Dell™ Remote Access Controller 4

Firmware Version 1.30 User's Guide

www.dell.com | support.dell.com

Notes, Notices, and Cautions

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.

CAUTION: A CAUTION indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

May 2005 Rev. A00

Contents

1 DRAC 4 Overview

2 Installing and Setting Up the DRAC 4

5 Using the DRAC 4 With Microsoft® Active Directory

6 Using Console Redirection

7 Configuring and Using Virtual Media

8 Using the serial and racadm Commands

Figures

Tables

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 DRAC 4 in this Release?

For this release, DRAC 4 firmware version 1.30 supports the following:

- Secure Shell (SSH). For more information, see "Using the Secure Shell (SSH)."
- History buffer. For more information, see "Starting a Text Console."
- racadm vmdisconnect. For more information, see "vmdisconnect."
- ISO image support for Virtual Media
- Remote operating system deployment using the VM-CLI utility. See "Operating System Deployment Using the DRAC 4 Virtual Media CLI Feature."
- A new object named **cfgVirtualBootOnce** has been added to the Virtual Media configuration group "cfgRacVirtual." See "cfgVirtualBootOnce (Read/Write)."

DRAC 4 Hardware Features

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

Figure 1-1. DRAC 4/I Hardware Features

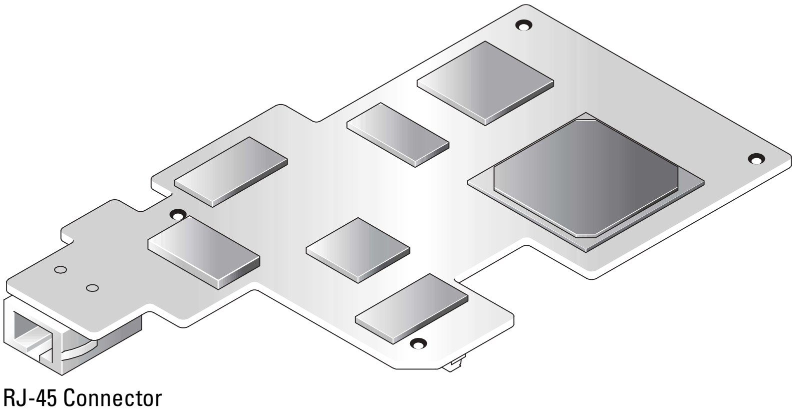
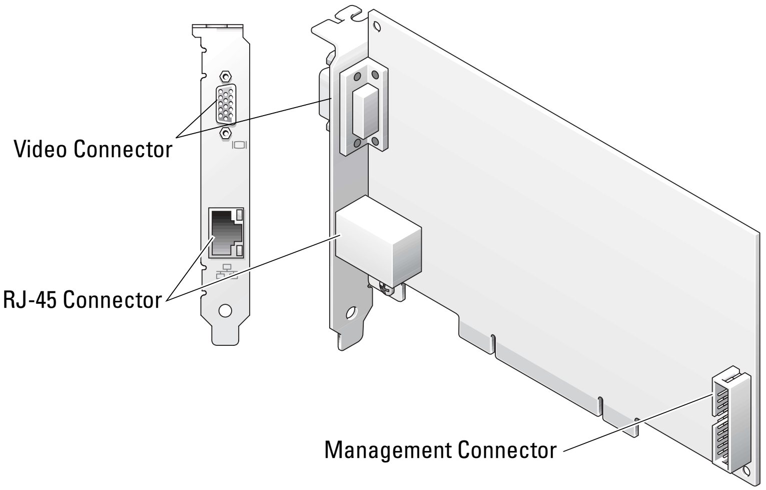


Figure 1-2. DRAC 4/P Hardware Features



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: Installation instructions for the DRAC 4 hardware can be found in the *Installing a Remote Access Card* document or the *Installation and Troubleshooting Guide* that comes 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)

Table 1-2. DRAC 4 Port Numbers *(continued)*

DRAC 4 Port Number	Used For
Ports that DRAC 4 uses as a client:	
25	SMTP (not configurable)
69	TFTP (not configurable)
162	SNMP trap (not configurable)
53	DNS (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	• 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	• 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:

- Authentication for users through Microsoft Active Directory (optional) or hardware-stored user IDs and passwords
- Role-based authority allows specific privileges to be configured for each user
- User ID and password configuration through the Web-based interface or racadm CLI
- racadm CLI and Web-based interface operation supports SSL encryption of 128 bit and 40 bit (for countries where 128 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
- Many of the commonly known DRAC 4 IP ports are configurable
- Secure Shell (SSH) that uses an encrypted transport layer for higher security. SSH is available on DRAC 4 firmware 1.30.

Supported Platforms

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

- PowerEdge 1850
- PowerEdge 2800
- PowerEdge 2850

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

- PowerEdge 800
- PowerEdge 1800
- PowerEdge 6800
- PowerEdge 6850

Supported Operating Systems

The DRAC 4 currently supports the following operating systems:

- Microsoft Windows Server™ 2003 Standard Edition SP1, Windows Server 2003 Enterprise Edition SP1, Windows Server 2003 Web Edition SP1, Windows Server 2003 x64, Windows Small Business Server (SBS) 2003 SP1
- Windows 2000 Server (SP4) and Windows 2000 Advanced Server (SP4)
- Novell® NetWare® 6.5 (SP1 or later)
- Red Hat® Enterprise Linux AS, ES, and WS (version 3) for Intel® Extended Memory 64-bit Technology (Intel EM64T) and Intel x86
- Red Hat Enterprise Linux (version 4) for Intel x86 and Intel EM64T

NOTICE: Currently, the Virtual Media feature is not supported under any version of the Novell NetWare operating system. NetWare drivers ignore the virtual drives and do not make them available to the system.

Supported Web Browsers

NOTE: The Console Redirection feature requires that you have installed 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.

- 32-bit versions of Microsoft Internet Explorer 6.0 on Windows
- 32-bit versions of Mozilla 1.6 or later on Red Hat Enterprise Linux
- 32-bit versions of Mozilla Firefox 1.0.1 on Red Hat Enterprise Linux

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.

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).
- Remote management and monitoring of a system through the DRAC 4 Web-based interface, serial connection, or telnet connection.
- Configuring Microsoft Active Directory service software 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 software.
- Console redirection feature 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 Dell OpenManage™ Server Administrator and Dell OpenManage 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 following system documents are also available to provide more information about the system in which your DRAC 4 is installed:

CAUTION: 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.
- 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.

2

Installing and Setting Up the DRAC 4

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

What You Need to Get Started

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 PowerEdge Installation and Server Management* CD
- *Dell Systems Management Consoles* CD
- *Dell PowerEdge 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: The removal of expansion cards, such as the DRAC 4, is documented in the *Installation and Troubleshooting Guide* that came with your system.

Software Installation and Configuration Overview

This section provides a high-level overview of the DRAC 4 software installation and configuration process. All configuration steps can be performed 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."

To install your DRAC 4 software, perform the following steps in their numbered 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."

To configure your DRAC 4 software, perform the following steps in their numbered order. All configuration steps can be performed using the Web-based interface, racadm CLI, or Serial/Telnet console. Network configuration can also be performed using operating system utilities (Option ROM).

NOTICE: Unexpected results may occur if you use more than one of the following configuration methods simultaneously: Web-based interface, racadm CLI, or Option ROM.

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

1 Configure the DRAC 4 network settings. See "Configuring the DRAC 4 Network Settings."

2 Add and configure DRAC 4 users. See "Adding and Configuring DRAC 4 Users."

3 Configure the Web browser to connect to the Web-based interface. See "Configuring a Supported Web Browser."

4 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.

5 Disable the Windows Automatic Reboot Option. See "Disabling the Windows Automatic Reboot Option."

6 Update the DRAC 4 Firmware. See "Updating the DRAC 4 Firmware."

7 Access the DRAC 4 through a network. See "Accessing the DRAC 4 Through a Network."

Installing the Software on the Managed System

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

To install the managed system software, install the software on the managed system using the *Dell Systems Management Consoles* 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, you must 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, you must 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 Click the **Start** button and select **Settings** → **Control Panel** → **System** → **System Properties.**

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 Click the **Start** button and select **Settings** → **Control Panel** → **System** → **System Properties.**

2 Click the **Advanced** tab.

3 Click the **Startup and Recovery...** button.

4 Deselect the **Automatically Reboot** check box.

Installing the Software on the Management Station

Install the software, including Server Administrator, on the management station using the *Dell Systems Management Consoles* CD.

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 Management Consoles* CD.

To install the racadm CLI utility, insert the *Dell Systems Management Consoles* 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 Internet Explorer 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 need to configure the Web browser to connect properly.

1. From the Internet Explorer main window, click **Tools**, and then click **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.

Viewing Localized Versions of the Web-Based Interface

When using Internet Explorer on systems running Microsoft Windows to view localized versions of the DRAC 4 Web-based interface, do the following:

1 Open the Windows **Control Panel** and double-click the **Regional Options** icon.

2 Select the desired locale from the **Your locale (location)** drop-down menu.

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, you must install the supported Sun Java plug-in and also clear and disable the Java cache from the Java plug-in control panel on Windows systems.

