this option is grayed out and you cannot modify this field.
Static DNS Server 2:	Indicates the preset static IP address of the second DNS server that the DRAC 4 uses if Servers from DHCP is disabled. The default is 192.168.0.6. Press <2> to change this address. If you do not have a second DNS server, you may enter 0.0.0.0 for the IP address. If Servers from DHCP is Enabled , this option is grayed out and you cannot modify this field.
Register RAC Name	The available settings are Disabled and Enabled . Press <c> to toggle the setting. The default setting is Disabled . The default RAC name is <i>RAC-service tag</i> , where <i>service tag</i> is the service tag number of the Dell server (for example, RAC-EK00002). When this option is selected, the RAC name is displayed. You can modify the RAC name only when toggling from the Disabled setting . If this option is set to Enabled , you can modify the RAC name by pressing <c> twice.

Table 2-1. DRAC 4 IDE Option ROM Utility Properties (continued)

Properties	Description
Static Domain Name	The default setting is Disabled . The default static domain name is MYDOMAIN . Press <f> to toggle the setting. When this option is selected, the static domain name is displayed. You can modify the domain name only when toggling from the Disabled setting by pressing <f>. However, if Use DHCP (described earlier in this table) is set to Disabled , you cannot set Static Domain Name to Disabled . If Register RAC Name is Disabled , this option is grayed out and you cannot modify this field.

Virtual Media Configuration Options

Virtual Media is: Indicates whether Virtual Media is enabled or disabled. Press <e> to toggle the setting.

3 When finished, do one of the following:

- Press <Esc> to cancel all changes and exit the **Setup** menu.
- Press <r> to save the changes and reboot the DRAC 4.

The following message appears:

```
IMPORTANT: In order for your changes to take
effect, they need to be saved. Your computer will
then continue booting normally.
```


```
Would you like to save the changes and continue
now (<Y> or <N>)?
```


Or if Virtual Media settings have changed, the following message appears:

```
IMPORTANT: In order for your changes to take
effect, they need
to be saved. For Virtual Media settings to take
effect, a reboot is required.
```

```
Would you like to save the changes and reboot now
(<Y> or <N>)?
```

4 Press <Y> to save the changes or <N> to return to the setup menu.

 **NOTE:** When the DRAC 4 registers with the DNS server, it adds an extra line with a long string of characters. This TXT entry in the database is an encrypted string that is used to uniquely identify the owner of the DDNS entry and to serialize update operations. The TXT entry is associated with the RAC DDNS name.


 **NOTE:** The DRAC 4 DDNS implementation requires that DNS servers be configured to allow non-secure updates.

Adding and Configuring DRAC 4 Users

Add and configure DRAC 4 users using one of the following tools:

- Web-based interface — See "Adding and Configuring DRAC 4 Users."
- racadm CLI — See "cfgUserAdmin."


Adding and Configuring SNMP Alerts

 **NOTE:** DRAC 4 Alert information in Management Information Base (MIB) format is located in the **rac_host MIB**.


Add and configure SNMP alerts using one of the following tools:

- Web-based Interface — See "Adding and Configuring SNMP Alerts."
- racadm CLI — See "cfgTraps."

Updating the DRAC 4 Firmware


 **NOTICE:** Updating your DRAC 4 firmware may disconnect your current network connection.

Use one of the following methods to update your DRAC 4 firmware.

 **NOTE:** You must add and configure a DRAC 4 user before using the Web-based interface, racadm CLI, or Serial/Telnet consoles to update your firmware.

- Web-based Interface — See "Updating the DRAC 4 Firmware."
- racadm CLI — See "fwupdate."

- Repair utility (diskette-based update): This update restores all DRAC 4 configurations back to factory defaults. Go to the Dell Support website at support.dell.com, download the appropriate DRAC 4 firmware image file, and follow the instructions to create two diskettes. Insert the first diskette into the system to be updated and follow the instructions on the screen.

 **NOTICE:** The Repair utility is only supported when used locally.

After you perform a firmware upgrade, perform the following instructions to clear the Web browser cache to ensure that all new Web-based interface pages are loaded.

Clearing the Web Browser Cache With Internet Explorer

- 1 From the drop-down menu, select **Tools**→**Internet Options**.
- 2 In the **Internet Options** window under **Temporary Internet Files**, click **Delete Files**.
- 3 Click the **Delete all offline content** box.
- 4 Click **OK** twice.
- 5 Close and restart the browser.

Clearing the Web Browser Cache With Mozilla

- 1 From the drop-down menu, select **Edit Preferences**.
- 2 In the **Preferences** window, select **Advance**→**Cache**.
- 3 Click **Clear Disk Cache**.
- 4 Click **Clear Memory Cache**.
- 5 Click **OK**.
- 6 Close and restart the browser.

Accessing the DRAC 4 Through a Network

This section provides information about how to access the DRAC 4 after you install the hardware and configure the software.

After you configure the DRAC 4, you can remotely access the managed system using one of the DRAC 4 interfaces listed in Table 2-2.

Table 2-2. DRAC 4 Interfaces

Interface	Description
Web-based interface	Connects to the managed system using a supported Web browser through the DRAC 4 NIC. For a list of supported Web browsers, see "Supported Web Browsers."
racadm CLI	<p>Connects to the managed system using a remote console. You can execute racadm commands (racadm remote capability option [-r]) or connect to the management station using its IP address.</p> <p>NOTE: The racadm remote capability is supported only on management stations. For more information, see "Supported Web Browsers."</p> <p>NOTE: When using the racadm remote capability, you must have write permission on the folders where you are using the racadm subcommands involving file operations, for example:</p> <pre>racadm getconfig -f <file name></pre> <p>or:</p> <pre>racadm sslcertupload -t 1 -f c:\cert\cert.txt subcommands</pre>
Telnet Console	Provides access through the DRAC 4 to the server COM1 port, video, and hardware management interfaces through the DRAC 4 NIC and provides support for serial and racadm commands including powerdown , powerup , powercycle , hardreset , graceshutdown , and gracereboot commands.
SSH Interface	Provides the same capabilities as the telnet console using an encrypted transport layer for higher security.
Terminal Emulation Software	Provides access through the DRAC 4 to the server COM1 port and hardware management interfaces through the serial connector. The terminal emulation software provides support for serial and racadm commands including powerdown , powerup , powercycle , hardreset , graceshutdown , and gracereboot commands.



NOTE: The DRAC 4 default user name is `root` and the default password is `calvin`.

You can access the DRAC 4 Web-based interface through the DRAC 4 NIC by using a supported Web browser, or through Server Administrator or IT Assistant.

Accessing the DRAC 4 Using a Supported Web Browser

- 1 Open a Web browser window.
- 2 In the **Address** field, type the DRAC 4 IP address.
- 3 Log in with your DRAC 4 user name and password.

The default user name and password are `root` and `calvin`, respectively.

See the remote access interface online help for more information.

Accessing the DRAC 4 Using Server Administrator

- 1 Launch Server Administrator.
- 2 In the **Server Administrator** home page system tree in the left window pane, click **System**→**Main System Chassis**→**Remote Access Controller**.

See your Server Administrator User's Guide for more information about using the Server Administrator remote access features.

Accessing the DRAC 4 Using racadm CLI

See "Using the Serial and racadm Commands" for information about accessing the DRAC 4 using the racadm CLI.

DRAC 4 Software Basics for Red Hat Enterprise Linux

The DRAC 4 is supported on precompiled kernels that are a part of the Red Hat Enterprise Linux distribution. The DRAC 4 is not supported on recompiled kernels with other configuration options (for example, kernels configured for performance-tuning purposes).



NOTICE: Red Hat Enterprise Linux may fail to load when started on recompiled kernels. If this situation occurs, you must either restore the kernel and modules from backup, or you must reinstall the kernel from the Red Hat Package Manager (RPM).

The following list describes basic software information for using a DRAC 4 with the Red Hat Enterprise Linux operating system:

- To verify that the DRAC 4 event server for the managed system is loaded, type the following command:

```
service racsvc status
```

- To start, stop, get status of, restart, or reload the racsvc service, type the following command:

```
service racsvc <action>
```

where <action> is start, stop, status, or probe.

- For additional information on one of the three DRAC 4 services, type the following command:

```
man racsvc
```



NOTE: All three services (racser, racsvc, and racvnc) start automatically when they are installed and when the system is booted. These services stop automatically when they are uninstalled or when the system is shut down.

- To determine which version of a particular RPM package you have installed, use a package management tool such as GnoRPM, or use the RPM query command (`rpm -q`).

For example:

```
rpm -q <package_name>
```

- To determine which files were installed and where they are located, type the following command:

```
rpm -ql <package_name>
```

- To remove a package, type the following command:

```
rpm -e <package_name>
```

Additional Information

Removing the DRAC 4

See the *Installation and Troubleshooting Guide* included with your system for information about removing expansion cards, such as the DRAC 4.

Removing DRAC 4-Related Applications and Drivers

- 1** Remove the RAC module included with Server Administrator by uninstalling Server Administrator.
 - a** Click **Start** and select **Settings**→**Control Panel**→**Add or Remove Programs**.
 - b** In the **Add or Remove Programs** window, select and uninstall **Server Administrator**.
- 2** Remove the RAC drivers in Device Manager.
 - a** Right click **My Computer** and select **Properties**.
 - b** In the **System Properties** window, click the **Hardware** tab.
 - c** In the **Hardware** tab in the **Device Manager** box, click **Device Manager**.
 - d** In the **Device Manager** window, locate and uninstall the following drivers:
 - Remote Access Controller — RAC Virtual UART Port
 - System Devices — RAC PCI Function 0
 - System Devices — RAC PCI Function 2
- 3** If using Extended Schema Active Directory, review all Active Directory RAC Objects associated with the removed DRAC 4 expansion card to ensure proper security.

Configuring the DRAC 4 to Use a Serial or Telnet Text Console

The DRAC 4 provides serial and telnet command interfaces designed to perform all of the configuration and systems management functions using the DRAC 4 Web-based interface or `racadm` CLI.

This section provides information about the serial/telnet text console features, and explains how to set up your system so you can perform systems management actions through a serial/telnet console.


Serial and Telnet Console Features

The DRAC 4 supports the following serial and telnet console redirection features:

- One serial client connection and up to four telnet client connections at one time
- Access to the managed system consoles through the system serial port and through the DRAC 4 NIC
- Serial/telnet console commands that allow you to power-on, power-off, power-cycle, reset, view logs, view sensor status, or configure the DRAC 4
- Serial/telnet console support for the `racadm` command, which is useful for scripting
- Command-line editing and history
- The `connect com2` serial command to connect, view, and interact with the managed system text console that is being output through a serial port (including BIOS and the operating system)





NOTE: If you are running Red Hat Enterprise Linux on the managed system, the `connect com2` serial command provides a true Red Hat Enterprise Linux console stream interface.

- Menu-based VT-100 block screen interface that provides easy operation of commonly used commands including reset, power-on, and power-off
 -  **NOTE:** Because the **racadm** command does not have access to a file system on a serial or telnet console, several options (such as reading or writing a file) are not supported by the **racadm** command through a serial or telnet console. For more information about supported **racadm** commands for the serial and telnet consoles, see "Using the Serial and racadm Commands."
- Optional idle timeout setting on SSH connections for enhanced security, which is controlled by the "cfgSsnMgtSshTelnetIdleTimeout (Read/Write)" object

Enabling and Configuring the Managed System to Use a Serial or Telnet Console


This section provides information about enabling and configuring a serial/telnet console on the managed system.

 **NOTE:** The **connect com2** serial command requires that the **Serial Port** setting under the BIOS setup group **Integrated Devices** be set to **RAC**. When a telnet session is established to the DRAC 4 and the setting of this serial port is not **RAC**, **connect com2** yields a blank screen.

 **NOTE:** The **connect com2** serial command is not supported on systems running the Novell NetWare operating system.

Configuring the System Setup Program on the Managed System

Perform the following steps to configure your System Setup program to redirect output to a serial port.


 **NOTE:** You must configure the System Setup Program in conjunction with the **connect serial/telnet** command.


- 1 Turn on or restart your system.
- 2 Press <F2> immediately after you see the following message:

```
<F2> = System Setup
```
- 3 Scroll down and select **Integrated Devices** by pressing <Enter>.
- 4 In the submenu, scroll down to **Serial Port 1** and set to **RAC**.
- 5 Scroll down and select **Console Redirection**.

- 6 Set the **Console Redirection** screen to the following settings:
Console Redirection – Serial Port 1
Redirection After Boot – Disabled
- 7 Press <Esc> to exit the System Setup program to complete the System Setup program configuration.

Configuring Red Hat Enterprise Linux for Serial Redirection During Boot

 **NOTE:** The following instructions are specific to the Red Hat Enterprise Linux GRand Unified Bootloader (GRUB). Similar changes would be necessary for using a different boot loader.

 **NOTE:** In configuring the client VT100 emulation window, you must set the window or application that is displaying the redirected console to 25 rows x 80 columns to ensure proper text display; otherwise, some text screens may be garbled.

Edit the `/etc/grub.conf` file by performing the following steps. The sample file (see Table 3-1) shows the changes described in this procedure.

- 1 Add the following two new lines in the *general settings* section of the file:

```
serial --unit=0 --speed=57600
terminal --timeout=10 serial
```
- 2 Append two options to the kernel line:

```
kernel ..... console=ttyS0,57600
```
- 3 If the `/etc/grub.conf` contains a `splashimage` directive, comment it out of the file.

Table 3-1. Sample File: /etc/grub.conf

```
# grub.conf generated by anaconda
#
Note that you do not have to rerun grub after making
changes to this file
# NOTICE: You do not have a /boot partition. This
means that
#         all kernel and initrd paths are relative
to /, e.g.

#         root (hd0,0)
#         kernel /boot/vmlinuz-version ro root=
/dev/sda1
#         initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=0 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
    root (hd0,0)
    kernel /boot/vmlinuz-2.4.9-e.3smp ro root=
/dev/sda1 hda=ide-scsi console=tty0 console=
ttyS0,57600
    initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3
    root (hd0,00)
    kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
    initrd /boot/initrd-2.4.9-e.3.im
```

Additional information for editing the `grub.conf`:

- You may need to disable GRUB's graphical interface and use the text-based interface; otherwise, the GRUB screen will not be displayed in RAC console redirection. To do so, comment out the line starting with `splashimage`.
- If you have multiple options in GRUB and you want all of them to start a console session through the RAC serial connection, add `console=ttyS1,57600` to all options. The example in Table 3-1 shows `console=ttyS0,57600` added to only the first option.

Enabling Login to the Console After Boot

Edit the file `/etc/inittab` by adding the following new line to configure a `getty` on the COM1 serial port:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS0 vt100
```

The sample file (see Table 3-2) shows the new line.

Table 3-2. Sample File: /etc/inittab

```
#

# inittab      This file describes how the INIT
process should set up
#              the system in a certain run-level.

#
# Author:      Miquel van Smoorenburg,
<miquels@drinkel.nl.mugnet.org
#              Modified for RHS Linux by Marc Ewing
and Donnie Barnes
#

# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if
you do not have
#     networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6
```

Table 3-2. Sample File: /etc/inittab (continued)

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we
have a few
# minutes of power left. Schedule a shutdown for 2
minutes from now.
# This does, of course, assume you have power
installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power
Failure; System Shutting Down"
# If power was restored before the shutdown kicked
in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power
Restored; Shutdown Cancelled"

# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Edit the file `/etc/securetty` by adding a new line with the name of the serial tty for COM1:

```
ttyS1
```

The sample file (see Table 3-3) shows the new line.


Table 3-3. Sample File: `/etc/securetty`

```
vc/1  
vc/2  
vc/3  
vc/4  
vc/5  
vc/6  
vc/7  
vc/8  
vc/9  
vc/10  
vc/11  
tty1  
tty2  
tty3  
tty4  
tty5  
tty6  
tty7  
tty8  
tty9  
tty10  
tty11  
ttyS1
```


Enabling the Serial/Telnet Console on the DRAC 4

You can enable the serial/telnet console locally or remotely.

Enabling the Serial/Telnet Console Locally

 **NOTE:** You (the current user) must have **Configure DRAC 4** permission in order to perform the steps in this section.

To enable the serial/telnet console from the managed system, type the following local `racadm` CLI commands from a command prompt.


 **NOTE:** For detailed information about how to use the `racadm` CLI, **serial/telnet**, and **racadm** commands, see "Using the Serial and `racadm` Commands."

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1
```

Enabling the Serial/Telnet Console Remotely

To enable the serial/telnet console remotely, type the following remote `racadm` commands from a command prompt:

```
racadm -u <username> -p <password> -r <DRAC 4 IP
address> config -g cfgSerial cfgSerialConsoleEnable 1
racadm -u <username> -p <password> -r <DRAC 4 IP
address> config -g cfgSerial cfgSerialTelnetEnable 1
```

 **NOTE:** Use the DRAC 4 IP address for your managed system; not **192.168.10.1** as shown in the example.

```
racadm -u root -p calvin -r 192.168.10.1 config -g
cfgSerial -o cfgSerialConsoleEnable 1
racadm -u root -p calvin -r 192.168.10.1 config -g
cfgSerial -o cfgSerialTelnetEnable 1
```

Using the `racadm` Command to Configure the Settings for the Serial and Telnet Console

This subsection provides steps to configure the default configuration settings for serial/telnet console redirection. To configure the settings, type the `racadm config` command with the appropriate group, object, and object value(s) for the setting that you want to configure. For a complete list of available serial/telnet and `racadm` CLI commands, see "Using the Serial and `racadm` Commands."

You can type `racadm` commands locally or remotely. When using `racadm` commands remotely, include the user name, password, and managed system DRAC 4 IP address.

Using racadm Locally

To type **racadm** commands locally, type the commands from a command prompt on the managed system:

```
racadm config -g <group> -o <object> <value>
```

Using racadm Remotely

To use **racadm** commands remotely, type the commands from a command prompt on a management station with the following syntax:

```
racadm -u <username> -p <password> -r <DRAC 4 IP address> config -g <group> -o <object> <value>
```

Displaying Configuration Settings

To display the current settings for a particular group, type the following command from the command prompt on the managed system:

```
racadm getconfig -g <group>
```

For example, to display a list of all of the settings for the **cfgSerial** group, type the following:

```
racadm getconfig -g cfgSerial
```

To display the current settings for a particular group remotely, type the following from a remote command prompt:

```
racadm -u <user> -p <password> -r <DRAC 4 IP address> getconfig -g cfgSerial
```

For example, to display a list of all of the settings for the **cfgSerial** group remotely, type the following from a management station:

```
racadm -u root -p calvin -r 192.168.0.1 getconfig -g cfgSerial
```


Configuring the Telnet Port Number

Type the following command to change the telnet port number on the DRAC 4.


```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <new port number>
```

Using the Secure Shell (SSH)

Secure Shell (SSH) is a command line session that includes the same capabilities as a telnet session, but with higher security. The DRAC 4 supports SSH version 2 with password authentication. SSH is enabled on the DRAC 4 when you install or update your DRAC 4 firmware.

 **NOTE:** SSH is not available for the first fifteen minutes of operation after installing/updating the DRAC 4 firmware. During this time the host keys are generated internally. No intervention is required for host key generation. If this operation is interrupted for any reason, key generation will start again when the DRAC 4 is restarted.

You can use either PuTTY or OpenSSH on the management station to connect to the managed system's DRAC 4.

 **NOTE:** Run OpenSSH from a VT100 or ANSI terminal emulator on Windows. Running OpenSSH at the Windows command prompt does not result in full functionality (for example, some keys do not respond and no graphics are displayed).

Only one SSH session is supported at any given time. The session timeout is controlled with the `cfgSsnMgtSshTelnetIdleTimeout` object as described in the "DRAC 4 Property Database Group and Object Definitions."

Enabling SSH

You can enable the SSH on the DRAC 4 with the following command:

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Changing the SSH Port

You can change the SSH port with the following command:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort  
0x<port number>
```

For more information on `cfgSerialSshEnable` and `cfgRacTuneSshPort` objects, see "DRAC 4 Property Database Group and Object Definitions."

Supporting Cryptography Schemes

The DRAC 4 SSH implementation supports multiple cryptography schemes:

- Asymmetric Cryptography:
 - Diffie-Hellman DSA/DSS 512-1024 (random) bits per NIST specification
- Symmetric Cryptography:
 - AES256-CBC
 - RIJNDAEL256-CBC
 - AES192-CBC
 - RIJNDAEL192-CBC
 - AES128-CBC
 - RIJNDAEL128-CBC
 - BLOWFISH-128-CBC
 - 3DES-192-CBC
 - ARCFOUR-128
- Message Integrity:
 - HMAC-SHA1-160
 - HMAC-SHA1-96
 - HMAC-MD5-128
 - HMAC-MD5-96
- Authentication:
 - Password
 - SSHv2 (SSHv1 is not supported)

Connecting to the Managed System Through the Local Serial Port or Telnet Management Station (Client System)

The managed system provides access between the DRAC 4 and the serial port on your system to enable you to power on, power off, or reset the managed system and access logs.

The serial console is available on the DRAC 4 through the managed system external serial connector. Only one serial client system (management station) can be active at any given time.

The telnet and SSH consoles are available on the DRAC 4 through the DRAC 4 NIC. Up to four telnet client systems and one SSH client can connect at any given time.

The management station connection to the managed system serial or telnet console requires the use of management station terminal emulation software (see "Configuring the Management Station Terminal Emulation Software" for more information).

The following subsections explain how to connect your management station to the managed system through a managed system external serial port using terminal software and a null modem cable, or by telnet using terminal software through the managed system DRAC 4 NIC.

Connecting the DB-9 Cable

To connect to the managed system using a serial text console, connect a DB-9 null modem cable to the COM port that you are using on the managed system. Not all DB-9 cables carry the pinout/signals necessary for this connection. The DB-9 cable for this connection must conform to the specification shown in Table 3-4.



NOTE: You can also use this cable for BIOS text console redirection with the DRAC 4 serial console disabled.

Table 3-4. Required Pinout for DB-9 Null Modem Cable

Signal Name	DB-9 Pin (server pin)	DB-9 Pin (workstation pin)
FG (Frame Ground)	–	–
TD (Transmit data)	3	2
RD (Receive Data)	2	3
RTS (Request To Send)	7	8
CTS (Clear To Send)	8	7
SG (Signal Ground)	5	5
DSR (Data Set Ready)	6	4
CD (Carrier Detect)	1	4
DTR (Data Terminal Ready)	4	1 and 6

Configuring the Management Station Terminal Emulation Software

Your DRAC 4 supports a serial or telnet text console from a management station running one of the following types of terminal emulation software:

- Red Hat Enterprise Linux Minicom in an Xterm
- Hilgraeve’s HyperTerminal Private Edition (version 6.3)
- Red Hat Enterprise Linux Telnet in an Xterm
- Microsoft Telnet

Perform the steps in the following subsections to configure your type of terminal software. Configuration is not required when using Microsoft Telnet.

Configuring Red Hat Enterprise Linux Minicom for Serial Console Emulation

Minicom is the serial port access utility for Red Hat Enterprise Linux. The following steps are valid for configuring Minicom version 1.8. Other Minicom versions may differ slightly but require the same basic settings. Use the information in "Required Minicom Settings for Serial Console Emulation" to configure other versions of Minicom.


Configuring Minicom Version 1.8 for Serial Console Emulation



NOTE: To ensure that the text displays properly, Dell recommends that you use an Xterm window to display the telnet console instead of the default window provided by the Red Hat Enterprise Linux installation.

- 1 To start a new Xterm session, type `xterm &` at the command prompt.
- 2 In the Xterm window, move your mouse arrow to the lower right-hand corner of the window and resize the window to 80 x 25.
- 3 If you do not have a Minicom configuration file, go to the next step.
If you have a Minicom configuration file, type `minicom <Minicom config file name>` and skip to step 17.
- 4 At the Xterm command prompt, type `minicom -s`.
- 5 Select **Serial Port Setup** and press <Enter>.
- 6 Press <a> and select the appropriate serial device (for example, `/dev/ttySo`).
- 7 Press <e> and set the **Bps/Par/Bits** option to 115200 8N1.
- 8 Press <f> and set **Hardware Flow Control** to **Yes** and set **Software Flow Control** to **No**.
- 9 To exit the **Serial Port Setup** menu, press <Enter>.
- 10 Select **Modem and Dialing** and press <Enter>.
- 11 In the **Modem Dialing and Parameter Setup** menu, press <Backspace> to clear the **init**, **reset**, **connect**, and **hangup** settings so that they are blank.
- 12 Press <Enter> to save each blank value.
- 13 When all specified fields are clear, press <Enter> to exit the **Modem Dialing and Parameter Setup** menu.
- 14 Select **Save setup as config_name** and press <Enter>.

- 15 Select **Exit From Minicom** and press <Enter>.
- 16 At the command shell prompt, type `minicom <Minicom config file name>`.
- 17 To expand the Minicom window to 80 x 25, drag the corner of the window.
- 18 To exit Minicom, press <Ctrl+a>, <z>, <x>.

 **NOTE:** If you are using Minicom for serial text console redirection to configure the managed system BIOS, it is recommended that you turn on color in Minicom. To turn on color, at the command prompt type `minicom -c on`.

Ensure that the Minicom window displays a command prompt such as `[DRAC 4\root]#`. When the command prompt appears, your connection is successful and you are ready to connect to the managed system console using the **connect** serial command.

Required Minicom Settings for Serial Console Emulation

Use Table 3-5 to configure any version of Minicom.

Table 3-5. Minicom Settings for Serial Console Emulation

Setting Description	Required Setting
Bps/Par/Bits	115200 8N1
Hardware flow control	Yes
Software flow control	No
Terminal emulation	ANSI
Modem dialing and parameter settings	Clear the init , reset , connect , and hangup settings so that they are blank
Window size	80 x 25 (to resize, drag the corner of the window)

Configuring HyperTerminal for Serial Console Redirection

HyperTerminal is the Microsoft Windows serial port access utility. To set the size of your console screen appropriately, use Hilgraeve's HyperTerminal Private Edition version 6.3.

To configure HyperTerminal for serial console redirection, perform the following steps:

- 1 Start the HyperTerminal program.
- 2 Type a name for the new connection and click **OK**.
- 3 Next to **Connect using**, select the COM port on the management station (for example, COM2) to which you have connected the DB-9 null modem cable and click **OK**.
- 4 Configure the COM port settings as shown in Table 3-6.


Table 3-6. Management Station COM Port Settings

Setting Description	Required Setting
Bits per second:	115200
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	Hardware


- 5 Click **OK**.
- 6 Click **File**, select **Properties**, and click the **Settings** tab.
- 7 Set the **Telnet terminal ID:** to **ANSI**.
- 8 Click **Terminal Setup** and set **Screen Rows** to **26**.
- 9 Set **Columns** to **80** and click **OK**.

The HyperTerminal window displays a command prompt, such as [DRAC 4\root]#. When the command prompt appears, your connection is successful and you are ready to connect to the managed system console using the **connect com2** serial command.

Configuring Red Hat Enterprise Linux XTerm for Telnet Console Redirection

 **NOTE:** When you are using the `connect com2` command through a telnet console to display the System Setup screens, set the terminal type to **ANSI** in System Setup and for the telnet session.

To run telnet on a system running Red Hat Enterprise Linux, perform the following steps:


 **NOTE:** To ensure that the text is properly displayed, Dell recommends that you use an Xterm window to display the telnet console instead of the default window provided by the Red Hat Enterprise Linux installation.

- 1 Start a new Xterm session by typing `xterm &` at the command prompt.
- 2 Drag the lower right-hand corner of the window to resize it to 80 x 25 prior to using telnet. This can be done by dragging the lower-right-corner with the mouse.

Red Hat Enterprise Linux Xterm is now ready to connect by telnet to the managed system DRAC 4.

To connect to the DRAC 4, at the Xterm prompt, type `telnet <DRAC 4 IP address>`.

Enabling Microsoft Telnet for Telnet Console Redirection

 **NOTE:** Some telnet clients on Microsoft operating systems may not display the BIOS setup screen correctly when BIOS console redirection is set for VT100 emulation. If this issue occurs, you can correct the display by changing BIOS console redirection to ANSI mode. From the BIOS setup menu, select **Console Redirection** → **Remote Terminal Type** → **ANSI**.

Microsoft telnet requires that you first enable **Telnet in Windows Component Services**.

After telnet is enabled, connect to the DRAC 4 by performing the following steps:


- 1 Open a command prompt.
- 2 Type the following and press <Enter>:


```
telnet <IP address>:<port number>
```

where <IP address> is the IP address for the DRAC 4 and <port number> is the telnet port number (if it has been changed).

Using a Serial or Telnet Console

 **NOTE:** If you are running Windows XP or Windows 2003 and experience problems with characters in a DRAC 4 telnet session, navigate to the Microsoft Support website located at support.microsoft.com website and search for Knowledge Base article 824810, which provides a hot fix for this issue. This problem may manifest itself as an apparently frozen login (the return key does not respond and the password prompt does not appear).

 **NOTE:** On a management station running Windows 2000, pressing the <F2> key does not enter the BIOS setup. To resolve this issue, use the telnet client that is included with the Windows Services for UNIX[®] 3.5 (a recommended free download from Microsoft). Browse to www.microsoft.com/downloads/ and search for "*Windows Services for UNIX 3.5*."

 **NOTE:** When a telnet login attempt is invalid, a single session is counted toward the maximum of four sessions for approximately one minute after the invalid login attempt. If three valid sessions exist, this invalid session will prevent further login attempts for that minute.

Serial and **telnet** commands, and **racadm** CLI can be typed in a serial or telnet console. These commands can be executed on the server locally or remotely. The local **racadm** CLI is installed for use as a root user only. For more information about the **serial/telnet** commands and **racadm** CLI, see "Using the Serial and **racadm** Commands."

Managing and Recovering a Remote System

The DRAC 4 provides a Web-based interface and the racadm CLI (command-line interface), which allows you to perform the following tasks:

- Configure the DRAC 4 properties and users
- Perform remote management tasks
- Troubleshoot a remote (managed) system for problems

For routine systems management, use the DRAC 4 Web-based interface.

This section provides information about how to perform common systems management tasks with the DRAC 4 Web-based interface and provides links to the information you may need.

All Web-based interface configuration tasks can also be performed with the racadm CLI. For a list of all racadm CLI and serial/telnet console commands that can be used to perform the text-based equivalents of each task, see "Using the Serial and racadm Commands."



NOTE: When using the Web-based interface, see the DRAC 4 online help for context sensitive information about each Web-based interface page.

Accessing the Web-Based Interface

To access the DRAC 4 Web-based interface, perform the following steps:

- 1 Open a supported Web browser window.
See "Supported Web Browsers" for more information.
- 2 In the **Address** field, type the following and press <Enter>:

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

where <IP address> is the IP address for the DRAC 4 and <port number> is the HTTPS port number (if it has been changed).

The DRAC 4 **Log in** window appears.

Logging In



NOTE: To log in, you must have **Log In to DRAC 4** permission.

You can log in as either a DRAC 4 user or as a Microsoft® Active Directory® user. The default user name and password is **root** and **calvin**, respectively.

To log in, perform the following steps:

- 1 In the **User Name** field, type one of the following:

- Your DRAC 4 user name.

For example:

john_doe

The DRAC 4 user name for local users is case sensitive.

- Your Active Directory user name.

For example,

<domain>\<username>, *<domain>/<username>* or
<user>@<domain>

Examples of an Active Directory user name are: **dell.com\john_doe** or
john_doe@dell.com.

- 2 In the **Password** field, enter your DRAC 4 user password or Active Directory user password. This field is case sensitive.
- 3 Click **OK** or press **<Enter>**.

Logging Out

Click **Log Out** in the upper-right corner of the main window.



NOTE: The **Log Out** button does not appear until you log in.

Adding and Configuring DRAC 4 Users and Alerts

To manage your system with the DRAC 4, you can create unique users with specific administrative permissions (role-based authority). Additionally, you can configure alerts that are emailed to different users.

This subsection provides instructions about how to perform the following tasks:

- Adding and Configuring DRAC 4 Users
- Configuring the DRAC 4 NIC
- Adding and Configuring SNMP Alerts

Adding and Configuring DRAC 4 Users

- 1 Click the **Configuration** tab and select **Users**.
- 2 In the **User Name** column, click [Available].
- 3 Use the **Add/Configure DRAC 4 User** page to configure the user name, password, access permissions, and email alert settings for a new or existing DRAC 4 user.

Configuring a New User Name and Password

Use Table 4-1 to configure a new or existing DRAC 4 user name and password.

Table 4-1. User Properties

Property	Description
User Name	Specifies a DRAC 4 user name. After you enter a user name, it cannot be changed. Each user must be created with a different user name. NOTE: User names on the local DRAC 4 must not contain the / (forward slash) or . (period) characters.
Password	Specifies or edits the DRAC 4 user's password.
Confirm New Password	Requires you to retype the DRAC 4 user's password to confirm.

Configuring User Permissions

Under **User Permissions**, click the **User Group** drop-down menu and select the user's permissions group.

Use Table 4-2 to determine the **User Group** (permissions) for the user.

Table 4-2. User Group Permissions

User Group	Permissions Granted
Administrator	Login to DRAC, Configure DRAC, Configure Users, Clear Logs, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts, Execute Diagnostic Commands, and receive email alerts (if Enabled)
Power User	Login to DRAC, Clear Logs, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts, and receive email alerts (if Enabled)
Guest User	Login to DRAC, and receive email alerts (if Enabled)
email Alerts Only	Receive email alerts (if Enabled)
Custom	Allows you to select any combination of the following permissions: Login to DRAC, Configure DRAC, Configure Users, Clear Logs, Execute Server Action Commands, Access Console Redirection, Access Virtual Media, Test Alerts, Execute Diagnostic Commands, and receive email alerts (if Enabled)

Configuring User email Alerts

Enabling User email Alerts

Use the information in Table 4-3 to enable email alerts.

Table 4-3. Enable email Alert Properties

Property	Description
Enable email Alerts	Enables the DRAC 4 email alerts feature and allows you to select which events, according to their severity, will cause an email alert to be sent.
email Address	Allows you to specify the email address to which alerts are sent.
Message	Allows you to specify the email message text.

Configuring email Alerts by Severity

The information under **email Alerts** in the Web-based interface enables you to select the events—according to their severity—that generate an email alert. Select the severity of the temperature, voltage, fan, or miscellaneous sensor for the generated e-mail alert. You can specify three severities:

- **Informational** (lowest severity)
- **Warning** (medium severity)
- **Severe** (highest severity)

Alerts will be sent to the email address you typed in **Enabling User email Alerts**.

Table 4-4 provides descriptions for each e-mail alert severity.

Table 4-4. email Alert Severity

Severity	Description
Informational	The DRAC 4 sends an alert if the corresponding event listed under Alert Description occurs with an Informational severity.
Warning	The DRAC 4 sends an alert if the corresponding event listed under Alert Description occurs with a Warning severity.
Severe	The DRAC 4 sends an alert if the corresponding event listed under Alert Description occurs with a Severe severity.
Alert Description	<p>Lists the following events monitored by the DRAC 4. A specified alert (either Informational, Warning, or Severe) is sent when the event is triggered at the level of severity you selected in the check boxes to the left.</p> <ul style="list-style-type: none">• Select All — Monitors all of the sensors available on the system.• System Temperature Sensors — Monitors the system temperature sensors.• System Voltage Sensors — Monitors the system voltage sensors.• System Fan Sensors — Monitors the system fan speed in rpm.• System Miscellaneous Sensors — Monitors other available system sensors such as chassis intrusion.

Table 4-4. email Alert Severity (continued)

Severity	Description
Apply Changes	Adds a new DRAC 4 user or commits changes made to the current DRAC 4 user.
Go Back To User Configuration Page	Opens the DRAC 4 Users page.

Printing the Page

Click the **Print** button in the top-right corner of the screen to print the Add/Configure DRAC 4 User page.

Configuring the DRAC 4 NIC

- 1 Click the **Configuration** tab and select **Network**.
- 2 In the **Network Configuration** page, configure the DRAC 4 NIC settings and configure email alert settings.

Table 4-5 describes the **Network Configuration** page settings.
Table 4-6 describes the **Network Configuration** page buttons.



NOTE: You must have **Configure DRAC 4** permission to change the **Network Configuration** page settings.



NOTE: Most DHCP servers require a server to store a client identifier token in its reservations table. The client (DRAC 4, for example) must provide this token during DHCP negotiation. For RACs, the DRAC 4 supplies the client identifier option using a one-byte interface number (0) followed by a six-byte MAC address.

Table 4-5. DRAC 4 Network Configuration Page Settings

Setting	Description
MAC Address	Displays the DRAC 4 MAC address.
Enable NIC (default: Enabled)	Enables the DRAC 4 NIC and activates the remaining controls in this group.
Use DHCP (For NIC IP Address) (default: Disabled)	Enables Dell OpenManage™ Server Administrator to obtain DRAC 4 NIC IP address from the Dynamic Host Configuration Protocol (DHCP) server. Selecting the check box deactivates the Static IP Address , Static Gateway , and Static Subnet Mask controls.

Table 4-5. DRAC 4 Network Configuration Page Settings (continued)

Setting	Description
Static IP Address	Specifies or edits the static IP address for the DRAC 4 NIC. To change this setting, you must first deselect the Use DHCP (For NIC IP Address) check box.
Static Gateway	Specifies or edits the static gateway for the DRAC 4 NIC. To change this setting, deselect the Use DHCP (For NIC IP Address) check box.
Static Subnet Mask	Specifies or edits the static subnet mask for the DRAC 4 NIC. To change this setting, deselect the Use DHCP (For NIC IP Address) check box.
Use DHCP to obtain DNS server addresses (default: Disabled)	Enables the primary and secondary DNS server to obtain their IP addresses from the DHCP server, rather than the static settings.
Static Preferred DNS Server	Uses the primary DNS server IP address only when Use DHCP to obtain DNS server addresses is not selected.
Static Alternate DNS Server	Uses the secondary DNS server IP address only when Use DHCP to obtain DNS server addresses is not selected. You can enter an IP address of 0.0.0.0 if you do not have an alternate DNS server.
Register DRAC 4 on DNS (default: Disabled)	Registers the DRAC 4 name on the DNS server.
DNS DRAC 4 Name	Displays the DRAC 4 name only when Register DRAC 4 on DNS is selected. The default DRAC 4 name is RAC-service tag , where <i>service tag</i> is the service tag number of the Dell server (for example, RAC-EK00002).
Use DHCP for DNS Domain Name (default: Disabled)	Uses the default DNS domain name. When the check box is not selected and the Register DRAC 4 on DNS option is selected, you can modify the DNS domain name in the DNS Domain Name field.
DNS Domain Name	The default DNS domain name is MYDOMAIN . When the Use DHCP for DNS Domain Name check box is selected, this option is grayed out and you cannot modify this field.


Table 4-5. DRAC 4 Network Configuration Page Settings (continued)

Setting	Description
Auto Negotiation	Determines whether the DRAC 4 automatically sets the Duplex Mode and Network Speed by communicating with the nearest router or hub (On) or allows you to set the Duplex Mode and Network Speed manually (Off).
Duplex Mode	Sets the duplex mode to full or half to match your network environment. This option is not available if Auto Negotiation is set to On .
Network Speed	Sets the network speed to 100 Mb or 10 Mb to match your network environment. This option is not available if Auto Negotiation is set to On .
GUI Session Timeout	Specifies the time (from 5 to 60 minutes in 5-minute intervals) before the session screen is locked. You must re-type your password to unlock and resume the session.
Apply	Saves the changes made to the network configuration.
Email Alert Settings	Enables email messaging and activates the SMTP (email) Server Address control.
Enable Email Alerts (check box is selected: default)	Enables email messaging.
SMTP (Email) Server Address	Specifies the SMTP server IP address that receives e-mails sent by the DRAC 4.


Table 4-6. DRAC 4 Network Configuration Page Buttons

Button	Action
Print	Prints the Network Configuration page
Refresh	Reloads the Network Configuration page
Apply	Saves the changes made to the network configuration.

Adding and Configuring SNMP Alerts


 **NOTE:** You must have **Configure DRAC 4** permission to add or delete an SNMP alert; otherwise, these options will not be available.

- 1 Click the **Configuration** tab and select **Alerts**.
- 2 In the **Add/Configure SNMP Alerts** page, add, delete, configure, and test the SNMP alerts.

 **NOTE:** The DRAC 4 supports three severity levels: **Informational**, **Warning**, and **Severe**. Some events support only the informational severity level because they deliver only a message.

Adding an Alert

- 1 Locate an available **Destination IP Address** in the **Destination IP Address** column.

 **NOTE:** If all **Destination IP Addresses** are filled with existing IP addresses, you have configured all of your existing alerts and must delete one to continue.

- 2 Click **[Available]** to open the **Add/Configure SNMP Alerts** page.
- 3 Use Table 4-7 to configure the following properties under **General**.

Table 4-7. Alert Properties

Property	Description
Enable SNMP Alert	Enables the current SNMP alert.
Community	Specifies or edits the community name to which the destination IP address belongs.
IP Address	Specifies or edits the destination IP address to which the alert is sent.
Apply Changes	Commits changes made to the current alert.
Go Back To SNMP Alerts Page	Returns you to the Configure SNMP Alerts page.

Configuring Alerts by Severity

- 1 Use the **Severity Configuration** section to select which events, according to their severity, will cause an SNMP alert to be sent to the IP address you typed in **Configuring Alert Properties**.
- 2 Select the severity of the sensor for which you want an SNMP alert generated.
- 3 Use Table 4-8 to decide which events you want to cause an SNMP alert.

Table 4-8. Severity Options

Option	Description
Informational	The DRAC 4 sends an alert if the corresponding event listed under Alert Description occurs with a severity of Informational (lowest severity).
Warning	The DRAC 4 sends an alert if the corresponding event listed under Alert Description occurs with a severity of Warning (medium severity).
Severe	The DRAC 4 sends an alert if the corresponding event listed under Alert Description occurs with a severity of Severe (highest severity).
Alert Description	<p>Lists the following events monitored by the DRAC 4. An alert (specified as either informational, warning, or severe) is sent when the event is triggered at the level of severity you selected in the check boxes to the left.</p> <p>NOTE: For information about how to manage events, see the <i>Server Administrator User's Guide</i>.</p> <ul style="list-style-type: none">• Select All — Monitors all of the sensors available on the system.• System Temperature Sensors — Monitors the temperature sensors on the system.• System Voltage Sensors — Monitors the voltage sensors on the system.• System Fan Sensors — Monitors the system fan speed (RPM).• System Miscellaneous Sensors — Monitors other available system sensors such as chassis intrusion.

Viewing Information About Existing Alerts

Click an alert in the **SNMP Alert List** to display the properties for existing SNMP alerts. See Table 4-9 for descriptions.



NOTE: During the first 40 seconds after a DRAC 4 reset, the DRAC 4 is synchronizing with the system BMC and the managed system service. If an alert is generated during this time, some of the values may be reported as "unknown." The time field contains the number of seconds since DRAC 4 startup. After synchronization has completed, all values are reported correctly.

Table 4-9. SNMP Alert Properties

Property	Description
Enabled?	Enables or disables the SNMP alerts. Checked=Enabled; Unchecked=Disabled.
Destination IP Address	If the Available link appears under Destination IP Address , click the link to open the Add/Configure SNMP Alerts page, which enables you to configure a new alert. Displays the destination IP address to which the corresponding alert is sent. Click the IP address to open the Add/Configure SNMP Alerts window.
Community	Displays the SNMP community to which the Destination IP Address belongs.

Testing an Alert



NOTE: You must have **Test Alert** permission to test an alert, otherwise this option will not be available.

You can force an alert to be sent to the specified destination IP address. In the **SNMP Alert List**, click **Test Alert** next to the alert you want to test.



NOTE: Only users with **Test Alerts** permission will have the **Test Alert** option available next to their names.

Deleting an Alert

In the **SNMP Alert List**, click **Remove Alert** next to the alert you want to delete.

Other Options

The **SNMP Alerts** and **Add/Configure SNMP Alerts** pages provide the buttons in Table 4-10 in the top-right corner of the screen.

Table 4-10. SNMP Alerts Page Buttons

Button	Action
Print	Prints the SNMP Alerts page
Refresh	Reloads the SNMP Alerts page

Managing a Remote System

This section provides instructions about how to perform the following systems management tasks to manage a remote system:

- Updating the DRAC 4 Firmware
- Securing DRAC 4 Communications Using SSL and Digital Certificates
- Viewing System Information
- First Steps to Troubleshoot a Remote System

Updating the DRAC 4 Firmware

Use the **Firmware Update** page to update the DRAC 4 firmware to the latest revision.

The following data is included in the DRAC 4 firmware package:

- Compiled DRAC 4 firmware code and data
- Expansion ROM image
- Web-based interface, JPEG, and other user interface data files
- Default configuration files



NOTE: The firmware update retains the current DRAC 4 settings.



NOTE: Before beginning the firmware update, download and install the latest firmware version on your local system.

- 1 Open a Windows Explore window.
- 2 In the **Address** field, type the path to the firmware image.

For example:

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

The default firmware image name is **firmimg.dml**.

- 3 Click **Update Firmware**.

The update may take several minutes to complete. When the update is completed, a dialog box appears.

- 4 Click **OK** to close the session and automatically log out.
- 5 After the DRAC 4 resets, click **Log In** to log in to the DRAC 4 again.

Securing DRAC 4 Communications Using SSL and Digital Certificates

The DRAC includes a Web server that is configured to use the industry-standard SSL security protocol to transfer encrypted data over the Internet. Built upon public-key and private-key encryption technology, SSL is a widely accepted technique for providing authenticated and encrypted communication between clients and servers to prevent eavesdropping across a network.

SSL allows an SSL-enabled system to perform the following tasks:

- Authenticate itself to an SSL-enabled client
- Allow the client to authenticate itself to the server
- Allow both systems to establish an encrypted connection

This encryption process provides a high level of data protection. The DRAC employs the 128-bit SSL encryption standard, the most secure form of encryption generally available for Internet browsers in North America.

The DRAC Web server includes a Dell self-signed SSL digital certificate (Server ID). To ensure high security over the Internet, replace the Web server SSL certificate by submitting a request to the DRAC to generate a new Certificate Signing Request (CSR).

Certificate Signing Request (CSR)

A CSR is a digital request to a Certificate Authority (CA) for a secure server certificate. Secure server certificates ensure the identity of a remote system and ensure that information exchanged with the remote system cannot be viewed or changed by others. To ensure this security for your DRAC 4, it is strongly recommended that you generate a CSR and submit the CSR to a CA.

A Certificate Authority is a business entity that is recognized in the IT industry for meeting high standards of reliable screening, identification, and other important security criteria. Examples of CAs include Thawte and VeriSign. After the CA receives your CSR, they review and verify the information the CSR contains. If the applicant meets the CA's security standards, the CA issues a certificate to the applicant that uniquely identifies that applicant for transactions over networks and on the Internet.

After the CA approves the CSR and sends you a certificate, you must upload the certificate to the DRAC 4 firmware. The CSR information stored on the DRAC 4 firmware must match the information contained in the certificate.

Viewing a Server Certificate

Use the **Server Certificate Information** page to view a server certificate for your DRAC 4. Table 4-11 provides information about the server certificate.

Table 4-11. Server Certificate Information

Field	Description
Attribute	Value
Type	Type of certificate; server certificate
Serial	Certificate serial number
Key Size	Encryption key size
Valid From	Issue date of the certificate
Valid To	Expiry date of the certificate
Subject	Certificate attributes entered by the subject
Issuer	Certificate attributes returned by the issuer

The buttons in Table 4-12 are available on the **Viewing a Server Certificate** page.

Table 4-12. View Server Certificate Page Buttons

Button	Action
Print	Prints the contents of the open window to your default printer
Go Back to Certificate Management Page	Returns to the previous page



Generating, Uploading, and Viewing a Server Certificate

- 1 Click the **Configuration** tab and click **Security**.
- 2 Use the **Certificate Management** page options (see Table 4-13) to generate a certificate signing request (CSR) to send to a certificate authority (CA). The CSR information is stored on the DRAC 4 firmware.



NOTE: You must have **Configure DRAC 4** permission to generate or upload a server certificate.

Table 4-13. Certificate Management Page Options

Option	Action
Generate a New CSR	Click Next to open the Certificate Signing Request Generation page that enables you to generate a CSR to send to a CA to request a secure Web certificate.  NOTICE: Each new CSR overwrites any pervious CSR on the firmware. For a CA to accept your CSR, the CSR in the firmware must match the certificate returned from the CA.
Upload Certificate	Click Next to upload an existing certificate that your company has title to, and uses to control access to the DRAC 4.  NOTICE: Only X509, Base 64 encoded certificates are accepted by the DRAC 4. DER encoded certificates are not accepted. Upload a new certificate to replace the default certificate you received with your DRAC 4.
View Server Certificate	Click Next to view an existing server certificate.

Generating a Certificate Signing Request

- 1 Type a value in the field for each CSR attribute. Table 4-14 describes what values are valid for each required field.

The **Email Address** field is optional. You may type your company's email address, or any email address that you want to have associated with the CSR.


 **NOTICE:** Each new CSR overwrites any previous CSR on the firmware. Before a certificate authority (CA) can accept your CSR, the CSR in the firmware must match the certificate returned from the CA, or the DRAC 4 will not upload the certificate.

Table 4-14. Required CSR Fields

Properties	Description
Common Name (CN)	The exact name being certified (usually the Web server's domain name, for example, www.xyzcompany.com). Only alphanumeric characters, hyphens, underscores, and periods are valid. Spaces are not valid.
Organization Unit (OU)	The name associated with an organizational unit, such as a department (for example, Enterprise Group). Only alphanumeric characters, hyphens, underscores, periods, and spaces are valid.
Organization (O)	The name associated with this organization (for example, XYZ Corporation). Only alphanumeric characters, hyphens, underscores, periods and spaces are valid.
Country Code (C)	The name of the country where the entity applying for certification is located. Use the drop-down menu to select the country.
Locality (L)	The city or other location of the entity being certified (for example, Round Rock). Only alphanumeric characters and spaces are valid. Do not separate words using an underscore or some other character.
State (S)	The state or province where the entity who is applying for a certification is located (for example, Texas). Only alphanumeric characters and spaces are valid. Do not use abbreviations.

The buttons in Table 4-15 are available on the **Certificate Signing Request Generation** page.

Table 4-15. Certificate Signing Request Generation Page Buttons

Button	Action
Print	Prints the contents of the window's data area using the default printer for your system.
Go Back to Certificate Management Page	Returns to the previous page.
Generate	Generates a CSR and then prompts you to either open it or save it in the directory you specify.

Uploading a Certificate

To upload your server certificate to the DRAC 4 firmware, type the file path of the certificate or browse to the certificate file and click **Upload**.



NOTE: The **File Path** value displays the relative file path of the certificate to be uploaded. You must type the absolute file path (for example, the full path and the complete file name including the file extension).

The buttons in Table 4-16 are available on the **Certificate Management** page.

Table 4-16. Certificate Management Page Buttons

Button	Action
Print	Prints the contents of the Upload Certificate page data.
Go Back to Certificate Management Page	Returns to the previous page.
Upload	Uploads the certificate to the DRAC 4 firmware.

Viewing System Information

The **System Summary** page displays system information (see Table 4-17 through Table 4-20) and DRAC 4 session information (see Table 4-21).

System Information

This section provides information about the types of system information.

Table 4-17. Types of System Information

Field	Description
DRAC 4 Information	Information about the DRAC 4 firmware and hardware.
System Information	Information about the system on which the DRAC 4 is installed.
Watchdog Information	Information about configured watchdog events; actions taken by the system when specific system events occur. To receive watchdog information, you must have DRAC 4 services installed on the managed system. The watchdog settings must be configured using Server Administrator. For more information, see the <i>Server Administrator User's Guide</i> . Watchdog provides the same functionality as the automatic recovery feature. It is recommended that you use the watchdog feature and disable the automatic recovery feature.

DRAC 4 Information

Table 4-18. DRAC 4 Information Fields

Field	Description
DRAC 4 Date/Time	DRAC 4 internal clock setting.
Firmware Version	Current firmware version level.
Firmware Updated	Date and time that the firmware was last updated.
Hardware Version	DRAC 4 hardware version level.
MAC Address	MAC address assigned to the DRAC 4.
Current IP Address	IP address assigned to the DRAC 4 NIC.

Table 4-18. DRAC 4 Information Fields (continued)

Field	Description
Current IP Gateway	IP address of the switch or router servicing the DRAC 4 NIC.
Current IP Netmask	IP address of the subnet to which the DRAC 4 is connected.
DHCP Enabled? (Default No)	Yes if DHCP is enabled on the DRAC 4. No if DHCP is disabled.
Use DHCP to Obtain DNS Server Addresses	If TRUE , the primary and secondary DNS server addresses are obtained from the DHCP server (rather than the static settings).
Static Preferred DNS Server Address	If Use DHCP to Obtain DNS Server Addresses is FALSE , the IP address of the primary DNS server is used.
Static Alternate DNS Server Address	If Use DHCP to Obtain DNS Server Addresses is FALSE , IP address of the secondary DNS server is used.

System Information

To receive **OS Type**, **Host Name**, and **OS Name** information, you must have DRAC 4 services installed on the managed system.

Table 4-19. System Information Fields

Field	Description
System ID	System identifier
System Model	System model and type
BIOS Version	BIOS version level
Service Tag	System service tag number, if assigned
OS Type	Type of operating system installed on the system
Host Name	Name of the managed system where the DRAC 4 is installed
OS Name	Name of the operating system installed on the DRAC 4 managed system, including version, build, and service pack information
BMC Version	Managed system firmware version

Watchdog Information

Table 4-20. Watchdog Information Fields

Field	Description
Recovery Action	Specifies whether to reset, power cycle, shut down, or to not take action if the system hangs.
Present countdown value	Number of seconds remaining before the watchdog initiates the recovery action. This value may fluctuate because it is displayed in real time.
Initial countdown value	Number of seconds from where the countdown begins.

Session Information

This section provides information about DRAC 4 sessions.



NOTE: Closing the browser without gracefully logging out causes the session to remain open until it times out. It is strongly recommended that you click the **logout** button to end the session; otherwise, the session remains active until the session timeout is reached.

Session Status

Table 4-21. Session Status Fields

Field	Description
Valid Sessions	Current number of DRAC 4 Web-based interface sessions (equal to the number of users that are logged on to the DRAC 4)
Unused Sessions	Current number of unused sessions. The DRAC 4 is capable of supporting up to 4 concurrent sessions (maximum of 4 Web sessions, 4 Telnet sessions, 1 Serial session, and 4 remote racadm CLI sessions).
Session Type	Current session type (Web , Telnet , or Serial).
Session User	Name of the user initiating the session
User's IP Address	IP address of the system from which the user is connecting to the DRAC 4

Table 4-21. Session Status Fields (continued)

Field	Description
Login Date/Time	Time and date that the user logged in according to the DRAC 4 internal clock
Active Consoles	One of the following consoles per session: Console Redirect — A console redirection session is active. Virtual Media — A virtual media session is active.

Recovering and Troubleshooting the Managed System

This section explains how to perform tasks related to recovering and troubleshooting a crashed remote system using the DRAC 4 Web-based interface. For information about troubleshooting your DRAC 4, see "Troubleshooting."

- First Steps to Troubleshoot a Remote System
- Managing Power on a Remote System
- Using the SEL
- Using the DRAC 4 Log
- Viewing the Last System Crash Screen
- Using the Diagnostic Console

First Steps to Troubleshoot a Remote System

The following questions are commonly used to troubleshoot high-level problems in the managed system:

- 1** Is the system powered on or off?
- 2** If powered on, is the operating system functioning, crashed, or just frozen?
- 3** If powered off, did the power turn off unexpectedly?

For crashed systems, you can check the last crash screen (see "Viewing the Last System Crash Screen"), and use console redirection (see "Using Console Redirection") and remote power management (see "Managing Power on a Remote System") to restart the system and monitor the reboot process.

Managing Power on a Remote System

The DRAC 4 allows you to remotely perform several power management actions on the managed system to try and recover after a system crash or other problem. Use the **Server Control** page to perform an orderly shutdown through the operating system when rebooting, and power the system on or off.



NOTE: You must have **Execute Server Action Commands** permission to perform power management actions.

Selecting Server Control Actions

- 1 Select whether to perform an **Operating System Shutdown** (only for the **Reboot System**, and **Power Off System**, **Server Control Actions**).

If you want to make the system perform an orderly shutdown through the operating system before the selected **Server Control Action**, select **Operating System Shutdown**.



NOTE: To use the **Operating System Shutdown** option, you must first install the DRAC 4 managed system software, otherwise this option will be unavailable. For more information, see your *Dell OpenManage Server Administrator's User's Guide*.

- 2 Select one of the following **Server Control Actions**.
 - **Reboot System** — Resets the system (equivalent to pressing the reset button); the power is not turned off by using this function.
 - **Power Cycle System** — Turns off the system power and turns it on again (equivalent to pressing the power button twice).
 - **Power Off System** — Turns off the system power (equivalent to pressing the power button when the system power is on).
 - **Power On System** — Turns on the system power (equivalent to pressing the power button when the system power is off).
- 3 Click **Apply** to perform the power management action (for example, cause the system to power cycle).

Other Options

The **Server Control** page provides buttons (see Table 4-22) in the top-right corner of the screen.

Table 4-22. Server Control Page Buttons (Top Right)





Button	Action
Print	Prints the Server Control page
Refresh	Reloads the Server Control page

Using the SEL

The **System Event Log (SEL)** page displays system-critical events that occur on the managed system. The SEL is generated by the Baseboard Management Controller (BMC) on the managed system and by the DRAC 4 if you have configured it to monitor any managed system events. This page displays the date, time, and a description of each event generated by the BMC and other instrumentation on the managed system. You can configure the DRAC 4 to send email or SNMP alerts when specified events occur.

The SEL displays the event severity and provides other information as shown in Table 4-23.

Table 4-23. Status Indicator Icons

Icon	Description
	A green check mark indicates a healthy (normal) status condition.
	A yellow triangle containing an exclamation point indicates a warning (noncritical) status condition.
	A red X indicates a critical (failure) status condition.
	A blank space indicates that the status is unknown.
Date/Time	The date and time that the event occurred
Description	A brief description of the event

The SEL provides buttons (see Table 4-24) in the top-right corner of the screen.

Table 4-24. SEL Buttons (Top Right)





Button	Action
Print	Prints the SEL.
Clear Log	Clears the SEL. NOTE: The Clear Log button appears only if you have Clear Logs permission.
Save As	Opens a pop-up window that enables you to save the SEL to a directory of your choice.
Refresh	Reloads the SEL page.

Using the DRAC 4 Log

The **DRAC 4 Log** is a persistent log maintained in the DRAC 4 firmware. The log contains a list of user actions (such as log in and log out) and alerts issued by the DRAC 4. The oldest entries are overwritten when the log becomes full. If the DRAC 4 loses communication with the managed system, all entries that the DRAC 4 would have added to the System Event Log (**SEL**), such as a power failure, are added to the **DRAC 4 Log** until communication is re-established.

The **DRAC 4 Log** provides the information in Table 4-25.

Table 4-25. Status Indicator Icons

Icon	Description
	A green check mark indicates a healthy (normal) status condition.
	A yellow triangle containing an exclamation point indicates a warning (noncritical) status condition.
	A red X indicates a critical (failure) status condition.
	A blank space indicates that the status is unknown.
Date/ Time	The date and time (for example, Sat Dec 19 16:55:47 2004). When the DRAC 4 is unable to communicate with the managed system, the letters DSU (DRAC 4 start up) appear before the time, followed by the time elapsed since the DRAC 4 was started.
User	The name of the user logging into the DRAC 4.
ID	The event identification number of the message displayed.
Description	A brief description of the event.


Using the DRAC 4 Log Page Buttons

The DRAC 4 Log page provides the following buttons (see Table 4-26).

Table 4-26. DRAC 4 Log Buttons

Button	Action
Print	Prints the DRAC 4 Log page.
Clear Log	Clears the DRAC 4 Log entries. NOTE: The Clear Log button only appears if you have Clear Logs permission.
Save As	Opens a pop-up window that enables you to save the DRAC 4 Log to a directory of your choice.
Refresh	Reloads the DRAC 4 Log page.

Viewing the Last System Crash Screen

 **NOTICE:** To capture the last crash screen, you must have managed system software installed.

Use the **Last Crash Screen** page to view the most recent crash screen, which allows you to obtain information about events leading up to the system crash. Last system crash information is saved in DRAC 4 memory and is remotely accessible. The date of the system crash appears on the last crash screen.

The **Last Crash Screen** page provides the following buttons (see Table 4-27) in the top-right corner of the screen:

Table 4-27. Last Crash Screen Page Buttons

Button	Action
Print	Prints the Last Crash Screen page.
Save As	Opens a pop-up window that enables you to save the Last Crash Screen to a directory of your choice.
Refresh	Reloads the Last Crash Screen page.
Delete Last Crash Screen	Deletes the Last Crash Screen page.



NOTE: Due to fluctuations in the watchdog timer, the **Last Crash Screen** has a higher probability of not being captured when the System Reset Timer is set to a value less than 30 seconds. Use Server Administrator or IT Assistant to set the System Reset Timer to at least 30 seconds to ensure that the **Last Crash Screen** functions properly. See "Configuring the Managed System to Capture the Last Crash Screen" for additional information.