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 on your *Dell Systems Management Consoles 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. Perform the following steps to install JRE:

1 Launch the installation script by using the following commands from the directory in which the script is located:

```
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, which you are prompted to accept before continuing the installation. After you have accepted the license agreement, the installation script creates the file **j2re-1_4_**`<version number>`**-linux-i586.rpm** in the current directory.

2 To become the root user, type the **su** command and type the power-user password.

3 Run the following **rpm** command to install the packages. This command installs the packages comprising the Java 2 Runtime Environment (J2RE):

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

Only one Java plug-in can be registered at a time. If you have never registered a Java plug-in, go to the next step; otherwise, go to step 5.

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.

For example:

```
cd /usr/lib/mozilla<version number>/plugins
```

```
rm libjavaplugin_oji.so
```

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

For example:

```
cd <Mozilla>/plugins
```

```
ln s j2re1.4<version number>/plugin/i386/ns610/libjavaplugin_o
ji.so libjavaplugin_oji.so
```

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

5 Start Mozilla and go to **Tools** → **Web Development** → **Java Console**.

The version of JRE is displayed at the top of the **Java Console** window. If the version that is shown is not the same as the one you downloaded, then registration did not work. The same is true if the **Java Console** menu option is grayed out.

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."

NOTE: The DRAC 4 resets its NIC every 30 seconds when the network is idle to ensure that the physical hardware mechanisms remain operational.

Configuring the DRAC 4 Network Settings Using the Option ROM

The DRAC 4 contains an integrated NIC that has a default address of **192.168.0.120** and a default gateway of **192.168.0.1**. Perform the following steps to use the DRAC 4 IDE Option ROM utility to configure these settings and a limited number of additional DRAC 4 network settings.

1 To access the DRAC 4 IDE Option ROM utility during the managed system's boot, press <Ctrl><d> within 5 seconds of the time the DRAC 4 banner, firmware version, and current NIC IP address are displayed.

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

2 Use Table 2-1 to select and change the DRAC 4 NIC properties. Make changes by typing one-keystroke menu selections. The menu selections are not case sensitive.

Virtual Media settings are on page two. Use the `<Page Up>` and `<Page Down>` keys to move between the two pages.

NOTE: When modifying any of the following options, you can 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`
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 IP address that the DRAC 4 uses if DHCP is disabled. The default is 192.168.0.120. Press <i> to change this address.
Static Netmask	Indicates the preset static masked IP address of the DRAC 4 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 speed at which the DRAC 4 NIC is set to communicate. 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.
LAN Duplex Setting	Indicates the duplex setting of the DRAC 4 NIC. 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 at any given moment it can either receive or transmit information, but not both. 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.

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

Properties	Description
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 RAC-*service tag*, where *service tag* 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.
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 After you have made the changes you want, you can press <r> to save the changes and reboot the DRAC 4, or you can press <Esc> to cancel all changes and exit the setup menu. If you decide to save your changes, 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. Manually removing or modifying either the A record or TXT record associated with **cfgDNSRacName**, through the DNS server administrative interface, causes unexpected results (for example, the server cannot resolve the name, the server cannot update the name, and the server returns the incorrect information for the name).

NOTE: The DRAC 4 DDNS implementation requires that DNS servers be configured to allow nonsecure updates.

NOTE: DDNS events can be found in the DRAC 4 trace log. To view DDNS events, use the **gettracelog** command on the Web-based interface **Diagnostics** page or use the racadm **gettracelog** command.

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 can be found 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 the hardware is installed and the software is configured.

After you configure the DRAC 4, you can remotely access the managed system using one of four remote access interfaces. Table 2-2 describes each of the DRAC 4 interfaces.

Table 2-2. DRAC 4 Interfaces

Interface	Description
Web-based interface	Enables you to remotely access 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	Allows you to connect to the managed system and execute racadm commands from a remote console (racadm remote capability option [-r]), or management station using only the IP address of the managed system. **NOTE:** The racadm remote capability is supported only on management stations running Windows Server 2003, Windows 2000 Server, Windows XP Professional, Windows 2000 Professional, and Red Hat Linux operating systems.
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.

To access the DRAC 4 using a supported Web browser, type the IP address of the DRAC 4. Log in with your DRAC 4 user name and password (the default user name and password are `root` and `calvin` respectively). For more information about using the DRAC 4 remote access interface, see the remote access interface online help.

To access the DRAC 4 remote access interface using Server Administrator, first launch Server Administrator. From the system tree on the left pane of the Server Administrator home page, click **System → Main System Chassis → Remote Access Controller**. For more information about using Server Administrator remote access features, see your *Server Administrator User's Guide*.

For information about accessing the DRAC 4 using the racadm CLI, see "Using the serial and racadm Commands."

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 racsrvc 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, racsrvc, 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

The removal of expansion cards, such as the DRAC 4, is documented in the *Installation and Troubleshooting Guide* that came with your system.

Removing DRAC 4-Related Applications and Drivers

You must uninstall Server Administrator to remove the RAC module that was installed with Server Administrator. Use **Add or Remove Programs** to uninstall Server Administrator.

You must also remove the RAC drivers from all locations in your device manager. To do so, go to **Control Panel** and click **System** → **Hardware** → **Device Manager**.

For each of the following drivers, select the device, and then click **Action** → **Uninstall**.

- Remote Access Controller — RAC Virtual UART Port
- System Devices — RAC PCI Function 0
- System Devices — RAC PCI Function 2

In addition, 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.

The following 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

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

- 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 time-out setting on SSH connections for enhanced security, controlled by the "cfgSsnMgtSshIdleTimeout (Read/Write)" object

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

The following subsections provide information about how to enable and configure 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 file **/etc/grub.conf**, as follows. See the sample file that follows, which 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, you must comment it out.

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

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

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

serial --unit=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**:

1 You may need to disable GRUB's graphical interface and use the text-based interface instead; otherwise, the GRUB screen will not be displayed in RAC console redirection. To do so, comment out the line starting with `splashimage`.

2 If you have multiple options in GRUB and you want all of them to start a console session through the RAC serial connection, you need to add `console=ttyS1,57600` to all options. The preceding example shows `console=ttyS0,57600` added to only the first option.

Enabling Login to the Console After Boot

Edit the file **/etc/inittab**, as follows:

Add a new line to configure a getty on the COM1 serial port:

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

See the sample file, which shows the addition of the new line.

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

```
#
# 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
```

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

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
# Things to run in every runlevel.
ud::once:/sbin/update

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

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


# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS0 vt100
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**, as follows:

Add a new line, with the name of the serial tty for COM1:

```
ttyS0
```

See the sample file, which shows the addition of 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
ttyS0
```

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, you must 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 commands 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)

It is mission critical for devices and device management to be secure. Connected embedded devices are at the core of many business processes. If their security is compromised, your customer's business may be at high risk and it also places new security demands on command line interface (CLI) device management software. Secure Shell (SSH) is a command line session that has 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 the host key generation. If this operation is interrupted for any reason, key generation will start over the next time the DRAC 4 starts up.

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

NOTE: OpenSSH should be run from a VT100 or ANSI terminal emulator on Windows®. Running OpenSSH at the Windows command prompt does not result in full functionality (that is, some keys do not respond and no graphics are displayed).

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

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

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

You can change the SSH port with the 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."

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) may 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 may 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

If you want to connect to the managed system using a serial text console, you must 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. Drag the lower right-hand corner of the window to resize it to 80 x 25 prior to using Minicom. Drag the lower right corner with the mouse.
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 To save each blank value, press <Enter>.

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 may be useful to 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.

5 Click **OK**.

6 Click **File** → **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**.

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

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.

When running telnet with 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 To start a new Xterm session, type `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 you have enabled telnet, you can connect to the DRAC 4 by performing the following steps:

1. Open a command prompt.
2. Type `telnet <IP address>:<port number>` and press `<Enter>` (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 a Windows XP or Windows 2003 user who is having problems with characters in a DRAC 4 telnet session, go to the **support.microsoft.com** website, and search the knowledge base for article 824810 for 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: With a Windows 2000 management station, pressing the <F2> key does not enter BIOS setup. This problem is resolved by using the telnet client supplied with the Windows Services for UNIX® 3.5 (recommended free download from Microsoft). You can download Windows Services for UNIX 3.5 from **www.microsoft.com/windows/sfu/downloads/default.asp**.

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 there are already three valid sessions, 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) that allows you to configure the DRAC 4 properties and users, perform remote management tasks, and troubleshoot a remote (managed) system for problems. For everyday systems management, you will use the DRAC 4 Web-based interface. This chapter 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 you are working in the Web-based interface, see your DRAC 4 online help for context sensitive information about each Web-based interface page.

Accessing the Web-Based Interface

To link to the DRAC 4 remote Web-based interface **Log in** window, open your Web browser and type `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) in the address field, and press <Enter>. 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 an Active Directory user. To log in, perform the following steps.

NOTE: The default user name and password are "root" and "calvin."

1 In the **User Name** field, enter either your DRAC 4 user name as <*username*>, or Active Directory user name as <*domain*>\<*username*>, <*domain*>/<*username*>, or <*user*>@<*domain*>. The DRAC 4 user name for local users is case sensitive; the Active Directory user name is not case sensitive. 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 may want to create unique users with specific administrative permissions (role-based authority). You can also configure alerts to be emailed to different users.

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

- Adding and Configuring SNMP Alerts
- 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	Allows you to specify a DRAC 4 user name. (Once the user name is specified, you cannot change it. Every 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	Allows you to specify or edit 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 permissions group for the user.

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 4**, **Configure DRAC 4**, **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 4**, **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 4**, 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 4**, **Configure DRAC 4**, **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 which events, according to their severity, will cause an email alert to be sent. Select the severity of the temperature, voltage, fan, or miscellaneous sensor for which you want an email alert generated. You can specify three severities: **Informational** (lowest severity), **Warning** (medium severity), and **Severe** (highest severity). Alerts will be sent to the email address you typed in **Enabling User email Alerts**. For information about each email alert severity type, see Table 4-4.