Using the Diagnostic Console

The DRAC 4 provides a standard set of network diagnostic tools, similar to those found on Microsoft Windows or Red Hat Enterprise Linux-based systems. Using the DRAC 4 Web-based interface, you can access the following network debugging tools by clicking the **Diagnostics** tab.

The Diagnostic Console allows you to perform debugging tasks and paging. Table 4-28 shows the options that are available on the **Diagnostic Console** page.



NOTE: After entering one of the following commands, click **Submit**. The results of the debugging tasks are displayed in the **Results of the Diagnostic Command** box at the bottom of the page.

Table 4-28. Diagnostic Commands

Command	Description
<code>arp</code>	Displays the contents of the Address Resolution Protocol (ARP) table. ARP entries may not be added or deleted.
<code>ifconfig</code>	Displays the contents of the network interface table.
<code>netstat</code>	Prints the content of the routing table. If the optional interface number is provided in the text field to the right of the <code>netstat</code> option, then <code>netstat</code> prints additional information regarding the traffic across the interface, buffer usage, and other network interface information.
<code>ping <IP Address></code>	Verifies that the destination IP address is reachable from the DRAC 4 with the current routing-table contents. A destination IP address must be entered in the field to the right of this option. An Internet control message protocol (ICMP) echo packet is sent to the destination IP address based on the current routing-table contents.
<code>getcoredump</code>	Displays the last controller crash, including detailed information such as register values and a memory map recorded when the most recent controller crash occurred; displays the message "No CORE dump available" if no previous controller crash has occurred or if the data has been deleted.
<code>settracelog</code>	Enables you to set debug trace levels to identify the types of messages being sent on the local network. The <code>-d</code> option traces the DHCP packets sent and received. The <code>-i</code> option traces IP packets sent and received. For example, type <code>settracelog -i</code> to trace IP packets sent and received. To disable the trace log, type <code>settracelog</code> without any arguments.
<code>gettracelog</code>	Displays a UNIX [®] style system log. This log is a volatile, memory-resident log that contains time-stamped entries.
<code>nettrace</code>	Enables you to view your current trace log settings.

The **Diagnostic Console** page provides buttons (see Table 4-29) in the top-right corner of the screen.

Table 4-29. Diagnostic Console Page Buttons (Top Right)

Button	Action
Refresh	Reloads the Diagnostic Console page.

Troubleshooting Network Problems

The internal DRAC 4 Trace Log can be used by administrators to debug alerting, or networking from the DRAC 4. The Trace Log can be accessed from the DRAC 4 Web-based interface by clicking the **Diagnostics** tab, and typing the `gettracelog` command. The Trace Log will appear and tracks the following information:

- DHCP — Traces packets sent to and received from a DHCP server.
- IP — Traces IP packets sent and received.



NOTE: In the DRAC 4 Trace Log, nonprintable ASCII characters are translated to printable ASCII characters. If the character code is less than **0x20**, or between **0x7f** and **0xa0** (inclusive), the value **0x40** is exclusive and the character before printing, after a "^" is added to the beginning. As a result, the ASCII carriage return character, **0xd**, is printed as "^M" in the Trace Log.



NOTE: The DRAC 4 will not echo an ICMP (ping) with a packet size larger than 1500 bytes.

The trace log may also contain DRAC 4 firmware-specific error codes (relating to the internal DRAC 4 firmware, not the managed system's operating system). Use Table 4-30 to help diagnose network problems reported by the internal DRAC 4 operating system.

Table 4-30. DRAC 4 Network Error Codes

Error Code	Description
0x5006	ENXIO: No such address.
0x5009	EBADS: The socket descriptor is invalid.
0x500D	EACCESS: Permission denied.
0x5011	EEXIST: Duplicate entry exists.

Table 4-30. DRAC 4 Network Error Codes (continued)

Error Code	Description
0x5016	EINVALID: An argument is invalid.
0x5017	ENFILE: An internal table has run out of space.
0x5020	EPIPE: The connection is broken.
0x5023	EWOULDLOCK: The operation would block; socket is nonblocking.
0x5024	EINPROGRESS: Socket is nonblocking; connection not completed immediately.
0x5025	EALREADY: Socket is nonblocking; previous connection attempt not complete.
0x5027	EDESTADDRREQ: The destination address is invalid.
0x5028	EMSGSIZE: Message too long.
0x5029	EPROTOTYPE: Wrong protocol type for socket.
0x502A	ENOPROTOOPT: Protocol not available.
0x502B	EPROTONO SUPPORT: Protocol not supported.
0x502D	EOPNOTSUPP: Requested operation not valid for this type of socket.
0x502F	EAFNOSUPPORT: Address family not supported.
0x5030	EADDRINUSE: Address is already in use.
0x5031	EADDRNOTAVAIL: Address not available.
0x5033	ENETUNREACH: Network is unreachable.
0x5035	ECONNABORTED: The connection has been aborted by the peer.
0x5036	ECONNRESET: The connection has been reset by the peer.
0x5037	ENOBUFS: An internal buffer is required but cannot be allocated.
0x5038	EISCONN: The socket is already connected.
0x5039	ENOTCONN: The socket is not connected.
0x503B	ETOOMANYREFS: Too many references, cannot splice.
0x503C	ETIMEDOUT: Connection timed out.
0x503D	ECONNREFUSED: The connection attempt was refused.

Table 4-30. DRAC 4 Network Error Codes (continued)

Error Code	Description
0x5041	EHOSTUNREACH: The destination host could not be reached.
0x5046	ENIDOWN: NI_INIT returned -1.
0x5047	ENMTU: The MTU is invalid.
0x5048	ENHWL: The hardware length is invalid.
0x5049	ENNOFIND: The route specified cannot be found.
0x504A	ECOLL: Collision in select call; these conditions already selected by another task.
0x504B	ETID: The task ID is invalid.

Troubleshooting Alerting Problems

You can use logged SNMP trap information to troubleshoot a particular type of DRAC 4 alert. SNMP trap deliveries are logged in the Trace Log by default. However, since SNMP does not confirm delivery of traps, it is best to trace the packets on the managed system using a network analyzer or a tool such as Microsoft's `snmputil`.

DRAC 4 Log Messages

DRAC 4 Log messages can be used by administrators to debug alerting from the DRAC 4. Table 4-31 provides a list of the DRAC 4 log message ID numbers, messages, and suggested actions to take.



NOTE: In Table 4-31, the character "L" is sometimes displayed in the **Message ID** column. "L" represents the severity level or type of the message, which can be one of the following: W (warning), E (error), S (severe), F (fatal), or A (always).

Table 4-31. DRAC 4 Log Messages

Message ID	Description	Suggested Action
RAC186W	DHCP: no response from server, need LAN address. The NIC cannot be enabled until a response is received from the DHCP server.	Provides information only. No specific corrective action is indicated. Ensure that the DHCP server is operational.
RAC188W	DHCP: no response from server, warm starting with <IP address>.	Provides information only. No specific corrective action is indicated. Ensure that the DHCP server is operational.
RAC189A	Email page successful.	Provides information only. No corrective action is necessary.
RAC191E	SNMP: internal failure during trap generation	Reset the DRAC 4 and retry the operation.
RAC198A	SNMP: trap sent to <IP address>	Provides information only. No corrective action is necessary.
RAC199W	Email paging attempts failed, SMTP protocol failure	A trace of the SMTP connection may be found in the trace log. Examine the trace log to identify the source of the protocol failure, such as the connection could not be established (SMTP server is down or an invalid IP address), an invalid email destination address, an invalid domain in the email address, or the SMTP server does not support forwarding email. Correct the problem and try again.
RAC256A RAC257W RAC258E	DRAC 4 hardware log event: <formatted hardware log event>	Provides information only. No corrective action is necessary, unless the contents of the hardware log indicate a problem. In this case, the corrective action is based on the problem reported.
RAC016A	DRAC 4 log cleared	Provides information only.

Table 4-31. DRAC 4 Log Messages (continued)

Message ID	Description	Suggested Action
RAC030A	DRAC 4 time was set	Provides information only.
RAC048A	DRAC 4 firmware update was initiated.	Provides information only.
RAC049A	DRAC 4 Firmware Update was initiated with config to defaults option.	Provides information only.
RAC064A	Clear crash screen	Provides information only.
RAC065A	DRAC 4 hard reset, delay <seconds> was initiated	Provides information only.
RAC066A	DRAC 4 soft reset, delay <seconds> was initiated	Provides information only.
RAC067A	DRAC 4 graceful reset, delay <seconds> was initiated	Provides information only.
RAC068A	DRAC 4 cfg2default reset, delay <seconds> was initiated	Provides information only.
RAC069A	DRAC 4 shutdown was initiated	Provides information only.
RAC114A	Requested server {powerdown powerup powercycle hardreset graceshutdown gracereboot gracereboot}	Provides information only.
RAC115A	Could not log graceful server action to hardware log	Provides information only.
RAC122A	DRAC 4 booted	Provides information only.
RAC138A	Console redirect session enabled	Provides information only.
RAC139A	Console redirect session disabled	Provides information only.
RAC154A	Logout from <IP address>	Provides information only.
RAC155A	Login from <IP address>	Provides information only.

Table 4-31. DRAC 4 Log Messages (continued)

Message ID	Description	Suggested Action
RAC156A	Session cancelled from <IP address>, max log in attempts exceeded.	Provides information only.
RAC157A	Session cancelled from <IP address>, due to inactivity.	Provides information only.
RAC158A	Nonvalidated session from <IP address> cancelled.	Provides information only.
RAC159A	Start console redirection.	Provides information only.
RAC160A	End console redirection.	Provides information only.
RAC161E	Maximum sessions exceeded.	Wait until another user closes a session.
RAC162E	Maximum per user connections exceeded.	Close one of your sessions.
RAC163E	User lacks permission.	Log in as a user with appropriate permissions.

Frequently Asked Questions

Table 4-32 lists frequently asked questions and answers.

Table 4-32. Managing and Recovering a Remote System: Frequently Asked Questions

Question	Answer
The following message is displayed for unknown reasons: Remote Access: SNMP Authentication Failure Why does this happen?	<p>As part of discovery, IT Assistant attempts to verify the get and set community names of the device. In IT Assistant, you have the get community name = public and the set community name = private. By default, the community name for the DRAC 4 agent is public. When IT Assistant sends out a set request, the DRAC 4 agent generates the SNMP authentication error because it will only accept requests from community = public.</p> <p>You can change the DRAC 4 community name using the racadm command line utility.</p> <p>To see the DRAC 4 community name, use the following command:</p> <pre>racadm getconfig -g cfgOobSnmp</pre> <p>To set the DRAC 4 community name, use the following command:</p> <pre>racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name></pre> <p>To prevent SNMP authentication traps from being generated, you must input community names that will be accepted by the agent. Since the DRAC 4 only allows one community name, you must input the same get and set community name for IT Assistant discovery setup.</p>

Table 4-32. Managing and Recovering a Remote System: Frequently Asked Questions (continued)

Question	Answer
<p>Why are the remote racadm and Web-based services unavailable after a property change?</p>	<p>It may take several minutes for the remote racadm services and the Web-based interface to become available again after a reset of the DRAC 4 Web server</p> <p>The DRAC 4 Web server is reset after the following occurrences:</p> <ul style="list-style-type: none"> • When the <code>cfgRacTuneHttpsPort</code> property is changed (including when a <code>config -f <config file></code> changes it) • When <code>racresetcfg</code> is used • When the DRAC 4 is reset
<p>When accessing the DRAC 4 Web-based interface, I get a security warning stating the hostname of the SSL certificate does not match the hostname of the DRAC 4.</p>	<p>DRAC 4 includes a default DRAC 4 server certificate to ensure network security for the Web-based interface and remote racadm features. When this certificate is used, the Web browser displays a security warning because the default certificate is issued to RAC default certificate which does not match the host name of the DRAC 4 (for example, the IP address). To address this security concern, upload a DRAC 4 server certificate issued to the IP address of the DRAC 4. When generating the certificate signing request (CSR) to be used for issuing the certificate, ensure that the common name (CN) of the CSR matches the IP address of the DRAC 4 (for example, 192.168.0.120). See "Securing DRAC 4 Communications Using SSL and Digital Certificates" for more information about generating CSRs and issuing certificates.</p>

Table 4-32. Managing and Recovering a Remote System: Frequently Asked Questions (continued)

Question	Answer
When accessing the DRAC 4 Web-based interface, I get a security warning stating the SSL certificate was issued by a certificate authority (CA) that is not trusted.	DRAC 4 includes a default DRAC 4 server certificate to ensure network security for the Web-based interface and remote racadm features. This certificate was not issued by a trusted CA. To address this security concern, upload a DRAC 4 server certificate issued by a trusted CA (for example, Thawte or Verisign). See "Securing DRAC 4 Communications Using SSL and Digital Certificates" for more information about issuing certificates.
Why doesn't my DNS server register my DRAC 4?	Some DNS servers only register names of 31 characters or fewer.

Using the DRAC 4 With Microsoft Active Directory

A directory service is used to maintain a common database of all information needed for controlling users, computers, printers, etc. on a network.

If your company uses the Microsoft® Active Directory® service software, it can be configured to give you access to the DRAC 4, allowing you to add and control DRAC 4 user privileges to your existing users in your Active Directory software.



NOTE: Using Active Directory to recognize DRAC 4 users is supported on the Microsoft Windows® 2000 and Windows Server® 2003 operating systems.

You can use Active Directory to define user access on DRAC 4 through two methods: you can use the extended schema solution, which uses Dell-defined Active Directory objects, or a standard schema solution, which uses Active Directory group objects only.

Advantages and Disadvantages of Extended Schema and Standard Schema

When using Active Directory to configure access to the DRAC 4, you must choose either the extended schema or the standard schema solution.

The advantages of using the extended schema solution are:

- All of the access control objects are maintained in Active Directory.
- Maximum flexibility in configuring user access on different DRAC 4 cards with different privilege levels.

The advantages of using the standard schema solution are:

- No schema extension is required because standard schema uses Microsoft Active Directory objects only.
- Configuration on the Active Directory side is simple.

Extended Schema Active Directory Overview

There are two ways to enable Extended Schema Active Directory:

- Via the DRAC 4 web-based user interface. See "Configuring the DRAC 4 with Extended Schema Active Directory and the Web-Based Interface."
- Via the RACADM CLI tool. See "Configuring the DRAC 4 with Extended Schema Active Directory and the racadm CLI."

Active Directory Schema Extensions

The Active Directory data is a distributed database of Attributes and Classes. The Active Directory schema includes the rules that determine the type of data that can be added or included in the database. The user class is one example of a Class that is stored in the database. Some example user attributes can include the user's first name, last name, phone number, and so on. Companies can extend the Active Directory database by adding their own unique Attributes and Classes to solve environment-specific needs. Dell has extended the schema to include the necessary changes to support remote management Authentication and Authorization.

Each Attribute or Class that is added to an existing Active Directory Schema must be defined with a unique ID. To maintain unique IDs across the industry, Microsoft maintains a database of Active Directory Object Identifiers (OIDs) so that when companies add extensions to the schema, they can be guaranteed to be unique and not to conflict with each other. To extend the schema in Microsoft's Active Directory, Dell received unique OIDs, unique name extensions, and uniquely linked attribute IDs for our attributes and classes that are added into the directory service.

Dell extension is: dell

Dell base OID is: 1.2.840.113556.1.8000.1280

RAC LinkID range is:12070 to 12079

The Active Directory OID database maintained by Microsoft can be viewed at <http://msdn.microsoft.com/certification/ADAcctInfo.asp> by entering our extension Dell.

Overview of the RAC Schema Extensions

To provide the greatest flexibility in the multitude of customer environments, Dell provides a group of properties that can be configured by the user depending on the desired results. Dell has extended the schema to include an Association, Device, and Privilege property. The Association property is used to link together the users or groups with a specific set of privileges to one or more RAC devices. This model provides an Administrator maximum flexibility over the different combinations of users, RAC privileges, and RAC devices on the network without adding too much complexity.

Active Directory Object Overview

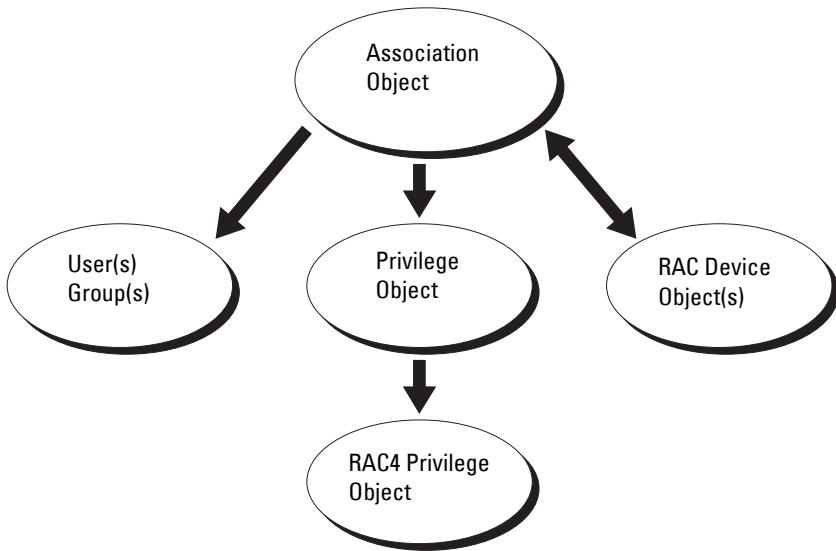
For each of the physical RACs on the network that you want to integrate with Active Directory for Authentication and Authorization, you must create at least one Association Object and one RAC Device Object. You can create as many Association Objects as you want, and each Association Object can be linked to as many users, groups of users, or RAC Device Objects as desired. The users and RAC Device Objects can be members of any domain in the enterprise.

However, each Association Object can be linked (or, may link users, groups of users, or RAC Device Objects) to only one Privilege Object. This allows an Administrator to control which users have what kind of privileges on specific RACs.

The RAC Device object is the link to the RAC firmware for querying Active Directory for authentication and authorization. When a RAC is added to the network, the Administrator must configure the RAC and its device object with its Active Directory name so that users can perform authentication and authorization with Active Directory. The Administrator will also need to add the RAC to at least one Association Object in order for users to authenticate.

Figure 5-1 illustrates that the Association Object provides the connection that is needed for all of the Authentication and Authorization.

Figure 5-1. Typical Setup for Active Directory Objects

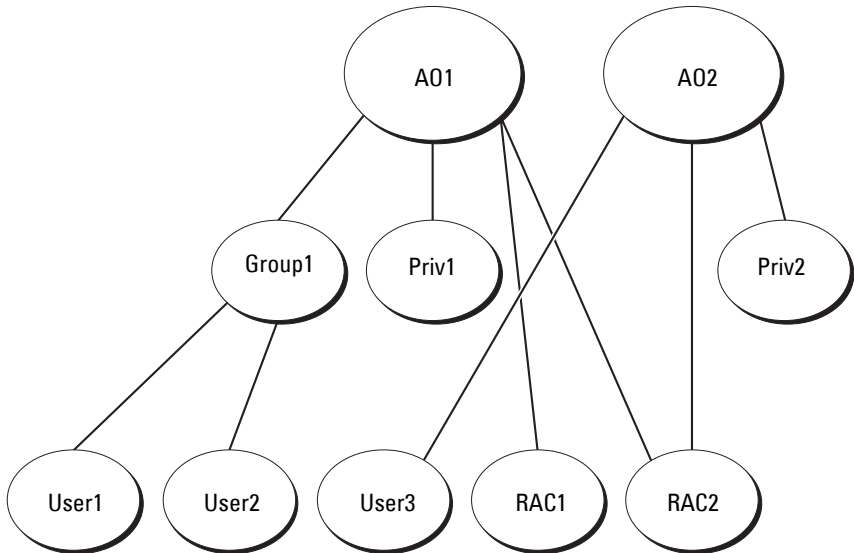


You can create as many or as few association objects as required. However, you must create at least one Association Object, and you must have one RAC Device Object for each RAC (DRAC 4) on the network that you want to integrate with Active Directory for Authentication and Authorization with the RAC (DRAC 4).

The Association Object allows for as many or as few users and/or groups as well as RAC Device Objects. However, the Association Object only has one Privilege Object per Association Object. The Association Object connects the "Users" who have "Privileges" on the RACs (DRAC 4s).

Additionally, you can configure Active Directory objects in a single domain or in multiple domains. For example, you have two DRAC 4 cards (RAC1 and RAC2) and three existing Active Directory users (user1, user2, and user3). You want to give user1 and user2 an administrator privilege to both DRAC 4 cards and give user3 a login privilege to the RAC2 card. Figure 5-2 shows how you set up the Active Directory objects in this scenario.

Figure 5-2. Setting Up Active Directory Objects in a Single Domain



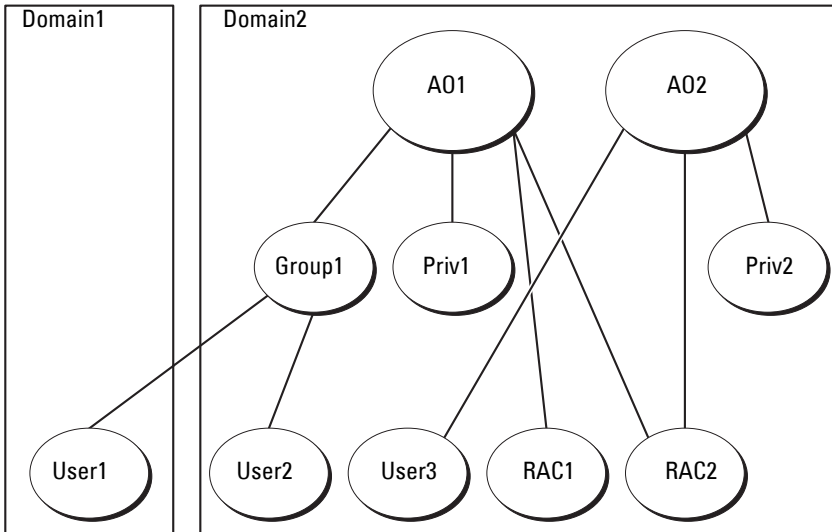
To set up the objects for the single domain scenario, perform the following tasks:

- 1** Create two Association Objects.
- 2** Create two RAC Device Objects, RAC1 and RAC2, to represent the two DRAC 4 cards.
- 3** Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (administrator) and Priv2 has login privileges.
- 4** Group user1 and user2 into Group1.
- 5** Add Group1 as Members in Association Object 1 (AO1), Priv1 as Privilege Objects in AO1, and RAC1, RAC2 as RAC Devices in AO1.
- 6** Add User3 as Members in Association Object 2 (AO2), Priv2 as Privilege Objects in AO2, and RAC2 as RAC Devices in AO2.

See "Adding DRAC 4 Users and Privileges to Active Directory" for detailed instructions.

Figure 5-3 shows how you can set up the Active Directory objects in multiple domains. In this scenario, you have two DRAC 4 cards (RAC1 and RAC2) and three existing Active Directory users (user1, user2, and user3). User1 is in Domain1, and user2 and user 3 are in Domain2. You want to give user1 and user 2 an administrator privilege to both DRAC 4 cards and give user3 a login privilege to the RAC2 card.

Figure 5-3. Setting Up Active Directory Objects in Multiple Domains



To set up the objects for the multiple domain scenario, perform the following tasks:

- 1 Ensure that the domain forest function is in Native or Windows 2003 mode.
- 2 Create two Association Objects, AO1 (of Universal scope) and AO2, in any domain. The figure shows the objects in Domain2.
- 3 Create two RAC Device Objects, RAC1 and RAC2, to represent the two DRAC 4 cards.

- 4 Create two Privilege Objects, Priv1 and Priv2, in which Priv1 has all privileges (administrator) and Priv2 has login privileges.
- 5 Group user1 and user2 into Group1. The group scope of Group1 must be Universal.
- 6 Add Group1 as Members in Association Object 1 (AO1), Priv1 as Privilege Objects in AO1, and RAC1, RAC2 as RAC Devices in AO1.
- 7 Add User3 as Members in Association Object 2 (AO2), Priv2 as Privilege Objects in AO2, and RAC2 as RAC Devices in AO2.

Configuring Active Directory to Access Your DRAC 4

Before you can use Active Directory to access your DRAC 4, configure the Active Directory software and the DRAC 4 by performing the following steps in order:

- 1 Extend the Active Directory schema. (See "Extending the Active Directory Schema.")
- 2 Extend the Active Directory Users and Computers Snap-in. (See "Installing the Dell Extension to the Active Directory Users and Computers Snap-In.")
- 3 Add DRAC 4 users and their privileges to Active Directory. (See "Adding DRAC 4 Users and Privileges to Active Directory.")
- 4 Enable SSL on each of your domain controllers. (See "Enabling SSL on a Domain Controller.")
- 5 Configure the DRAC 4 Active Directory properties using either the DRAC 4 Web-based interface or the racadm CLI. (See "Configuring the DRAC 4 with Extended Schema Active Directory and the Web-Based Interface" or "Configuring the DRAC 4 with Extended Schema Active Directory and the racadm CLI.")

Extending the Active Directory Schema

Extending your Active Directory schema adds a Dell organizational unit, schema classes and attributes, and example privileges and association objects to the Active Directory schema. Before you extend the schema, you must have **Schema Admin** privileges on the Schema Master Flexible Single Master Operation (FSMO) Role Owner of the domain forest.

You can extend your schema using one of the following methods:

- Dell Schema Extender utility
- LDIF script file.

If you use the LDIF script file, the Dell organizational unit will not be added to the schema.

The LDIF files and Dell Schema Extender are located on your *Dell Systems Console and Agent* CD in the following respective directories:

- *CD drive:\support\OMActiveDirectory Tools\RAC4\LDIF Files*
- *CD drive:\support\OMActiveDirectory Tools\RAC4\Schema Extender*

To use the LDIF files, see the instructions in the readme that is in the LDIF files directory. To use the Dell Schema Extender to extend the Active Directory Schema, perform the steps in "Using the Dell Schema Extender."

You can copy and run the Schema Extender or LDIF files from any location.

Using the Dell Schema Extender



NOTICE: The Dell Schema Extender uses the **SchemaExtenderOem.ini** file. To ensure that the Dell Schema Extender utility functions properly, do not modify the name of this file.

- 1 In the **Welcome** screen, click **Next**.
- 2 Read and understand the warning and click **Next** again.
- 3 Select **Use Current Log In Credentials** or enter a user name and password with schema administrator rights.
- 4 Click **Next** to run the Dell Schema Extender.
- 5 Click **Finish**.

The schema is extended. To verify the schema extension, use the Microsoft Management Console (MMC), the Active Directory Schema snap-in to verify that the following exist:

- Classes (see Table 5-1 through Table 5-6)
- Attributes (see Table 5-7).

See your Microsoft documentation for more information on how to enable and use the Active Directory Schema snap-in the MMC.

Table 5-1. Class Definitions for Classes Added to the Active Directory Schema

Class Name	Assigned Object Identification Number (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
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Table 5-2. dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Description	This class represents the Dell RAC device. The RAC device must be configured as dellRacDevice in Active Directory. This configuration enables the DRAC 4 to send Lightweight Directory Access Protocol (LDAP) queries to Active Directory.
Class Type	Structural Class
SuperClasses	dellProduct
Attributes	dellSchemaVersion dellRacType

Table 5-3. dellAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Description	This class represents the Dell Association Object. The Association Object provides the connection between the users and the devices.
Class Type	Structural Class
SuperClasses	Group
Attributes	dellProductMembers dellPrivilegeMember

Table 5-4. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	This class is used to define the privileges (Authorization Rights) for the DRAC 4 device.
Class Type	Auxiliary Class
SuperClasses	None
Attributes	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Table 5-5. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Description	This class is used as a container Class for the Dell Privileges (Authorization Rights).
Class Type	Structural Class
SuperClasses	User
Attributes	dellRAC4Privileges

Table 5-6. dellProduct Class

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Description	This is the main class from which all Dell products are derived.
Class Type	Structural Class
SuperClasses	Computer
Attributes	dellAssociationMembers

Table 5-7. List of Attributes Added to the Active Directory Schema

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellPrivilegeMember List of dellPrivilege Objects that belong to this Attribute.	1.2.840.113556.1.8000.1280.1.1.2.1 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers List of dellRacDevices Objects that belong to this role. This attribute is the forward link to the dellAssociationMembers backward link. Link ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE if the user has Login rights on the device.	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 if the user has Card Configuration rights on the device.	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

Table 5-7. List of Attributes Added to the Active Directory Schema (continued)

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellIsUserConfigAdmin TRUE if the user has User Configuration rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.5 Boolean (LDAPATYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE if the user has Log Clearing rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolean (LDAPATYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE if the user has Server Reset rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.7 Boolean (LDAPATYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE if the user has Console Redirection rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.8 Boolean (LDAPATYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE if the user has Virtual Media rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolean (LDAPATYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE if the user has Test Alert User rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.10 Boolean (LDAPATYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

Table 5-7. List of Attributes Added to the Active Directory Schema (continued)

Attribute Name/Description	Assigned OID/Syntax Object Identifier	Single Valued
dellIsDebugCommandAdmin TRUE if the user has Debug Command Admin rights on the device.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolean (LDAPATYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion The Current Schema Version is used to update the schema.	1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String (LDAPATYPE_CASEIGNORE STRING 1.2.840.113556.1.4.905)	TRUE
dellRacType This attribute is the Current Rac Type for the dellRacDevice object and the backward link to the dellAssociationObjectMembers forward link.	1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String (LDAPATYPE_CASEIGNORE STRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers List of dellAssociationObjectMembers that belong to this Product. This attribute is the backward link to the dellProductMembers Linked attribute. Link ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Distinguished Name (LDAPATYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Installing the Dell Extension to the Active Directory Users and Computers Snap-In

When you extend the schema in Active Directory, you must also extend the Active Directory Users and Computers snap-in so that the administrator can manage RAC (DRAC 4) devices, Users and User Groups, RAC Associations, and RAC Privileges. When you install your systems management software using the *Dell Systems Console and Agent* CD, you can extend the snap-in by selecting the **Dell Extension to the Active Directory User's and Computers**

Snap-In option during the installation procedure. See the *Dell OpenManage Software Quick Installation Guide* for additional instructions about installing systems management software.

For more information about the Active Directory Users and Computers snap-in, see your Microsoft documentation.

Installing the Administrator Pack

You must install the Administrator Pack on each system that is managing the Active Directory DRAC 4 Objects. If you do not install the Administrator Pack, then you cannot view the Dell RAC Object in the container.

See "Opening the Active Directory Users and Computers Snap-In" for more information.

Opening the Active Directory Users and Computers Snap-In

To open the Active Directory Users and Computers snap-in, perform the following steps:

- 1** If you are on the domain controller, click **Start Admin Tools→Active Directory Users and Computers**.

If you are not on the domain controller, you must have the appropriate Microsoft Administrator Pack installed on your local system. To install this Administrator Pack, click **Start→Run**, type MMC and press **Enter**.

The Microsoft Management Console (MMC) appears.

- 2** In the Console 1 window, click **File** (or **Console** on systems running Windows 2000).
- 3** Click **Add/Remove Snap-in**.
- 4** Select the **Active Directory Users and Computers** snap-in and click **Add**.
- 5** Click **Close** and click **OK**.

Adding DRAC 4 Users and Privileges to Active Directory

Using the Dell-extended Active Directory Users and Computers snap-in, you can add DRAC 4 users and privileges by creating RAC, Association, and Privilege objects. To add each type of object, perform the following procedures:

- Create a RAC Device Object
- Create a Privilege Object
- Create an Association Object
- Add Objects to an Association Object

Creating a RAC Device Object

- 1** In the MMC Console **Root** window, right-click a container.
- 2** Select **New**→**Dell RAC Object**.
This opens the **New Object** window.
- 3** Type a name for the new object. This name must match the DRAC 4 Name that you will type in step 5 of "Configuring the DRAC 4 with Extended Schema Active Directory and the Web-Based Interface."
- 4** Select **RAC Device Object**.
- 5** Click **OK**.

Creating a Privilege Object

Privilege Objects must be created in the same domain as the Association Object to which it is associated.

- 1** In the **Console Root** (MMC) window, right-click a container.
- 2** Select **New**→**Dell RAC Object**.
This opens the **New Object** window.
- 3** Type a name for the new object.
- 4** Select **Privilege Object**.
- 5** Click **OK**.
- 6** Right-click the privilege object that you created, and select **Properties**.
- 7** Click the **RAC 4 Privileges** tab and select the DRAC 4 privileges that you want the user to have (for more information, see Table 4-2).

Creating an Association Object

The Association Object is derived from a Group and must contain a Group Type. The Association Scope specifies the Security Group Type for the Association Object. When you create an Association Object, you must choose the Association Scope that applies to the type of objects you intend to add. Selecting Universal, for example, means that association objects are only available when the Active Directory Domain is functioning in Native Mode or above.

- 1** In the **Console Root** (MMC) window, right-click a container.
- 2** Select **New**→**Dell RAC Object**.
The **New Object** window appears
- 3** Type a name for the new object.
- 4** Select **Association Object**.
- 5** Select the scope for the **Association Object**.
- 6** Click **OK**.

Adding Objects to an Association Object

Using the **Association Object Properties** window, you can associate users or user groups, privilege objects, and RAC devices or RAC device groups. If your system is running Windows 2000 mode or higher, use Universal Groups to span domains with your user or RAC objects.

You can add groups of Users and RAC devices. The procedure for creating Dell-related groups and non-Dell-related groups is identical.

Adding Users or User Groups

- 1** Right-click the **Association Object** and select **Properties**.
- 2** Select the **Users** tab and click **Add**.
- 3** Type the user or User Group name and click **OK**.

Click the **Privilege Object** tab to add the privilege object to the association that defines the user's or user group's privileges when authenticating to a RAC device. Only one privilege object can be added to an Association Object.

Adding Privileges

- 1 Select the **Privileges Object** tab and click **Add**.
- 2 Type the Privilege Object name and click **OK**.

Click the **Products** tab to add one or more RAC devices to the association. The associated devices specify the RAC devices connected to the network that are available for the defined users or user groups. Multiple RAC devices can be added to an association object.

Adding RAC Devices or RAC Device Groups

- 1 Select the **Products** tab and click **Add**.
- 2 Type the RAC device or RAC device group name and click **OK**.
- 3 In the **Properties** window, click **Apply** and then **OK**.

Configuring the DRAC 4 with Extended Schema Active Directory and the Web-Based Interface



NOTE: If you are using Standard Schema with Active Directory, the DRAC 4 Name and DRAC 4 Domain Name fields are unavailable.

- 1 Open a supported Web browser. See "Supported Web Browsers."
- 2 Log in to the Web-based interface using the default user, root, and password.
- 3 Click the **Configuration** tab and select **Active Directory**.
- 4 On the **Active Directory Configuration** page, select the **Enable Active Directory** check box.
- 5 Type the **DRAC 4 Name**.
This name must be the same as the common name of the RAC object you created in your Domain Controller (see step 3 of "Creating a RAC Device Object").
- 6 Type the **Root Domain Name**. The **Root Domain Name** is the fully qualified root domain name for the forest.
- 7 Type the **DRAC 4 Domain Name** (for example, drac4.com). Do not use the NetBIOS name.

The **DRAC 4 Domain Name** is the fully qualified domain name of the sub-domain where the RAC Device Object is located.

- 8 Click **Apply** to save the Active Directory settings.
- 9 Click **Upload Active Directory CA Certificate** to upload your domain forest Root CA certificate into the DRAC 4.

The domain controllers' SSL certificates should have been signed by the root CA. Have the root CA certificate available on your management station accessing the DRAC 4 (see "Exporting the Domain Controller Root CA Certificate").

- 10 Click the **Configuration** tab and select **Network**.
- 11 If **DRAC 4 NIC DHCP** is enabled, select **Use DHCP to obtain DNS server address**. If you want to input a DNS server IP address manually, deselect **Use DHCP to obtain DNS server address** and type your primary and alternate DNS Server IP addresses.
- 12 Click **Apply**.

The DRAC 4 Extended Schema Active Directory feature configuration is complete.

Starting with DRAC 4 firmware version 1.60, you can log into DRAC with a short domain name (DRAC 4 domain name) only. This is because DRAC 4 now appends the root domain name to the user domain name. For example, if you set the root domain to *xyz.com*, and the DRAC 4 domain name to *abc*, you can log into DRAC as *abc\username*. The DRAC 4 takes the login name as *username@abc.xyz.com*

Configuring the DRAC 4 with Extended Schema Active Directory and the racadm CLI

Use the following commands to configure the DRAC 4 Active Directory Feature with Extended Schema using the racadm CLI instead of the Web-based interface.

- 1 Open a command prompt and type the following racadm commands:

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

```
racadm config -g cfgActiveDirectory -o cfgADType  
0x1
```

```
racadm config -g cfgActiveDirectory -o  
cfgADRacDomain <fully qualified rac domain name>
```

```
racadm config -g cfgActiveDirectory -o  
cfgADRootDomain <fully qualified root domain name>
```

```
racadm config -g cfgActiveDirectory -o  
cfgADRacName <RAC common name>
```

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

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

- 2 If you want to specify an LDAP or Global Catalog server instead of using the servers returned by the DNS server to search for a user name, type the following command to enable the Specify Server option:

```
racadm config -g cfgActive Directory -o  
cfgADSpecifyServer Enable 1
```



NOTE: If you use this option, the hostname in the CA certificate is not matched against the name of the specified server. This is particularly useful if you are a DRAC administrator because you can enter a hostname as well as an IP address.

After the Specify Server option is enabled, you can specify an LDAP server with an IP address as well as a fully qualified domain name (FQDN) of the server. The FQDN consists of the hostname and the domain name of the server.

To specify an LDAP server, type:

```
racadm config -g cfgActive Directory -o  
cfgADDomainController <fully qualified domain name  
or IP address>
```

To specify a Global Catalog server, type:

```
racadm config -g cfgActive Directory -o  
cfgGlobalCatalog <fully qualified domain name or IP  
address>
```



NOTE: If you specify the IP address as 0.0.0.0, DRAC 4 will not search for any server.



NOTE: You can specify a list of LDAP or Global Catalog servers separated by commas. DRAC 4 allows you to specify up to three IP addresses or hostnames.



NOTE: If LDAPS is not correctly configured for all domains and applications, enabling it may result in unexpected results during the functioning of the existing applications/domains.

- 3 If DHCP is enabled on the DRAC 4 and you want to use the DNS provided by the DHCP server, type the following racadm command:

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

- 4 If DHCP is disabled on the DRAC 4 or you want manually to input your DNS IP address, type the following racadm commands:

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

```
racadm config -g cfgLanNetworking -o cfgDNSServer1  
<primary DNS IP address>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2  
<secondary DNS IP address>
```

Standard Schema Active Directory Overview

As shown in Figure 5-4, using standard schema for Active Directory integration requires configuration on both Active Directory and the DRAC 4. On the Active Directory side, a standard group object is used as a role group. A user with DRAC 4 access is a member of the role group. In order to give this user access to a specific DRAC 4 card, the role group name and its domain name need to be configured on the specific DRAC 4 card. Unlike the extended schema solution, the role and the privilege level is defined on each DRAC 4 card, not in the Active Directory. Up to five role groups can be configured and defined in each DRAC 4. Table B-3 shows the privileges level of the role groups and Table 5-8 shows the default role group settings.


 **NOTE:** You can enable Standard Schema via the `racadm` CLI tool only. For more information, see "Configuring the DRAC 4 with Standard Schema Active Directory and the `racadm` CLI."

Figure 5-4. Configuration of DRAC 4 with Microsoft Active Directory and Standard Schema

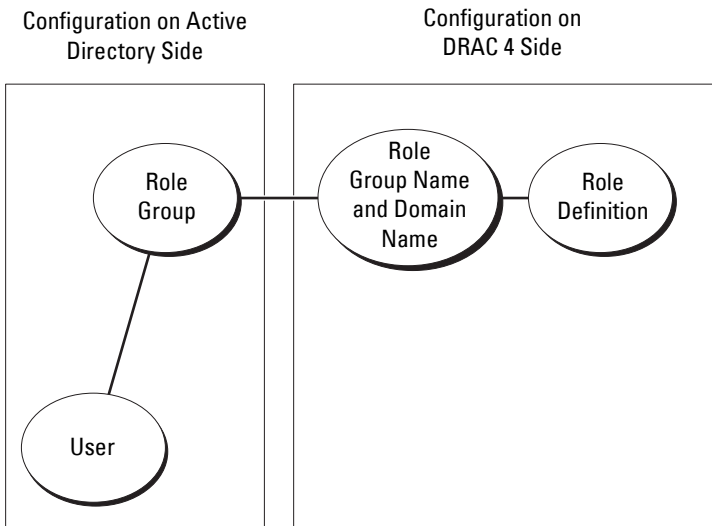



Table 5-8. Default Role Group Privileges

Role Groups	Default Privilege Level	Permissions Granted	Bit Mask
Role Group 1	Administrator	Login to DRAC, Configure DRAC, Configure Users, Clear Logs, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts, Execute Diagnostic Commands	0x000001ff
Role Group 2	Power User	Login to DRAC, Clear Logs, Execute Server Control Commands, Access Console Redirection, Access Virtual Media, Test Alerts	0x000000f9
Role Group 3	Guest User	Login to DRAC	0x00000001
Role Group 4	None	No assigned permissions	0x00000000
Role Group 5	None	No assigned permissions	0

 **NOTE:** The Bit Mask values are used only when setting Standard Schema via the racadm CLI tool.

In this version of DRAC 4, there is one way to enable Standard Schema Active Directory:

- Via the RACADM CLI tool. See "Configuring the DRAC 4 with Standard Schema Active Directory and the racadm CLI."

Configuring Standard Schema Active Directory to Access Your DRAC 4

You need to perform the following steps to configure the Active Directory before an Active Directory user can access the DRAC 4:

- 1 On an Active Directory server (domain controller), open the Active Directory Users and Computers Snap-in.
- 2 Create a group or select an existing group. The name of the group and the name of this domain will need to be configured on the DRAC 4 via the racadm CLI tool (see "Configuring the DRAC 4 with Standard Schema Active Directory and the racadm CLI").
- 3 Add the Active Directory user as a member of the Active Directory group to access the DRAC 4.

Configuring the DRAC 4 with Standard Schema Active Directory and the racadm CLI

Use the following commands to configure the DRAC 4 with Standard Schema Active Directory using the racadm CLI tool.

- 1 Open a command prompt and type the following racadm commands:

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

```
racadm config -g cfgActiveDirectory -o cfgADType 0x2
```

```
racadm config -g cfgActiveDirectory -o  
cfgADRootDomain <fully qualified root domain name>
```


```
racadm config -g cfgStandardSchema -i <index> -o  
cfgSSADRoleGroupName <common name of the role  
group>
```

```
racadm config -g cfgStandardSchema -i <index> -o  
cfgSSADRoleGroupDomain <fully qualified domain  
name>
```

```
racadm config -g cfgStandardSchema -i <index> -o  
cfgSSADRoleGroupPrivilege <Bit Mask Number for  
specific user permissions>
```

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

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

 **NOTE:** For Bit Mask number values, see Table B-3.

- 2 If DHCP is enabled on the DRAC 4 and you want to use the DNS provided by the DHCP server, type the following racadm command:

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

- 3 If DHCP is disabled on the DRAC 4 or you want manually to input your DNS server IP address, type the following racadm commands:

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

```
racadm config -g cfgLanNetworking -o cfgDNSServer1  
<primary DNS IP address>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2  
<secondary DNS IP address>
```

Enabling SSL on a Domain Controller

If you are using the Microsoft Enterprise Root CA to automatically assign all your domain controllers to an SSL certificate, perform the following steps to enable SSL on each domain controller.

- 1 Install a Microsoft Enterprise Root CA on a Domain Controller.
 - a Click **Start** and select **Settings**→**Control Panel**→**Add or Remove Programs**.
 - b In the **Add or Remove Programs** window, click **Add/Remove Windows Components**.
 - c In the **Windows Components Wizard**, select the **Certificate Services** check box.
 - d Select **Enterprise root CA** as **CA Type** and click **Next**.
 - e Select **Common name for this CA**, click **Next**, and click **Finish**.

- 2 Enable SSL on each of your domain controllers by installing the SSL certificate for each controller.
 - a Click **Start** and select **Settings**→**Control Panel**→**Administrative Tools**→**Domain Security Policy**.
 - b Expand the **Public Key Policies** folder, right-click **Automatic Certificate Request Settings** and click **Automatic Certificate Request**.
 - c In the **Automatic Certificate Request Setup Wizard**, click **Next** and select **Domain Controller**.
 - d Click **Next** and click **Finish**.

Exporting the Domain Controller Root CA Certificate



NOTE: If your system is running Windows 2000, the following steps may vary.

- 1 Locate the domain controller that is running the Microsoft Enterprise CA service.
- 2 Click **Start** and select **Run**.
- 3 In the **Run** field, type **mmc** and click **OK**.
- 4 In the **Console 1** (MMC) window, click **File** (or **Console** on Windows 2000 systems) and select **Add/Remove Snap-in**.
- 5 In the **Add/Remove Snap-In** window, click **Add**.
- 6 In the **Standalone Snap-In** window, select **Certificates** and click **Add**.
- 7 Select **Computer** account and click **Next**.
- 8 Select **Local Computer** and click **Finish**.
- 9 Click **OK**.
- 10 In the **Console 1** window, expand the **Certificates** folder, expand the **Personal** folder, and click the **Certificates** folder.
- 11 Locate and right-click the root CA certificate, select **All Tasks**, and click **Export...**
- 12 In the **Certificate Export Wizard**, click **Next**, and select **No do not export the private key**.
- 13 Click **Next** and select **Base-64 encoded X.509 (.cer)** as the format.
- 14 Click **Next** and save the certificate to a directory on your system.

- 15 Upload the certificate you saved in step 14 to the DRAC 4.

To upload the certificate using racadm CLI commands, see "Configuring the DRAC 4 with Extended Schema Active Directory and the racadm CLI."

To upload the certificate using the Web-based interface, perform the following steps:

- a Open a supported Web browser window. See "Supported Web Browsers."
- b Log in to the DRAC 4 Web-based interface.
- c Expand the **System** tree and click **Remote Access**.
- d Click the **Configuration** tab and then click **Active Directory**.
- e In the **Certificate Upload** page, click **Browse** and select the certificate or type the path to the certificate in the **Value** field.
- f Click **Apply**.
- g Click **Finish** and then click **OK**.

Importing the DRAC 4 Firmware SSL Certificate

Use the following procedure to import the DRAC 4 firmware SSL certificate to all domain controller trusted certificate lists.



NOTE: If the DRAC 4 firmware SSL certificate is signed by a well-known CA, you do not need to perform the steps described in this section.



NOTE: The following steps may vary slightly if you are using Windows 2000.

The DRAC 4 SSL certificate is the identical certificate used for the DRAC 4 Web server. All DRAC 4 controllers are shipped with a default self-signed certificate. To access the certificate using the DRAC 4 Web-based interface, click the **Configuration** Tab, click **Active Directory**, and then click **Download DRAC 4 Server Certificate**.

- 1 On the domain controller, open an **MMC Console** window and select **Certificates**→**Trusted Root Certification Authorities**.
- 2 Right-click **Certificates**, select **All Tasks** and click **Import**.
- 3 Click **Next** and browse to the SSL certificate file.

- 4 Install the RAC SSL Certificate in each domain controller's **Trusted Root Certification Authority**.

If you have installed your own certificate, ensure that the CA signing your certificate is in the **Trusted Root Certification Authority** list. If the Authority is not in the list, you must install it on all your Domain Controllers.

- 5 Click **Next** and select whether you would like Windows to automatically select the certificate store based on the type of certificate, or browse to a store of your choice.
- 6 Click **Finish** and click **OK**.

Using Active Directory to Log In to the DRAC 4

You can use Active Directory to log in to the DRAC 4 through the Web-based interface, remote racadm, or the serial or telnet console.

The login syntax is consistent for all three methods:

```
<username@domain> or <domain>\<username> or  
<domain>/<username>
```

where *<username>* is an ASCII string of 1–256 bytes. No white space and no special characters (such as \, /, or @) are allowed in either the user name or the domain name.




NOTE: You cannot specify NetBIOS domain names, such as Americas, since those names cannot be resolved.

4096-Bit Key Encryption

DRAC 4 firmware version 1.40 and later support 4096-bit key encryption between the managed system and the Active Directory server—a practice that is recommended by Microsoft.

In the standard Active Directory environment, the user name and password is authenticated by exchanging user information between Active Directory systems in a corporate network. In firmware 1.40 and later, user authentication is achieved by exchanging user information and the CA certificate directly between the DRAC 4 card and the Active Directory system using 4096-bit key encryption. The Active Directory server transmits a trusted CA certificate to

the DRAC card for validation. The DRAC card validates the CA certificate and extracts the private key from the certificate, which is used to decrypt transmissions between the DRAC card and the Active Directory server.

 **NOTE:** Depending on your network configuration, authentication may require up to 90 seconds to complete.

Frequently Asked Questions

Table 5-9 lists frequently asked questions and answers.

Table 5-9. Using the DRAC 4 With Active Directory: Frequently Asked Questions

Question	Answer
Can I log into the DRAC 4 using Active Directory across multiple trees?	Yes. The DRAC 4's Active Directory querying algorithm supports multiple trees in a single forest.
Does the log in to the DRAC 4 using Active Directory work in mixed mode (that is, the domain controllers in the forest run different operating systems, such as Microsoft Windows NT® 4.0, Windows 2000, or Windows Server 2003)?	Yes. In mixed mode, all objects used by the DRAC 4 querying process (among user, RAC Device Object, and Association Object) have to be in the same domain. The Dell-extended Active Directory Users and Computers snap-in checks the mode and limits users in order to create objects across domains if in mixed mode.
Does using the DRAC 4 with Active Directory support multiple domain environments?	Yes. The domain forest function level must be in Native mode or Windows 2003 mode. In addition, the groups among Association Object, RAC user objects, and RAC Device Objects (including Association Object) must be universal groups.
Can these Dell-extended objects (Dell Association Object, Dell RAC Device, and Dell Privilege Object) be in different domains?	The Association Object and the Privilege Object must be in the same domain. The Dell-extended Active Directory Users and Computers snap-in forces you to create these two objects in the same domain. Other objects can be in different domains.

Table 5-9. Using the DRAC 4 With Active Directory: Frequently Asked Questions (continued)

Question	Answer
Are there any restrictions on Domain Controller SSL configuration?	Yes. All Active Directory servers' SSL certificates in the forest must be signed by the same root CA since DRAC 4 only allows uploading one trusted CA SSL certificate.
I created and uploaded a new RAC certificate and now the Web-based interface does not launch.	If you use Microsoft Certificate Services to generate the RAC certificate, one possible cause of this issue is that you inadvertently chose User Certificate instead of Web Certificate when creating the certificate. To recover, generate a CSR and create a new Web certificate from Microsoft Certificate Services and load it using the racadm CLI from the managed system by typing: <pre>racadm sslcsrgen [-g] [-u] [-f {filename}] racadm sslcertupload -t 0x1 -f <web_sslcert></pre>

Table 5-9. Using the DRAC 4 With Active Directory: Frequently Asked Questions (continued)

Question	Answer
What can I do if I cannot log into the DRAC 4 using Active Directory authentication? How do I troubleshoot the issue?	<p>Troubleshoot as follows:</p> <ul style="list-style-type: none">• Ensure that you have checked the Enable Active Directory box on the DRAC 4 Active Directory configuration page.• Ensure that the DNS setting is correct on the DRAC 4 Networking configuration page.• Ensure that you have uploaded the Active Directory certificate from your Active Directory root CA to the DRAC 4.• Check the Domain Controller SSL certificates to ensure that they have not expired.• Ensure that your "DRAC 4 Name", "Root Domain Name", and "DRAC 4 Domain Name" match your Active Directory environment configuration.• Ensure that you use the correct user domain name during a login and not the NetBIOS name.

Using Console Redirection

Overview

The DRAC 4 console redirection feature allows you to access the local server console remotely in either graphic or text mode.

Today, with the power of networking and the Internet, you do not have to sit in front of each server to perform all the routine maintenance. You can manage the servers from another city or even from the other side of the world from your desktop or laptop computer. You can also share the information with others—remotely and instantly.

Using Console Redirection



NOTICE: Before using console redirection, install the Sun Java Virtual Machine Plug-in (version 1.4.2 and later) on all supported Web browsers. Additionally, clear and disable Java cache from the Java plug-in control panel in your operating system. For more information, see "Configuring a Supported Web Browser" and "Installing the Sun Java Plug-In."



NOTE: When you open a console redirection session, there is no indication on the managed system that the console has been redirected.



NOTE: On supported Linux (Red Hat® or Novell®) systems, there are known mouse arrow synchronization issues. To minimize mouse synchronization problems, ensure that all users use the default mouse settings.

The **Console Redirection** page enables you to manage the remote system by using the keyboard, video, and mouse on your local management station to control the corresponding devices on a remote managed system. This feature can be used in conjunction with the Virtual Media feature to perform remote software installations. You can have a maximum of two simultaneous console redirection sessions. Console Redirection requires a minimum available network bandwidth of 128 Kbps.

Keyboard, Video, and Mouse Encryption

The DRAC 4 firmware version 1.40 and later provides RC4 128-bit encryption for your keyboard, video, and mouse functions. This encryption feature provides a secure environment when transmitting data and video to and from the DRAC 4 in the managed system. All keyboard and mouse functions are encrypted by default.

To enable 128-bit video encryption, use the following racadm CLI command:

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

To disable 128-bit video encryption, use the following racadm CLI command:

```
racadm config -g cfgRacTuning -o  
cfgRacTuneConRedirEncryptEnable 0
```

See "cfgRacTuneConRedirEncryptEnable (Read/Write)" for more information.

Opening a Console Redirection Session



NOTE: The recommended display resolution on the managed system is 1024 x 768 pixels at 256 colors or the **Medium** setting (16-bit).

- 1 Open a Web browser on your management station.
- 2 Connect and log into the DRAC 4.
- 3 In the left window pane, click **Console**.
- 4 In the **Console Redirection** page, read and follow the instructions for starting a console redirection session.
- 5 Examine the information provided on the **Console Redirection** page (see Table 6-1 and Table 6-2) to ensure that a console redirection session is currently available.

Table 6-1. Console Redirection Page Information

Information	Description
Current console redirection status	Displays the status of console redirection.
Maximum console redirection sessions	Displays the number of console redirection sessions that are available.
Current console redirection sessions	Displays the number of active console redirection sessions.

Table 6-2. Other Console Redirection Page Buttons

Button	Action
Open	Opens the Console Redirection page.
Print	Prints the Console Redirection page.
Refresh	Reloads the Console Redirection page.

- 6** Click **Open Console** to open a new console.
- 7** Use the buttons on the **Console Redirection Viewer** page (see Table 6-3) to help you perform actions on the remote system.

Table 6-3. Console Redirection Viewer Page Buttons

Button	Action
Keyboard Macros	Selects and types one of the following keystroke combinations that cannot be typed using your local keyboard without affecting your local system. <Ctrl><Alt><Delete> <Tab> <Alt><Tab> <Alt><Esc> <Ctrl><Esc> <Ctrl><Enter> <Alt><Space> <Alt><Enter> <Alt><Hyphen> <Alt><F4> <Print Screen> <Alt><Print Screen> <F1> <Pause> <SysRq> <Alt><SysRq> <Alt><(Left) Shift><(Right) Shift><Esc>
Send	Sends the selected keystroke macro.
Keystroke Prefix	Selects a key that acts as a previous keystroke to your actual keystrokes. Select either <Ctrl>, <Alt>, or <SysRq>.
Mouse Acceleration	Selects the operating system you are using to optimize console redirection mouse performance. Select Windows , Linux , or NetWare .
Refresh	Completely updates the entire remote system-screen viewport.
Help	Opens the online help for the Console Redirect screen.

Table 6-3. Console Redirection Viewer Page Buttons (continued)

Button	Action
Create Snapshot	Captures the current remote system screen to a .jpg file on the local system. A dialog box is displayed that allows you to save the .jpg file to a specified location.
Close	Exits the Console Redirection page.

Frequently Asked Questions

Table 6-4 lists frequently asked questions and answers.

Table 6-4. Using Console Redirection: Frequently Asked Questions

Question	Answer
I have just installed the Sun Java Runtime Environment on a management station running the Microsoft® Windows® XP operating system. Do I have to reboot the system?	You must reboot your system after you install the Sun Java Runtime Environment to complete the installation.
Why doesn't the default video driver for Novell Netware® 6.5 work correctly at 800x600 screen resolution when using Console Redirection?	To correct this problem, go to the screen resolution setting and select ATI RADEON VE, 32MB. The resolution selection is not limited to 1024x768. Do not select any resolution higher than 1024x768. Console Redirection supports these resolutions: 640x480, 800x600, and 1024x768.

Table 6-4. Using Console Redirection: Frequently Asked Questions (continued)

Question	Answer
During Console Redirection, the keyboard and mouse became locked after coming back from hibernation on a Windows 2000 system. What caused this to happen?	To resolve this issue, you must reset the DRAC 4 by running the racadm racreset command. If the problem is still not resolved, you must reset the DRAC 4 by running the racadm racreset hard command.
During Console Redirection, the mouse became locked after coming back from hibernation on a Windows 2003 system. Why did this happen?	To resolve this issue, select a different operating system than Windows for mouse acceleration from the virtual KVM (vKVM) window pull-down menu, wait 5 to 10 seconds, and then select Windows again. If the problem is not resolved, you must reset the DRAC 4 by running the racadm racreset command. If the problem is still not resolved, you must reset the DRAC 4 by running the racadm racreset hard command.
Why does the remote console get a blank screen in BIOS or DOS?	You may have an old version of the ATI video BIOS or a bad ATI chip.
Why aren't the vKVM keyboard and mouse working?	You must set the USB controller to On with BIOS support in the BIOS settings of the managed system. Restart the managed system and press <F2> to enter setup. Select Integrated Devices , and then select USB Controller . Save your changes and restart the system.
Why does the managed system console screen go blank when Windows has a blue screen?	The managed system does not have the correct ATI video driver. You must update the video driver by using the <i>Dell Systems Console and Agent</i> CD or the <i>Dell Systems Management Tools and Documentation</i> DVD.

Table 6-4. Using Console Redirection: Frequently Asked Questions (continued)

Question	Answer
Why do I get a blank screen on the remote console after completing a Windows 2000 installation?	The managed system does not have the correct ATI video driver. The DRAC 4 Console Redirection will not run correctly on the SVGA video driver on the Windows 2000 distribution CD. You must install Windows 2000 by using the <i>Dell Systems Build and Update Utility</i> CD or the <i>Dell Systems Management Tools and Documentation</i> DVD to ensure that you have the latest, supported drivers for the managed system.
Why do I get a blank screen on the managed system when loading the Windows 2000 operating system?	The managed system does not have the correct ATI video driver. You must update the video driver by using the <i>Dell Systems Console and Agent</i> CD or the <i>Dell Systems Management Tools and Documentation</i> DVD.
Why do I get a blank screen on the managed system in the Windows full screen DOS window?	The managed system does not have the correct ATI video driver. You must update the video driver by using the <i>Dell Systems Console and Agent</i> CD or the <i>Dell Systems Management Tools and Documentation</i> DVD.
After I click Open Console , the message <i>Please wait while vKVM applet is loaded...</i> is displayed with the Wait icon. Why is nothing happening?	Make sure that you have installed Sun Java JRE 1.4.2 or later on the management station. You must also disable the Java cache from the Java Control Panel. You can download this JRE version from java.sun.com .
After I upgrade the firmware to get a vKVM fix, why is the fix not there?	You need to clear the browser cache and the Java plug-in cache. Then, you must disable the Java plug-in cache.
Why can't I enter BIOS setup by pressing the <F2> key?	This behavior is typical in a Windows environment. Use your mouse to click on an area of the Console Redirection window to adjust the focus. To move the focus to the bottom menu bar of Console Redirection window, use the mouse and click one of the objects on the bottom menu bar.

Table 6-4. Using Console Redirection: Frequently Asked Questions (*continued*)

Question	Answer
How can I set the server display to 256 colors on Windows 2003?	<p>To set the server display to 256 colors:</p> <ul style="list-style-type: none">• Right-click desktop.• Select Properties.• Click the Settings tab.• Click the Advanced button.• Click the Adapter tab.• Click the List All Modes... button.• Select, for example: 1024x768, 256 Colors, 60 Hertz.
Why doesn't the vKVM mouse sync when I use the <i>Dell Systems Console and Agent CD</i> (or the <i>Dell Systems Management Tools and Documentation DVD</i>) to remotely install the operating system?	<p>Reason for setting the server display to 256 colors:</p> <p>The FPGA does color matching the best it can. However, sometimes when a color is borderline, it displays differently than what you would expect. If you can't see the color correctly, change the color depth to 256 colors on the managed system.</p> <p>Select Linux for mouse acceleration on the vKVM window pull-down menu.</p>
Why doesn't the vKVM mouse sync after coming back from hibernation on a Windows system?	<p>Select a different operating system for mouse acceleration on the vKVM window pull-down menu. Then, go back to the original operating system to initialize the USB mouse device.</p>

Table 6-4. Using Console Redirection: Frequently Asked Questions (continued)

Question	Answer
Why doesn't the mouse sync in DOS when performing Console Redirection?	The Dell BIOS is emulating the mouse driver as a PS/2 mouse. By design, the PS/2 mouse uses relative position for the mouse pointer, which causes the lag in syncing. DRAC 4 has a USB mouse driver, which allows absolute position and closer tracking of the mouse pointer. Even if DRAC 4 passes the USB absolute mouse position to the Dell BIOS, the BIOS emulation would convert it back to relative position and the behavior would remain.
Why doesn't the mouse sync under the Red Hat Enterprise Linux text console?	Virtual KVM requires the USB mouse driver, but the USB mouse driver is available only under X-Windows.
Is there a way to verify that the ATI video driver update is installed on Red Hat Enterprise Linux version 2.1?	Red Hat Enterprise Linux version 3 update 3 or greater and Red Hat Enterprise Linux version 2.1 update 5 or greater already have suitable video drivers. On other versions you can verify the video driver update with the command: <pre>rpm -qa grep radeon_7000m_dell_server</pre> The RPM <code>rhel**_radeon_7000m_dell_server-0.4-1</code> or later should be installed. This RPM is available at www.dell.com .

Table 6-4. Using Console Redirection: Frequently Asked Questions (continued)

Question	Answer
Why doesn't the vKVM mouse work with Red Hat Enterprise Linux, version 2.1, update 3?	<p>Red Hat Enterprise Linux, version 2.1 does not fully support multiple input devices.</p> <p>You must manually select the USB mouse if there is a PS/2 mouse already connected to the managed system. You can do this by running the Red Hat Enterprise Linux mouseconfig command and then selecting the type of mouse (USB) from the mouseconfig GUI. Only one of the mice (either the USB or the PS/2) can be active at a given time. Other solutions are to upgrade to Red Hat Enterprise Linux, version 3, or to remove the mouse attached to the managed system.</p> <p>To use mouseconfig to enable RAC mouse control for XWindows:</p> <ol style="list-style-type: none">1 Run Xconfigurator (if not previously run before).2 Run mouseconfig GUI.3 Select Generic Mouse (USB).4 Run Xwindows (startx). <p>To use mouseconfig to re-enable local mouse control:</p> <ol style="list-style-type: none">1 Run mouseconfig GUI.2 Select Generic Mouse (PS/2).3 Logout and log back in to activate the PS/2 mouse.
Is there a vKVM mouse sync issue in Novell NetWare 6.5 operating system with 800x600 screen resolution? The mouse sync works OK with 1024x768.	<p>Use the <i>Dell Systems Console and Agent</i> CD or the <i>Dell Systems Management Tools and Documentation</i> DVD to install the NetWare operating system. The default screen resolution is 1024x768 so you won't have the issue with mouse sync.</p>
Why doesn't the vKVM mouse and keyboard work when changing mouse acceleration for different operating systems?	<p>The USB vKVM keyboard and mouse are inactive from 5 to 10 seconds after changing the mouse acceleration. The network load can sometimes cause this operation to take longer than normal (more than 10 seconds).</p>

Table 6-4. Using Console Redirection: Frequently Asked Questions (continued)

Question	Answer
Why can't I see the bottom of the server screen from the vKVM window?	Make sure the server screen resolution is in one of the supported resolutions (640x480, 800x600, and 1024x768).
Why can't I use a keyboard or mouse while installing a Microsoft operating system remotely by using DRAC4 Console Redirection?	<p>When you remotely install a supported Microsoft operating system on a system with Console Redirection enabled in the BIOS, you receive an EMS Connection Message that requires that you select OK before you can continue. You cannot use the mouse to select OK remotely. You must either select OK on the local system or restart the remotely managed system, reinstall, and then turn Console Redirection Off in the BIOS.</p> <p>This message is generated by Microsoft to alert the user that Console Redirection is enabled. In order to ensure that this message does not appear, always turn off Console Redirection in the BIOS before installing an operating system remotely.</p>
I manually selected Other Display as Primary from the vKVM window and now I cannot remotely control the system.	<p>In order to allow remote access after manually selecting Other Display as Primary, you must perform the following steps:</p> <ol style="list-style-type: none"><li data-bbox="392 826 1006 850">1 Use the DRAC 4's power control to power cycle the unit.<li data-bbox="392 858 1006 970">2 During reboot, press <F8> and select to boot windows in safe mode (the POST screen will be visible from the DRAC 4 user interface). Safe mode uses the DRAC 4 as the primary video.<li data-bbox="392 978 1006 1034">3 Go to the Windows device manager and uninstall both video adaptors.<li data-bbox="392 1042 1006 1066">4 Reboot the system.<li data-bbox="392 1074 1006 1195">5 Reload the operating system. The hardware wizard finds both video controllers and restores the DRAC 4 as the primary display (the screen blinks a few times after you press <Ctrl><Alt> to login).

Table 6-4. Using Console Redirection: Frequently Asked Questions (continued)

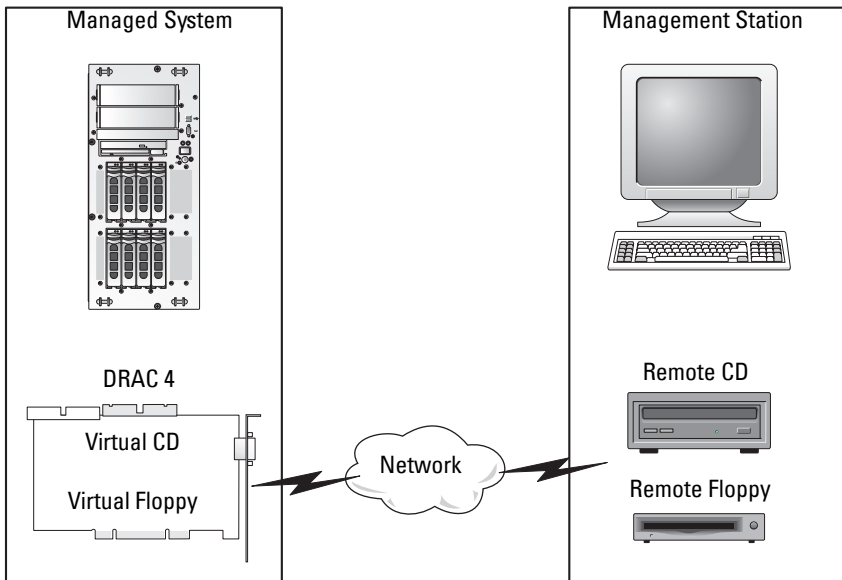
Question	Answer
Why does console redirection fail to show the operating system boot menu in the Chinese, Japanese, and Korean versions of Microsoft Windows 2000?	On systems running Windows 2000 that can boot to multiple operating systems, change the default boot operating system by performing the following steps: 1 Right-click the My Computer icon and select Properties . 2 Click the Advanced tab. 3 Click Startup and Recovery . 4 Select the new default operating system from the Startup list. 5 In the Show list for box, type the number of seconds that the list of choices should be displayed before the default operating system automatically boots.
Why doesn't the Num Lock indicator on my management station reflect the status of the Num Lock on the remote server?	When accessed through the DRAC 4, the Num Lock indicator on the management station does not necessarily coincide with the state of the Num Lock on the remote server. The state of the Num Lock is dependent on the setting on the remote server when the remote session is connected, regardless of the state of the Num Lock on the management station.
Why do I have mouse synchronization problems?	On Linux (Red Hat or Novell) systems, there are known mouse arrow synchronization issues. To minimize mouse synchronization problems, ensure that all users use the default mouse settings.

Configuring and Using Virtual Media

Overview

The Virtual Media feature provides the managed system with a virtual floppy diskette drive and a virtual CD drive, which can use standard media from anywhere on the network. Figure 7-1 shows the overall architecture of virtual media.

Figure 7-1. Overall Architecture of Virtual Media



Using Virtual Media, administrators can remotely boot their managed systems, install applications, update drivers, or even install new operating systems remotely from the virtual CD/floppy diskette drives.

The managed system is configured with a DRAC 4 card. The virtual CD and floppy drives are two electronic devices embedded in the DRAC 4 that are controlled by the DRAC 4 firmware. These two devices are present on the managed system's operating system and BIOS at all times, whether virtual media is connected or disconnected.

The management station provides the physical media or image file across the network. For the virtual media feature to work, the virtual media plug-in must be installed on the management station. When you launch the RAC browser for the first time and you access the virtual media page, the virtual media plug-in is downloaded from the DRAC 4 Web server and is automatically installed on the management station.

When virtual media is connected, all virtual CD/floppy drive access requests from the managed system are directed to the management station across the network. Connecting virtual media is identical to inserting media into virtual devices. When virtual media is not connected, virtual devices on the managed system behave just like two drives without media present. Virtual media requires a minimum available network bandwidth of 128 Kbps.

Table 7-1 lists the supported drive connections for virtual floppy and virtual optical drives.



NOTE: Changing virtual media while connected could stop the system boot sequence.

Table 7-1. Supported Drive Connections

Supported Virtual Floppy Drive Connections	Supported Virtual Optical Drive Connections
Legacy 1.44 floppy drive with a 1.44 floppy diskette	CD-ROM, CDRW, or a combination drive with CD-ROM media
USB floppy drive with a 1.44 floppy diskette	DVD, DVD-RW, or combination drive with DVD media
1.44 floppy image	CD-ROM image file in the ISO 9660 format
USB memory key	USB CD-ROM or DVD drive with CD-ROM or DVD media

Installing the Virtual Media Plug-In

The virtual media browser plug-in must be installed on your management station to use the virtual media feature. After you open the DRAC 4 user interface and launch the Virtual Media page, the browser automatically downloads the plug-in, if required. If the plug-in is successfully installed, the Virtual Media page displays a list of floppy diskettes and optical disks that connect to the virtual drive.

Windows-Based Management Station

To run the virtual media feature on a management station running the Microsoft® Windows® operating system, install a supported version of Internet Explorer with the ActiveX Control plug-in. Set the browser security to **Medium** or a lower setting to enable Internet Explorer to download and install signed ActiveX controls.

See "Supported Web Browsers" for the supported Internet Explorer browser version.


Additionally, you must have administrator rights to install and use the virtual media feature. Before installing the ActiveX control, Internet Explorer may display a security warning. To complete the ActiveX control installation procedure, accept the ActiveX control when prompted by Internet Explorer.

Linux-Based Management Station

To run the virtual media feature on a management station running the Red Hat® Enterprise Linux® operating system, install a supported version of Mozilla or Firefox. If the virtual media plug-in is not installed or if a newer version is available, a dialog box appears during the installation procedure to confirm the plug-in installation on the management station. Ensure that the user ID running the browser has write permissions in the browser's directory tree. If the user ID does not have write permissions, you cannot install the virtual media plug-in.

See "Supported Web Browsers" for a list of support Red Hat Enterprise Linux Web browsers.


Using the Virtual Media Feature


-  **NOTE:** If your system is running a supported 64-bit operating system (see Table 1-4), install and run a supported 32-bit Web browser (see Table 1-5). Otherwise, you may experience unexpected results when running Virtual Media and other processes. See "Supported Web Browsers for 64-Bit Operating Systems" for more information.

To use the virtual media feature, perform the following steps:


- 1 Open a supported Web browser on your management station. See "Supported Web Browsers."
- 2 Connect and log into the DRAC 4.
- 3 Click **Media** in the left pane to display a new page and download the virtual media plug-in, if it has not already been installed.

All the available drives are listed under **Floppy Drive** or **CD-ROM Drive**.

-  **NOTE:** A USB memory key or a floppy image file is also listed under **Floppy Drive** because they could be virtualized as a virtual floppy. You can choose one CD-ROM and one floppy at the same time, or only one of them if you want.

-  **NOTE:** The drive letters of virtual devices on the managed system have no correlation to the drive letters of physical drives on the management station.

- 4 Select the drives that you want to virtualize and click **Connect**.

-  **NOTE:** To virtualize a floppy drive, the drive cannot be in use by another application. If the floppy drive is in use, it will not appear as a selectable option. This behavior occurs as designed by Microsoft.

If this connection is authenticated, the connection status becomes **Connected** and a list of all connected drives is displayed.

Booting From the Virtual Media

On supported systems, the system BIOS allows you boot from virtual CD or virtual floppy drives. You need to enter the BIOS setup window to ensure that the virtual drives are enabled in the boot sequence menu and that bootable devices are in the correct order.

To change the BIOS setting, perform the following steps:

- 1 Boot the managed system.
- 2 Press <F2> to enter the BIOS setup window.


- 3 Scroll to the boot sequence and press <Enter>.

In the pop-up window, the virtual CD and virtual floppy drives are listed along with other regular boot devices.


- 4 Ensure that the virtual drive is enabled and that it is the first device with bootable media present among the listed devices. If it is not the first device, you can change the boot order by following the on-screen instructions.
- 5 Save the changes and exit.

The managed system reboots.

The managed system attempts to boot from a bootable device based on the boot order. If virtual device is connected and a bootable media is present, the system boots to this virtual device. Otherwise, the system skips it, just like a physical device without bootable media.

 **NOTE:** You have to connect the virtual media before the IDE option ROM runs in order to boot from the virtual media.

Installing Operating Systems Using Virtual Media

 **NOTE:** The two virtual drives work simultaneously only when the operating system is running. During the operating system installation using the virtual CD drive, the virtual floppy drive is not available.

- 1 Ensure that your operating system installation CD is inserted in the management station's CD drive.
- 2 Ensure that you have selected your local CD drive and that you have connected to the virtual drives.
- 3 Follow the steps for booting from the virtual media in the "Booting From the Virtual Media" section to ensure that the BIOS is set to boot from the CD drive that you are installing from.
- 4 Follow the on-screen instructions to complete the installation.

Using Virtual Media When the Server's Operating System Is Running

Windows-Based System

On Windows systems, the virtual media drives are mounted and given a drive letter.

Using the virtual drives from within Windows is similar to using your physical drives. Once connected to the media at a management station, the media is available at the system by simply clicking the drive and browsing its content.

Linux-Based System

On a Red Hat Enterprise Linux system, the virtual drives must be mounted before the drives can be accessed. Before mounting the drive, connect to the media at the management station.

Red Hat Enterprise Linux automatically creates mount points in the `/etc/fstab` file for the virtual floppy and CD drives.

To identify the assigned virtual media devices, type the following command:

```
cat /var/log/messages | grep VIRTUAL
```

The virtual CD has an entry for a device named `/dev/cdromX` (where `X` is an optional index that is assigned by Red Hat Enterprise Linux). Normally, the virtual CD drive is named `/dev/cdrom1` and the local CD drive is named `/dev/cdrom`.

The virtual floppy drive has an entry for a device named `/dev/floppyX` (where `X` is an optional index that is assigned by Red Hat Enterprise Linux). Depending upon whether or not there is a local floppy drive, the virtual floppy drive is named `/dev/floppy` or `/dev/floppy1`.

Enabling and Disabling the Virtual Media Feature

Virtual media can be enabled and disabled using the `racadm` command. You can run this command at any time; however, enabling or disabling the virtual media feature does not take effect until you restart your system.

Virtual Media can also be enabled or disabled in the Option ROM, as described in Table 2-1.



NOTE: You cannot use the Web user interface to enable or disable virtual media.

After system restart, the DRAC 4 IDE Option ROM utility will time-out for up to 15 seconds (about 7.5 seconds per virtual device) when the virtual media feature is disabled.

The virtual media feature is enabled by default. When disabled, DRAC disables the virtual CD/floppy diskette drives from the IDE bus and generates the following messages:

```
Drive Number: 0 failed to detect Virtual device
Drive Number: 1 failed to detect Virtual device
```

Enabling Virtual Media

To enable the virtual media feature, type the following command. The default flag state is 0, indicating that the feature is enabled.

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

Disabling Virtual Media

To disable the virtual media feature, type the following command:

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

Configuring the Virtual Floppy Feature For Your Operating System

The DRAC 4 configures the virtual floppy device as a removable media disk. Use the **racadm** command to configure the virtual floppy device to appear as a hard drive or a super-floppy drive to your operating system.

The virtual floppy device configuration determines how your operating system will assign new drive letters. For example, if your system is running Windows Server 2000 with Service Pack 4 or Windows Server 2003, the operating system detects and configures the first detectable hard drive as the C drive. This Windows behavior may assign drive letter C to the virtual floppy if it was configured to appear as a hard drive. However, when Windows detects your virtual floppy drive as a super-floppy drive during the installation procedure or when it first detects the drive, it assigns a drive letter starting with A.

To modify how the virtual floppy appears to the operating system (as a super-floppy drive or hard drive), use the `racadm` command to reconfigure the `cfgFloppyEmulation` object.



NOTE: In the Windows Control Panel, **Dell VSF** and **Dell Virtual VCD** identify the Virtual Floppy and Virtual CD-ROM, respectively.

Configuring the Virtual Floppy Feature as a Super Floppy

To configure your operating system to identify your virtual floppy as a super floppy starting with drive letter A, change the `cfgFloppyEmulation` object setting to 1.

For example:

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

The DRAC 4 IDE Option ROM utility displays the following string during system restart:

```
DELL-VIRTUALS-120 Removable Media Drive
```

Configuring the Virtual Floppy as a Hard Drive

To configure your operating system to identify your virtual floppy as a hard drive starting with drive letter C, change the `cfgFloppyEmulation` object setting to 0.

For example:

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

In this example, the DRAC 4 IDE Option ROM utility displays the following string during system restart:

```
VIRTUALFLOPPY DRIVE Removable Media Drive
```

Frequently Asked Questions

Table 7-2 lists frequently asked questions and answers.

Table 7-2. Using Virtual Media: Frequently Asked Questions

Question	Answer
When I boot my system, the following messages appear during POST: Drive Number: 0 failed to detect Virtual device Drive Number: 1 failed to detect Virtual device	<ul style="list-style-type: none">• The Dell Virtual Media devices may have been disabled. To verify the device configurations, type the following command: <code>racadm getconfig -g cfgRacVirtual</code>• Ensure that the <code>cfgVirMediaDisable</code> object is set to 0 (Enabled).• You can enable the Virtual Media feature by changing the <code>cfgVirMediaDisable</code> object. Use the <code>racadm config</code> command to reset the object and then restart your system.
The virtual media device appears as drive letter C. This issue affects my scripts. How can I modify the drive letter?	<p>By default, the Dell Virtual Media Floppy device appears as a disk-drive device to the Windows operating system. This type of device is enumerated by Windows as drive letter C or higher. The Dell Virtual Media Floppy device can be configured to appear as a super-floppy drive using the <code>racadm</code> command. After you configure the virtual media device, the operating system assigns drive letter A or B to the virtual floppy device when the system is installed or when the drives are first discovered.</p> <p>To configure your Dell Virtual Media Floppy device as a super-floppy device:</p> <ol style="list-style-type: none">1 Type the following command: <code>racadm config -g cfgRacVirtual -o cfgFloppyEmulation 1</code>2 Restart your system.

Table 7-2. Using Virtual Media: Frequently Asked Questions (continued)

Question	Answer
I modified the virtual floppy device to emulate a super-floppy device and restarted my system. After restart, the drive letter(s) did not change.	The Dell Virtual Media drive letter enumeration is assigned when the operating system is first installed or if the DRAC 4 IDE controller is deleted and rescanned by the Microsoft Windows Device Manager.
Sometimes when I try to access virtual floppy media, the Windows File Explorer displays a "Not Responding" message in the title bar, but the floppy access light indicates that the floppy is still being accessed. Why does this happen?	The access to a 1.44 floppy is slow, especially over a network. As a result, you must wait long enough for Windows to read the floppy. The Windows File Explorer may display a "Not Responding" message in the title bar while it continues to read the floppy. Note that USB keys are faster to access.
Why does the Eject command fail to work?	The Eject command fails to work with Virtual CD devices if no Virtual Media client was connected at the time the Red Hat Enterprise Linux host was booted. To eject CD media from a Virtual CD device in this situation, ensure that the CD is not mounted, and then press the Eject button on the client CD drive.
I was using Internet Explorer and I did not install the Virtual Media plug-in when I was prompted to do so. Now, I can't use the Virtual Media feature.	To return to the dialog box for installing the Virtual Media plug-in, you can navigate away from the Media page and then navigate back to it to be prompted for the plug-in installation again.
A user has established a Virtual Media connection, but forgot about it. How can another user remove this connection?	Use the <code>racadm vmdisconnect</code> command to forcibly disconnect the virtual media connection

Table 7-2. Using Virtual Media: Frequently Asked Questions (continued)

Question	Answer
Why do error messages like the following display on the console when Red Hat Enterprise Linux boots a Dell server with a DRAC 4 present?	The Red Hat Enterprise Linux IDE driver writes all error responses that it receives to the console log for diagnostic purposes. However, in this case, the messages are not indications of any real errors and should be ignored.
... other console startup messages ... Apr 16 14:48:27 localhost kernel: hde: VIRTUALFLOPPY DRIVE, ATAPI FLOPPY drive	The reason these error responses are generated is because a Virtual Media client is not connected to the DRAC 4 management board while the system is being booted, but the Red Hat Enterprise Linux IDE driver is requesting information regarding the Virtual floppy media size. This information is not available until a Virtual Media client connects its floppy device to the DRAC 4.
Apr 16 14:48:27 localhost kernel: hdf: VIRTUALCDROM DRIVE, ATAPI CD/DVD-ROM drive	The error response, in this case, (key=2, asc=3a) from the DRAC 4 hardware indicates "media not present."
Apr 16 14:48:27 localhost kernel: ide0 at 0x1f0-0x1f7,0x3f6 on irq 14	
Apr 16 14:48:27 localhost kernel: ide-floppy: hde: I/O error, pc = 23, key = 2, asc = 3a, ascq = 0	
Apr 16 14:48:27 localhost kernel: ide-floppy: Can't get floppy parameters	
... other console startup messages ...	

Table 7-2. Using Virtual Media: Frequently Asked Questions (continued)

Question	Answer
I am viewing the contents of a floppy drive or USB memory key. If I try to establish a Virtual Media connection using the same drive, I receive a connection failure and am asked to retry. Why?	Simultaneous access to Virtual Floppy drives is not allowed. Before you virtualize the drive, close the application that you are using to view the drive contents.
Do I need to install drivers on the server to make the Virtual Media feature work?	No. Drivers are not required on either the managed system or the management station. The operating system provides what is required for this feature.
When I performed a firmware update remotely using the DRAC 4 user interface, I noticed that the Virtual Drives on the managed system disappeared.	Firmware updates cause the DRAC 4 to reset, which causes the Virtual Drives to be unmounted. You can restore the Virtual Drives on systems running Windows by either restarting the system or by using the Windows device manager to scan for new hardware. You can restore the Virtual Drives on systems running Red Hat Enterprise Linux by re-mounting the drives after the firmware update completes.
What will my Virtual Media feature look like before the system is booted?	During system boot, the BIOS lists the virtual devices that are available. You should see a message that lists 2 devices as follows: Drive Number : 0 VIRTUALFLOPPY DRIVE Removable Media Drive Drive Number : 1 VIRTUALCDROM DRIVE
How do I set my virtual device to be bootable?	You must go into the BIOS setup at the managed system and then go to the boot menu. Once in the boot menu, you find a listing for the virtual CD drive and the virtual floppy drive. You can change the order of the virtual devices in the boot order. For example, to boot from a CD drive, you must put the CD drive first in the boot order.

Table 7-2. Using Virtual Media: Frequently Asked Questions (continued)

Question	Answer
What media can I boot from?	<p>DRAC 4 allows you to boot from any of the following bootable media:</p> <ul style="list-style-type: none">• CDROM media• 1.44 floppy disk• 1.44 floppy image• USB key• CD/DVD image file in ISO9660 format.
How can I make my USB key bootable?	<p>Dell provides a Windows utility for formatting its USB Solid State devices as bootable devices on the <i>Dell Resource</i> CD that ships with a Dell system. You can use this utility to make the Memory Key bootable. You can also use the utility to format the Memory Key, to add an active partition, and to transfer basic MS-DOS® system files to the Memory Key.</p> <p>This utility is also available on the Dell Support website at support.dell.com. You can find the utility by searching for "Memory Key Boot."</p>
What does Virtual Media look like at the server?	<p>On Windows systems, you see additional CD and removable media drives appear in "My Computer." On Red Hat Enterprise Linux systems, you see devices that can be mounted. You can find the device names by looking at <code>/etc/fstab</code>.</p>
How do I know which drives are my virtual media drives?	<p>When you connect your management station drive to the managed system drive then the title of the inserted media should automatically appear next to the drive letter on Windows systems. However, the best way to know which drive is the virtual media drive and which is the physical drive is by opening/mounting the drive and looking at its content.</p>
Will the drive letters change on Windows systems?	<p>Generally, the drive letters will not change. So if you have a CD drive that is labeled D: and a removable media drive that is labeled F:, then those drive letters will remain the same.</p>

Table 7-2. Using Virtual Media: Frequently Asked Questions (continued)

Question	Answer
How do I find my device names on Red Hat Enterprise Linux systems so I can mount them?	<p>You can look at the <code>/etc/fstab</code> file which lists the device names for all your devices. When you know the device name, then you can use the mount and umount command to mount and unmount your CD or floppy drives.</p> <p>To manually identify the virtual media devices, type the following command:</p> <pre>cat /var/log/messages grep VIRTUAL</pre> <p>Next, look for mount points for those devices in the <code>/etc/fstab</code> file. For example:</p> <pre>cat /etc/fstab grep /dev/hde</pre> <p>Finally, use the associated mount point on the mount command. For example:</p> <pre>mount /mnt/cdrom1</pre>
What do I need to install on the client side for the Virtual Media feature to work?	<p>For a Windows management station, you must install an ActiveX Web plug-in. For a Red Hat Enterprise Linux management station, you must install a Mozilla plug-in. The plug-in is installed automatically when you access the Virtual Media page for the first time or when a newer version of the plug-in is available.</p>
Do I need to install this plug-in every time I use the Virtual Media feature?	<p>No. You only need to install the plug-in once when the feature is used for the first time unless a newer version becomes available.</p>
Will I need to have administrator rights in Windows to install the ActiveX plug-in.	<p>You must have administrator privileges on Windows systems to install and use the Virtual Media feature.</p>

Table 7-2. Using Virtual Media: Frequently Asked Questions (continued)

Question	Answer
What privileges do I need to install and use the Virtual Media plug-in on a Red Hat Enterprise Linux management station?	You must have write privileges on the browser's directory tree in order to successfully install the Virtual Media plug-in.
Can I use my virtual drives under any version of Novell NetWare?	Currently, the Virtual Media feature is not supported under any version of the NetWare operating system. NetWare drivers ignore the virtual drives and do not make them available to the system.

Using the Serial and racadm Commands

The DRAC 4 provides **serial** and **racadm** commands that allow you to manage and configure the managed system locally or remotely.

The serial/telnet console provides a set of **serial** commands. The **serial** commands, which include the **racadm** command, give you access to all of the text-based features supported by the DRAC 4 Web-based interface.

The **racadm** CLI allows you to locally or remotely configure and manage your DRAC 4. The **racadm** CLI runs on the management station and the managed system, and is available on the *Dell Systems Console and Agent* CD.

You can use the **racadm** CLI to write scripts to automatically configure multiple DRAC 4s. For more information about configuring multiple DRAC 4s, see "Configuring Multiple DRAC 4s."

The following sections provide information about using the **serial** and **racadm** commands (see "Using a Serial or Telnet Console" or "Using the **racadm** CLI"). Examples of the **racadm** command for configuring your DRAC 4 and information about using the **racadm** configuration file to configure multiple DRAC 4s are also provided.

Using a Serial or Telnet Console

The serial commands in Table 8-1 can be run from the serial or telnet console command prompt or the **racadm** CLI locally or remotely.

Logging into the DRAC 4

After you have configured your management station terminal emulator software, perform the following steps to log into the DRAC 4:

- 1 Connect to the DRAC 4 using your management station terminal emulation software.
- 2 Type your DRAC 4 user name and press <Enter>.
- 3 Type your DRAC 4 password and press <Enter>.

You are now logged into the DRAC 4.

Starting a Text Console

After you have logged into the DRAC 4 through your management station terminal software or by telnet, you can redirect the managed system text console by using `connect com2`, which is a **serial/telnet** command. Only one `connect com2` client is supported at a time (out of four total sessions shared with the DRAC 4 Web-based interface).

To connect to the managed system text console, type `connect com2` from the DRAC 4 command prompt (displayed through Minicom or HyperTerminal).



NOTE: When accessing a DOS console through `connect com2`, characters in the output may be dropped during the output of large amounts of data (for example, the dump of large files greater than 30 lines). This can cause incorrect displays in `connect com2` over telnet sessions. Red Hat Enterprise Linux and the Microsoft Windows Special Administration Console (SAC) work correctly.

`connect com2` also supports the `-h` option. This option displays the history of the last characters written to the text console. The default (and maximum) size of the history buffer is 8192 characters. You can set this number to a smaller value using the command:

```
racadm config -g cfgSerial -o cfgSerialHistorySize <number>
```

The `connect -h com2` command displays the contents of the serial history buffer before waiting for input from the keyboard or new characters from the serial port.



NOTE: The terminal emulation type (ANSI or VT100) of the client terminal must match the type on the server serial port output when using the `-h` option; otherwise, the output may be garbled. In addition, the number of rows and columns of the client terminal must be set to 25.

Viewing a List of Serial/Telnet Commands

Type `help` to display the entire serial/telnet command list. Commands that are not supported on the system or interface that you are using are labeled as such. For example, if a specific command is not supported on the system, the following text is displayed next to the command:

```
<NOT SUPPORTED>
```

If you type a command that is not supported on the system you are using, an error similar to the following is displayed.

```
setsvctag: Firmware: UNSUPPORTED COMMAND
```

Table 8-1 lists the **serial/telnet** commands. These commands are also supported as **racadm** commands. The descriptions and "man page" information including required syntax for the **serial/telnet** commands are identical for the **racadm** command. You do not need to type **racadm** before typing a **serial/telnet** command because the **serial/telnet** commands are not **racadm** commands. They are at the same "level." For detailed information about the required syntax for each **racadm** command see "racadm Subcommand Man Pages."

Table 8-1. Serial/Telnet Commands

Command	Description
help	Lists DRAC 4 commands.
help <i><subcommand></i>	Lists the usage statement for the specified subcommand.
logout	Logs out of a DRAC 4 session and then prints a new login prompt.
quit	Logs out of a DRAC 4 session and then prints a new login prompt.
exit	Logs out of a DRAC 4 session and then prints a new login prompt.
getsysinfo	Displays general DRAC 4 and system information.
serveraction	Executes a graceful hard server reset, or power-on, power-off, or power-cycle.
getraclog	Displays DRAC 4 log entries.
clrtraclog	Clears the DRAC 4 log entries.
gettracelog	Displays Trace Log entries.
getsel	Displays System Event Log entries.
clrsel	Clears the System Event Log entries.
connect com1 or connect com2	Connects the DRAC 4 to the system serial port.
racadm	Command line status and configuration utility for the DRAC 4.

Using the racadm CLI

The racadm CLI commands can be run locally or remotely from the serial or telnet console command prompt or through a normal DOS or Linux command prompt.

Use the **racadm** command to configure DRAC 4 properties, perform remote management tasks, or recover a crashed system. Table 8-2 lists the **racadm** command that you can type into the racadm CLI.

When using the racadm CLI, type `racadm help` to display the entire **racadm** subcommand list, which lists all the commands supported by the DRAC 4. The following sections provide information about how to use the **racadm** commands.



NOTE: MS-DOS version 6.22 is required to use the DOS racadm command-line feature. To limit DOS racadm output to a single screen, use the MS-DOS **more.com** utility. Type the following command at the prompt: `a: racadm help | more.`

racadm Command Description

Table 8-2. racadm Command

Command	Description
racadm	Command line status and configuration utility for the DRAC 4.

Without options, the **racadm** command executes the **help** command, which displays a list of available commands and a one-line description of each. Type `racadm help <subcommand>` to display any syntax and command-line options for the *<subcommand>*.

Using the racadm CLI Remotely

- ➔ **NOTICE:** Configure the IP address on your DRAC 4 before using the racadm remote capability. For more information about initially configuring your DRAC 4, including a list of other documents you may need, see "Installing and Setting Up the DRAC 4."

The racadm CLI provides a remote capability option (-r) that allows you to connect to the managed system and execute **racadm** subcommands from a remote console or management station. To use the remote capability, you need a valid user name (-u option) and password (-p option), and the IP address of the managed system.

- ✍ **NOTE:** The racadm remote capability is supported only on management stations. For more information, see "Supported Web Browsers."

- ✍ **NOTE:** When using the racadm remote capability, you must have write permission on the folders where you are using the **racadm** subcommands involving file operations, for example:

```
racadm getconfig -f <file name>
```

or:

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

racadm Synopsis

```
racadm <options> <subcommand> <subcommand_options>
```

```
racadm <options> [-u <user name>] -p <password> -r  
<racIpAddr> <subcommand>
```

```
racadm <options> -i -r <racIpAddr> <subcommand> or  
racadm <options> -i -r <racIpAddr>:<new port number>  
<subcommand> if the DRAC 4 HTTPS port number has been changed.
```

```
racadm <options> -r <racIpAddr> <subcommand>
```

racadm Options

Table 8-3 lists the options for the **racadm** command.

Table 8-3. racadm Command Options

Option	Description
-r <i><racIpAddr></i> or -r <i><racIpAddr>:<port number></i> if the DRAC 4 port number has been changed	Specifies the remote IP address of the controller.
-i	Tells racadm to interactively query the user for the user's user name and password.
-u <i><userName></i>	Specifies the user name that is used to authenticate the command transaction. If not specified, the default user name "racadmusr" is used. If the -u option is used, the -p option must be used, and the -i option (interactive) is not allowed.
-p <i><password></i>	Specifies the password used to authenticate the command transaction. If the -p option is used, the -i option is not allowed.
-l <i><lvl></i>	Specifies the log level for debug. NOTE: If you use the -l <lvl> option without using the -L <file> option, a default log file named racadm.log is created in the current working directory.
-v <i><lvl></i>	Specifies the verbose level for screen output.
-t <i><secs></i>	Specifies the transport time-out.
-L <i><file></i>	Specifies a debug log file.

If you use the **-r** option, you must also use the **-u** and **-p** options to configure the DRAC 4 to accept **racadm** commands. Using the **-r** option without the previously listed options will result in a command failure.

Enabling and Disabling the racadm Remote Capability



NOTE: It is recommended that you run these commands on your local system.

The racadm CLI remote capability is enabled by default. If you have disabled it, type the following command to enable the remote capability:

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

Type the following command to disable the remote capability:

```
racadm config -g cfgRacTuning -o  
cfgRacTuneRemoteRacadmEnable 0
```

Log/Verbose Levels

Use the log/verbose level options in Table 8-4 to control how racadm command output is displayed.

Table 8-4. Log/Verbose Level Options

Option	Description
0x1	Standard output messages
0x2	Standard error messages
0x4	Debug messages

Example:

```
racadm -l 0x3 -L log <subcommand [subcommand_options]>
```

The argument 0x3 for the log level is the OR of STDOUT and STDERR messages. Both of these message types are written to the file name **log**. The verbose, or -v, option defaults to 0x3, (OR of STDOUT and STDERR).

racadm Subcommand Descriptions

The following subsections provide descriptions of subcommands that you can run under the racadm CLI. Table 8-5 briefly describes each racadm subcommand. For a detailed listing of every racadm subcommand including syntax and valid entries, see the "racadm Subcommand Man Pages."

Table 8-5. racadm Subcommands

Command	Description
help	Lists DRAC 4 subcommands.
help <subcommand>	Lists usage statement for the specified subcommand.
clearasrscreen	Clears the last System Reset Timer screen (last blue screen).
config/getconfig	Configures the DRAC 4 and displays the DRAC 4 configuration.
coredump	Displays the last DRAC 4 coredump.
coredumpdelete	Deletes the coredump stored in the DRAC 4.
fwupdate	Executes or displays status on DRAC 4 firmware updates.
getssninfo	Displays information about active sessions.
getsysinfo	Displays general DRAC 4 and system information.
getractime	Displays the DRAC 4 time.
ifconfig	Sets or displays the current DRAC 4 IP configuration.
getsvctag	Displays service tags.
racdump	Dumps DRAC 4 status and state information for debug.
racreset	Resets the DRAC 4.
racresetcfg	Resets the DRAC 4 to the default configuration.
serveraction	Executes a graceful hard server reset, power-on, power-off, or power-cycle.
setrac	Sets managed system name, operating system name, and type from the managed system to the DRAC 4.
sslcsrgen	Generates and downloads the secure sockets layer (SSL) certificate signing request (CSR).
sslcertupload	Uploads a CA certificate or server certificate to the DRAC 4.
sslcertdownload	Downloads a CA certificate.
sslcertview	Views a CA certificate or server certificate in the DRAC 4.

Table 8-5. racadm Subcommands (continued)

testemail (see Email Test Command)	Forces the DRAC 4 to send an email over the DRAC 4 NIC.
testtrap (see Trap Test Command)	Forces the DRAC 4 to send an SNMP over the DRAC 4 NIC.
vmdisconnect	Forces a virtual media connection to close.

racadm Error Messages

For information about racadm CLI error messages, see "Frequently Asked Questions" in this chapter.

Configuring Multiple DRAC 4s

One of the major features of the racadm CLI is the ability to configure a DRAC 4 using a configuration file. The racadm CLI parses the DRAC 4 configuration file, called **racadm.cfg**, and then sends individual configuration requests to one or more DRAC 4s.

This method may be used to configure multiple DRAC 4 database properties. You must first run the racadm CLI to query a configured DRAC 4 for its database properties, which are accessed using their object group IDs and object IDs. The racadm CLI creates the **racadm.cfg** file from the retrieved information. You can then configure other cards with the same database information by exporting this file out to the other DRAC 4s.




NOTE: Some configuration files contain unique DRAC 4 information (such as the static IP address) that must be modified before configuring other cards.

Configuration File Overview

To use the configuration file, perform the following high-level steps:

- 1 Get the configuration from the DRAC 4 that contains the appropriate configuration.
- 2 Modify the configuration (optional).
- 3 Push the configuration to a target DRAC 4.
- 4 Reset the target DRAC 4.

The `getconfig -f racadm.cfg` subcommand requests the configuration of the DRAC 4 and generates a `racadm.cfg` file (you can choose any name for this file).

 **NOTE:** The generated `.cfg` file does not contain user passwords.

Other options for the `getconfig` command enable you to perform such actions as:


- Displaying all configuration properties in a group (specified by group name and index)
- Displaying all configuration properties for a user by user name

The `config` subcommand loads the information into other DRAC 4s. Other options for `config` enable you to perform such actions as:

- Removing passwords in the `racadm.cfg` file used to configure the card
- Synchronizing the user and password database with Server Administrator

The initial configuration file, `racadm.cfg`, is named by the user. In the following example, the configuration file is named `myfile.cfg`. To obtain this file, type the following command at the command prompt:


```
racadm getconfig -f myfile.cfg
```

 **NOTICE:** It is recommended that you edit this file with a simple text editor; the `racadm` utility uses an ASCII text parser, and any formatting confuses the parser and might corrupt the `racadm` database.

Creating a DRAC 4 Configuration File

The DRAC 4 configuration file `<filename>.cfg` is used with the `racadm config -f <filename>.cfg` command. The configuration file is a simple text file that allows the user to build a configuration file (similar to an `.ini` file) and configure the DRAC 4 from this file. You may use any file name, and the file does not require a `.cfg` extension (although it is referred to by that designation in this subsection). The `.cfg` file can be:

- Created
- Obtained from a `racadm getconfig -f <filename>.cfg` command
- Obtained from a `racadm getconfig -f <filename>.cfg` command, and then edited

 **NOTE:** See "config/getconfig" for information about the `getconfig` command.

The `.cfg` file is first parsed to verify that valid group and object names are present and that some simple syntax rules are being followed. Errors are flagged with the line number in which the error was detected, and a simple message explains the problem. The entire file is parsed for correctness, and all errors are displayed. Writes are not performed to the DRAC 4 if an error is found in the `.cfg` file. The user must correct *all* errors before any configuration can take place. The `-c` option may be used in the `config` subcommand, which verifies syntax only and does *not* perform writes to the DRAC 4.

Remember the following important points:

- If the parser encounters an indexed group, it is the value of the anchored object that differentiates the various indexes.

The parser reads in all of the indexes from the DRAC 4 for that group. Any objects within that group are simple modifications at configuration time. If a modified object represents a new index, the index is created on the DRAC 4 during configuration.

- The user cannot specify a desired index in a `.cfg` file.

Indexes may be created and deleted, so over time the group may become fragmented with used and unused indexes. If an index is present, it is modified. If an index is not present, the first available index is used. This method allows flexibility when adding indexed entries, where the user does not need to make exact index matches between all the RACs being managed; new users are added to the first available index. A `.cfg` file that parses and runs correctly on one DRAC 4 may not run correctly on another if all indexes are full and a new user is to be added.

- Use the `racresetcfg` subcommand to keep all DRAC 4s the same.

To keep all DRAC 4s the same, use the `racresetcfg` subcommand to reset the DRAC 4 to original defaults, and then run the `racadm config -f <filename>.cfg` command. Ensure that the `.cfg` file has all the desired objects, users, indexes, and other parameters.



NOTICE: Use the `racresetcfg` subcommand to reset the database and the DRAC 4 NIC settings to the original default settings and remove all users and user configurations. While the root user is available, other users' settings are also reset to the default.

Parsing Rules

- All lines that start with '#' are treated as comments.

A comment line *must* start in column one. A '#' character in any other column is treated as a # character. (Some modem parameters may have # characters as part of their string. An escape character is not required. You may want to generate a .cfg from a `racadm getconfig -f <filename>.cfg` command, and then perform a `racadm config -f <filename>.cfg` command to a different DRAC 4, without adding escape characters).

Example:

```
#
# This would be a comment
[cfgUserAdmin]
cfgUserAdminPageModemInitString=<Modem init # not
a comment>
```

- All group entries must be surrounded by "[" and "]" characters.

The starting "[" character denoting a group name *must* start in column one. This group name *must* be specified before any of the objects in that group. Objects that do not have an associated group name generate an error. The configuration data is organized into groups as defined in "DRAC 4 Property Database Group and Object Definitions."

The following example displays a group name, object, and the object's property value.

Example:

```
[cfgLanNetworking]
cfgNicIpAddress=143.154.133.121
```

- All parameters are specified as "object=value" pairs without any white space between the object, =, or value.


White spaces after the value are ignored. A white space inside a value string is left unmodified. Any character to the right of the '=' is taken as is (for example, a second '=', or a '#', '[', ']', and so forth). All of these characters are valid modem chat script characters.

See the example in the previous bullet.

- An indexed object entry is ignored by the `.cfg` parser.

The user *cannot* specify which index is used. If the index already exists, it is used, or else the new entry is created in the first available index for that group.

The `racadm getconfig -f <filename>.cfg` command places a comment in front of index objects, which allows the user to see which comments are being used.


 **NOTE:** The user may create an indexed group manually using the following command:

```
racadm config -g <groupName> -o <anchored object>
-i <index 1-16> <unique anchor name>
```

- The line for an indexed group *cannot* be deleted from a `.cfg` file.

The user must remove an indexed object manually using the following command:

```
racadm config -g <groupName> -o <objectName> -i
<index 1-16> ""
```

 **NOTE:** A NULL string (two "" characters) directs the DRAC 4 to delete the index for the specified group.


To view the contents of an indexed group, use the following command:

```
racadm getconfig -g <groupName> -i <index 1-16>
```

- For indexed groups the object anchor *must* be the first object after the "[]" pair. The following are examples of the current indexed groups:

```
[cfgUserAdmin]
cfgUserAdminUserName=<USER_NAME>
"

[cfgTraps]
cfgTrapsDestIpAddress=<IP_ADDRESS>
,
,
```

 **NOTE:** Type `racadm getconfig -f <myexample>.cfg`. This command builds a `.cfg` file for the current DRAC 4 configuration. This configuration file can be used as an example and as a starting point for your unique `.cfg` file.

Configuration File Example

The following example describes the IP address of the DRAC 4. Remove all unnecessary `<variable>=value` entries. In this situation, only the actual variable group's label with "[" and "]" will remain along with the two `<variable>=value` entries pertaining to the IP address change.

The file contents are as follows:

```
#
#   Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

This file will be updated as follows:

```
#
#   Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```

The command `racadm config -f myfile.cfg` parses this file and identifies any errors by line number. A correct file will update the proper entries. You may use the same `getconfig` command used in the previous example to confirm the update.

You can use this file to download company-wide changes or to configure new systems over the network.

Using the racadm Utility to Configure the DRAC 4

The DRAC 4 Web-based interface is the fastest way to configure a DRAC 4. If you prefer command-line or script configuration, or need to configure multiple DRAC 4s, you can also use the racadm CLI. The racadm CLI is installed along with the DRAC 4 agents on the managed system.

To configure multiple DRAC 4s to contain the same user configuration settings, you can do either of the following:

- Use the racadm CLI examples in this section as a guide to create a batch file of **racadm** commands, and then execute the batch file on each managed system.
- Create the DRAC 4 configuration file as described in "racadm Subcommand Man Pages" and then execute the **racadm config** subcommand on each managed system using that same configuration file.

Before Adding a DRAC 4 User

The DRAC 4 allows up to 16 users to be configured into the DRAC 4 property database. Before manually adding the DRAC 4 user, you need to know which, if any, users exist. If the DRAC 4 is new, or the **racadm racresetcfg** command has been run, then the only user is **root** with the password **calvin**. The **racresetcfg** subcommand resets the DRAC 4 back to the original defaults.



NOTICE: Use caution when using this command because *all* configuration parameters are reset to the original defaults; any previous changes are lost.



NOTE: Users can be added and deleted over time, so it is possible that users on the DRAC 4 do not have the same index number as the same user on a different DRAC 4.

To find out if a user exists, you can type the following command at the command prompt:

```
racadm getconfig -u <username>
```

or you can type the following command once for each index of 1–16:

```
racadm getconfig -g cfgUserAdmin -i <index>
```



NOTE: An alternate method to obtain this information is to type **racadm getconfig -f <myfile.cfg>**, then view or edit the **myfile.cfg** file, which includes all DRAC 4 configuration parameters.

Several parameters and object IDs are displayed along with their current values. The two objects of interest are:

```
# cfgUserAdminIndex=XX
cfgUserAdminUserName=
```

If the `cfgUserAdminUserName` object has no value, that index number, which is indicated by the `cfgUserAdminIndex` object, is available for use. If a name appears after the "=", that index is taken by that user name.



NOTE: When you manually add or remove a user with the `racadm config` subcommand, you *must* specify the index with the `-i` option. Observe that the `cfgUserAdminIndex` object displayed in the previous example contains a '#' character. Also, if you use the `racadm config -f racadm.cfg` command to specify any number of groups/objects to write, the index cannot be specified. A new user is added to the first available index. This behavior allows more flexibility in configuring multiple DRAC 4s with the same settings.

Adding a DRAC 4 User Without Alert Capabilities

To add a simple user without any alert information, first locate an available user index by performing the steps in "Before Adding a DRAC 4 User." Next, type the following two command lines with the new user name and password:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i <index> <username>

racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i <index> <password>
```

Example:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 2 123456
```

A user name "john" with the password of "123456" is created. This user name and password can now be used to log into the Web-based remote access interface. You can verify this using either of the following two commands:

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 2
```

Deleting a DRAC 4 User

All users must be deleted manually. You cannot delete users by specifying them in a `racadm.cfg` file.

To delete the user "john" created in the previous example, type the following command line:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName  
-i <index> ""
```

A null string of double quote characters("") indicates to the DRAC 4 to delete the index for the specified group.



NOTE: You can delete all users, including users with administrative privileges; however, this will disable all remote access to the DRAC 4 card. If you delete all users, use the local `racadm` CLI tool to re-add users.

Adding a DRAC 4 User With Alerting Capabilities

To add a DRAC 4 user that is able to receive email and SNMP traps, first locate an available DRAC 4 user index by performing the steps in "Before Adding a DRAC 4 User." The following example has an available user index at index 2.



NOTE: See "DRAC 4 Property Database Group and Object Definitions" for details about each specific object.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName  
-i 2 john  
  
racadm config -g cfgUserAdmin -o cfgUserAdminPassword  
-i 2 123456  
  
racadm config -g cfgUserAdmin -o  
cfgUserAdminEmailAddress -i 2 "<email address>"  
  
racadm config -g cfgUserAdmin -o  
cfgUserAdminEmailCustomMsg -i 2 "RAC Alert Email Test"  
  
racadm config -g cfgUserAdmin -o  
cfgUserAdminEmailEnable -i 2 1  
  
racadm config -g cfgUserAdmin -o  
cfgUserAdminAlertFilterRacEventMask -i 2 0x0
```

```

racadm config -g cfgUserAdmin -o
cfgUserAdminAlertFilterSysEventMask -i 2 0x0
racadm config -g cfgTraps -o cfgTrapsSnmpCommunity -i
2 public
racadm config -g cfgTraps -o cfgTrapsEnable -i 2 1
racadm config -g cfgTraps -o
cfgTrapsFilterRacEventMask -i 2 0x0
racadm config -g cfgTraps -o
cfgTrapsFilterSysEventMask -i 2 0x0
racadm config -g cfgTraps -o cfgTrapsDestIpAddr -i 2
<SNMP trap destination>
racadm config -g cfgOobSnmp -o cfgOobSnmpTrapsEnable 1
racadm config -g cfgRemoteHosts -o
cfgRhostsSmtpServerIpAddr 143.166.224.254
racadm racreset

```

You can type the commands manually, run a batch file, or build a `.cfg` file using the command `racadm config -f racadm.cfg`. After doing so, you may want to test each of the alerts.

Testing Email Alerting

Email alerting is enabled by the following command. A "0" disables this feature; a "1" enables it.

```

racadm config -g cfgUserAdmin -o
cfgUserAdminEmailEnable -i 2 1
racadm testemail -i 2

```

Testing SNMP Trap Alerting

SNMP traps are enabled by the following command. A "0" disables this feature; a "1" enables it.

```

racadm config -g cfgTraps -o cfgTrapsEnable -i 2 1
racadm testtrap -i 2

```

Adding a DRAC 4 User With Permissions

To add a user with specific administrative permissions (role-based authority), first locate an available user index by performing the steps in "Before Adding a DRAC 4 User." Next, type the following command lines with the new user name and password.



NOTE: See Table B-1 for a list of the Bit Mask numbers to enable specific user permissions. The default user permission is 0, which provides full administrative permission.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i <index> <username> <Bit Mask
Number for specific user permissions>
```

Configuring DRAC 4 Network Properties

Type the following command to get a list of the available network properties:

```
racadm getconfig -g cfgLanNetworking
```

If you want to use DHCP to obtain an IP address, you can use the command to write the object `cfgNicUseDhcp` to enable it. You may also type a static IP address, netmask, and gateway.

The commands provide the same configuration functionality as the option ROM does at boot-up time when you are prompted to type `<Ctrl><d>`. For more information about configuring network properties with the option ROM, see "Configuring DRAC 4 Network Properties."

The following is an example of how the command may be used to configure desired LAN network properties.

```
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

```

 **NOTE:** If `cfgNicEnable` is set to `0`, the DRAC 4 LAN is disabled even if DHCP is enabled.

Frequently Asked Questions

Table 8-6 lists frequently asked questions and answers.

Table 8-6. Using the serial and racadm Commands: Frequently Asked Questions

Question	Answer
<p>After performing a DRAC 4 reset (using the <code>racadm racreset</code> command), I issue a command and the following message is displayed:</p> <pre>racadm <command name> Transport: ERROR: (RC=-1)</pre> <p>What does this message mean?</p>	<p>You must wait until the DRAC 4 completes the reset before issuing another command.</p>

Table 8-6. Using the serial and racadm Commands: Frequently Asked Questions (continued)

Question	Answer
When I use the <code>racadm</code> commands and subcommands, I get errors that I don't understand.	<p>You may encounter one or more of the following errors when using the <code>racadm</code> commands and subcommands:</p> <ul style="list-style-type: none">• Local error messages — Occur when problems occur with syntax, typographical errors, incorrect names, and so on. Example: <pre>racadm <subcmd>: ERROR: <message></pre>• Transport error messages — Occur when the <code>racadm</code> CLI communication paths to the DRAC 4 are not accessible. Transport error messages occur if Server Administrator is not running when the command is executed. If you are using the <code>racadm</code> CLI remotely, transport error messages may indicate network communication problems or that the management station is unable to communicate with the DRAC 4. Example: <pre>racadm <subcmd> : Transport : ERROR : <message></pre>• DRAC 4 firmware errors — Occur when a fault exists in the DRAC 4 firmware operation. Example: <pre>racadm <subcmd> : Firmware : ERROR : <message></pre>

Troubleshooting

Troubleshooting the DRAC 4

See the following tables for help with troubleshooting the DRAC 4 and the racadm CLI:

Table 4-30, "DRAC 4 Network Error Codes"

Table 4-32, "Managing and Recovering a Remote System: Frequently Asked Questions"

Table 5-8, "Using the DRAC 4 With Active Directory: Frequently Asked Questions"

Table 6-4, "Using Console Redirection: Frequently Asked Questions"

Table 7-1, "Using Virtual Media: Frequently Asked Questions"

Table 8-6, "Using the serial and racadm Commands: Frequently Asked Questions"

racadm Subcommand Man Pages

This section provides descriptions of the subcommands that you can run in the racadm CLI.

help



NOTE: To use this command, you must have **Log In DRAC 4** permission.

Table A-1 describes the **help** command.

Table A-1. Help Command

Command	Definition
help	Lists all of the subcommands available to use with racadm and provides a short description for each.

Synopsis

```
racadm help
```

```
racadm help <subcommand>
```

Description

The **help** subcommand lists all of the subcommands that are available under the **racadm** command along with a one-line description. You may also type a subcommand after **help** to get the syntax for a specific subcommand.

Output

The **racadm help** command displays a complete list of subcommands.

The **racadm help <subcommand>** command displays information for the specified subcommand only.

arp


 **NOTE:** To use this command, you must have **Execute Diagnostic Commands** permission.

Table A-2 describes the **arp** command.

Table A-2. arp Command

Command	Definition
arp	Displays the contents of the ARP table. ARP table entries may not be added or deleted.

Synopsis

```
racadm arp
```

clearasrscreen


 **NOTE:** To use this command, you must have **Execute Debug Commands** permission.

Table A-3 describes the **clearasrscreen** subcommand.

Table A-3. clearasrscreen

Subcommand	Definition
clearasrscreen	Clears the last crash screen that is in memory.

Synopsis

```
racadm clearasrscreen
```

config/getconfig


 **NOTE:** To use the `getconfig` command, you must have **Log In DRAC 4** permission.

Table A-4 describes the `config` and `getconfig` subcommands.

Table A-4. config/getconfig

Subcommand	Definition
<code>config</code>	Configures the DRAC 4.
<code>getconfig</code>	Gets the DRAC 4 configuration data.

Synopsis

```
racadm config [-s -p -c] -f <filename>
```

```
racadm config [-s] -g <groupName> -o <objectName> [-i  
<index>] <Value>
```

```
racadm getconfig [-p] -f <filename>
```

```
racadm getconfig -g <groupName> [-i <index>]
```

```
racadm getconfig -u <username>
```

```
racadm getconfig -h
```

config Subcommand Description

The `config` subcommand allows the user to set DRAC 4 configuration parameters individually or to batch them as part of a configuration file. After the `.cfg` file has been correctly parsed, each object is read. If the content is the same, a write to the DRAC 4 does not occur. If the data is different, that DRAC 4 object is written with the new value.

Input

Table A-5 describes the `config` subcommand options.


 **NOTE:** The `-f`, `-s`, and `-p` options are not supported for the serial/telnet console.

Table A-5. config Subcommand Options and Descriptions

Option	Description
-f	The -f <i><filename></i> option causes config to read the contents of the file specified by <i><filename></i> and configure the DRAC 4. The file must contain data in the format specified in "Parsing Rules."
-s	The -s, or synchronize option, directs config to synchronize the user and password database with Server Administrator (if any user passwords were modified).
-p	The -p, or password option, directs config to delete the password entries contained in the config file -f <i><filename></i> after the configuration is complete.
-g	The -g <i><groupName></i> , or group option, must be used with the -o option. The <i><groupName></i> specifies the group containing the object that is to be set.
-o	The -o <i><objectName></i> <i><Value></i> , or object option, must be used with the -g option. This option specifies the object name that is written with the string <i><value></i> .
-i	The -i <i><index></i> , or index option, is only valid for indexed groups and can be used to specify a unique group. The <i><index></i> is a decimal integer from 1 through 16. The index is specified here by the index value, not a "named" value.
-c	The -c, or check option, is used with the config subcommand and allows the user to parse the .cfg file to find syntax errors. If errors are found, the line number and a short description of what is incorrect are displayed. Writes do not occur to the DRAC 4. This option is a check only.

Output

This subcommand generates error output upon encountering either of the following:

- Invalid syntax, group name, object name, index, or other invalid database members
- racadm CLI transport failures

If errors are not encountered, this subcommand returns an indication of how many configuration objects that were written out of how many total objects were in the .cfg file.

getconfig Subcommand Description

The `getconfig` subcommand allows the user to retrieve DRAC 4 configuration parameters on an individual basis, or all the configuration groups may be retrieved and saved into a file.

Input

Table A-6 describes the `getconfig` subcommand options.

Table A-6. getconfig Subcommand Options

Option	Description
-f	The -f <i><filename></i> , or <i>filename</i> option, causes <code>getconfig</code> to create the file <i><filename></i> . It then reads all the configuration data from the DRAC 4 and places it into the file <i><filename></i> . The created file is a format that can be used with the <code>racadm config -f <filename></code> command.
-p	The -p, or <code>password</code> option, causes <code>getconfig</code> to include password information in the file for all passwords except for the user passwords (which are stored encrypted and cannot be decrypted). A <code>#cfgUserAdmPassword</code> line is displayed as an indication that the password is present, but the password text is not displayed.
-g	The -g <i><groupName></i> , or <code>group</code> option, can be used to display the configuration for a single group. The <i>groupName</i> is the name for the group used in the <code>racadm.cfg</code> files. If the group is an indexed group, use the -i option.
-h	The -h, or <code>help</code> option, displays a list of all available configuration groups that you can use. This option is useful when you do not remember exact group names.
-i	The -i <i><index></i> , or <code>index</code> option, is valid only for indexed groups and can be used to specify a unique group. The <i><index></i> is a decimal integer from 1 through 16. If -i <i><index></i> is not specified, a value of 1 is assumed for groups, which are tables that have multiple entries. The index is specified by the index value, not a "named" value.
-u	The -u <i><username></i> , or <code>user name</code> option, can be used to display the configuration for the specified user. The <i><username></i> option is the log in user name for the user.

Output

This subcommand generates error output upon encountering either of the following:

- Invalid syntax, group name, object name, index, or other invalid database members
- racadm CLI transport failures

If errors are not encountered, this subcommand displays the contents of the specified configuration.

Examples

- **racadm getconfig -g cfgLanNetworking** — Displays all of the configuration parameters (objects) that are contained in the group **cfgLanNetworking**.
- **racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100** — Sets the **cfgNicIpAddress** configuration parameter (object) to the value 10.35.10.110. This IP address object is contained in the group **cfgLanNetworking**.
- **racadm getconfig -f myrac.cfg** — Writes *all* of the configuration objects, from all of the DRAC 4 group configuration parameters, in to **myrac.cfg**.
- **racadm config -f myrac.cfg** — Configures or reconfigures the DRAC 4. The **myrac.cfg** file may be created from the command specified in the previous example if the DRAC 4 has a desired configuration to be replicated. The **myrac.cfg** file may also be edited manually as long as the parsing rules are followed.



NOTE: The **myrac.cfg** file does not contain password information. To include this information in the file, it must be input manually. If you want to remove password information from the **myrac.cfg** file, use the **-p** option.

- **racadm getconfig -h** — Displays a list of the available configuration groups on the DRAC 4.
- **racadm getconfig -u root** — Displays the configuration parameters for the user named root.

coredump


 **NOTE:** To use this command, you must have **Execute Debug Commands** permission.

Table A-7 describes the **coredump** subcommand.

Table A-7. coredump

Subcommand	Definition
coredump	Displays the last DRAC 4 core dump.

Synopsis

```
racadm coredump
```

Description

The **coredump** subcommand displays detailed information, including register values, recorded when the most recent bus error occurred, or the message `No CORE dump available` (if a previous bus error has not occurred, or if the data has been cleared).

This bus error information is persistent across power cycles of the DRAC 4—the data remains in the flash memory of the DRAC 4 until either:

- It is cleared using the **coredumpdelete** subcommand.
- Another bus error occurs, replacing the previous information with the more recent bus error information.

See the **coredumpdelete** subcommand for information about deleting this information.

Output Example

```
FW d_cmdCoreDump:
Last CORE dump at Wed, 23 Oct 2004 15:49:41 GMT-05:00
Data Access Abort Running: 'IPEV' -#005E0000
-----
CPSR = A0000013 (NzCv if SVC32) SP =018616DC LR =
01023C34
```

R0 =D000AEB2 R1 =01151C1C R2 =0186179C R3 =00000007 R4
=01861700

R5 =C854E35C R6 =018617A0 R7 =00000011 R8 =01383C44 R9
=F1C729C6

R10=00000004 R11=01151C1C R12=0000005F USP=DEADBEEF
ULR=00000000

SSP=018616DC SLR=01023C34 SPSR_svc=60000013

PC =01151C88-01151C88:

Image ID: jon Wed Oct 23 14:55:53 CDT 2004
//DG0YN811/c/esm4/10_23/RAC2.0/FW/rmc

Sysuptime: 67f

FIQ stack

<binary data>

IRQ stack

<binary data>

UNDEF stack

<binary data>

ABORT stack

<binary data>

SVC stack

<binary data>

SWI stack

<binary data>

Enter stack

<binary data>

Current task stack: 'IPEV' -#005e0000

<binary data>

where <binary data> is the binary information that was generated by the
DRAC 4 firmware.

Example output (when data is not available):

FW d_cmdCoreDump: No CORE dump available.

coredumpdelete


 **NOTE:** To use this command, you must have **Clear Logs** or **Execute Debug Commands** permission.

Table A-8 describes the `coredumpdelete` subcommand.

Table A-8. coredumpdelete

Subcommand	Definition
<code>coredumpdelete</code>	Deletes the core dump stored in the DRAC 4.

Synopsis

```
racadm coredumpdelete
```

Description

The `coredumpdelete` command clears the area reserved for persistent storage of bus error information. This operation is performed regardless of whether any bus error information is currently stored in the area reserved for this information.

See the `coredump` command for information about displaying the bus error information.

fwupdate


 **NOTE:** To use this command, you must have **Configure DRAC 4** permission.

Table A-9 describes the `fwupdate` subcommand.

Table A-9. fwupdate

Subcommand	Definition
<code>fwupdate</code>	Updates the firmware on the DRAC 4.

Synopsis

```
racadm fwupdate -u [-w] [-D]
racadm fwupdate -s
racadm fwupdate -g [-u ] [-w] [-D] [-a <IP address>] [-f <path/file>]
racadm fwupdate -c
racadm fwupdate -p -f <update filename> [-u] [-w] [-D]
```

Description

The **fwupdate** subcommand allows the caller to update the firmware on the DRAC 4. The user may:

- Start updating a firmware update file that has previously been loaded into the RAMdisk update area.
- Check the status of the firmware update process.
- Instruct the DRAC 4 firmware to get the firmware update file from a TFTP server and load it into the RAMdisk area.

The user may specify the IP address and path/filename or IP address and directory, or use the default values found in the database. The user may also specify that the update be started after loading, or to terminate and make a separate call to start the update process.

- Load the update file into the DRAC 4 RAMdisk area.

Input

Table A-10 describes the **fwupdate** subcommand options.



NOTE: The **-p** and **-u** options are not supported for the serial/telnet console.

Table A-10. fwupdate Subcommand Options

Option	Description
-u	The update option performs a checksum of the firmware update file and starts the actual update process. If this option is typed by itself, it is assumed that a firmware update file has already been loaded into the RAMdisk using the -g or -p options. This option may also be used along with the -g or -p options. After the firmware update file has been loaded, the update process is started within the same call. At the end of the update, the DRAC 4 performs a soft reset.
-w	The wait option represents a delay in seconds to wait before proceeding with the update. The -w option is only valid with the -u option.
-s	The status option returns the current status of where you are in the update process. This option is always typed by itself. Do not type the -s options with other options. If you do, the status will display as if it was the only option typed.
-g	The get option instructs the firmware to get the firmware update file from the TFTP server and place it in the RAMdisk area. The user may also specify the -a and/or the -f or -d options that are described next. In the absence of the -a or -f options the defaults are read from properties contained in the group cfgRemoteHosts , using properties cfgRhostsFwUpdateIpAddr and cfgRhostsFwUpdatePath .
-a	The IP Address option specifies the IP address of the TFTP server.
-d	The -d , or directory , option specifies the directory on the TFTP server or on the DRAC 4's host server where the firmware update file resides. Do not use the -f option with the -d option.
-D	After the update is complete, the DRAC 4 is reset. Upon boot, a call is made to reset all firmware configuration parameters to the default values. For more information, see "racresetcfg."

Table A-10. fwupdate Subcommand Options (continued)

Option	Description
-c	The -c , or checksum , option allows the user to verify an update file that has been loaded into the RAMdisk area. The update file can be loaded by one of the two loading mechanisms (racadm CLI or TFTP). This option essentially gets the size of the firmware update file and calculates the checksum, and verifies the file token. The TFTP interface verifies the checksum after loading automatically. This option is used mainly when using FTP. The -c option is not used with other options. (The -u option will <i>always</i> checksum before programming. It can be used along with the -u option).
-p	The -p , or put , option is used when you want to FTP the firmware update file from the managed system to the DRAC 4. If the -f option is used, the name of the update image must be firmimg.dml . The update file is sent by way of FTP into the DRAC 4. Checksum runs on the newly loaded image. If the checksum is not correct, an error message is displayed. The user is not required to use fwupdate -s option to do this. If you type the -u option on the same command line, the update process starts.

Output

Displays a message indicating which operation is being performed.

Examples

- `racadm fwupdate -g -a 143.166.154.143 -f firmimg.dml`

In this example, the **-g** option tells the firmware to download the firmware update file from a location (specified by the **-f** option) on the TFTP server at a specific IP address (specified by the **-a** option). The update file is then loaded into RAMdisk. Since the **-u** option is not present, an update does *not* occur.

- `racadm fwupdate -s`

This option reads the current status of the firmware update.

- **racadm fwupdate -u**

The **-u** option starts the update process. This command assumes that a valid firmware update file has been previously loaded using the **-g** or **-p** option. The update file checksum is verified for correctness before proceeding.

- **racadm fwupdate -g -u -a 143.166.154.143 -f firmimg.dml**

In this example, the **-g** option tells the firmware to download the firmware update file from a location (specified by the **-f** option) on the TFTP server at a specific IP address (specified by the **-a** option). The update file is then loaded into RAMdisk. The **-u** option tells the firmware to proceed with the update after the firmware is loaded.

Updating the Firmware

If you use the **-f** option, specify the **firmimg.dml** file. See the **-p** option description in Table A-10 for more information.

If you are updating your firmware *locally*, use one of the following commands to update your firmware:

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

```
racadm fwupdate -p -u -f firmimg.dml
```

Example:

```
racadm fwupdate -p -u -d \my\updatefiles\path
```

```
racadm fwupdate -p -u -f  
\my\updatefiles\path\<filename>
```

If you are updating your firmware *remotely*, use the following command to update your firmware:

```
racadm -r <RAC_IP> -u <user> -p <password> fwupdate -  
g -u -a <TFTP_IP> -d <TFTP_dir_path>
```



NOTE: The **-p** option does not support remote firmware updates.

getssninfo


 **NOTE:** To use this command, you must have **Log In To DRAC 4** permission.

Table A-11 describes the **getssninfo** subcommand.

Table A-11. getssninfo Subcommand

Subcommand	Definition
getssninfo	Retrieves session information for one or more currently active or pending sessions from the Session Manager's session table.

Synopsis

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

Description

The **getssninfo** command returns a list of currently active or pending users and optionally includes summary session table information. The summary information provides the total number of sessions in each of the defined Session Manager states:

- Free
- Preliminary
- Unvalidated
- Valid
- Invalid

Input

Table A-12 describes the **getssninfo** subcommand options.

Table A-12. getssninfo Subcommand Options

Option	Description
-A	The -A option eliminates the printing of data headers.
-u	The -u <username> user name option limits the printed output to only the detail session records for the given user name. If an "*" symbol is given as the user name, all users are listed. Summary information is not printed when this option is specified.

Examples

- `racadm getssninfo`

Session table summary status:

1 VALID

3 AVAILABLE

Table A-13 provides an example of output from the `racadm getssninfo` command.

Table A-13. getssninfo Subcommand Output Example

Type	User	IP Address	Login Date/Time	Consoles
Web	DRAC 4	root	Thu, 06 Mar 2004	NONE
		143.166.174.19	10:32:39	
			GMT-06:00	

- `racadm getssninfo -A`

1 3

```
"Web" "RAC\root" 143.166.174.19 "Thu, 06 Mar 2004  
10:32:39 GMT-06:00" "NONE"
```

- `racadm getssninfo -A -u *`

```
"Web" "RAC\root" 143.166.174.19 "Thu, 06 Mar 2004  
10:32:39 GMT-06:00" "NONE"
```

getsysinfo



NOTE: To use this command, you must have **Log In To DRAC 4** permission.

Table A-14 describes the `getsysinfo` subcommand.

Table A-14. getsysinfo

Command	Definition
<code>getsysinfo</code>	Displays DRAC 4 information, system information, and watchdog status information.

Synopsis

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

Description

The `getsysinfo` command returns information about watchdog status, depending on the command options.

Input

Table A-15 describes the `getsysinfo` subcommand options.

Table A-15. getsysinfo Subcommand Options

Option	Description
-d	Displays DRAC 4 information.
-s	Displays system information
-w	Displays watchdog information
-A	Eliminates the printing of headers/labels.

If the `-w` option is not specified, then the other options are used as defaults.

Output

The following data element is output as a string:

```
Watchdog information/recovery action
```

Enumeration values or bitmaps are defined for these elements. When the `-A` (API) option is included on the command, the enumeration/bit value of the element is listed in the output. Otherwise, the enumeration or bit value is mapped to a string before being output.

The bulleted items listed in Table A-16 define the mapping of values to strings.

Table A-16. Watchdog Recovery Action Number Descriptions

Value	Description
Watchdog recovery action	An enumeration defines the meaning of this value: <ul style="list-style-type: none">• 0 = no-action• 1 = hard-reset• 2 = power-down• 3 = power-cycle

Examples

- `racadm getsysinfo -A -w -s`
"123456" "PowerEdge 2800" "A08" "EF23VQ-0023" ""
0x100 "Server1"

"Microsoft Windows 2000 version 5.0, Build Number
2195, Service Pack 2" "1.60"

"Watchdog Info:" 2 39 40
- `racadm getsysinfo -w -s`
System Information:

System ID = 123456
System Model = PowerEdge 2800
BIOS Version = A08
Asset Tag = EF23VQ-0023
Service Tag = 2MP9Z01
Hostname = Server1
OS name = Microsoft Windows 2000 version
5.0,

Build 2195 Service Pack 2
BMC Version = 1.60

Watchdog Information:

Recovery Action = Power Down

Present countdown value = 36

Initial countdown value = 40

getractive



NOTE: To use this command, you must have **Log In DRAC 4** permission.

Table A-17 describes the `getractive` subcommand.

Table A-17. getractive

Subcommand	Definition
<code>getractive</code>	Displays the time from the controller.

Synopsis

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

Description

The `getractive` subcommand displays the time in one of the following two formats:

- `u` — The UTC hexadecimal value followed by the offset in signed decimal (default).
- `d` — The `yyyymmddhhmmss.mmmmmsofff` string with no option is displayed in the same format as the UNIX `date` command.

Output

The `getractive` subcommand displays the output on one line.

ifconfig


 **NOTE:** To use this command, you must have **Execute Diagnostic Commands** or **Configure DRAC 4** permission.

Table A-18 describes the **ifconfig** subcommand.

Table A-18. ifconfig

Subcommand	Definition
ifconfig	Displays the contents of the network interface table.

Synopsis

```
racadm ifconfig
```

netstat


 **NOTE:** To use this command, you must have **Execute Diagnostic Commands** permission.

Table A-19 describes the **netstat** subcommand.

Table A-19. netstat

Subcommand	Definition
netstat	Prints the contents of the routing table. If the optional interface number is provided, then netstat prints additional information regarding the traffic across the interface, buffer usage, and other network interface information.

Synopsis

```
racadm netstat [<network interface number>]
```

ping


 **NOTE:** To use this command, you must have **Execute Diagnostic Commands** or **Configure DRAC 4** permission.

Table A-20 describes the `ping` subcommand.


Table A-20. `ping`

Subcommand	Definition
<code>ping</code>	Verifies that the destination IP address is reachable from the DRAC 4 with the current routing-table contents. A destination IP address is required. An ICMP echo packet is sent to the destination IP address based on the current routing-table contents.

Synopsis