Table 4-4. email Alert Severity

Severity	Description
Informational	Select the check boxes in this column to cause the DRAC 4 to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Informational**.
Warning	Select the check boxes in this column to cause the DRAC 4 to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Warning**.
Severe	Select the check boxes in this column to cause the DRAC 4 to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Severe**.
Alert Description	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. • **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.
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 page if you want to print the **Add/Configure DRAC 4 User** page.

Configuring the DRAC 4 NIC

1. Click the **Configuration** tab and select **Network**.
2. Use the **Network Configuration** page to configure the DRAC 4 NIC settings and configure email alert settings. Table 4-5 describes each setting on the **Network Configuration** page. Table 4-6 describes the **Network Configuration** page buttons.

NOTE: To change any of the settings on the **Network Configuration** page, you must have **Configure DRAC 4** permission.

NOTE: Assigning a predefined IP address to the DRAC 4 using a DHCP server: most DHCP servers require a client identifier token to be stored in the server's reservations table. The client (DRAC 4, for example) has to provide that token during the DHCP negotiation phase. In the case of RACs, the DRAC 4 supplies the client identifier option as follows: 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 MAC address of the DRAC 4
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)	Causes Server Administrator to obtain the IP address for the DRAC 4 NIC from the Dynamic Host Configuration Protocol (DHCP) server; selecting the check box deactivates the **Static IP Address**, **Static Gateway**, and **Static Subnet Mask** controls.
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, you must first 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, you must first deselect the **Use DHCP (For NIC IP Address)** check box.
Use DHCP to obtain DNS server addresses (default: Disabled)	Causes the primary and secondary DNS server addresses to be obtained from the DHCP server, rather than the static settings, when selected.
Static Preferred DNS Server	Causes the IP address of the primary DNS server to be used only when **Use DHCP to obtain DNS server addresses** is **not selected**.
Static Alternate DNS Server	Causes the IP address of the secondary DNS server to be used when **Use DHCP to obtain DNS server addresses** is **not selected**. You may 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)	Select this option to register the DRAC 4 name on the DNS server.

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

Setting	Description
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 *service tag* is the service tag number of the Dell™ server (for example, RAC-EK00002).
Use DHCP for DNS Domain Name (default: Disabled)	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.
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	Enables you to set 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	Enables you to set 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 Time-out	Enables you to specify 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 or edits the IP address of the SMTP server to which you want all email messages to be sent.

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 Use the **Add/Configure SNMP Alerts** page to add, delete, configure, and test 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	Determines whether you want to enable 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	Select the check boxes in this column to cause the DRAC 4 to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Informational** (lowest severity).
Warning	Select the check boxes in this column to cause the DRAC 4 to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Warning** (medium severity).
Severe	Select the check boxes in this column to cause the DRAC 4 to send an alert if the corresponding event listed under **Alert Description** occurs with a severity of **Severe** (highest severity).
Alert Description	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. **NOTE:** For information about how to manage events, see the *Server Administrator User's Guide*. • **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?	Displays (**Yes** or **No**) whether you have enabled SNMP alerts on the **Add/Configure SNMP Alerts** page.
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 page.

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
- Ensuring DRAC 4 Network Security
- 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, you must first acquire the latest firmware version and save it on your local system.

1 Type the system path where the firmware image file resides (for example: `C:\Updates\V1.0\<image_name>`). The default firmware image name is **firmimg.dm1**.

2 Click **Update Firmware**.

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

3 Click **OK** to close the session and automatically log out.

4 After the DRAC 4 resets, click **Log In** to log in to the DRAC 4 again.

Ensuring DRAC 4 Network Security

The DRAC 4 uses certificate management to ensure security for your DRAC 4 network communications.

Certificate Management Overview

A Certificate Signing Request (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, submit the CSR to a CA.

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.

Table 4-14. Required CSR Fields *(continued)*

Properties	Description
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 *Server Administrator User's Guide*. 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.
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).

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

Field	Description
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 time-out 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
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 ("Using Console Redirection") and remote power management (see "Managing Power on a Remote System") to restart the system and watch 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 page.

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 page.

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 **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 page:

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
arp	Displays the contents of the Address Resolution Protocol (ARP) table. ARP entries may not be added or deleted.
ifconfig	Displays the contents of the network interface table.
netstat	Prints the content of the routing table. If the optional interface number is provided in the text field to the right of the **netstat** option, then netstat prints additional information regarding the traffic across the interface, buffer usage, and other network interface information.
ping <*IP Address*>	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.
getcoredump	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.
settracelog	Enables you to set debug trace levels to identify the types of messages being sent on the local network. The **-d** option traces the DHCP packets sent and received. The **-i** option traces IP packets sent and received. For example, type `settracelog -i` to trace IP packets sent and received.
gettracelog	Displays a UNIX-style system log. This log is a volatile, memory-resident log that contains time-stamped entries.
nettrace	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 page.

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.
0x5016	EINVALID: An argument is invalid.
0x5017	ENFILE: An internal table has run out of space.
0x5020	EPIPE: The connection is broken.
0x5023	EWOULDBLOCK: 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.

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

Error Code	Description
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.
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

Administrators can use DRAC 4 log messages 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 following characters, that represent the severity level or type of message, are sometimes appended to the message identifier that is displayed in the **Message ID** column: 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.
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.

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

Message ID	Description	Suggested Action
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.
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?
	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.
	You can change the DRAC 4 community name using the racadm CLI.
	To see the DRAC 4 community name, use the following command:
	`racadm getconfig -g cfgOobSnmp`
	To set the DRAC 4 community name, use the following command:
	`racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name>`
	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.

Why are the remote racadm and Web-based services unavailable after a property change?	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 The DRAC 4 Web server is reset after the following occurrences: • When the **cfgRacTuneHttpsPort** property is changed (including when a config -f <*config file*> changes it) • When **racresetcfg** is used • When the DRAC 4 is reset

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 hostname of the SSL certificate does not match the hostname of the DRAC 4.	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 "Ensuring DRAC 4 Network Security" for more information about generating CSRs and issuing certificates.
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 "Ensuring DRAC 4 Network Security" 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.
Why am I getting multiple keystrokes even when I press the key only once?	Set the key repetition rate to `slow` on the server when Console Redirection is desired and network bandwidth is low.

5

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.

Active Directory Schema Extensions

The Active Directory data, simply explained, can be conceptualized as a distributed database of Attributes and Classes. The rules for what data can be added or included in the database is the Active Directory schema. An example of a Class that is stored is the user class. Some example attributes of the user class might be 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.

Every 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 objects that can be configured by the user depending on the desired results. Dell has extended the schema to include an Association, Device, and Privilege object. The Association object 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

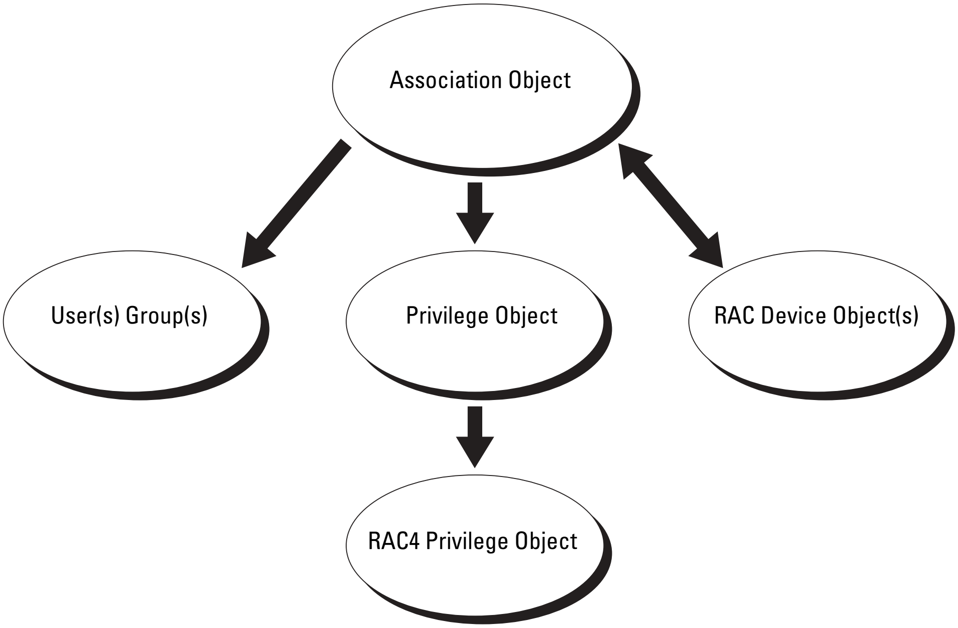
For each of the physical RACs on the network that you want to integrate with Active Directory for Authentication and Authorization, you must create at least one Association Object and one RAC Device Object. You can create as many Association Objects as you want, and each Association Object can be linked 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 may 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.

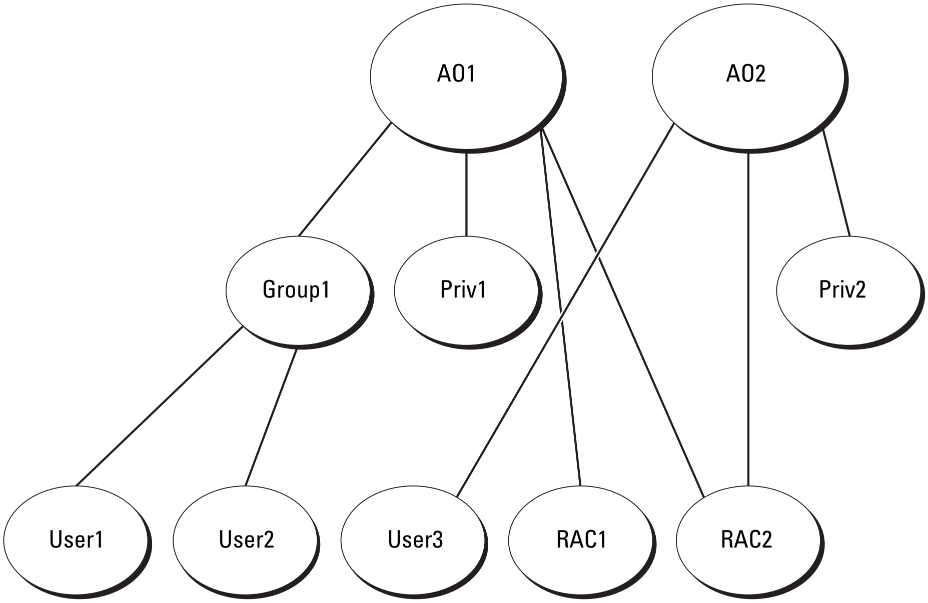
Figure 5-1. Typical Setup for Active Directory Objects



You can create as many or as few association objects as you want or need. 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).

In addition, you can set up 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



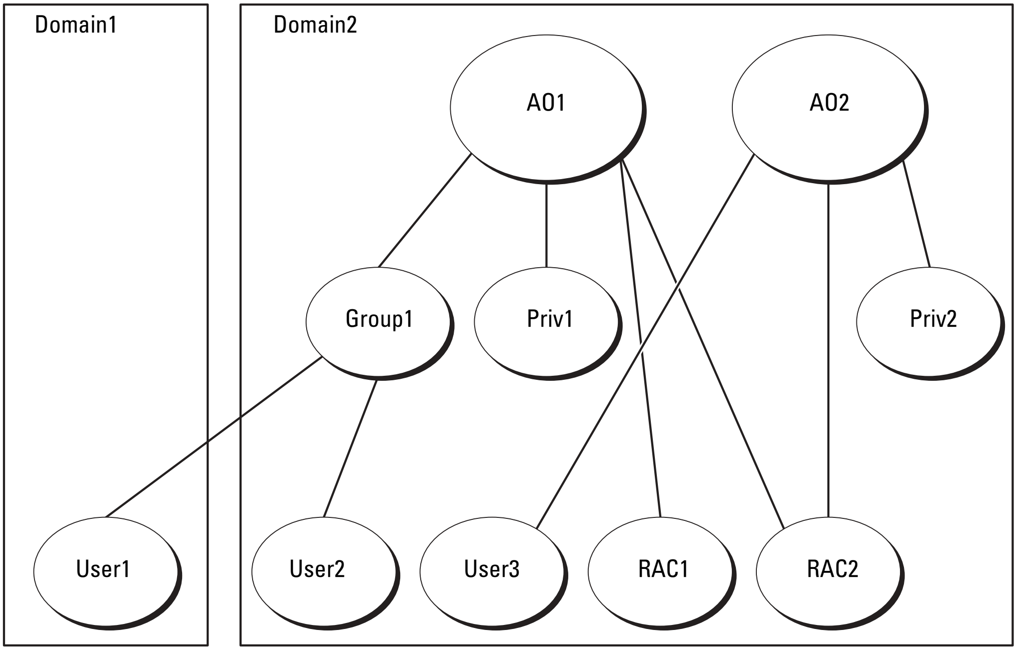
To set up the objects for the single domain scenario, perform the following tasks:

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, you must configure the Active Directory software and the DRAC 4 by performing the following steps in their numbered 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").

Extending the Active Directory Schema

Extending your Active Directory schema will add a Dell organizational unit, schema classes and attributes, and example privileges and association objects to the Active Directory schema.

NOTE: 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 two different methods. You can use the Dell Schema Extender utility, or you can use the LDIF script file.

NOTE: The Dell organizational unit will not be added if you use the LDIF script file.

The LDIF files and Dell Schema Extender are located on your *Dell Systems Management Consoles* 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. Click **Next** on the Welcome screen.
2. Read the warning and click **Next** again.
3. Either 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 the existence of the following classes (listed in Table 5-1, Table 5-2, Table 5-3, Table 5-4, Table 5-5, and Table 5-6) and attributes (listed in 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	1.2.840.113556.1.8000.1280.1.1.2.1	FALSE
List of dellPrivilege Objects that belong to this Attribute.	Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellProductMembers	1.2.840.113556.1.8000.1280.1.1.2.2	FALSE
List of dellRacDevices Objects that belong to this role. This attribute is the forward link to the dellAssociationMembers backward link. Link ID: 12070	Distinguished Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellIsLoginUser	1.2.840.113556.1.8000.1280.1.1.2.3	TRUE
TRUE if the user has Login rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsCardConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.4	TRUE
TRUE if the user has Card Configuration rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsUserConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.5	TRUE
TRUE if the user has User Configuration rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
delIsLogClearAdmin	1.2.840.113556.1.8000.1280.1.1.2.6	TRUE
TRUE if the user has Log Clearing rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsServerResetUser	1.2.840.113556.1.8000.1280.1.1.2.7	TRUE
TRUE if the user has Server Reset rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsConsoleRedirectUser	1.2.840.113556.1.8000.1280.1.1.2.8	TRUE
TRUE if the user has Console Redirection rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsVirtualMediaUser	1.2.840.113556.1.8000.1280.1.1.2.9	TRUE
TRUE if the user has Virtual Media rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsTestAlertUser	1.2.840.113556.1.8000.1280.1.1.2.10	TRUE
TRUE if the user has Test Alert User rights on the device.	Boolean (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	

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 (LDAPTYPE_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 (LDAPTYPE_CASEIGNORESTRING 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 (LDAPTYPE_CASEIGNORESTRING 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 (LDAPTYPE_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. The Dell Extension to the Active Directory User's and Computers Snap-In is an option that can be installed when you install your systems management software using the *Dell Systems Management Consoles* CD. See the *Dell OpenManage Software Quick Installation Guide* for further instructions on installing systems management software.

NOTE: You must install the Administrator Pack on each system that is managing the Active Directory DRAC 4 Objects. The installation is described in the following section, "Opening the Active Directory Users and Computers Snap-In." If you do not install the Administrator Pack, then you cannot view the Dell RAC Object in the container.

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

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>.

  This opens the Microsoft Management Console (MMC).

2 Click **File** (or **Console** on systems running Windows 2000) in the **Console 1** window.

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

The Dell-extended Active Directory Users and Computers snap-in allows you to add DRAC 4 users and privileges by creating RAC, Association, and Privilege objects. To add each type of object, perform the steps in each subsections.

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 4 of "Configuring the DRAC 4."

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**.

This opens the **New Object** window.

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

By using the **Association Object Properties** window, you can associate users or user groups, privilege objects, and RAC devices or RAC device groups.

NOTE: When using Windows 2000 mode or higher, you must use Universal Groups to span domains with your users or RAC objects.

You can add groups of Users and RAC devices. Creating Dell-related groups is done the same way you create other groups.

To add 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.

NOTE: You can add only one privilege object to an association object.

To add a privilege:

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.

NOTE: You can add multiple RAC devices to an association object.

To add 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**.

Enabling SSL on a Domain Controller

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

1 Install a Microsoft Enterprise Root CA on a Domain Controller.

  a Select **Start** → **Control Panel** → **Add or Remove Programs**.

  b Select **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 Enter **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** → **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: The following steps may vary slightly if you are using Windows 2000.

1 Go to the domain controller on which you installed the Microsoft Enterprise CA service.

2 Click **Start** → **Run**.

3 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 location of your choice. You will need to upload this certificate to the DRAC 4. To do this, go to the **DRAC 4 Web-based interface** → **Configuration** tab → **Active Directory page**. Alternately, you may use the **racadm** CLI commands (see "Configuring the DRAC 4 Active Directory Settings Using the racadm CLI").

15 Click **Finish** and click **OK**.

Importing the DRAC 4 Firmware SSL Certificate to All Domain Controllers 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.

1 The DRAC 4 SSL certificate is the same certificate that is used for the DRAC 4 Web server. All DRAC 4 controllers are shipped with a default self-signed certificate. You can get this certificate from the DRAC 4 by selecting the DRAC 4 Web-based interface **Configuration** tab → **Active Directory** subtab → **Download DRAC 4 Server Certificate**.

2 On the domain controller, open an **MMC Console** window and select **Certificates** → **Trusted Root Certification Authorities**.

3 Right-click **Certificates**, select **All Tasks** and click **Import**.

4 Click **Next** and browse to the SSL certificate file.

5 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.

6 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.

7 Click **Finish** and click **OK**.

Configuring the DRAC 4

1 Log in to the Web-based interface using the default user, root, and its password.

2 Click the **Configuration** tab and select the **Active Directory**.

3 Select the **Enable Active Directory** check box.

4 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").

5 Type the **Root Domain Name**. The **Root Domain Name** is the fully qualified root domain name for the forest.

6 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.

7 Click **Apply** to save the Active Directory settings.

8 Click **Upload Active Directory CA Certificat**e to upload your domain forest Root CA certificate into the DRAC 4. Your domain forest domain controllers' SSL certificates need to have signed this root CA certificate. Have the root CA certificate available on your local system (see "Exporting the Domain Controller Root CA Certificate"). Specify the full path and filename of the root CA certificate and click **Upload** to upload the root CA certificate to the DRAC 4 firmware. The DRAC 4 Web server automatically restarts after you click **Upload**. You must log in again to complete the DRAC 4 Active Directory feature configuration.

9 Click the **Configuration** tab and select **Network**.

10 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.

11 Click **Apply**.

This completes the DRAC 4 Active Directory feature configuration.