```
racadm ping <ipaddress>
```

setniccfg/getniccfg

 **NOTE:** To use the `setniccfg` command, you must have **Configure DRAC 4** permission.



 **NOTE:** To use the `getniccfg` command, you must have **Log In To DRAC 4** permission.

Table A-21 describes the `setniccfg` and `getniccfg` subcommands.

Table A-21. `setniccfg/getniccfg`

Subcommand	Definition
<code>setniccfg</code>	Sets the IP configuration for the controller.
<code>getniccfg</code>	Displays the current IP configuration for the controller.

 **NOTE:** The terms NIC and Ethernet management port may be used interchangeably.

Synopsis

```
racadm setniccfg -d
racadm setniccfg -s [<ipAddress> <netmask> <gateway>]
racadm setniccfg -o
racadm getniccfg
```

Description for setniccfg

The **setniccfg** subcommand sets the controller IP address.

- The **-d** option enables DHCP for the Ethernet management port (default is DHCP enabled).
- The **-s** option enables static IP settings. The IP address, netmask, and gateway can be specified. Otherwise, the existing static settings are used.
- The **-o** option disables the Ethernet management port completely.

<ipAddress>, <netmask>, and <gateway> must be typed as dot-separated strings.

Description for getniccfg

The **getniccfg** subcommand displays the current Ethernet management port settings.

Output

The **setniccfg** subcommand returns without output if successful. The **getniccfg** subcommand output displays the following information:

```
Network adapter = Enabled/Disabled
DHCP = Enabled/Disabled
Static IP Settings: <ipAddress> <netmask> <gateway>
Current IP Settings: <ipAddress> <netmask> <gateway>
```

getsvctag


 **NOTE:** To use this command, you must have **Log In To DRAC 4** permission.

Table A-22 describes the `getsvctag` subcommand.

Table A-22. `getsvctag`

Subcommand	Definition
<code>getsvctag</code>	Displays a service tag.

Synopsis

```
racadm getsvctag
```

Description

The `getsvctag` subcommand displays the Service Tag for the system.

Example

Type `getsvctag` at the command prompt. The output is displayed as follows:

```
Y76TP0G
```

The command returns 0 on success and nonzero on errors.

racdump


 **NOTE:** To use this command, you must have **Log In DRAC 4** permission.

Table A-23 describes the `racdump` subcommand.

Table A-23. `racdump`

Subcommand	Definition
<code>racdump</code>	Displays status and general DRAC 4 information.

Synopsis

```
racadm racdump
```


Description

The **racdump** subcommand provides a single command to get dump, status, and general DRAC 4 board information.

The following commands are executed as a result of the single **racdump** subcommand:

- **getsysinfo**
- **coredump**
- **memmap**
- **netstat**
- **getssninfo**

Output

The output of the individual commands are displayed.

racreset



NOTE: To use this command, you must have **Configure DRAC 4** permission.

Table A-24 describes the **racreset** subcommand.

Table A-24. racreset

Subcommand	Definition
racreset	Resets the DRAC 4.



NOTICE: You must wait until the DRAC 4reset is completed before issuing another command. If the DRAC 4 reset is not completed, you may receive the following error: `racadm <command name> Transport: ERROR: (RC=-1)`

Synopsis

```
racadm racreset [hard | soft | graceful] [delay in seconds]
```

Description

The **racreset** subcommand issues a reset to the DRAC 4. The user is allowed to select how many seconds of delay occur before the reset sequence is started. The reset event is written into the DRAC 4 log.

The default option is **soft**. If you do not type an option, the **racadm** CLI waits three seconds and then runs the **soft** option with the **racreset** subcommand.


 **NOTICE:** You must reboot your system after performing a hard reset of the DRAC 4 as described in Table A-25.

Table A-25 describes the **racreset** subcommand options.

Table A-25. racreset Subcommand Options

Option	Description
hard	A <i>hard</i> reset resets the entire DRAC 4 and is as close to a power-on reset as can be achieved using software. The DRAC 4 log, database, and selected daemons are shut down gracefully prior to the reset. A hard reset should be considered as a final effort. PCI configuration is lost.
soft	A <i>soft</i> reset is a processor and processor subsystem reset that resets the processor core to restart the software. PCI configurations are preserved. The DRAC 4 log, database, and selected daemons are shut down gracefully prior to the reset.
graceful	A <i>graceful</i> reset is the same as a soft reset.
<delay>	The user is allowed to select how many seconds of delay occur before the reset sequence is started. A valid delay entry is between 1-60 seconds. The default is 3 seconds.

Examples

- **racadm racreset soft 1**
Start the DRAC 4 soft reset sequence in 1 second.
- **racadm racreset soft 20**
Start the DRAC 4 soft reset sequence after 20 seconds.

racresetcfg


 **NOTE:** To use this command, you must have **Configure DRAC 4** permission.

Table A-26 describes the `racresetcfg` subcommand.

Table A-26. `racresetcfg`


Subcommand	Definition
<code>racresetcfg</code>	Resets all database configuration parameters to default values; equivalent to a soft reset.


Synopsis

```
racadm racresetcfg
```

Description

The `racresetcfg` command removes all database property entries that have been configured by the user. The database has default properties for all entries that are used to restore the card back to its original default settings. After resetting the database properties, the DRAC 4 resets automatically.

 **NOTICE:** Before using this command, ensure that you want to restore your database to its original default state with default user `root` and default password `calvin`.

 **NOTE:** After issuing a `racresetcfg` subcommand, stop and then restart the following services: Server Agent, Server Agent Event Monitor, and SNMP. See the *Dell OpenManage Server Administrator's User's Guide* for information on stopping and restarting the services in your operating system.

serveraction


 **NOTE:** To use this command, you must have **Execute Server Control Commands** permission.

Table A-27 describes the **serveraction** subcommand.

Table A-27. serveraction

Subcommand	Definition
serveraction	Executes a managed system reset or power-on/off/cycle.

Synopsis

```
racadm serveraction [-d <delay>] <action>
```

Description

The **serveraction** command provides an interface to control system reset and power control. Table A-28 describes the **serveraction** subcommand option values.

Table A-28. serveraction Subcommand Options

String	Definition
<action>	Specifies the action. The options for the <action> string are: <ul style="list-style-type: none">• powerdown — Powers down the system.• powerup — Powers up the system.• powercycle — Issues a power-cycle to the system.• hardreset — Issues a hard reset to the system.• graceshutdown — Powers down the system gracefully.• gracereboot — Powers down the system gracefully (same as the graceshutdown option)
<delay>	Specifies the time in seconds after the command is received before the action is executed. The default is 1 second.

Output

The **serveraction** command returns without output if successful.

getraclog


 **NOTE:** To use this command, you must have **Log In DRAC 4** permission.

Table A-29 describes the **getraclog** command.


Table A-29. getraclog

Command	Definition
<code>getraclog -i</code>	Displays the number of entries in the DRAC 4 log.
<code>getraclog</code>	Displays the DRAC 4 log entries.

Synopsis

```
racadm getraclog -i
racadm getraclog [-A] [-c count] [-d delay-seconds]
\[-s start-record] [-v] [-V] [-m]
```

Description

 **NOTE:** The command name and the **racadm** subcommand names may be different. This is normal.

The **getraclog -i** command displays the number of entries in the DRAC 4 log.

The following options allow the **getraclog** command to read entries:

- **-A** — Provides API-formatted output (no header).
- **-c** — Provides the maximum count of entries to be returned.
- **<blank>** — Displays the entire log; racadm and serial only (default).
- **-d** — Provides the number of seconds to delay the recording of any new log entries.
- **-s** — Provides the associated number of the first displayed entry (default = 0 [list begins with the first DRAC 4 log entry]).
- **-v** — Provides "verbose" output.
- **-V** — Provides "Very verbose" output.
- **-m** — Displays 24 rows at a time, and queries for more (such as the UNIX **more** command).


Output

One line of output is displayed for each DRAC 4 log entry.

Restrictions

The output buffer size is too big for execution across IPMI transport.


clrraclog

 **NOTE:** To use this command, you must have **Clear Logs** permission.

Synopsis

```
racadm clrraclog
```

Description

 **NOTE:** The command name and the **racadm** subcommand names may be different. This is normal.

The **clrraclog** command completely clears the DRAC 4 log. A single entry is made to indicate the user and time that the log was cleared.

getsel


 **NOTE:** To use this command, you must have **Log In To DRAC 4** permission.

Table A-30 describes the **getsel** command.

Table A-30. getsel

Command	Definition
<code>getsel -i</code>	Displays the number of entries in the System Event Log.
<code>getsel</code>	Displays SEL entries.

Synopsis

```
racadm getsel -i
```

```
racadm getsel [-E] [-R] [-A] [-c count] [-d delay-seconds] \ [-s count] [-v] [-V] [-m]
```

Description

The `getsel -i` command displays the number of entries in the SEL.

The `clrsel` command completely clears the SEL.

The following `getsel` options (without the `-i` option) are used to read entries.

`-A` — Provides API-formatted output (no header).

`-c` — Provides the maximum count of entries to be returned.

`<blank>` — Default is to display the entire log `racadm` and `serial` commands only (default).

`-d` — Provides the number of seconds to delay the recording of any new log entries.

`-s` — Provides the number of records to skip before returning entries (default=0).

`-v` — Provides "verbose" output.

`-V` — Provides "Very verbose" output.

`-E` — Places the 16 bytes of raw SEL at the end of each line of output as a sequence of hex values.

`-R` — Only the raw data is printed.

`-m` — Displays 24 rows at a time, and queries for more (such as the UNIX `more` command).

Output

One line of output is displayed for each SEL entry.

clrsel



NOTE: To use this command, you must have **Clear Logs** permission.

Synopsis

```
racadm clrsel
```

Description

The `clrsel` command completely clears the System Event Log entries.

gettracelog


 **NOTE:** To use this command, you must have **Log In To DRAC 4** permission.

Table A-31 describes the **gettracelog** subcommand.

Table A-31. gettracelog

Command	Definition
<code>gettracelog -i</code>	Displays the number of entries in the DRAC 4 trace log.
<code>gettracelog</code>	Displays the DRAC 4 trace log.

Synopsis

```
racadm gettracelog -i  
racadm gettracelog [-m]
```

Description

The **gettracelog -i** command displays the number of entries in the DRAC 4 trace log. The **gettracelog** (without the **-i** option) command reads entries.

The **-m** option displays 24 rows at a time, and queries for more (such as the UNIX **more** command).

Output

One line of output is displayed for each trace log entry.

setrac

Table A-32 describes the **setrac** subcommand.

Table A-32. setrac

Subcommand	Definition
<code>setrac</code>	Sets DRAC 4 parameters from the managed system. When used remotely, sets DRAC 4 parameters from the management station.

Synopsis

```
racadm setrac [-h -o -T -d]
```

Description



NOTE: The **racadm setrac** command cannot be used remotely.

The **setrac** command sets the managed system name, operating system name, or operating system type from the managed system to the DRAC 4. If options are not typed, all four parameters are set. The **-d** option allows the user to display the parameters only without actually writing them to the DRAC 4 firmware. Any combination of options, or no options, may be typed.

Input

Table A-33 describes the **setrac** subcommand options.

Table A-33. setrac Subcommand Options

Option	Description
-h	Gets the "Hostname" from the managed system and writes it to the DRAC 4. This parameter is available for viewing using the getsysinfo command, and under the object ID interface using config/getconfig as [ifcRacManagedNodeOs] ifcRacMnOsHostname .
-o	Gets the "OS Name" from the managed system and writes it to the DRAC 4. This parameter is available for viewing under the object ID interface using config/getconfig as [ifcRacManagedNodeOs] ifcRacMnOsName .
-T	Gets the "OS Type" from the managed system and writes it to the DRAC 4. This parameter is available for viewing using the getsysinfo command and under the object ID interface using config/getconfig as [ifcRacManagedNodeOs] ifcRacMnOsOsType .
-d	The -d , or display option, allows the user to get the "Hostname," "OS Name," and "OS Type" from the managed system and display these items only. Parameters are not written to the DRAC 4. If the -d option is typed along with other options, then those parameters are displayed only.

Output

A message is displayed indicating the values obtained from the managed system, and if they are being written to the DRAC 4 or only displayed.

Examples

- `racadm setrac -d` — Only the parameter values are displayed.
- `racadm setrac -h` — The UTC time and managed system name are taken from the managed system and written to the DRAC 4.

sslcsrgen



NOTE: To use this command, you must have **Configure DRAC 4** permission.

Table A-34 describes the `sslcsrgen` subcommand.

Table A-34. sslcsrgen

Subcommand	Description
<code>sslcsrgen</code>	Generates and downloads the SSL CSR.

Synopsis

```
racadm sslcsrgen [-g] [-u] [-f <filename>]
```

```
racadm sslcsrgen -s
```

Description

The `sslcsrgen` subcommand is used to generate the CSR and download it to a file, *<filename>*.

Options



NOTE: The `-u` and `-f` options are not supported for the serial/telnet console.

Table A-35 describes the `sslcsrgen` subcommand options.

Table A-35. sslcsrgen Subcommand Options

Option	Description
-g	Generates a new CSR.
-s	Returns the status of a CSR generation process (generation in progress, active, or none).
-u	Uploads the CSR to the filename specified by the -f option.
-f	Specifies the filename of the location, <filename>, where the CSR will be downloaded.



NOTE: If the **-f** option is not specified, the filename defaults to **sslcsr** in your current directory.

If options are not specified, the default is **-g -u**. The **-g -u** options (together) cannot be used with the **-s** option. The **-f** option must be used with the **-u** option.

The **sslcsrgen -s** subcommand returns one of the following status codes:

0x00000000 — CSR was generated successfully.

0x40040014 — CSR does not exist.

0x40040006 — CSR generation in progress.

0x40040009 — Key size is not supported.

The **sslcsrgen -u** subcommand downloads the CSR from the DRAC 4 by FTP. This command returns 0 when successful and returns a nonzero number when unsuccessful.

Restrictions

The **sslcsrgen** command can only run on a system that has the managed system software installed.

Examples

```
racadm sslcsrgen -s
```

or

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

sslcertupload


 **NOTE:** To use this command, you must have **Configure DRAC 4** permission.

Table A-36 describes the `sslcertupload` subcommand.

Table A-36. sslcertupload

Subcommand	Description
<code>sslcertupload</code>	Downloads a CA certificate to the DRAC 4.

Synopsis


```
racadm sslcertupload -t <type> [-f <filename>]
```

Options

Table A-37 describes the `sslcertupload` subcommand options.

Table A-37. sslcertupload Subcommand Options

Option	Description
-t	Specifies the type of certificate to upload, either the CA certificate or server certificate. 0x1 = server certificate 0x2 = CA certificate
-f	Specifies the filename, <filename>, to be uploaded.

 **NOTE:** If the `-f` option is not specified, the filename defaults to `sslcert` in your current directory.

The `sslcertupload` command returns 0 when successful and returns a nonzero number when unsuccessful.

Restrictions

The `sslcertupload` command can only run on a system that has the managed system software installed.

Example

```
racadm sslcertupload -t 0x1 -f c:\cert\cert.txt
```

sslcertdownload


 **NOTE:** To use this command, you must have **Configure DRAC 4** permission.

Table A-38 describes the `sslcertdownload` subcommand.

Table A-38. sslcertdownload

Subcommand	Description
<code>sslcertupload</code>	Downloads a CA certificate to the DRAC 4.

Synopsis


```
racadm sslcertdownload -t <type> [-f <filename>]
```

Options

Table A-39 describes the `sslcertdownload` subcommand options.

Table A-39. sslcertdownload Subcommand Options

Option	Description
<code>-t</code>	Specifies the type of certificate to download, either the CA certificate or server certificate. 0x1 = server certificate 0x2 = Active Directory certificate
<code>-f</code>	Specifies the filename, <filename>, to be uploaded.

 **NOTE:** If the `-f` option is not specified, the filename defaults to `sslcert` in your current directory.

The `sslcertdownload` command returns 0 when successful and returns a nonzero number when unsuccessful.

Restrictions

The `sslcertdownload` command can only run on a system that has the managed system software installed.

Example

```
racadm sslcertdownload -t 0x1 -f c:\cert\cert.txt
```

sslcertview


 **NOTE:** To use this command, you must have **Configure DRAC 4** permission.

Table A-40 describes the `sslcertview` subcommand.

Table A-40. sslcertview

Subcommand	Description
<code>sslcertview</code>	Displays a CA certificate or server certificate that is located in the DRAC 4.

Synopsis

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

Options

Table A-41 describes the `sslcertview` subcommand options.

Table A-41. sslcertview Subcommand Options

Option	Description
<code>-t</code>	Specifies the type of certificate to upload, either the CA certificate or server certificate. 0x1 = server certificate 0x2 = Active Directory certificate
<code>-A</code>	Prevents printing headers/labels.

Output Examples

For the `racadm sslcertview -t 1` subcommand, you receive output similar to the following example, where **C** is the country, **CN** is the common name, **O** is the organization, **OU** is the organizational unit, **L** is the locality, **S** is the state, and **E** is the email address:

```
certificate type=1
serial number=00
key size=1024
valid from=DSU+12:34:31
valid to=DSU+15:34:31
```

```
subject.C=US
subject.CN=RMC Default Certificate
subject.O=Dell Inc.
subject.OU=BVS
subject.L=Round Rock
subject.S=Texas
subject.E=john@dell.com
issuer.C=US
issuer.CN=RMC Default Certificate
issuer.O=Dell Inc.
issuer.OU=BVS
issuer.L=Round Rock
issuer.S=Texas
issuer.E=john@dell.com
```

For the **racadm sslcertview -t l -A** subcommand, you receive output similar to the following example:

```
1
00
1024
DSU+12:34:31
DSU+15:34:31
US
RMC Default Certificate
Dell Inc.
BVS
Round Rock
Texas
john@dell.com
US
RMC Default Certificate
Dell Inc.
BVS
Round Rock
Texas
john@dell.com
```

testemail

Table A-42 describes the **testemail** subcommand.

Table A-42. testemail

Subcommand	Description
testemail	Tests an email alert.

Synopsis

```
racadm testemail -i <index> | -u <username>
```

Description

The testemail subcommand forces the DRAC 4 to send an email over the DRAC 4 network adapter.

Options

Table A-43 describes the **testemail** subcommand options.

Table A-43. testemail Subcommand Options

Option	Description
-u	Specifies the user who receives the email. The necessary properties must be set up to correctly send email messages.
-i	Specifies the index of the user.

Output

None.

testtrap



NOTE: To use this command, you must have **Test Alerts** permission.

Table A-44 describes the **testtrap** subcommand.

Table A-44. testtrap

Subcommand	Description
testtrap	Tests an SNMP trap.

Synopsis

```
racadm testtrap -i <index>
```

Description

The **testtrap** subcommand forces the DRAC 4 to send an SNMP trap over the DRAC 4 NIC.

Input

Table A-45 describes the **testtrap** subcommand options.

Table A-45. testtrap Subcommand Options

Option	Description
-i	Specifies the index of the trap.

vmdisconnect



NOTE: To use this command, you must have **Access Virtual Media** permission.

Table A-46 describes the **vmdisconnect** subcommand.

Table A-46. vmdisconnect

Subcommand	Description
vmdisconnect	Forces a virtual media connection to close.

Synopsis

`racadm vmdisconnect`

Description

The `vmdisconnect` subcommand allows a user to forcibly disconnect another user's virtual media session. Once disconnected, the GUI will reflect the updated connection status. This is available only through the use of local or remote `racadm`.

DRAC 4 Property Database Group and Object Definitions

The DRAC 4 property database contains the configuration information for the DRAC 4. Data is organized by associated object, and objects are organized by object group. The IDs for the groups and objects that the property database supports are listed in this section.

Use the group and object IDs with the `racadm` utility to configure the DRAC 4. The following sections describe each object and indicate whether the object is readable, writable, or both.

idRacInfo

This group contains display parameters to provide information about the specifics of the DRAC 4 being queried.

One instance of the group is allowed. The following subsections describe the objects in this group.

idRacProductInfo (Read Only)

Legal Values

String of up to 63 ASCII characters.

Default

DRAC 4

Description

Uses a text string to identify the product.

idRacDescriptionInfo (Read Only)

Legal Values

String of up to 255 ASCII characters.

Default

RAC

Description

A text description of the RAC type.

idRacVersionInfo (Read Only)**Legal Values**

String of up to 63 ASCII characters.

Default

RAC Firmware Version *x.x*

Description

A string containing the current firmware version of the product, where *x* is the current revision.

idRacName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

String of up to 15 ASCII characters.

Default

RAC

Description

A user assigned name to identify this controller.

idRacMisc (Read/Write)**Legal Values**

String of up to 63 ASCII characters.

Default

Null string

Description

Generic property undefined at this release.

idRacType (Read)**Default**

5

Description

Identifies the remote access controller type as the DRAC 4.

cfgLanNetworking

This group contains parameters to configure the DRAC 4 NIC.

One instance of the group is allowed. All objects in this group will require the DRAC 4 NIC to be reset, which may cause a brief loss in connectivity. Objects that change the DRAC 4 NIC IP address settings will close all active user sessions and require users to reconnect using the updated IP address settings.

cfgDNSDomainNameFromDHCP (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).


Default

0

Description


Obtains the domain name from the DHCP server. This parameter is only valid if **cfgDNSRegisterRac** is set to 1 (TRUE).

cfgDNSDomainName (Read/Write)

 **NOTE:** To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

String of up to 254 ASCII characters. At least one of the characters must be alphabetic.

 **NOTE:** Microsoft Active Directory only supports Fully Qualified Domain Names (FQDN) of 64 bytes or fewer.


Default

MYDOMAIN

Description


The DNS domain name. This parameter is only valid if `cfgDNSRegisterRac` is set to 1 (TRUE) and if `cfgDNSDomainNameFromDHCP` is set to 0 (FALSE).

cfgDNSRacName (Read/Write)

 **NOTE:** To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

String of up to 63 ASCII characters. At least one of the characters must be alphabetic.

 **NOTE:** Some DNS servers only register names of 31 characters or fewer.

Default

RAC-*service tag*

Description

Displays the RAC name, which is RAC-*service tag* (by default). This parameter is only valid if `cfgDNSRegisterRac` is set to 1 (TRUE).

cfgDNSRegisterRac (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

Description

Registers the DRAC 4 name on the DNS server.

cfgDNSServersFromDHCP (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

Description

Retrieves DNS server addresses from the DHCP server.

cfgDNSServer1 (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Any legal IP address.

Default

192.168.0.5

Description

Retrieves the IP address for DNS server 1. This parameter is only valid if `cfgDNSServersFromDHCP` parameter is set to 0 (FALSE).



NOTE: `cfgDNSServer1` and `cfgDNSServer2` may be set to identical values while swapping addresses.

cfgDNSServer2 (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Any legal IP address, including 0.0.0.0.

Default

192.168.0.6

Description

Retrieves the IP address for DNS server 2. This parameter is only valid if `cfgDNSServersFromDHCP` is set to 0 (FALSE).



NOTE: `cfgDNSServer1` and `cfgDNSServer2` may be set to identical values while swapping addresses.

cfgNicEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=Disable.

1=Enable the DRAC 4 NIC.

cfgNicIpAddress (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of "." separated numeric fields containing the static IP address.

Default

192.168.0.120

Description

The IP address of the DRAC 4 NIC.

cfgNicNetmask (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of "." separated numeric fields containing the static network mask.

Default

255.255.255.0

Description

The network mask used by the DRAC 4 NIC.

cfgNicGateway (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of "." separated numeric fields containing the static gateway.

Default

192.168.0.120

Description

The gateway used by the DRAC 4 NIC.

cfgNicUseDhcp (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE)

Default

0

Description

0=Use the static DRAC 4 NIC parameters described above.

1=Use DHCP and obtain the necessary parameters from the DHCP server for the DRAC 4 NIC.

cfgNicMacAddress (Read Only)

Description

MAC address for the integrated NIC.

cfgCurrentLanNetworking

This group contains parameters that are currently in use by the DRAC 4 NIC. One instance of the group is allowed. The following subsections describe the objects in this group.

cfgNicCurrentIpAddress (Read Only)

Legal Values

A string of "." separated numeric fields containing the IP address

Default

None

Description

The current IP address of the DRAC 4 NIC.

cfgNicCurrentNetmask (Read Only)

Legal Values

A string of "." separated numeric fields containing the network mask.

Default

None

Description

The current network mask used by the DRAC 4 NIC.

cfgNicCurrentGateway (Read Only)

Legal Values

A string of "." separated numeric fields containing the gateway address.

Default

None

Description

The current gateway used by the DRAC 4 NIC.

cfgNicCurrentDhcpWasUsed (Read Only)

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

None

Description

Indicates whether or not DHCP was used to configure the NIC.

0 = IP address is static

1 = IP address was obtained from a DHCP server.

cfgDNSCurrentDomainName (Read Only)

Description

Current DNS domain name.

cfgDNSCurrentServer1 (Read Only)

Description

Current IP address used for DNS Server 1.

cfgDNSCurrentServer2 (Read Only)

Description

Current IP address used for DNS Server 2.

cfgRemoteHosts

The group contains parameters to configure various firmware update loading, IP addresses, enables, and so on.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgRhostsSntpEmailEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=disable, 1=enable the SMTP protocol to send email alerts.

cfgRhostsSmtplibAddr (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of "." separated numeric fields containing the IP address.

Default

127.0.0.1

Description

The IP address of the server used in email alerts.

cfgRhostsFirmwareUpdateTftpEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=Disable, 1=Enable loading the firmware update file through TFTP.

cfgRhostsFirmwareUpdateIpAddr (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of "." separated numeric fields containing the IP address.


Default

192.168.0.4

Description

The address of the TFTP server where the firmware update image is located.

cfgRhostsFwUpdatePath (Read/Write)

 **NOTE:** To modify this property, you must have **Configure DRAC 4** permission.

Legal Values


String of up to 255 ASCII characters that designate a valid path name.

Default

""

Description

The path name pointing to the firmware update binary file. If this is a file name only, then the path needs to be specified in the TFTP server. Otherwise, the entire path can be specified here.


 **NOTE:** The server may still require you to specify the drive (for example, **C**).

cfgUserAdmin

This group contains parameters that you can use to configure which users are allowed access to the DRAC 4.

Sixteen instances of the group are allowed, which corresponds to a user for each index. The following subsections describe the objects in this group.

cfgUserAdminPrivilege (Read/Write)

 **NOTE:** To modify this property, you must have **Configure Users** permission.

Legal Values

0x80000000 to 0x800001ff, and 0x0

Default

0


Description

Use the bit mask numbers in Table B-1 to set role-based authority privileges for a DRAC 4 user.

Table B-1. Bit Masks for User Privileges

User Privilege	Bit Mask
Log In To DRAC 4	0x80000001
Configure DRAC 4	0x80000002
Configure Users	0x80000004
Clear Logs	0x80000008
Execute Server Control Commands	0x80000010
Access Console Redirection	0x80000020
Access Virtual Media	0x80000040
Test Alerts	0x80000080
Execute Debug Commands	0x80000100

cfgUserAdminUserName (Read/Write)

 **NOTE:** To modify this property, you must have **Configure Users** permission.

Legal Values


A string of up to 19 ASCII characters.

Default


None

Description

The name of the user for this index. The user index is created by writing a string into this name field if the index is empty. Writing a string of double quotes ("") deletes the user at that index. You cannot change the name. You must delete and then recreate the name. The string must not contain "/" (forward slash), "\" (backslash), "." (period), "@" (at symbol) or quotations marks.

 **NOTE:** This command is the "anchor" for this indexed group.

cfgUserAdminPassword (Write Only)

 **NOTE:** To modify this property, you must have **Configure Users** permission.

Legal Values

A string of up to 20 ASCII characters.

Default

None

Description

The password for this user. The user passwords are encrypted and cannot be seen or displayed after this property is written.

cfgUserAdminAlertFilterRacEventMask (Read/Write)

NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

See "DRAC 4-Generated Event Mask Definitions."

Default

0x777777

Description

See "DRAC 4-Generated Event Mask Definitions." (Type hexadecimal values.)

cfgUserAdminAlertFilterSysEventMask (Read/Write)

NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

See "System-Generated Alert Mask Definitions."

Default

0x777777

Description

See "System-Generated Alert Mask Definitions." (Type hexadecimal values.)

cfgUserAdminEmailEnable (Read/Write)



NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

Boolean either 1 or 0 (TRUE or FALSE).

Default

0

Description

0=Disable, 1=Enable email alerting on a per user basis.

cfgUserAdminEmailAddress (Read/Write)



NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

A string of up to 63 ASCII characters.

Default

""

Description

Standard email address, such as john_doe@mycompany.com.

cfgUserAdminEmailCustomMsg (Read/Write)



NOTE: To modify this property, you must have **Configure Users** permission.

Legal Values

A string of up to 31 ASCII characters.

Default

""

Description

User-defined message to be sent on a email alert.

cfgUserAdminIndex (Read Only)

Description

Index of user entry.

cfgTraps

This group contains parameters to configure the delivery of SNMP traps. Sixteen instances of this group are allowed, which represent sixteen unique trap destinations. The following subsections describe the objects in this group.

cfgTrapsDestIpAddr (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of "." separated numeric fields containing the IP.

Default

""

Description

IP address of an SNMP trap daemon.



NOTE: This object is the "anchor" for this indexed group.

cfgTrapsEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=Disabled, 1=Enabled for this indexed entry.

cfgTrapsSnmpCommunity (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of up to 31 ASCII characters.

Default

""

Description

A SNMP community name.

cfgTrapsFilterRacEventMask (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

See "DRAC 4-Generated Event Mask Definitions."

Default

0x300000

Description

See "DRAC 4-Generated Event Mask Definitions." (Type hexadecimal values.)

cfgTrapsFilterSysEventMask (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

See "DRAC 4-Generated Event Mask Definitions."

Default

0x77777

Description

See "DRAC 4-Generated Event Mask Definitions." (Type hexadecimal values.)

cfgTrapsIndex (Read Only)**Legal Values**

See "DRAC 4-Generated Event Mask Definitions."

Default

0x77777

Description

Index of Trap entry.

cfgSessionManagement

This group contains parameters to configure the number of sessions that can connect to the DRAC 4.

One instance of the group is allowed. All objects in this group require a DRAC 4 reset before they become active. The following subsections describe the objects in this group.

cfgSsnMgtMaxSessions (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0x1 through 0x4

Default

0x4

Description

The maximum number of simultaneous sessions that are allowed at one time from the DRAC 4 Web-based remote access interface. (Type hexadecimal values.)

cfgSsnMgtMaxSessionsPerUser (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0x1 through 0x4

Default

0x4

Description

The maximum number of simultaneous sessions allowed per user. (Type hexadecimal values.)

cfgSsnMgtSshTelnetIdleTimeout (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0x0 through 0x780 seconds (0-32 minutes)

0 = No timeout

Default

0x12C seconds (5 minutes)

Description

Defines the Secure Shell idle timeout. This property sets the amount of time in seconds that a connection is allowed to remain idle (there is no user input). The session is cancelled if the time limit set by this property is reached. Changes to this setting do not affect the current session (you must log out and log in again to make the new settings effective).

cfgSerial

This group contains configuration parameters for the system external serial port.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgSerialBaudRate (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.



NOTE: For best results redirecting BIOS System Setup screens, Dell recommends using 115200.

Legal Values

9600, 28800, 57600, 115200

Default

115200

Description

Sets the baud rate on the external serial port. (Type decimal values).

cfgSerialConsoleEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

0

Description

0=Disabled, 1=Enabled. Enables the serial port and terminal interface.

cfgSerialConsoleQuitKey (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of 3 or less characters.

Default

The <CR><~><. > key combination

The <CR> key represents a carriage return; press <Enter> as a substitute for <CR>.

Description

This key sequence terminates text console redirection when using VT-100.

cfgSerialConsoleIdleTimeout (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer from 1 to any positive number. Type hexadecimal values.

Default

0x12c

Description

The maximum number of time (in seconds) of line idle time before the line is disconnected. (Type hexadecimal values.)

cfgSerialConsoleShellType (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

1 = VT100 block screen interface, has limited command function compared to type 2.

2 = UNIX-style command line data stream interface.

Default

Default 2

Description

Sets the serial console shell type. (Type hexadecimal values.)

cfgSerialConsoleNoAuth (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

- 0 – Login prompt is **Enabled** on the serial shell.
- 1 – Login prompt is **Disabled** on serial shell.

Default

0

Description

Allows you to disable authentication on the serial shell.

cfgSerialConsoleCommand (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Description

The **serial** command runs after login at the start of a session and allows you to set up a command such as **connect com2** that autoruns when a session begins.

Default

Empty string (no command).

Example

```
connect com2
```


cfgSerialHistorySize (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Any integer less than or equal to 8192. (If a value larger than 8192 is supplied, no error is returned and the history size is set to 8192.)

Default

8192 characters

Description

Sets the size of the serial history buffer.

cfgSerialSshEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0=disabled, 1=enabled

Default

1=enabled

Description

Enables/disables secure shell on the DRAC 4.

cfgSerialTelnetEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Description

Enables/disables telnet console

Default

0=telnet disabled

Legal Values

0=disabled, 1=enabled

cfgSerialCom2RedirEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Description

Enables/disables the console through the COM 2 port

Default

1=COM 2 (console enabled)

Legal Values

0=Disabled, 1=Enabled

cfgSerialTelnet7flsBackspace (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Description

When enabled, the DRAC 4 will interpret 0x7f characters as backspaces from a telnet session. Some telnet clients send 0x7f characters when you press <Backspace>. Normally, when you press <Backspace>, 0x08 characters are sent.

Default

0

Legal Values

0=Disabled, 1=Enabled

cfgNetTuning

The group contains parameters to tune the DRAC 4 network configuration.

One instance of the group is allowed. All objects in this group require a DRAC 4 reset before they become active. The following subsections describe the objects in this group.

cfgNetTuningNicAutoneg (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

1 or 0

Default

1

Description

Enables autonegotiation of physical link speed and duplex. If enabled, autonegotiation takes priority over values set in the `cfgNetTuningNic100MB` and `cfgNetTuningNicFullDuplex` objects.

cfgNetTuningNic100MB (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

1 or 0

Default

1

Description

Sets the DRAC 4 link speed to 100 Mbit (1) or 10 Mbit (0).

cfgNetTuningNicFullDuplex (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

1 or 0

Default

1

Description

Sets the duplex to full duplex(1) or half duplex (0).

cfgNetTuningNicMtu (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer from 576 to 1500.

Default

0x5dc (1500).

Description

The size in bytes of the maximum transmission unit used by the DRAC 4 NIC. (Type hexadecimal values.)

cfgNetTuningIpTtl (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer from 1 to 255.

Default

0x40 (64)

Description

The maximum IP packet time to live in seconds. (Type hexadecimal values.)

cfgNetTuningIpReassTtl (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer from 60 to 240.

Default

0x3c (60)

Description

The maximum IP packet fragment reassembly time in 1/2 second units. (Type hexadecimal values.)

cfgNetTuningTcpSrttBase (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer from 0 to 256.

Default

0x0 (0)

Description

The smoothed round trip time-out base minimum value for TCP round trip retransmission time in 1/2 second units. (Type hexadecimal values.)

cfgNetTuningTcpSrttDflt (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer from 6 to 384.


Default

0x6 (6)

Description

The smoothed round trip time-out base default value for TCP retransmission round trip time in 1/2 second units. (Type hexadecimal values.)

cfgNetTuningTcpReXmtMin (Read/Write)

 **NOTE:** To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer from 2 to 1024.


Default

0x2 (2)

Description

The minimum number of TCP retransmission time in 1/2 second units. (Type hexadecimal values.)

cfgNetTuningTcpReXmtMax (Read/Write)

 **NOTE:** To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer from 8 to 1024.


Default

0x80 (128)

Description

The maximum number of TCP retransmission time in 1/2 second units. (Type hexadecimal values.)

cfgNetTuningTcpMsl (Read/Write)

 **NOTE:** To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer from 60 to 240.

Default

0x3c (60)

Description

The maximum TCP segment lifetime in 1/2 second units. (Type hexadecimal values.)

cfgNetTuningIpSubnetsAreLocal (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

1 or 0

Default

1

Description

Packets addressed to subnets of the local net do not go to the gateway.

Tuning the DRAC 4 for Satellite Connectivity

The racadm CLI may be used to modify the network tuning properties of the DRAC 4. It is also possible to use the `racadm.cfg` file to modify these properties (similar to the manner in which `.ini` files are used).