Configuring the DRAC 4 Active Directory Settings Using the racadm CLI

Using the following commands to configure the DRAC 4 Active Directory Feature 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 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 DHCP is enabled on the DRAC 4 and you want to use the DNS provided by the DHCP server, type the following 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 IP address, type the following 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>
```

4 Press **Enter** to complete the DRAC 4 Active Directory feature configuration.

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, with remote **racadm**, or through 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.

Frequently Asked Questions

Table 5-8 lists frequently asked questions and answers.

Table 5-8. Using the DRAC 4 With Active Directory: Frequently Asked Questions

Question	Answer
Can I log into the DRAC 4 using Active Directory across multiple forests?	The DRAC 4's Active Directory querying algorithm only supports a single tree in a single forest.
Does the login 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.
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.

Table 5-8. Using the DRAC 4 With Active Directory: Frequently Asked Questions *(continued)*

Question	Answer
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 is you inadvertently chose **User Certificate** instead of **Web Certificate** when creating the certificate. To recover, create a new Web certificate from Microsoft Certificate Services and load it using the racadm CLI from the managed system by typing: `racadm sslcertupload -t 0x1 -f <web_sslcert>`
What can I do if I cannot log into the DRAC 4 using Active Directory authentication? How do I troubleshoot the issue?	Troubleshoot as follows: • 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.

6

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 you can use console redirection, all browsers must have a Sun Java Virtual Machine Plug-in (version 1.4.2 and later) installed, and the Java cache must be cleared and disabled 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."

NOTICE: Remote console sessions remain active even after the DRAC 4 user interface times out. This behavior may pose a possible security risk.

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

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.

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

NOTE: Localized keyboard support is available from the Console Redirection Applet for French, German, Spanish, and Simplified Chinese keyboards.

To open a console redirection session, perform the following steps:

1 Open a Web browser on your management station. Connect and log into the DRAC 4.

2 Click **Console** in the left pane to bring you to the **Console Redirection** page. Read and follow the instructions on this page for starting a console redirection session.

3 Examine the information provided on the **Console Redirection** page (see Table 6-1) 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.

4 Click **Open Console** to open a new console.

5 Use the buttons on the **Console Redirection** page (see Table 6-2 and Table 6-3) to help you perform actions on the remote system.

Table 6-2. Console Redirection Page Buttons

Button	Action
Keyboard Macros	Enables you to select and type 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	Enables you to select a key that acts as a previous keystroke to your actual keystrokes. Select either <Ctrl>, <Alt>, or <SysRq>.
Mouse Acceleration	Enables you to select 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** page.
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.

Table 6-3. Other Console Redirection Page Buttons

Button	Action
Print	Prints the **Console Redirection** page.
Refresh	Reloads 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.
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.

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

Question	Answer
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 *Dell PowerEdge Installation and Server Management* CD.
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 *Dell PowerEdge Installation and Server Management* CD 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 *Dell PowerEdge Installation and Server Management* CD.
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 *Dell PowerEdge Installation and Server Management* CD.
After I click **Open Console,** the message `Please wait while vKVM applet is loaded...` 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?	To set the server display to 256 colors: • 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. Reason for setting the server display to 256 colors: 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.
Why doesn't the vKVM mouse sync when I use the *Dell PowerEdge Installation and Server Management* CD to remotely install the operating system?	Select **Linux** for mouse acceleration on the vKVM window pull-down menu.
Why doesn't the vKVM mouse sync after coming back from hibernation on a Windows system?	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.
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.

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

Question	Answer
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: `rpm -qa | grep radeon_7000m_dell_server` The RPM *rhel**_radeon_7000m_dell_server-0.4-1* or later should be installed. This RPM is available at www.dell.com.
Why doesn't the vKVM mouse work with Red Hat Enterprise Linux, version 2.1, update 3?	Red Hat Enterprise Linux, version 2.1 does not fully support multiple input devices. 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. To use **mouseconfig** to enable RAC mouse control for XWindows: **1** Run **Xconfigurator** (if not previously run before). **2** Run **mouseconfig** GUI. **3** Select **Generic Mouse (USB)**. **4** Run Xwindows (`startx`). To use **mouseconfig** to re-enable local mouse control: **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?	Use the *Dell PowerEdge Installation and Server Management* CD to install the NetWare operating system. The default screen resolution is 1024x768 so you won't have the issue with mouse sync.
Why doesn't the vKVM mouse and keyboard work when changing mouse acceleration for different operating systems?	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).
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).

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

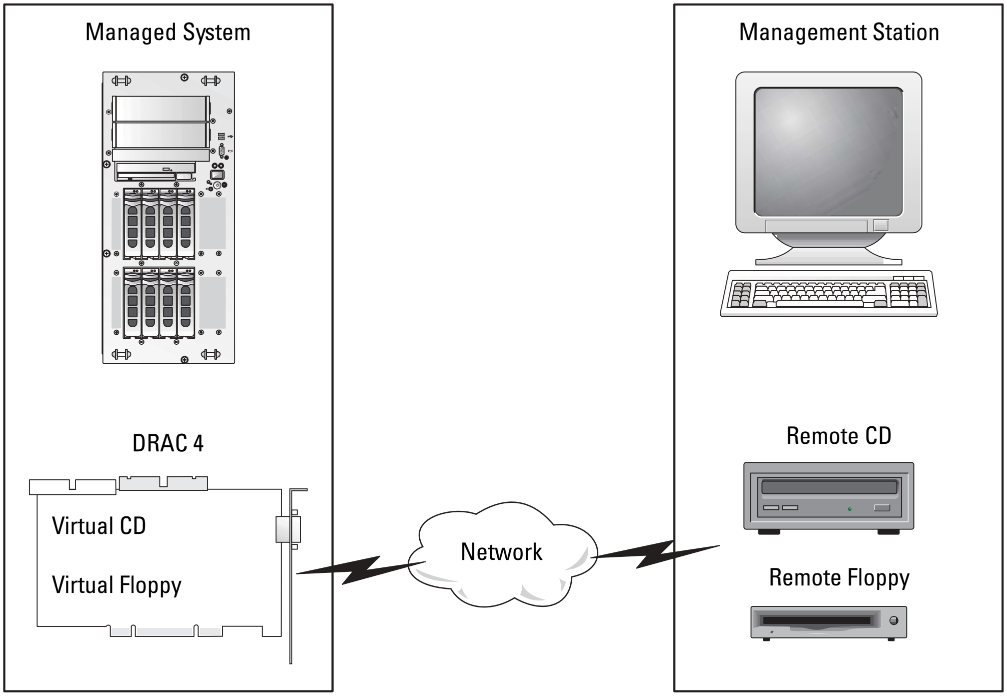
Question	Answer
Why can't I use a keyboard or mouse while installing a Microsoft operating system remotely by using DRAC 4 console redirection?	When you remotely install a supported Microsoft operating system on a system with Console Redirection enabled in the BIOS, you receive an EMS Connection Message 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. 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.
I manually selected **Other Display as Primary** from the **vKVM** window and now I cannot remotely control the system.	In order to allow remote access after manually selecting **Other Display as Primary**, you must perform the following steps: **1** Use the DRAC 4's power control to power cycle the unit. **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. **3** Go to the Windows device manager and uninstall both video adaptors. **4** Reboot the system. **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-Del> to login).
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.
I am experiencing video corruption. How can I correct the display?	Refresh the **Console Redirection** page by clicking the **Refresh** button. You may need to refresh the page multiple times to correct the video corruption problem.

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.) With this feature, 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.

Figure 7-1. Overall Architecture of Virtual Media



The managed system has a DRAC 4 card installed. The virtual CD and floppy drives are two electronic devices embedded in the DRAC 4 and are controlled by the DRAC 4 firmware.

NOTE: These two devices are present on the managed system's operating system and BIOS at all times, whether virtual media is connected or not. Connecting virtual media is just like inserting media into virtual devices.

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. 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.

Currently, the virtual floppy drive can be connected to a legacy 1.44 floppy drive with a 1.44 floppy diskette, a USB floppy drive with a 1.44 floppy diskette, a 1.44 floppy image, and USB keys. The virtual CD-ROM drive can be connected to a CD-ROM, DVD, CDRW, combination drive with CD-ROM media, or a CD-ROM image file in the ISO9660 format. The virtual CD-ROM drive can also be connected to a USB CD-ROM drive with CD-ROM media.

Virtual Media supports single session/single track CD/DVD/image data (that is, Virtual Media does not support multiple sessions, music CDs, and so on.)

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

Operating System Requirements on the Managed System

Virtual media is supported on systems running the following operating systems:

- Microsoft® Windows® 2000 Server with Service Pack 4
- Windows Server™ 2003
- Red Hat® Enterprise Linux AS, ES, and WS (version 3)
- Red Hat Enterprise Linux AS, ES, and WS (version 4)

NOTE: When using Virtual Media to install Windows 2000, the installation CD must have a built-in Service Pack 4. Service Pack 4 is required in order to access the virtual drives. This requirement also applies to using the virtual drives with Windows 2000. The drives do not appear until Service Pack 4 has been successfully installed.

Installing the Virtual Media Plug-In

To use the virtual media feature, you must successfully install the browser plug-in. After you have launched the virtual media page from within the DRAC 4 user interface, the browser automatically attempts to download the plug-in if it was not previously installed. If the plug-in is successfully installed, the virtual media page displays a list of floppy and CDs that the virtual drive can connect to.

Internet Explorer must be used on Windows management stations to use the virtual media feature. ActiveX Control is the plug-in that is used under Internet Explorer. The browser security must be set to the medium or lower setting for Internet Explore to be able to download and install signed ActiveX controls.

If you are using a Windows management station, 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 installation of the ActiveX control, you must first accept the control when Internet Explorer prompts you with a security warning.

On Red Hat Enterprise Linux management stations, the Mozilla browser is supported. If the plug-in has not yet been installed, or if a newer version is available, you are presented with a dialog box to confirm the plug-in installation on the management station. When presented with this plug-in installation dialog box, you must ensure that the user-ID running the browser has write permissions in the browser's directory tree. If not, the installation is not permitted.

Using the Virtual Media Feature

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

1. Open a Web browser on your management station.
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.

   NOTE: You cannot select a device that is present on the system but is locked for exclusive use by another application for use as Virtual Media. To make the device available, close the other application. When the application is closed, click the **Refresh** button on the **Virtual Media** page to finish making the device entry available.

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

   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 a 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. The DRAC 4 will accept a Virtual Media connection to a disabled virtual drive, which allows you to connect to the system and enable the virtual drive for the next boot. (The enable/disable feature for Virtual Media does not take effect until the next boot.)

   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

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, then the media is available at the system by simply clicking the drive and browsing its content.

On a Red Hat Enterprise Linux system, the virtual drives must be mounted before the drives can be accessed. Before mounting the drive, you must first 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.

On a system running Red Hat Enterprise Linux, type the following command to quickly identify the assigned virtual media devices:

```
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.

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

After system restart, the DRAC 4 IDE Option ROM utility will time-out after about 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
```

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
```

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

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

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

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 2000 Server with Service Pack 4 or Windows Server 2003, the operating system detects and configures the first detectable hard drive as the C drive. This behavior by Windows may cause the virtual floppy to be assigned with the drive letter C if the virtual floppy 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
```

racvmcli

The major capabilities of the Virtual Media command line interface (VM-CLI) utility are:

- Support for removable media devices or image files, consistent with the VM plugins.
- Support for command line option(s) to control/interact with the VM-CLI utility.
- Support for multiple, simultaneously active instances of the utility (with read-only image files only, not when actual floppy/CD devices are used).
- Optional feature: Support for a configuration file containing common options.
- Automatic termination upon disconnection – DRAC firmware **boot-once** option.

Installation

Standard installation methods are used to manage the installation and removal of the racvmcli utility on the Virtual Media client systems:

- For Windows clients, the utility is delivered as part of the RAC Management Station packaging, along with the racadm utility.
- For Linux clients, the VM-CLI utility is delivered as part of the RAC Management Station packaging, along with the racadm utility.

A sample deployment script is included in the packaging that illustrates how you can use the VM-CLI and racadm utilities to perform operating system or patch deployment against multiple target host systems. You can use this script as it is, or as a reference in developing a custom deployment framework that uses Virtual Media features.

Execution Environment

The **VM-CLI** command executes within the context of one of the following supported operating systems:

1. Windows XP
2. Windows 2000
3. Windows 2003
4. Red Hat Linux 9
5. Red Hat Linux AS/ES 2
6. Red Hat Linux AS/ES 3
7. Red Hat Linux AS/ES 4

The use of the VM-CLI utility requires valid DRAC 4 account credentials. The client host operating system must provide support for Secure Sockets Layer (SSL). The VM-CLI utility uses SSL to provide secure communications over its network connection to the DRAC 4 firmware (during initial connection setup).

Administrator level access (or VM-CLI group membership) is required to successfully run the VM-CLI utility where the operating system defines and supports it. The client system's administrator specifies the name of the **VM-CLI** group required for nonadministrator access to the utility. The client system's administrator can create this group specifically for VM-CLI access, or it can be the name of an existing user group. The client system's administrator also controls user membership within the specified group:

- For Windows systems, all users of the VM-CLI utility must have Power User privileges.
- For Linux systems, the recommended means for allowing nonadministrator access to the VM-CLI utility is through the **sudo** command. This command provides a centralized means of providing nonadministrator access and keeps a log of all commands issued by users. To add/edit users in the VM-CLI group, the administrator uses the **visudo** command. When added, nonadministrator users can add the sudo verb as a prefix to the VM-CLI command line (or to the script that uses VM-CLI) to obtain permission to run the utility.

Interfaces and APIs

This section details the supported command line options for the VM-CLI utility. The CLI interface is the same, regardless of the client system's operating system. The options used by the VM-CLI utility are consistent with the racadm utility options. For example, an option to specify the DRAC IP address requires the same format for both racadm and VM-CLI.

The format of a VM-CLI command is as follows:

```
racvmcli [parameters] [OS-shell options]
```

NOTE: Command line elements are described in detail in the VM-CLI Parameters section.

NOTE: Command line elements are case sensitive.

If the command line parameters are accepted, and the DRAC 4 authorizes the connection, the command continues to run until either of the following occurs:

- The DRAC 4 terminates the connection (DRAC 4 **boot once** option)

  Or

- The command/process is manually terminated, using features of the operating system/shell. For example, in Windows, you can use the Task Manager to terminate the process.

VM-CLI Parameters

DRAC 4 IP Address

`-r <RAC-IP-address>[:<RAC-SSL-port>]`

This parameter is used to provide the DRAC 4 IP address and SSL port. The VM-CLI utility needs this information to establish a Virtual Media connection with the specified DRAC 4.

If `<RAC-SSL-port>` is omitted, the default port (443) is used. Unless the DRAC 4's default SSL port was changed, the optional SSL port is not required.

`<`*`RAC-IP-address`*`>` is a valid IP address, in standard numbers-and-dots notation, or (if DRAC 4 support for DDNS is available and active) the DRAC 4 DDNS name.

If an invalid value is detected, an error message displays and the command terminates.

DRAC 4 User Name

`-u <`*`DRAC-user-name`*`>`

This parameter provides the name of the DRAC 4 user under whose authority the Virtual Media tasks will be performed.

- The user name must be valid.
- The user must have **DRAC Virtual Media User** permission.

If DRAC authentication fails, an error message displays and the command terminates.

DRAC User Password

`-p <`*`DRAC-user-password`*`>`

This parameter provides the password for the specified DRAC 4 user.

If DRAC 4 authentication fails, an error message displays and the command terminates.

Floppy/Disk Device or Image File

`-f <`*`device-name`*`> | <`*`image-file`*`>`

This parameter specifies the device or file to supply the virtual floppy/disk media.

<*image-file*> is the filename (including path) of a valid floppy/disk image file.

Example:

Windows operating system: `-f c:\temp\myfloppy.img`

Linux operating system: `-f /tmp/myfloppy.img`

NOTE: If the file is not write-protected, Virtual Media may write to the image file. Use the OS-provided mechanism to write-protect a floppy image file that should not be overwritten.

<device-name> on Windows systems: a valid floppy/disk drive letter.

<device-name> On Linux systems: a valid floppy/disk device special filename, including the number of the partition containing a mountable file system, if the disk is partitioned.

Example:

Windows operating system: `-f a:\`

Linux operating system: `-f /dev/sdb4 # 4th partition on disk device /dev/sdb`

NOTE: If the device provides a write-protection capability, you can use that mechanism to ensure that Virtual Media will not write to the media.

Omit this parameter from the command line if no floppy media is to be virtualized.

If an invalid value is detected, an error message displays and the command terminates.

CD/DVD Device or Image File

`-c <device-name> | <image-file>`

This parameter specifies the device or file to supply the virtual CD/DVD-ROM media:

- *`<image-file>`* is the filename (including path) of a valid ISO-9660 image file

  Example:

  Windows operating system: `-c c:\temp\mydvd.img`

  Linux operating system: `-c /tmp/mydvd.img`

- *`<device-name>`* **on Windows systems:** a valid CD/DVD drive letter

  `<device-name>` **on Linux systems:** a valid CD/DVD device special filename

  Example:

  Windows operating system: `-c d:\`

  Linux operating system: `-c /dev/cdrom`

Omit this parameter from the command line if no CD/DVD media is to be virtualized.

If an invalid value is detected, an error message is listed and the command terminates.

Version Display Switch

`-v`

This parameter is used to display the version of the VM-CLI utility.

If no other nonswitch options are provided, the command terminates without error.

Help Display Switch

`-h`

This parameter is used to display a summary of the VM-CLI utility parameters.

If no other nonswitch options are provided, the command terminates without error.

NOTE: Specify at least one media type (floppy/disk or CD/DVD) with the command, unless only switch options are provided. Otherwise, an error message displays and the command terminates with an error.

VM-CLI Operating System Shell Options

Features of the operating system shell can be used on the VM-CLI command line:

- **stderr/stdout redirection:** Redirects any printed output of the utility to a file. For example, the greater-than character (>), followed by a filename, overwrites the specified file with the printed output of the VM-CLI utility.

  NOTE: The VM-CLI utility does not read from standard input (`stdin`), so there is no need to use `stdin` redirection.

- **Background execution:** By default, the VM-CLI utility runs in the foreground. Use the operating system's command shell background character to cause the utility to run in the background. For example, under a Linux operating system, the ampersand character (&) following the command causes the program to be spawned as a new background process.

The latter technique is useful in script programs, as it allows the script to proceed after a new process is started for the VM-CLI command (otherwise, the script would block until the VM-CLI program is terminated). When multiple VM-CLI instances are started in this way, and one or more of the command instances must be manually terminated, use the operating system-specific facilities for listing and terminating processes.

VM-CLI return codes

The VM-CLI return codes are:

- 0 = No error
- 1 = Unable to connect
- 2 = VM-CLI command line error
- 3 = RAC firmware connection dropped

Text messages (English-only) are also issued to standard output whenever errors are encountered.

Frequently Asked Questions

Table 7-1 lists frequently asked questions and answers.

Table 7-1. 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`
	• The Dell™ Virtual Media devices may have been disabled. To verify the device configurations, type the following command:
	• `racadm getconfig -g cfgRacVirtual`
	• Ensure that the `cfgVirMediaDisable` object is set to `0` (Enabled).
	• You can enable the Virtual Media feature by changing the `cfgVirMediaDisable` object. Use the `racadm config` 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?	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 `racadm` 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. To configure your Dell Virtual Media Floppy device as a super-floppy device: **1** Type the following command: `racadm config -g cfgRacVirtual -o cfgFloppyEmulation 1` **2** Restart your system.
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.

Table 7-1. Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer
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 `racadm vmdisconnect` command to forcibly disconnect the virtual media connection

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?
`... other console startup messages ...`
`Apr 16 14:48:27 localhost kernel: hde: VIRTUALFLOPPY DRIVE, ATAPI FLOPPY drive`
`Apr 16 14:48:27 localhost kernel: hdf: VIRTUALCDROM DRIVE, ATAPI CD/DVD-ROM drive`
`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 ...`
	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.
	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.
	The error response, in this case, (key=2, asc=3a) from the DRAC 4 hardware indicates "media not present."

Table 7-1. Using Virtual Media: Frequently Asked Questions *(continued)*

Question	Answer
When I have a floppy drive or USB key open through Windows Explorer and I try to establish a Virtual Media connection on Windows for the same drives, I get a connection failure and I am asked to retry. Why?	You cannot establish a connection until you close the Windows Explorer that is accessing the floppy drive or USB key. DRAC 4 does not allow shared access for floppy drives and USB keys on Windows.
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. See "Operating System Requirements on the Managed System" for a list of supported operating systems.
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 remounting 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.
What media can I boot from?	DRAC 4 allows you to boot from a bootable CDROM media, a bootable 1.44 floppy disk, a bootable 1.44 floppy image, and a bootable USB key.

Table 7-1. **Using Virtual Media: Frequently Asked Questions** *(continued)*

Question	Answer
How can I make my USB key bootable?	Dell provides a Windows utility for formatting its USB Solid State devices as bootable devices on the *Dell Resource* 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. 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."
What does Virtual Media look like at the server?	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 **/etc/fstab**.
How do I know which drives are my virtual media drives?	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.
Will the drive letters change on Windows systems?	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.

Table 7-1. 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?	You can look at the **/etc/fstab** file which lists the device names for all your devices. When you know the device name, then you can use the **mount** and **umount** commands to mount and unmount your CD or floppy drives.
	To manually identify the virtual media devices, type the following command:
	`cat /var/log/messages | grep VIRTUAL`
	Then look for mount points for those devices in the **/etc/fstab** file, for example:
	`cat /etc/fstab | grep /dev/hde`
	Finally, use the associated mount point on the **mount** command, for example:
	`mount /mnt/cdrom1`

What do I need to install on the client side for the Virtual Media feature to work?	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.
Do I need to install this plug-in every time I use the Virtual Media feature?	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.
Will I need to have administrator rights in Windows to install the ActiveX plug-in.	You must have administrator privileges on Windows systems to install and use the Virtual Media feature.
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.

8

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 Management Consoles* 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 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 <*subcommand*>	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.

Table 8-1. Serial/Telnet Commands *(continued)*

Command	Description
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.
clrraclog	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 running Microsoft Windows 2000 Server, Windows 2000 Professional, Windows Server™ 2003, and Red Hat Enterprise Linux operating systems.

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 <*racIpAddr*> or -r <*racIpAddr*>:<*port number*> 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 <*usrName*>	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 <*password*>	Specifies the password used to authenticate the command transaction. If the -**p** option is used, the -**i** option is not allowed.

Table 8-3. racadm Command Options *(continued)*

Option	Description
-l <*lvl*>	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 <*lvl*>	Specifies the verbose level for screen output.
-L <*file*>	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.
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 brackets ([ ]) pair. The following are examples of the current indexed groups:

```
[cfgUserAdmin]

cfgUserAdminUserName=<USER_NAME>

"

[cfgTraps]

cfgTrapsDestIpAddr=<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.

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 admininstrative 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
After performing a DRAC 4 reset (using the racadm racreset command), I issue a command and the following message is displayed: racadm <*command name*> Transport: ERROR: (RC=-1). What does this message mean?	You must wait until the DRAC 4 completes the reset before issuing another command.

When I use the **racadm** commands and subcommands, I get errors that I don't understand.	You may encounter one or more of the following errors when using the **racadm** commands and subcommands:
	• Local error messages — Occur when problems occur with syntax, typographical errors, incorrect names, and so on.
	Example:
	`racadm <subcmd>: ERROR: <message>`
	• Transport error messages — Occur when the racadm 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 racadm CLI remotely, transport error messages may indicate network communication problems or that the management station is unable to communicate with the DRAC 4.
	Example:
	`racadm <subcmd> : Transport : ERROR : <message>`
	• DRAC 4 firmware errors — Occur when a fault exists in the DRAC 4 firmware operation.
	Example:
	`racadm <subcmd> : Firmware : ERROR : <message>`

9

Operating System Deployment Using the DRAC 4 Virtual Media CLI Feature

To accomplish remote operating system deployments for multiple target servers, interactive methods are time consuming, and error-prone. The DRAC 4 Virtual Media command line interface (VM-CLI) utility supports cost-effective, scripted methods for accomplishing remote operating system deployments to multiple target servers. Typically, a deployment infrastructure is already in place, within computing environments that require multiple remote operating system deployments. This section describes how the VM-CLI utility can be integrated into your existing deployment infrastructure in these computing environments.

NOTE: For occasional, one-time operating system deployments, interactive methods of performing the installation are typically used. A Dell™ technical publication describing how this procedure can be accomplished remotely with the use of DRAC 4 Virtual Media features is available on the Dell website at: **http://www.dell.com/downloads/global/power/ps1q05-20040170-Gujarathi.pdf**

Requirements

Ensure that your deployment infrastructure meets the following requirements before you start using the DRAC 4 VM-CLI utility to accomplish remote operating system installations:

1. Each remote target server requires DRAC 4 hardware, whose network interface is operational and accessible from the deployment host (which is the client system used to perform the remote deployment).

   NOTE: Dell Custom Factory Integration (CFI) options include the capability to have the network interface of DRAC 4 configured by default, to obtain its network address from a DHCP server. With this capability, the new DRAC 4 hardware obtains a unique network address and name *out-of-the-box* (the DRAC 4 network name is based on the host's unique service tag).

2. The virtual devices on each remote target server must be at the top of the BIOS boot order, so that the target server's virtual devices can be booted, when media is connected to them.

   NOTE: Dell Custom Factory Integration (CFI) options include the capability to have the Virtual Devices of DRAC 4 configured by default, at the top of the BIOS boot order. With this capability, the new server hardware can boot from its Virtual Media devices out-of-the-box.

3 A network share, accessible from the remote target servers, which hosts the operating system files and drivers needed during the operating system deployment procedure. This network share may also host the operating system deployment boot image file(s) described in the next requirement.

4 An operating system deployment boot image file, tailored to the deployment infrastructure:

- This file may be either a floppy image or a CD/DVD ISO image, with an industry-standard bootable format.
- This image file must be accessible by the deployment host (it may reside on a network share), for it is used to boot the target server during the first step of the deployment procedure.
- When booted, the programs or scripts that are included within the deployment image initialize the target host's network interface, access the network share (see requirement 3) to retrieve the needed operating system files and drivers, and perform all tasks needed to successfully complete the remote server's operating system installation.

  For example, the target host may require RAID setup and initialization, before starting the operating system installation step. When complete, the deployment procedure reboots the target host, and the virtual deployment media is automatically disconnected. And, the newly deployed server boots from its own hard drive.

Tasks

When the target server hardware is installed, perform the following tasks before beginning the operating system deployments to those servers.

NOTE: You may leverage some of this work during subsequent operating system deployments, as you need to perform some tasks only once.

1 Configure each target server's DRAC 4 network interface.

NOTE: Dell's CFI is available for this item.

2 Configure each target server's BIOS boot order to include the virtual devices at the top.

NOTE: Dell's CFI is available for this item.

3 Create/populate a network share with the operating system files needed for successful installation.

NOTE: Skip this step if the required operating system files are already in place.

4 Create a bootable deployment image file that performs the steps necessary to deploy the operating system. This bootable image file includes programs or scripts that understand the target deployment infrastructure, and use standard network-based installation methods to achieve the installation. For example, to deploy a Microsoft® Windows® server, this image file may include programs that utilize Microsoft Systems Management Server (SMS) methods to deploy the operating system to the target server.

   - See "Creating Bootable Deployment Image Files" for additional details on creating bootable deployment images.
   - During deployments to multiple targets, mark the deployment image as ‘read-only’ to ensure that each target server boots and executes the same deployment procedure.
   - Skip this step if the required deployment image file is already in place.

5 Integrate the racadm and RACVMCLI utility programs into your existing operating system deployment client application, or use the vmdeploy script included with the VM-CLI packaging as it is. In the former case, use the sample deployment script as a guide when integrating these DRAC 4 utilities into your existing operating system deployment client application.

   NOTE: Perform this step only once.

vmdeploy

When you perform the tasks listed in "Tasks", remote operating system deployments to multiple target servers can proceed. A summary of the steps used to accomplish this task are listed below.

1 Assemble the list of target DRAC 4 network names/addresses, whose hosts are to be installed.

2 For each target DRAC 4 network name/address in this list:

   a Start a VM-CLI process, supplying appropriate parameters:

      - Target DRAC 4 name/address.
      - Bootable deployment image filename.
      - DRAC 4 user name.
      - DRAC 4 user password.

   b Verify a successful Virtual Media connection.

   c Using racadm, set the boot once property on the target DRAC 4.

   d Using racadm, (re)boot the DRAC 4’s host server.

NOTE: Study the sample vmdeploy script included with the VM-CLI packaging. It offers detailed requirements to accomplish each of the above steps.