```
racadm config -g cfgNetTuning -o cfgNetTuningNicMtu  
<value>
```

```
racadm config -g cfgNetTuning -o cfgNetTuningIpTtl  
<value>
```

```
racadm config -g cfgNetTuning -o  
cfgNetTuningIpReassTtl <value>
```

```
racadm config -g cfgNetTuning -o  
cfgNetTuningTcpSrttBase <value>
```

```
racadm config -g cfgNetTuning -o  
cfgNetTuningTcpSrttDflt <value>
```

```

racadm config -g cfgNetTuning -o
cfgNetTuningTcpReXmtMin <value>
racadm config -g cfgNetTuning -o
cfgNetTuningTcpReXmtMax <value>
racadm config -g cfgNetTuning -o cfgNetTuningTcpMsl
<value>

```

where <value> is obtained from Table B-2.

Table B-2. DRAC 4 Properties for Satellite Connectivity

Property	Normal Value	Satellite Value
cfgNetTuningNicMtu	0x5dc	0x1f4
cfgNetTuningIpTtl	0x40	0x80
cfgNetTuningIpReassTtl	0x3c	0x78
cfgNetTuningTcpSrttBase	0	0x100
cfgNetTuningTcpSrttDflt	0x6	0x180
cfgNetTuningTcpReXmtMin	0	0
cfgNetTuningTcpReXmtMax	0x80	0x400
cfgNetTuningTcpMsl	0x3c	0xf0

➡ NOTICE: Although you can configure these parameters, it is recommended that you only use the settings described here. Other settings may adversely effect the DRAC 4's ability to communicate with other network nodes.

Following the modification of the network tuning, the DRAC 4 must be reset for the new tuning values to take effect. After the DRAC 4 has been reset, it should be available for use in a normal or satellite network configuration.

cfgOobSnmpp

The group contains parameters to configure the SNMP agent and trap capabilities of the DRAC 4.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgOobSnmppAgentCommunity (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of up to 31 ASCII characters.

Default

public

Description

Use this to modify the SNMP Community Name.

cfgOobSnmppTrapsEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission. This object requires a DRAC 4 reset before it becomes active.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE)

Default

1

Description

0=Disable, 1=Enable transmission of SNMP traps.

cfgOobSnmppAgentEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission. This object requires a DRAC 4 reset before it becomes active.

Legal Values

Boolean either 1 or 0 (TRUE or FALSE).

Default

0

Description

0=Disable, 1=Enable the DRAC 4 SNMP agent.

cfgRacTuning

The group contains various tuning configuration parameters.

One instance of the group is allowed. The following subsections describe the objects in this group.

cfgRacTuneHttpPort (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0 – 65535

Default

80

Description

Use this property to configure the DRAC 4 HTTP port. (Type hexadecimal values.)

cfgRacTuneHttpsPort (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0 – 65535

Default

443

Description

Use this property to configure the DRAC 4 HTTPS port. (Type hexadecimal values.)

cfgRacTuneSshPort (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0 – 65535

Default

22

Description

Use this property to configure the DRAC 4 SSH port. (Type hexadecimal values.)

cfgRacTuneTelnetPort (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0 – 65535

Default

23

Description

Use this property to configure the DRAC 4 telnet port. (Type hexadecimal values.)

cfgRacTuneFwUpdateResetDelay (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer from 0 to 600.

Default

0x46 or 70

Description

The maximum number in seconds to wait between when the firmware update file is loaded, and the update sequence is started. (Type hexadecimal values.)

cfgRacTuneD3debugEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=disable, 1=enable the DRAC 4 debug command.

cfgRacTuneRemoteRacadmEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Boolean, either 1 or 0 (TRUE or FALSE).

Default

1

Description

0=Disable, 1=Enable

cfgRacTuneHostCom2BaudRate (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

115200, 57600, 19200, and 9600

Default

57600



NOTE: For best results when redirecting BIOS System Setup screens, Dell recommends setting this baud rate to 57600.

cfgRacTuneConRedirPort (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0-65535

Default

5900 (0x170c)

Description

Determines the port used during vKVM sessions with the **Console Redirection** window. After changing this property, the RAC must be reset prior to opening any new Console Redirection sessions. (Type hexadecimal values.)



NOTE: This object requires a DRAC 4 reset before it becomes active.

cfgRacTuneConRedirEncryptEnable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

1 (TRUE)

0 (FALSE)

Default

0

Description

Encrypts the video in a console redirection session.

ifcRacManagedNodeOs

This group contains parameters to configure the DRAC 4 with managed system and operating system naming information.

One instance of the group is allowed. The following subsections describe the objects in this group.

ifcRacMnOsHostname (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of up to 255 ASCII characters.

Default

""

Description

The host name of the managed system.

ifcRacMnOsOsName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of any ASCII characters.

Default

""

Description

The operating system name of the managed system.

ifcRacMnOsOsType (Read Only)**Legal Values**

Not user-writable.

Default

0

Description

Manage system operating system type.

cfgRacSecurity

This group contains parameters to configure the DRAC 4 SSL (Secure Sockets Layer) security features.

cfgRacSecCsrCommonName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of any ASCII characters

Default

""

Description

The CSR (certificate signing request) common name.

cfgRacSecCsrOrganizationName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of any ASCII characters.

Default

""

Description

The CSR organization name.

cfgRacSecCsrOrganizationUnit (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of any ASCII characters.

Default

""

Description

The CSR organization unit.

cfgRacSecCsrLocalityName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of any ASCII characters.

Default

""

Description

The CSR locality name.

cfgRacSecCsrStateName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of any ASCII characters.

Default

""

Description

The CSR state.

cfgRacSecCsrCountryCode (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

The two-letter country code.

Default

""

Description

The CSR country code.

cfgRacSecCsrEmailAddr (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

A string of any ASCII characters.

Default

""

Description

The CSR email address.

cfgRacSecCsrKeySize (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Positive integers.

Default

0x400

Description

DRAC 4 SSL asymmetric key size. (Type hexadecimal values.)

cfgRacVirtual

This group contains parameters to configure the DRAC 4 Virtual Media feature. One instance of the group is allowed. The following subsections describe the objects in this group.

cfgFloppyEmulation (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

1 or 0 (True or False)

Default

0

Description

0 (False) is the default setting, causing the DRAC 4 IDE Option ROM utility to display `DELL VIRTUALS-120` instead of `VIRTUALFLOPPY DRIVE`. Operating systems, such as Microsoft Windows, assign drive letters A or B to the RAC Virtual Floppy drive and configure the drive as a floppy drive. The RAC *Virtual* CD is required to assign drive letters D and higher.

cfgVirMediaDisable (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

1 or 0 (Disabled or Enabled)

Default

0 (Enabled)

Description

0 (Enabled) enables the Dell Virtual floppy on the next system restart.

1 (Disabled) disables the Dell Virtual floppy and CD-ROM on the next system restart. After restart:

- The operating system cannot access the drives.
- The virtual devices do not appear in the BIOS Setup screen.

The DRAC 4 IDE Option ROM utility displays the following messages when this feature is disabled:

```
Drive Number: 0 failed to detect Virtual device
```

```
Drive Number: 1 failed to detect Virtual device
```



NOTE: You must restart your system to enable all changes.

cfgVirAtapiSrvPort (Read/Write)

NOTE: To modify this property, you must have **Access Virtual Media** permission.

Legal Values

Any unused port number between 0 and 65535 decimal.

Default

0E54 in hexadecimal(3668 in decimal)


Description

Sets the port number or virtual media connection. (Type hexadecimal values).

cfgActiveDirectory

This group contains parameters to configure the DRAC 4 Active Directory feature.

cfgAD RacDomain (Read/Write)

 **NOTE:** To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Any printable text string with no white space. Length is limited to 254 characters.


Default

(blank)

Description

Active Directory Domain in which the DRAC resides.

cfgAD RacName (Read/Write)

 **NOTE:** To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Any printable text string with no white space. Length is limited to 254 characters.


Default

(blank)

Description

Name of DRAC as recorded in the Active Directory forest.

cfgAD Enable (Read/Write)

 **NOTE:** To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

1 or 0 (True or False)

Default

0

Description

1 (True) allows Active Directory authentication to take place. 0 (False) enables local DRAC 4 authentication only.

cfgADSpecifyServerEnable (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

1 or 0 (True or False)

Default

0

Description

1 (True) enables you to specify an LDAP or a Global Catalog server. 0 (False) disables this option.

cfgADDomainController (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Valid IP address or fully qualified domain name (FQDN)

Default

No default values

Description

DRAC 4 uses the value you specify, to search the LDAP server for user names.

cfgADGlobalCatalog (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Valid IP address or FQDN

Default

No default values

Description

DRAC 4 uses the value you specify, to search the Global Catalog server for user names.

cfgADAuthTimeout (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Integer greater than 15

Default

0x78 (120 seconds)

Description

Time in seconds to wait for Active Directory queries to complete. (Type hexadecimal values.)

cfgADRootDomain (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Any printable text string with no white space. Length is limited to 254 characters.

Default

(blank)

Description

Root domain of the Domain Forest.

cfgADType (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0x1 = Enables Extended Schema with Active Directory.

0x2 = Enables Standard Schema with Active Directory.

Default

0x1 = Extended Schema

Description

Determines the schema type to use with Active Directory.

cfgStandardSchema

This group contains parameters to configure the Standard Schema settings.

cfgSSADRoleGroupIndex (Read Only)**Legal Values**

Integer from 1 to 5.

Description

Index of the Role Group as recorded in the Active Directory.

cfgSSADRoleGroupName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Any printable text string with no white space. Length is limited to 254 characters.

Default

(blank)

Description

Name of the Role Group as recorded in the Active Directory forest.

cfgSSADRoleGroupDomain (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

Any printable text string with no white space. Length is limited to 254 characters.

Default

(blank)

Description

Active Directory Domain in which the Role Group resides.

cfgSSADRoleGroupPrivilege (Read/Write)



NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

0x00000000 to 0x000001ff

Default

(blank)

Description

Use the bit mask numbers in Table B-3 to set role-based authority privileges for a Role Group.

Table B-3. Bit Masks for Role Group Privileges


Role Group Privilege	Bit Mask
Log In To DRAC 4	0x00000001
Configure DRAC 4	0x00000002
Configure Users	0x00000004
Clear Logs	0x00000008
Execute Server Control Commands	0x00000010

Table B-3. Bit Masks for Role Group Privileges (continued)

Role Group Privilege	Bit Mask
Access Console Redirection	0x00000020
Access Virtual Media	0x00000040
Test Alerts	0x00000080
Execute Debug Commands	0x00000100

Event Filter Operation and Event Mask Properties

The DRAC 4 alert filter scans the **alert enable** database properties before it scans the event masks. (An event mask is a bit sequence that specifies information about the DRAC 4- or managed-system-generated event, such as the event's origin, type, and severity).

 **NOTE:** Throughout this document, objects are always referred to by group name and object name, separated by a space.

The DRAC 4 alert filter operates according to the following general steps:

- The DRAC 4 alert filter scans all of the objects in the **alert enable** property group **ID** is **cfgUserAdmin**. The object ID for this group is:
 - **cfgUserAdmin cfgUserAdminPageEmailEnable**If this object's property values is **TRUE**, it scans the event masks in the User table.
- The DRAC 4 alert filter scans the **cfgTraps** **cfgTrapsEnable** object. If this object's property value is **TRUE**, it scans the event masks in the Traps table.

The following subsections describe the event masks for DRAC 4-generated events and managed-system-generated events defined in the User table and the Trap table.

DRAC 4-Generated Event Mask Definitions

The **cfgUserAdmin** **cfgUserAdminAlertFilter {Rac, Sys} EventMask** properties are an unsigned 32-bit integer property that holds the filter information for DRAC 4-generated events. The bit definitions in Table B-4 apply.

Table B-4. DRAC 4-Generated Event Mask Bit Definitions

Bits	Data	Type
28-31	DRAC 4 undefined	reserved
24-27	DRAC 4 miscellaneous alerts	<Miscmask>
20-23	DRAC 4 BMC communication alerts	<BMCmask>

where <bmcMask> has the following bit definitions:

- Bit-0: 1 = Send alert for DRAC 4 communication with BMC and lost or restored communication between the DRAC 4 and BMC.
- Bit-1: 1 = Send alert for DRAC 4 lost communication with BMC.
- Bit-2: Reserved.
- Bit-3: Reserved.

Examples

- If you want to define alerts for the following:
 - Critical voltage or temperature sensors
 - Lost communication with the BMC

then the event mask property value to use is **0x02244444**. The following command sets this property value:

```
racadm -g cfgUserAdmin -o  
cfgUserAdminAlertFilterRacEventMask -i1 0x22444444
```

- If you want to define alerts for the following:
 - Critical events
 - System power off
 - Watchdog timer hang

then the event mask property value to use is **0x00064444**. The following command sets this property value:

```
racadm -g cfgTraps -o cfgTrapsFilterSysEventMask -  
i1 0x00064444
```

System-Generated Alert Mask Definitions

The `cfgTraps` `cfgTrapsFilter` {`Rac`, `Sys`} `EventMask` properties are an unsigned 32-bit integer property that holds the filter information for managed-system generated events. The bit definitions in Table B-5 apply.

Table B-5. System-Generated Alert Mask Bit Definitions

Bits	Data	Type
28–31	System undefined	reserved
24–27	System undefined	reserved
20–23	System undefined	reserved
16–19	System status alerts	< <i>statMask</i> >
12–15	System miscellaneous sensor	< <i>senMask</i> >
8–11	System fan sensors	< <i>senMask</i> >
4–7	System voltage sensors	< <i>senMask</i> >
0–3	System temperature sensors	< <i>senMask</i> >

where <*senMask*> has the following bit definitions:

- Bit-0: 1 = Send alert for informational events (such as a return to lower severity range or normal).
- Bit-1: 1 = Send alert for warning (noncritical) events.
- Bit-2: 1 = Send alert for critical events.
- Bit-3: Reserved.

where <*statMask*> has the following bit definitions:

- Bit-0: 1 = Send alert when system transitions to a powered-on state.
- Bit-1: 1 = Send alert when system transitions to a powered-off state.
- Bit-2: 1 = Send alert when watchdog timer detects a system hang.
- Bit-3: Reserved.

Alert Filter Properties

The alert filter property group ID is `cfgUserAdmin`. The object IDs are shown in Table B-6.

Table B-6. Alert Filter Property Group and Object IDs

GroupID	Object ID	Object Default Value
cfgUserAdmin	cfgUserAdminPageEmailEnable	FALSE
cfgUserAdmin	cfgUserAdminPageEmailAddress	""
cfgUserAdmin	cfgUserAdminPageEmailCustomMsg	""
cfgUserAdmin	cfgUserAdminAlertFilterRacEventMask	0x777777
cfgUserAdmin	cfgUserAdminAlertFilterSysEventMask	0x777777
cfgRemoteHosts	cfgRhostsSmtpServerIpAddr	0.0.0.0
cfgOobSnmp	cfgOobSnmpTrapsEnable	TRUE
cfgTraps	cfgTrapsDestIpAddr	0.0.0.0
cfgTraps	cfgTrapsEnable	FALSE
cfgTraps	cfgTrapsSnmpCommunity	""
cfgTraps	cfgTrapsFilterRacEventMask	0x777777
cfgTraps	cfgTrapsFilterSysEventMask	0x777777

Alert Test Commands

You can test alerts using test commands. The `racadm` command has subcommands that test the different types of alert interfaces. These object ID sets cause the firmware to execute the subcommand with the option that indicates the test alert type to test. The test message is preset in properties for each test alert type. The types of alerts are email and trap.

The following subsection describes the command interfaces and the operation of the subcommand for each option.

Email Test Command

Synopsis

```
racadm testemail -e -i <index>  
racadm testemail -e -u <username>
```

Alert Data Definitions

The email alert contains the following information: message (including test message, if a paging test), event description, date, time, severity, system ID, model, BIOS version, asset tag, service tag, managed system name, operating system name, and BMC version. The following is an example test email (fields shown are examples only and may not reflect actual observed output for your environment):

```
Subject: Alert from Dell Remote Access Card:  
10.35.10.108
```

```
Message: TEST PAGE
```

```
Event: Email paging test to user 1
```

```
Date: 06-jun-2004
```

```
Time: 00:01:37
```

```
Severity: Info/Normal
```

```
System ID: Bbn
```

```
Model: Dell PowerEdge 2800
```

```
BIOS version: A00
```

```
Asset tag: 181676
```

```
Service tag: 6X713
```

```
Hostname: P2-750-08
```

```
OS Name: Linux 7.1 for the Itanium Processor
```

```
BMC Version: 1.3
```

Trap Test Command

Synopsis

```
racadm testtrap -t -i <trap index>
```

Alert Data Definitions

The "alertMessage" string (up to 1 KB) provides the specific information describing the cause and specific source of the event, which includes:

- Sensor identification: entity/IPMBSlaveAddress
- Sensor number
- Sensor ID string (if possible)
- Current reading and range (normal/warning/critical)
- Threshold values: minimum, maximum, normal

For more information, see the *Dell OpenManage™ Server Administrator SNMP Reference Guide*.

Glossary

Active Directory

Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperability with other directories. Active Directory is designed especially for distributed networking environments.

AGP

Abbreviation for accelerated graphics port, which is a bus specification that allows graphics cards faster access to main system memory.

ARP

Acronym for Address Resolution Protocol, which is a method for finding a host's Ethernet address from its Internet address.

ASCII

Acronym for American Standard Code for Information Interchange, which is a code representation used for displaying or printing letters, numbers, and other characters.

BIOS

Acronym for basic input/output system, which is the part of system software that provides the lowest-level interface to peripheral devices and which controls the first stage of the system boot process, including installation of the operating system into memory.

BMC

Abbreviation for baseboard management controller, which is the controller interface between the DRAC 4 and the managed system's BMC.

bus

A set of conductors connecting the various functional units in a computer. Buses are named by the type of data they carry, such as data bus, address bus, or PCI bus.

CA

A certificate authority is a business entity that is recognized in the IT industry for meeting high standards of reliable screening, identification, and other important security criteria. Examples of CAs include Thawte and VeriSign. After the CA receives your CSR, they review and verify the information the CSR contains. If the applicant meets the CA's security standards, the CA issues a certificate to the applicant that uniquely identifies that applicant for transactions over networks and on the Internet.

CD

Abbreviation for compact disc.

CHAP

Acronym for Challenge-Handshake Authentication Protocol, which is an authentication method used by PPP servers to validate the identity of the originator of the connection.

CIM

Acronym for Common Information Model, which is a protocol designed for managing systems on a network.

CLI

Abbreviation for command-line interface.

console redirection

Console redirection is a function that directs a managed system's display screen, mouse functions, and keyboard functions to the corresponding devices on a management station. You may then use the management station's system console to control the managed system.

DHCP

Abbreviation for Dynamic Host Configuration Protocol, which is a protocol that provides a means to dynamically allocate IP addresses to computers on a local area network.

DLL

Abbreviation for Dynamic Link Library, which is a library of small programs, any of which can be called when needed by a larger program that is running in the system. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (or file).

DDNS

Abbreviation for Dynamic Domain Name System.

DNS

Abbreviation for Domain Name System.

DRAC 4

Abbreviation for Dell Remote Access Controller 4.

DSU

Abbreviation for disk storage unit.

extended schema

A solution used with Active Directory to determine user access to DRAC 4; uses Dell-defined Active Directory objects.

FQDN

Acronym for Fully Qualified Domain Names. Microsoft Active Directory only supports FQDN of 64 bytes or fewer.

FSMO

Flexible Single Master Operation. It is Microsoft's way of guaranteeing atomicity of the extension operation.

GMT

Abbreviation for Greenwich Mean Time, which is the standard time common to every place in the world. GMT nominally reflects the mean solar time along the prime meridian (0 longitude) that runs through the Greenwich Observatory outside of London, UK.

GPIO

Abbreviation for general purpose input/output.

GRUB

Acronym for GRand Unified Bootloader, a new and commonly-used Red Hat Enterprise Linux loader.

GUI

Abbreviation for graphical user interface, which refers to a computer display interface that uses elements such as windows, dialog boxes, and buttons as opposed to a command prompt interface, in which all user interaction is displayed and typed in text.

hardware log

Records events generated by the DRAC 4 and the BMC.

ICMB

Abbreviation for Intelligent Chassis Management Bus.

ICMP

Abbreviation for Internet control message protocol.

ID

Abbreviation for identifier, commonly used when referring to a user identifier (user ID) or object identifier (object ID).

IP

Abbreviation for Internet Protocol, which is the network layer for TCP/IP. IP provides packet routing, fragmentation, and reassembly.

IPMB

Abbreviation for intelligent platform management bus, which is a bus used in systems management technology.

IPMI

Abbreviation for Intelligent Platform Management Interface, which is a part of systems management technology.

JVM

Abbreviation for Java Virtual Machine, which is a system-independent execution environment that converts compiled Java code (byte code) for a system processor so that it can perform a Java program instructions.

JRE

Abbreviation for Java Runtime Environment.

Kbps

Abbreviation for kilobits per second, which is a data transfer rate.

LAN

Abbreviation for local area network.

LDAP

Abbreviation for Lightweight Directory Access Protocol.

LED

Abbreviation for light-emitting diode.

MAC

Acronym for media access control, which is a network sublayer between a network node and the network physical layer.

MAC address

Acronym for media access control address, which is a unique address embedded in the physical components of a NIC.

managed system

The managed system is the system in which the DRAC 4 is installed or embedded.

management station

The management station is a system that remotely accesses the DRAC 4.

Mbps

Abbreviation for megabits per second, which is a data transfer rate.

MIB

Abbreviation for management information base.

NAS

Abbreviation for network attached storage.

NIC

Abbreviation for network interface card. An adapter circuit board installed in a computer to provide a physical connection to a network.

NLM

Abbreviation for NetWare Loadable Module.

OID

Abbreviation for Object Identifiers.

PCI

Abbreviation for Peripheral Component Interconnect, which is a standard interface and bus technology for connecting peripherals to a system and for communicating with those peripherals.

POST

Acronym for power-on self-test, which is a sequence of diagnostic tests that are run automatically by a system when it is powered on.

PPP

Abbreviation for Point-to-Point Protocol, which is the Internet standard protocol for transmitting network layer datagrams (such as IP packets) over serial point-to-point links.

RAM

Acronym for random-access memory. RAM is general-purpose readable and writable memory on systems and the DRAC 4.

RAM disk

A memory-resident program which emulates a hard drive. The DRAC 4 maintains a RAM disk in its memory.

RAC

Abbreviation for remote access controller.

ROM

Acronym for read-only memory, which is memory from which data may be read, but to which data cannot be written.

RPM

Abbreviation for Red Hat Package Manager, which is a package-management system for the Red Hat Enterprise Linux operating system that helps installation of software packages. It is similar to an installation program.

SAC

Acronym for Microsoft's Special Administration Console.

SEL

Acronym for system event log.

SMI

Abbreviation for systems management interrupt.

SMTP

Abbreviation for Simple Mail Transfer Protocol, which is a protocol used to transfer electronic mail between systems, usually over an Ethernet.

SNMP

Abbreviation for Simple Network Management Protocol, which is a protocol designed to manage nodes on an IP network. DRAC 4s are SNMP-managed devices (nodes).

SNMP trap

A notification (event) generated by the DRAC 4 or the BMC that contains information about state changes on the managed system or about potential hardware problems.

SSL

Abbreviation for secure sockets layer.

standard schema

A solution used with Active Directory to determine user access to DRAC 4; uses Active Directory group objects only.

TAP

Abbreviation for Telelocator Alphanumeric Protocol, which is a protocol used for submitting requests to a pager service.

TCP/IP

Abbreviation for Transmission Control Protocol/Internet Protocol, which represents the set of standard Ethernet protocols that includes the network layer and transport layer protocols.

TFTP

Abbreviation for Trivial File Transfer Protocol, which is a simple file transfer protocol used for downloading boot code to diskless devices or systems.

UPS

Abbreviation for uninterruptible power supply.

USB

Abbreviation for Universal Serial Bus.

UTC

Abbreviation for Universal Coordinated Time. *See* GMT.

VNC

Abbreviation for virtual network computing.

VT-100

Abbreviation for Video Terminal 100, which is used by the most common terminal emulation programs.

WAN

Abbreviation for wide area network.

Index

A

- Active Directory
 - configuring, 111
 - object overview, 107
 - schema extensions, 106
 - using with extended schema, 106
 - using with standard schema, 125
- alerts
 - adding, 71
 - configuring, 71
 - SNMP, 77
 - troubleshooting, 98
- arp, 188

B

- BIOS
 - updating the system, 29

C

- certificate signing request (CSR)
 - about, 82
 - viewing a server certificate, 82
- clearascreen, 188
- clrraclog, 214
- clrsel, 215
- config, 189

- configuring
 - the software, 49
- configuring the DRAC 4, 177
- connections
 - supported, 19
- connectors, 18
 - connecting the DB-9 cable, 61
- console redirection
 - using, 135
- coredump, 193
- coredumpdelete, 195

D

- digital certificates
 - about, 81
- DRAC 4
 - accessing through a network, 43
 - adding and configuring alerts, 71
 - adding and configuring users, 71
 - adding users, 42
 - configuring, 28, 121, 171
 - configuring Active Directory, 111
 - configuring network
 - properties, 181
 - configuring network settings, 37
 - configuring properties, 37
 - configuring the NIC, 74
 - configuring users, 42

- configuring using racadm, 177
- deleting a user, 179
- enabling serial/telnet console, 56
- installing hardware, 27
- installing software, 28
- updating firmware, 42
- using Active Directory to log in, 131

DRAC 4 log messages, 98

dracadm utility

- parsing rules, 174
- subcommands, 187

E

extended schema

- using with Active Directory, 106

F

features, 16, 24

- security, 19

Firefox

- configuring, 33
- disabling whitelist, 23
- supported version, 23

fwupdate, 195

G

getconfig, 189

getniccfg, 206

getraclog, 213

getractime, 204

getsel, 214

getssninfo, 200

getsvctag, 208

getsysinfo, 201

gettracelog, 216

I

ifconfig, 205

installation

- software, 49

Internet Explorer

- configuring, 33

J

Java plug-in

- installing, 34

L

last crash screen

- capturing, 30

last system crash screen

- viewing, 93

log messages, 98

M

- managed system
 - capturing the last crash screen, 30
 - configuring the system setup program, 50
 - connecting using the client system, 61
 - connecting using the local serial port, 61
 - enabling to use serial or telnet console, 50
 - installing software, 29
 - managing, 80
 - recovering, 89
 - troubleshooting, 89
- management station
 - configuring terminal emulation, 62
 - installing software, 31
- messages
 - DRAC 4 log, 98
- Microsoft Windows
 - disabling reboot option, 31
 - installing using Virtual Media, 151

N

- netstat, 205
- network
 - troubleshooting, 96
- network properties
 - configuring manually, 181

O

- operating systems
 - supported, 20

P

- parsing rules, 174
- ping, 206
- platforms
 - supported, 20
- plug-in
 - installing, 149
- ports, 18

R

- racadm
 - configuring the DRAC 4, 177
- racadm CLI
 - using, 166
- racadm utility, 177
- racdump, 208
- racreset, 209
- racresetcfg, 211
- reboot
 - disabling option, 31

- Red Hat Enterprise Linux
 - configuring for serial console emulation, 63
 - configuring for serial redirection during boot, 51
 - configuring XTerm, 66
 - DRAC 4 software basics, 45
 - installing the racadm CLI, 32
 - installing using Virtual Media, 151
- remote system
 - managing, 80

S

- Secure Shell (SSH)
 - changing the SSH port, 59
 - enabling, 59, 128
 - using, 59
- serial/telnet console
 - features, 49
 - using, 67, 163
- server certificate
 - generating, 83
 - uploading, 83, 85
 - viewing, 82-83
- serveraction, 212
- setniccfg, 206
- setrac, 216
- short domain name, 122
- SNMP
 - adding alerts, 77
 - configuring alerts, 77

- SNMP alerts
 - adding, 42
 - configuring, 42
- software configuration, 49
- software installation, 49
- specifications
 - hardware, 17
- specify
 - global catalog server, 124
 - LDAP server, 124
- SSL
 - about, 81
- sslcertdownload, 221
- sslcertupload, 220
- sslcertview, 222
- sslcsrgen, 218
- standard schema
 - using with Active Directory, 125
- system information
 - viewing, 86

T

- testemail, 224
- testtrap, 225
- troubleshooting
 - alerting problems, 98
 - basic, 185
 - network problems, 96

U

updating
 system BIOS, 29

V

Virtual Floppy
 configuring, 153

Virtual Media
 booting, 150
 disabling, 152
 enabling, 152
 installing operating systems, 151
 installing plug-in, 149
 using, 150

vmdisconnect, 225

W

warranty, 25

Web browser
 configuring, 33
 configuring Firefox, 33
 configuring Internet Explorer, 33

Web browsers
 for 64-bit operating systems, 23
 supported, 22

Web-based interface
 accessing, 69

what's new, 15