Creating Bootable Deployment Image Files

Observe the following guidelines when creating the bootable deployment image files.

NOTE: Regardless of the particular method used to create image files, it is recommended that you test the image file by ensuring that you can successfully boot to it before starting a mass deployment. A simple way to test the image file is to use the image file with the DRAC 4 interactive Web interface, which allows you to connect the image to a target server, and then reboot.

To create image files from existing bootable media:

Linux Users

- Use the dd (data duplicator) utility:

  `dd if=<input-file> of=<output-file>`

  `<input-file> =input device`

  (for example, `/dev/fd0, /dev/cdrom`)

  `<output-file> = output file`

  (for example, `myfloppy.img, mycd.iso`)

Windows Users

A number of utilities are available for creation of floppy and/or ISO images from removable media on Windows when creating CD/DVD image files. Ensure that you use one that supports copying the CD/DVD boot sectors. The following Web addresses provide information on available imaging utilities:

- **http://www.fdos.org/ripcord/rawrite/**
- **http://blogs.technet.com/brucecowper/archive/2005/03/09/391268.aspx**

To create a bootable CD/DVD image file from scratch, use one of the following imaging programs or a program with equivalent features:

Imaging Programs for Linux Users

- k3b: **http://www.k3b.org/**
- NeroLINUX: http://www.nero.com/

Imaging Programs for Windows Users

- Nero: **http://www.ahead.de/**
- MediaCreator: **http://www.roxio.com/**
- Magic ISO: **http://www.magiciso.com/**

10

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"

A

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
config	Configures the DRAC 4.
getconfig	Gets the DRAC 4 configuration data.

Synopsis

```
racadm config [ -p -c] -f <filename>
racadm config -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** ***<filename>*** option causes **config** to read the contents of the file specified by *<filename>* 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** ***<filename>*** after the configuration is complete.
-g	The **-g** ***<groupName>***, or group option, must be used with the **-o** option. The *<groupName>* specifies the group containing the object that is to be set.
-o	The **-o** ***<objectName> <Value>***, or object option, must be used with the **-g** option. This option specifies the object name that is written with the string *<value>*.
-i	The **-i** ***<index>,*** or index option, is only valid for indexed groups and can be used to specify a unique group. The *<index>* 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.

NOTE: The -f option will output the contents of the file to the terminal screen rather than writing to a file since no file system is available. For the serial/telnet console, the <*filename*> argument must be supplied, but it is ignored.

Table A-6. getconfig Subcommand Options

Option	Description
-f	The **-f** ***<filename>***, or **filename** option, causes **getconfig** to create the file <*filename*>. It then reads all the configuration data from the DRAC 4 and places it into the file <*filename*>. The created file is a format that can be used with the **racadm config -f** ***<filename>*** command.
-p	The **-p**, or **password** option, causes **getconfig** to include password information in the file for all passwords except for the user passwords (which are stored encrypted and cannot be decrypted). A **# cfgUserAdmPassword** line is displayed as an indication that the password is present, but the password text is not displayed.
-g	The **-g** ***<groupName>***, or **group** option, can be used to display the configuration for a single group. The **groupName** is the name for the group used in the **racadm.cfg** files. If the group is an indexed group, use the **-i** option.
-h	The **-h**, or **help** 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** ***<index>***, or **index** option, is valid only for indexed groups and can be used to specify a unique group. The <*index*> is a decimal integer from 1 through 16. If **-i** <*index*> 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** ***<username>***, or **user name** option, can be used to display the configuration for the specified user. The <*username*> 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
coredumpdelete	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
fwupdate	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.
-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 *always* checksum before programming. It can be used along with the **-u** 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."
-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 **firming.dm1**. 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.dm1**

  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.dm1**

  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.dm1** file.

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 <filename>
```

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 **getssinfo** subcommand.

Table A-11. getssinfo 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 **getssinfo** subcommand options.

Table A-12. getssinfo 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 143.166.174.19	Thu, 06 Mar 2004 10:32:39 GMT-06:00	NONE

- **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
getsysinfo	Displays DRAC 4 information, system information, and watchdog status information.

Synopsis

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

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
-r	Displays DRAC 4 information

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: • 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
  ```

Restrictions

The **Hostname** and **OS name** information fields in the Web-based interface and racadm **getsysinfo** command display accurate information only if the DRAC 4 managed system software is installed on the system.

getractime

NOTE: To use this command, you must have **Log In DRAC 4** permission.

Table A-17 describes the **getractime** subcommand.

Table A-17. getractime

Subcommand	Definition
getractime	Displays the time from the controller.

Synopsis

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

Description

The **getractime** 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.mmmmmms*off` string with no option is displayed in the same format as the UNIX® **date** command.

Output

The **getractime** 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
ping	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
setniccfg	Sets the IP configuration for the controller.
getniccfg	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
getsvctag	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
racdump	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 *hard* 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 *soft* 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 *graceful* 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

- **racadcm 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
racresetcfg	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: • **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
getraclog -i	Displays the number of entries in the DRAC 4 log.
getraclog	Displays the DRAC 4 log entries.

Synopsis

```
racadm getraclog -i
racadm getraclog [-A] [-c count] [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
getsel -i	Displays the number of entries in the System Event Log.
getsel	Displays SEL entries.

Synopsis

```
racadm getsel -i
```

```
racadm getsel [-E] [-R] [-A] [-c count] [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).

-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
gettracelog -i	Displays the number of entries in the DRAC 4 trace log.
gettracelog	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
setrac	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**.

Table A-33. setrac Subcommand Options *(continued)*

-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
sslcsrgen	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.
- While generating a CSR, the local racadm interface on the host becomes unavailable. Use remote racadm or the racadm available on serial or telnet command lines instead.

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
sslcertupload	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
sslcertupload	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
-t	Specifies the type of certificate to download, either the CA certificate or server certificate. 0x1 = server certificate 0x2 = Active Directory 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 **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
sslcertview	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
-t	Specifies the type of certificate to upload, either the CA certificate or server certificate. 0x1 = server certificate 0x2 = Active Directory certificate
-A	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 1 -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. When disconnected, the user interface will reflect the correct connection status. This subcommand is available only through the use of local or remote racadm.

B

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 alphanumeric ASCII characters, dot (.) or dash (-); must start with an alphanumeric character.

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). When **cfgDNSRacName** is not the default name and the firmware repair utility diskettes are used to update the DRAC 4, two RAC names (the original and the default) with the same IP address may be seen on the DNS server. Other DRAC 4 firmware update methods do not display this behavior.

cfgDNSRacName (Read/Write)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

Legal Values

String of up to 63 alphanumeric ASCII characters or dash (-); must start with an alphanumeric character.

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.

cfgRhostsSmtpEmailEnable (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.

cfgRhostsSmtpServerIpAddr (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.

cfgRhostsFwUpdateTftpEnable (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.

cfgRhostsFwUpdateIpAddr (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.

The last user in the **cfgUserAdmin** group cannot be deleted.

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)

NOTE: To modify this property, you must have **Configure DRAC 4** permission.

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.)

cfgSsnMgtSshIdleTimeout (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 time-out

Default

0x12C seconds (5 minutes)

Description

Defines the Secure Shell idle time-out. 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).

An expired SSH session displays the following error message only after your enter a carriage return:

```
Warning: Idle Timeout Expired
```

The system then returns you to the shell from which SSH was invoked.

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

cfgSerialTelnet7fIsBackspace (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 ½ 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 ½ 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 ½ 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 ½ 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 ½ 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 ½ 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

Table B-2. DRAC 4 Properties for Satellite Connectivity *(continued)*

Property	Normal Value	Satellite Value
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.

cfgOobSnmp

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.

cfgOobSnmpAgentCommunity (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.

cfgOobSnmpTrapsEnable (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.

cfgOobSnmpAgentEnable (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 the time that the firmware update file is loaded and the update sequence is started. (Type hexadecimal values.)

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.

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).

cfgVirtualBootOnce (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

When set to TRUE, the DRAC 4 firmware monitors system boots and drops the client Virtual Media connection on the second system boot. This setting boots the system only once from a bootable remote floppy or CD. On the second boot, the value of **cfgVirtualBootOnce** is reset to FALSE.

cfgActiveDirectory

This group contains parameters to configure the DRAC 4 Active Directory feature.

cfgADRacDomain (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.

cfgADRacName (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.

cfgADEnable (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.

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. The length is limited to 254 characters.

Default

(blank)

Description

Root domain of the Domain Forest.

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 cfgUserdminAlertFilter {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-3 apply.

Table B-3. 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 0x2244444
  ```

- 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-4 apply.

Table B-4. 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	<*statMask*>
12–15	System miscellaneous sensor	<*senMask*>
8–11	System fan sensors	<*senMask*>
4–7	System voltage sensors	<*senMask*>
0–3	System temperature sensors	<*senMask*>

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-5.

Table B-5. 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

Table B-5. Alert Filter Property Group and Object IDs *(continued)*

GroupID	Object ID	Object Default Value
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 -i <index>

racadm testemail -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 *Server Administrator SNMP Reference Guide*.

Glossary

AGP

Abbreviation for accelerated graphics port, which is a bus specification that allows graphics cards faster access to main system memory.

API

Acronym for application programming interface.

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. Busses 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.

CFI

Acronym for custom factory integration.

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 Naming System.

DNS

Abbreviation for Domain Name System.

DRAC 4

Abbreviation for Dell™ Remote Access Controller 4.

DSU

Abbreviation for disk storage unit.

DVD

Abbreviation for digital versatile disc (also known as digital video disc).

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.

ISO
Abbreviation for international standards organization.

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.

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.

RAID
Acronym for redundant array of independent disks.

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.

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.

VM
Abbreviation for Virtual Media.

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